



**Abertay
University**

Malware Analysis Investigation

A case study of the Ryuk ransomware

Ance Strazdina

CMP320: Advanced Ethical Hacking

BSc (Hons) Ethical Hacking, Year 3

2022/23

Note that Information contained in this document is for educational purposes.

Abstract

Malware remains a significant threat to computer systems and the complexity of it only continues to increase as technology advances. Nowadays, it is used for espionage, financial and intellectual property theft, and political sabotage, among others. Considering the severe disruption and losses a malware-based attack can cause to public and private organisations and individuals, it is important to ensure the computer systems in use are secure. To develop effective countermeasures and fully mitigate the impacts of malware attacks, it is vital to utilise effective malware analysis techniques to understand the behaviour and impacts of a specific malware so it can be successfully combated. This project aimed to perform a malware analysis investigation on a supplied malware sample with the goal of identifying it and understanding its capabilities.

To meet the aims, malware analysis was performed by utilising the methodology outlined in *Practical Malware Analysis*. Static, dynamic, and code analysis techniques were used on the sample to identify it and gain insight into its characteristics, components, functionality, and how it impacts the infected host. This was done within an isolated Windows 10 Virtual Machine with a Flare VM installation which contained specialised tools for reverse engineering and malware analysis. The findings of this investigation were then documented and analysed.

The investigation identified the malware sample as a strain of the Ryuk ransomware. It further uncovered the ransomware's use of recursive system enumeration and thread-based parallelism, which allowed it to rapidly encrypt files on the infected system. Behaviour hinting at the ransomware's ability to propagate to other hosts on the network was also observed. Furthermore, the ransomware used PDF file icons to trick a victim into executing it and employed several anti-debugging techniques, which made it more difficult to analyse. The findings of this investigation revealed that the resulting severity of a ransomware attack that utilises Ryuk would have severe consequences on a network, therefore countermeasures have been suggested and the overall importance of malware analysis to the field of cybersecurity has been discussed. Lastly, suggestions for future work relating to further analysis of the malware code, the memory image of the employed virtual machine, and additional networking capabilities of this ransomware have been outlined.

Contents

1	Introduction	1
1.1	Background.....	1
1.2	Aim	2
2	Procedure.....	3
2.1	Overview of Procedure.....	3
2.2	Static Analysis	5
2.3	Dynamic Analysis	8
2.4	Code Analysis.....	11
3	Results.....	13
3.1	Static Analysis	13
3.2	Dynamic Analysis	15
3.3	Code Analysis.....	17
4	Discussion.....	23
4.1	General Discussion.....	23
4.2	Conclusions.....	23
4.3	Future Work.....	24
	References	25
	Appendices.....	27
	Appendix A – Imported Functions.....	27
	Appendix B – Strings Output	29
	Appendix C – Regshot Comparison Results	46

1 INTRODUCTION

1.1 BACKGROUND

The continuous advancement of computer technology has revolutionised the way individuals and organisations alike operate. Nowadays, information systems are an essential part of banking, healthcare, energy, government, and defence sectors, to name a few. Simultaneously, however, so has progressed the use of the same technology for criminal activities (A, 2018).

With more people and organisations utilising online services, there are more opportunities for cybercriminals to exploit. According to the estimates from Statista's Cybersecurity Outlook (Figure 1-1), the global cost of cybercrime is expected to surge from 8.44 trillion USD in 2022 to 23.82 trillion USD by 2027 (Fleck, 2022).

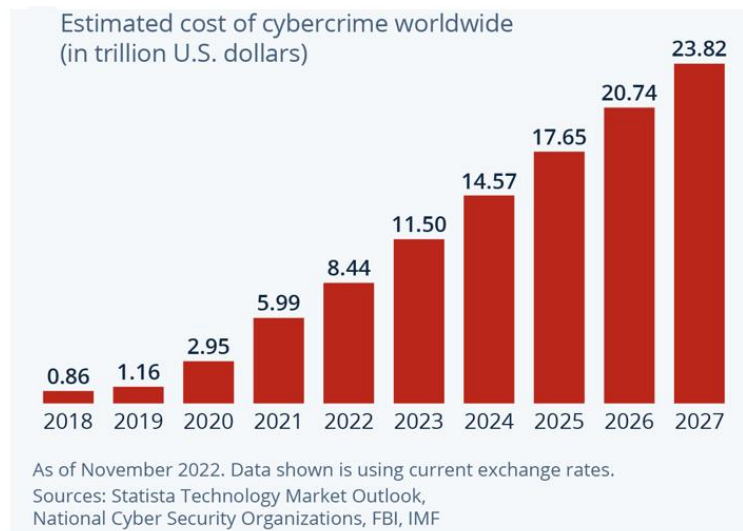


Figure 1-1 Estimated yearly costs (in trillion U.S. dollars) of cybercrime worldwide (Fleck, 2022)

To carry out cyberattacks, whether to conduct operations such as espionage, financial and intellectual property theft, and political sabotage, among others, threat actors often make use of malicious software, or malware (A, 2018). This umbrella term is used to describe any malicious program or code that is harmful to computer systems. Examples of such programs include viruses, worms, trojans, ransomware, and spyware. Malware can be spread through a variety of vectors, such as email attachments, malicious websites, and infected downloads (Malwarebytes, no date).

While countermeasures such as keeping systems up to date, using antivirus software, and user education exist (Gibson, 2011), they are not impenetrable. As malware continues to evolve, new attack vectors that users can fall victim to emerge and it is possible for antivirus software to not recognise novel malware as malicious, making it a significant threat to security.

Consequentially, there is an increased demand for malware researchers to be able to create the next generation of security protection technologies (Kleymentov & Thabet, 2019). A huge part of this process is

malware analysis – the examination of malicious software with the goals of identifying it, determining how it operates and its impacts, and recognising effective methods for detecting and removing it from affected systems in the future (Sikorski & Honig, 2012).

Malware analysis techniques fall into three main categories – static, dynamic, and hybrid. Static analysis involves looking for signs of malicious intent by examining the code and structure of the malware without executing it. This approach can be useful for identifying certain types of malware but may not be sufficient in detecting more advanced malware that exhibits malicious behaviour only on runtime. Dynamic analysis, on the other hand, executes malware in a safe environment. This closed system allows for the observation of the malware in action without the risk of letting it harm real systems (Baker, 2022). Hybrid analysis is a combination of the two and offers the best understanding of the specific malware (N-able, 2019).

In addition to these categories, malware analysis can involve memory analysis (memory forensics) and code analysis. Memory analysis involves investigating a capture of a computer's memory. It can assist in gaining an understanding of the malware's behaviour after infection and is especially useful to determine the stealth and evasion capabilities of the malware. Code analysis focuses on understanding the malware by looking at the information revealed in its code. This technique is also further divided into static and dynamic analysis. Static code analysis involves disassembling the binary and examining the code, while dynamic code analysis involves debugging the binary in a controlled environment to better understand its functionality (A, 2018).

Malware analysis helps to identify the behaviour and impacts of specific malware and is a crucial step to develop the technology for its effective detection and removal thus preventing future attacks. It is an essential part of cybersecurity as malware continues to evolve and pose new threats to the security of information systems, therefore it is important for cybersecurity professionals to be familiar with techniques related to malware analysis.

1.2 AIM

This project aims to perform an analysis of a malware sample with the aim to identify it and recognise its characteristics, components, and impacts on a computer system. This aim consists of the following sub-aims:

- Choosing a malware sample from a provided selection.
- Outlining an analysis methodology to follow.
- Performing the methodology steps by utilising the appropriate tools.
- Documenting and analysing the results.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

For this investigation, sample number 3 was chosen from the nine provided malware samples in the form of compressed folders.

2.1.1 Virtual Environment Setup

The testing environment for this investigation was a Windows 10 virtual machine with a FLARE VM installation. FLARE VM is a Windows-based security distribution that contains tools for reverse engineering, malware analysis, incident response, forensics, and penetration testing (Kacherginsky, 2017). The virtualisation platform used was VMWare Workstation Pro 16 and the virtual machine was configured with a custom network adapter with a host-only configuration. This adapter was not connected to a host virtual adapter (“Connect a host virtual adapter to this network” was disabled). Lastly, DHCP was enabled. For the virtual network configuration, see Figure 2-1. This network adapter configuration ensured that an analysis of the networking capabilities of the malware sample could be performed. Additionally, a snapshot containing the virtual machine in a clean state was created to revert to after each analysis procedure to ensure the machine is retained in a safe state.

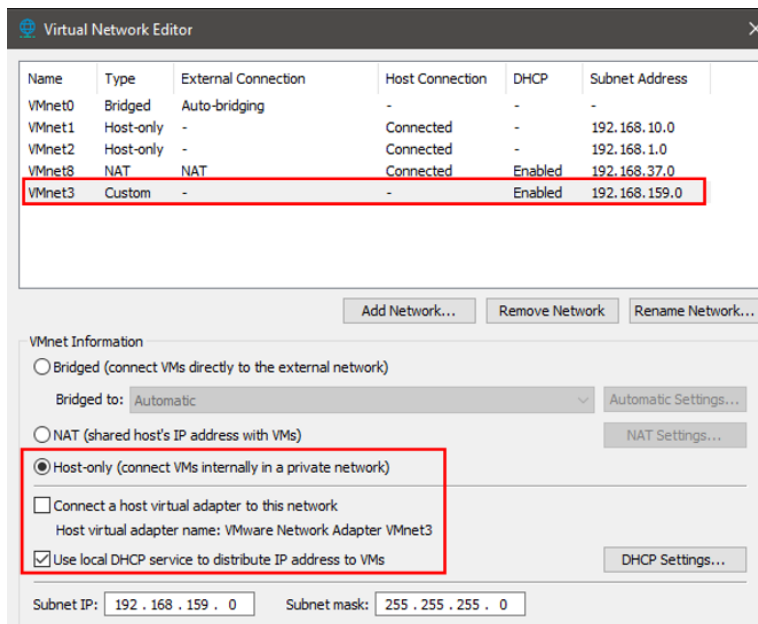


Figure 2-1 Virtual Network Configuration for the testing environment

2.1.2 Methodology

For this investigation, the used malware analysis method was that of the one outlined by Sikorski and Honig in *Practical Malware Analysis* (2012). It outlines the steps of hybrid (both static and dynamic) analysis of malware.

It further defines the following steps of static analysis: identification of malware by using hashing and antivirus tools, if possible, determining whether it is packed and/or otherwise obfuscated, and obtaining information about its functionality from PE File headers and sections, imported libraries and functions, and strings.

This publication also defines the following components of dynamic analysis: running the malware, monitoring its behaviour during this process, and comparing the state of the infected machine before and after the malware is executed. Additional aspects of this involve faking a network and capturing traffic to analyse the networking capability of the malware.

Additionally, Sikorski and Honig also outline both static and dynamic code analysis techniques. As discussed in Section 1.1, static code analysis involves using a disassembler to examine the code, while dynamic code analysis uses debuggers to examine the code as it is executing.

Section 2.2 onwards documents the steps performed while following the documented analysis methodology. The results of each stage are discussed in Section 3.

2.1.3 Used Tools

The following tools were used during the analysis:

- **Certutil** – Windows command-line tool. Used to obtain file hashes during the investigation.
- **FakeNet (v1.4.11)** – network analysis tool for intercepting and redirecting traffic to spoof a network connection.
- **Interactive Disassembler (IDA) (v7.6.210526 Windows x64)** – disassembler for static code analysis.
- **malapi.io** – a website used for identifying imported library and method functionality.
- **Microsoft Edge** – web browser, used to open HTML files.
- **OllyDbg (v1.10)** – debugger for dynamic code analysis.
- **PEiD (v0.95)** – tool for detecting packers and compilers for portable executable files.
- **Pestudio (v9.47)** – program used to investigate portable executable files.
- **Process Explorer (v17.02)** – tool for observing which handles and processes loaded or opened during malware execution.
- **Process Monitor (v3.92)** – Windows tool for observing file system, registry, process, and thread activity.
- **Regshot (v1.9.1 beta)** – a registry comparison utility used to observe differences in the Windows registry before and after executing malware.
- **Strings** – program for finding and printing text strings embedded in the malware sample.
- **VirusTotal** – web service that allows to identify whether files, URLs, and hashes, among others, are malicious by scanning it against numerous antivirus engines.
- **Wireshark (v4.0.3)** – packet analyser for examining the logs created by Fakenet.
- **010Editor (v12.0.1)** – hex editor, used to determine file signature.

2.2 STATIC ANALYSIS

2.2.1 Identification

This phase of the malware analysis methodology aimed to obtain a hash of the malware and use it to see if it has been identified by other sources. To obtain the hash, the malware sample was first extracted from the .zip folder. Certutil was then used to obtain the MD5 hash of the sample (Figure 2-2).

```
C:\Users\user>certutil -hashfile C:\Users\user\Desktop\Samples\3\180f82bbedb03dc29328e32e054069870a1e65078b78b2120a84c96aaed7d843 md5
MD5 hash of C:\Users\user\Desktop\Samples\3\180f82bbedb03dc29328e32e054069870a1e65078b78b2120a84c96aaed7d843:
a563c50c5fa0fd541248acaf72cc4e7d
CertUtil: -hashfile command completed successfully.
```

Figure 2-2 MD5 hash of the sample

The obtained hash (*a563c50c5fa0fd541248acaf72cc4e7d*) was then uploaded to VirusTotal. It was established that this malware sample has been previously identified as the Ryuk ransomware. Identifying this sample as a ransomware at this stage was a crucial step in prognosing its behaviour, therefore adjusting the subsequent analysis stages to gain the most accurate understanding of the malware sample. Figure 2-3 demonstrates a fragment of the VirusTotal output.

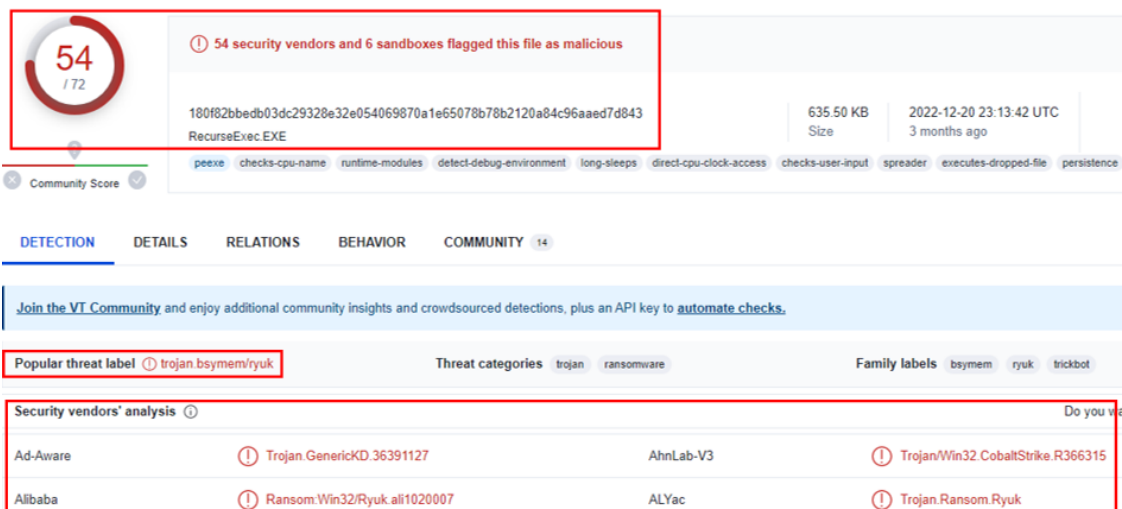


Figure 2-3 VirusTotal output

2.2.2 Portable Executable Format

Subsequently, the file was opened in 010Editor which allowed to see its file signature. The file signature 4D 5A (MZ) can be seen in Figure 2-4. This indicated the DOS MZ executable file format which is used by portable executables such as .exe files.

```
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....ÿÿ..
```

Figure 2-4 File signature of the malware sample

After this discovery, the file that was originally extracted from the zip folder was renamed to end with ".exe".

2.2.3 Detecting Packers

Before the portable executable was further investigated, it was first checked for any signs of being packed. This was done by using PEiD. Figure 2-5 displays the produced output of this stage.

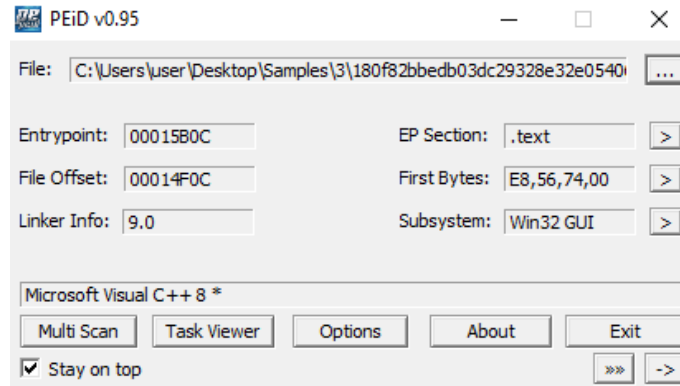


Figure 2-5 PEiD output

As the sample was not packed the investigation progressed to the next stage.

2.2.4 PE File Headers and Sections

Further investigation of the portable executable involved using Pestudio to obtain additional information from its headers. Figure 2-6 and Figure 2-7 display outputs from Pestudio *main* and *Version* tabs. Data relating to the compilation date, entropy, and file name could be observed.

entropy	6.236
imphash	n/a
signature	Microsoft Visual C++
tooling	Visual Studio 2005
entry-point	E8 56 74 00 00 E9 78 FE FF 6A 0C 68 58 6B 43 00 E8 16 22 00 00 83 65 E4 00 8B 75 08 3B 35 30 F9
file-version	1, 0, 0, 1
description	RecurseExec MFC Application
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	Thu Feb 11 02:51:01 2021 UTC

Figure 2-6 Pestudio main tab

file-type	executable
language	English-US
code-page	Unicode UTF-16, little endian
CompanyName	n/a
FileDescription	RecurseExec MFC Application
FileVersion	1, 0, 0, 1
InternalName	RecurseExec
LegalCopyright	Copyright (C) 2004
LegalTrademarks	n/a
OriginalFilename	RecurseExec.EXE
ProductName	RecurseExec Application
ProductVersion	1, 0, 0, 1

Figure 2-7 Pestudio version tab

2.2.5 Imported Libraries and Functions

Linked libraries and functions were also examined with Pestudio. Figure 2-8 displays a list of 10 identified dynamic linked libraries that this executable imports.

library (10)
KERNEL32.dll
USER32.dll
GDI32.dll
WINSPOOL.DRV
ADVAPI32.dll
SHELL32.dll
SHLWAPI.dll
ole32.dll
OLEAUT32.dll
oleacc.dll

Figure 2-8 Imported libraries identified with Pestudio

Additionally, 277 functions (see Appendix A – Imported Functions) were identified. A fragment from the function list can be seen in Figure 2-9.

```
DeleteCriticalSection  
DefWindowProcA  
CryptImportKey  
CryptEncrypt  
CryptAcquireContextW  
CreateWindowExA  
CreateStdAccessibleObject  
CreateProcessA  
CreatePipe  
CreateFileA
```

Figure 2-9 Identified function snippet

The full functionality of the libraries and their functions is further discussed in Section 3.1 where they are identified in conjunction with the malapi.io website.

2.2.6 Strings

Lastly, the Strings tool was used against the ransomware sample. The identified strings are contained in Appendix B – Strings. Many of the strings related to the file information, imported libraries, and functions identified in the previous sections, however, new discoveries such as copyright/program name related strings (Figure 2-10 and Figure 2-11), filepaths (Figure 2-12), and error handling (Figure 2-13) were made.

```
0003A948 Copyright (c) 1992-2004 by P.J. Plauger, licensed by Dinkumware, Ltd. ALL RIGHTS RESERVED.
```

Figure 2-10 Copyright string

```
0007B742 A Kamal Shankar Quick Tool - Recursive Executer
```

Figure 2-11 Program name in Strings output

```
0002E668 f:\dd\vctools\vc7libs\ship\atlmfc\src\mfc\appcore.cpp
```

Figure 2-12 Filepath in Strings output

```
0002D928 CloseHandle
0002D934 ReadFile error!
0002D944 Close handle error!
0002D958 Duplicate handle error 2!
0002D974 Duplicate handle error!
0002D98C Stdout pipe creation error!
```

Figure 2-13 Error strings

Furthermore, a mention of “RSA2” (Figure 2-14) and locale-related strings (Figure 2-15) could be observed.

```
000384C8 RSA2
```

Figure 2-14 “RSA2” in Strings output

```
00032098 Monday
000320A0 Sunday
000320C4 united-states
000320D4 united-kingdom
000320E4 trinidad & tobago
000320F8 south-korea
00032104 south-africa
00032114 south korea
00032120 south africa
00032130 slovak
```

Figure 2-15 Locale-related strings

2.3 DYNAMIC ANALYSIS

This analysis stage involved running the malware sample. Before executing this stage, the testing environment was prepared by running FakeNet for network connection spoofing and opening Process Monitor and Process Explorer to monitor the malware on runtime. An initial Regshot snapshot was also created.

2.3.1 Process Monitor

While the malware sample was actively running a lot of events could be observed in the Process Monitor when examining the malicious application that was executed and the subtree of processes it created. The extent of this was several million events in a relatively short time after first launching executable. This resulted in Process Monitor stopping functioning due to memory issues. A lot of the observed events were recurring as the ransomware was performing the same process of accessing a directory, enumerating it, and encrypting its files for the entire filesystem. Figure 2-16, Figure 2-17, and Figure 2-18 display fragments of the Process Monitor output. The ransomware could be observed accessing and manipulating registry keys and their values, creating threads, loading DLLs, and changing file permissions.

3:50:3...	180f82bbedb03...	4364	RegSetValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_BINARY, Length: 362, Data: 5F 02 00 00 00 00 0...
3:50:5...	180f82bbedb03...	4364	CreateFile	C:\Users\user\Desktop\Samples\3	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Op...
3:50:5...	180f82bbedb03...	4364	QueryBasicInfor...	C:\Users\user\Desktop\Samples\3	SUCCESS	CreationTime: 3/3/2023 2:20:09 AM, LastAccessTime: 4/7/2023...
3:50:5...	180f82bbedb03...	4364	CloseFile	C:\Users\user\Desktop\Samples\3	SUCCESS	
3:50:5...	180f82bbedb03...	4364	Thread Create		SUCCESS	Thread ID: 3708
3:50:5...	180f82bbedb03...	4364	CreateFile	C:\Users\user\Desktop\Samples\3	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Op...
3:50:5...	180f82bbedb03...	4364	QueryBasicInfor...	C:\Users\user\Desktop\Samples\3	SUCCESS	CreationTime: 3/3/2023 2:20:09 AM, LastAccessTime: 4/7/2023...
3:50:5...	180f82bbedb03...	4364	CloseFile	C:\Users\user\Desktop\Samples\3	SUCCESS	
3:50:5...	180f82bbedb03...	4364	ReadFile	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Offset: 1,909,760, Length: 32,768, I/O Flags: Non-cached, Pagin...
3:50:5...	180f82bbedb03...	4364	Thread Create		SUCCESS	Thread ID: 360
3:50:5...	180f82bbedb03...	4364	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
3:50:5...	180f82bbedb03...	4364	RegQueryKey	HKLM	SUCCESS	Query: Name
3:50:5...	180f82bbedb03...	4364	RegOpenKey	HKLM\Software\WOW6432Node\Micr...	SUCCESS	Desired Access: Query Value
3:50:5...	180f82bbedb03...	4364	RegSetInfoKey	HKLM\SOFTWARE\WOW6432Node\...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
3:50:5...	180f82bbedb03...	4364	RegQueryValue	HKLM\SOFTWARE\WOW6432Node\...	NAME NOT FOUND	Length: 16
3:50:5...	180f82bbedb03...	4364	RegCloseKey	HKLM\SOFTWARE\WOW6432Node\...	SUCCESS	

Figure 2-16 Main executable creating threads and performing operations on files and registry keys

3:50:5...	Conhost.exe	6276	CreateFile	C:\Users\user\Desktop\Samples\3\net...	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Op...
3:50:5...	Conhost.exe	6276	CreateFile	C:\Windows\System32\net.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Op...
3:50:5...	Conhost.exe	6276	QueryBasicInfor...	C:\Windows\System32\net.exe	SUCCESS	CreationTime: 3/19/2019 5:45:34 AM, LastAccessTime: 4/7/202...
3:50:5...	Conhost.exe	6276	CloseFile	C:\Windows\System32\net.exe	SUCCESS	
3:50:5...	Conhost.exe	6276	Load Image	C:\Windows\System32\shell32.dll	SUCCESS	Image Base: 0x7f9c4d20000, Image Size: 0x6e5000
3:50:5...	Conhost.exe	6276	Load Image	C:\Windows\System32\cfmqr32.dll	SUCCESS	Image Base: 0x7f9c3490000, Image Size: 0x4a000

Figure 2-17 Conhost launching executables and loading DLLs

3:12:3...	icacls.exe	3672	CreateFile	C:\Program Files (x86)\Common Files\Mi...	ACCESS DENIED	Desired Access: R...
3:12:3...	icacls.exe	3672	CreateFile	C:\Program Files (x86)\Common Files\Mi...	SUCCESS	Desired Access: R...
3:12:3...	icacls.exe	3672	QueryAttributeT...	C:\Program Files (x86)\Common Files\Mi...	SUCCESS	Attributes: A, Repa...
3:12:3...	icacls.exe	3672	QueryRemotePr...	C:\Program Files (x86)\Common Files\Mi...	INVALID PARAME...	
3:12:3...	icacls.exe	3672	QuerySecurityFile	C:\Program Files (x86)\Common Files\Mi...	SUCCESS	Information: Owner...
3:12:3...	icacls.exe	3672	CloseFile	C:\Program Files (x86)\Common Files\Mi...	SUCCESS	

Figure 2-18 File permissions being changed with icacls

2.3.2 Process Explorer

The processes created by the ransomware during its runtime were further examined with Process Monitor. A considerable usage of icacls.exe (and an issued command – icacls "C:*" /grant Everyone:F/T/C/Q) could be observed (Figure 2-19). The use of Microsoft’s conhost.exe, net.exe, and net1.exe could also be seen (Figure 2-20).

180f82bbedb03dc29328e32...	48.48	95,136 K	106,868 K	4364	RecurseExec	MFC Application
CNzMjpdwrep.exe		93,392 K	10,128 K	672	RecurseExec	MFC Application
hYRWwaKxylan.exe		93,308 K	10,272 K	1416	RecurseExec	MFC Application
JlnUXoSDolan.exe		93,284 K	10,248 K	3872	RecurseExec	MFC Application
icacls.exe	38.47	2,028 K	4,940 K	2412		Microsoft Corporation
conhost.exe	0.77	6,860 K	15,376 K	3268	Console Window Host	Microsoft Corporation

Command Line: icacls "C:*" /grant Everyone:F/T/C/Q
 Path: C:\Windows\SysWOW64\icacls.exe
 U Usage: 100% Physical Usage: 81.30%

Figure 2-19 Issued icacls command

net.exe (1708)	Net Command	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-14QC1.
Conhost.exe (6276)	Console Window ...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-14QC1.
net1.exe (4548)	Net Command	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-14QC1.

Figure 2-20 Use of net.exe, Conhost.exe, and net1.exe

Furthermore, the processes created by the malware during the active encryption stage utilised a lot of computational power quickly reaching 100% CPU usage.

2.3.3 Comparing Registry Snapshots

After the malware finished actively encrypting files on the system, a second Regshot snapshot was created. Figure 2-21 and Figure 2-22 display the dialog windows displayed by Regshot after the 1st snapshot (created in Section 2.3) and the 2nd snapshot. These snapshots were then compared, and the

output of this step is contained in Appendix C – Regshot. In total 1184 changes were recognized by Regshot all of them relating to registry keys and their values.

```

&1st shot

Datetime: 2023-04-25 13:39:20
Computer: DESKTOP-14QC1L8
Username: user
Keys: 441094
Values: 734713
Dirs: 0
Files: 0
  
```

Figure 2-21 1st Regshot snapshot

```

&2nd shot

Datetime: 2023-04-25 13:55:29
Computer: DESKTOP-14QC1L8
Username: user
Keys: 441141
Values: 735594
Dirs: 0
Files: 0
  
```

Figure 2-22 2nd Regshot snapshot

2.3.4 Monitoring Network Communication

The last stage of dynamic analysis was analysing the networking capabilities of the malicious application. Figure 2-23 displays a fragment of the FakeNet console where one of the executables which were created in the entry directory by the launched malicious application requested IP addresses 224.0.0.22 and 224.0.0.251.

```

VJpDolwfoclan.exe (6132) requested UDP 224.0.0.22:7
0000: FF FF FF FF FF FF 01 00 5E 00 00 16 01 00 5E 00 .....^.....^
0010: 00 16 01 00 5E 00 00 16 01 00 5E 00 00 16 01 00 .....^.....^
0020: 5E 00 00 16 01 00 5E 00 00 16 01 00 5E 00 00 16 .....^.....^
0030: 01 00 5E 00 00 16 01 00 5E 00 00 16 01 00 5E 00 .....^.....^
0040: 00 16 01 00 5E 00 00 16 01 00 5E 00 00 16 01 00 .....^.....^
0050: 5E 00 00 16 01 00 5E 00 00 16 01 00 5E 00 00 16 .....^.....^
0060: 01 00 5E 00 00 16 .....^.....^
VJpDolwfoclan.exe (6132) requested UDP 224.0.0.251:7
0000: FF FF FF FF FF FF 01 00 5E 00 00 FB 01 00 5E 00 .....^.....^
0010: 00 FB 01 00 5E 00 00 FB 01 00 5E 00 00 FB 01 00 .....^.....^
0020: FF FF FF FF FF FF 01 00 5E 00 00 FB 01 00 5E 00 .....^.....^
0030: 5E 00 00 FB 01 00 5E 00 00 FB 01 00 5E 00 00 FB .....^.....^
0040: 00 FB 01 00 5E 00 00 FB 01 00 5E 00 00 FB 01 00 .....^.....^
0050: 01 00 5E 00 00 FB 01 00 5E 00 00 FB 01 00 5E 00 .....^.....^
0060: 5E 00 00 FB 01 00 5E 00 00 FB 01 00 5E 00 00 FB .....^.....^
0070: 00 FB 01 00 5E 00 00 FB 01 00 5E 00 00 FB 01 00 .....^.....^
0080: 01 00 5E 00 00 FB .....^.....^
0090: 5E 00 00 FB .....^.....^
0100: 00 FB 01 00 5E 00 00 FB .....^.....^
0110: 01 00 5E 00 00 FB .....^.....^
0120: 5E 00 00 FB .....^.....^
0130: 00 FB 01 00 5E 00 00 FB .....^.....^
0140: 01 00 5E 00 00 FB .....^.....^
0150: 5E 00 00 FB .....^.....^
0160: 00 FB 01 00 5E 00 00 FB .....^.....^
0170: 01 00 5E 00 00 FB .....^.....^
0180: 5E 00 00 FB .....^.....^
0190: 00 FB 01 00 5E 00 00 FB .....^.....^
0200: 01 00 5E 00 00 FB .....^.....^
0210: 5E 00 00 FB .....^.....^
0220: 00 FB 01 00 5E 00 00 FB .....^.....^
0230: 01 00 5E 00 00 FB .....^.....^
0240: 5E 00 00 FB .....^.....^
0250: 00 FB 01 00 5E 00 00 FB .....^.....^
0260: 01 00 5E 00 00 FB .....^.....^
  
```

Figure 2-23 FakeNet console fragment showcasing a requested UDP connection

Figure 2-24 displays a fragment of the FakeNet log, opened in Wireshark, further detailing the communication with 224.0.0.22. Echo requests and responses can be observed.

No.	Time	Source	Destination	Protocol	Length	Info
1984	89.710000	192.168.228.128	224.0.0.22	ECHO	130	Request
1989	89.710000	224.0.0.22	192.168.228.128	ECHO	130	Response
2655	105.332000	192.168.228.128	224.0.0.22	ECHO	130	Request
2660	105.348000	224.0.0.22	192.168.228.128	ECHO	130	Response

Figure 2-24 FakeNet log opened in Wireshark

When running the malware another time, more IP addresses were observed such as 239.255.255.250 (Figure 2-25). Again, Echo requests were sent.

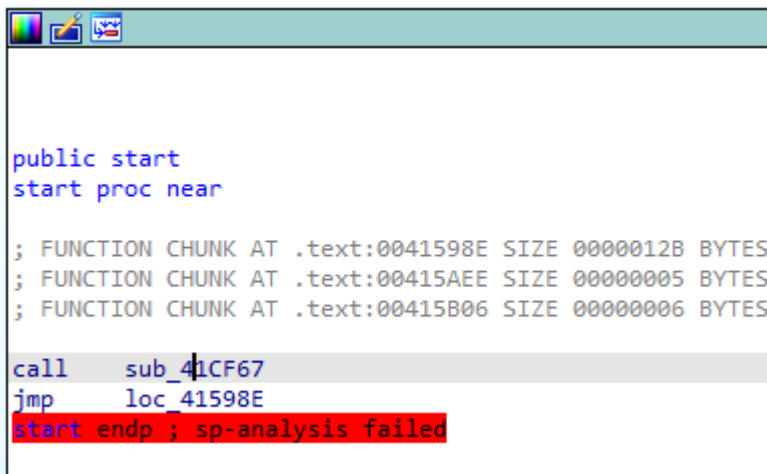
```
Divertor] hYRWwKxylan.exe (1416) requested UDP 239.255.255.250:7
RawUDPListener] 0000: FF FF FF FF FF FF 01 00 5E 7F FF FA 01 00 5E 7F .....^.....^
RawUDPListener] 0010: FF FA 01 00 5E 7F FF FA 01 00 5E 7F FF FA 01 00 .....^.....^
RawUDPListener] 0020: 5E 7F FF FA 01 00 5E 7F FF FA 01 00 5E 7F FF FA .....^.....^
RawUDPListener] 0030: 01 00 5E 7F FF FA 01 00 5E 7F FF FA 01 00 5E 7F .....^.....^
RawUDPListener] 0040: FF FA 01 00 5E 7F FF FA 01 00 5E 7F FF FA 01 00 .....^.....^
RawUDPListener] 0050: 5E 7F FF FA 01 00 5E 7F FF FA 01 00 5E 7F FF FA .....^.....^
RawUDPListener] 0060: 01 00 5E 7F FF FA .....^.....
RawUDPListener] 0060: 01 00 5E 7F FF FA .....^.....
```

Figure 2-25 A different IP address requested by the ransomware

2.4 CODE ANALYSIS

2.4.1 Static Analysis

Static code analysis first involved loading the malware sample into IDA. The starting location was then identified (Figure 2-26), and the flow of the graph generated by the disassembler was followed, observing function calls and their contents. This provided insight into the specifics of the order of how the ransomware performs the enumeration and encryption of the system files.



```
public start
start proc near

; FUNCTION CHUNK AT .text:0041598E SIZE 0000012B BYTES
; FUNCTION CHUNK AT .text:00415AEE SIZE 00000005 BYTES
; FUNCTION CHUNK AT .text:00415B06 SIZE 00000006 BYTES

call sub_41CF67
jmp loc_41598E
start endp ; sp-analysis failed
```

Figure 2-26 Starting block in IDA

Some DLL function calls were looked for using the disassemblers search feature. This allowed for quick identification of the locations they were called from which in turn gave a better understanding in their role in the code. The findings of this stage are discussed in Section 3.3.1.

2.4.2 Dynamic Analysis

The debugger used for this step was OllyDbg. It identified 755 calls to known and 1072 to assumed functions, 365 loops, and 30 switches in the code (Figure 2-27).

```
1235 heuristical procedures
775 calls to known, 1072 calls to guessed functions
365 loops, 30 switches
```

Figure 2-27 Identified code constructs

When debugging, the program quickly reached an access violation which it was not able to process even when stepping over it in the debugger was attempted (Figure 2-28). This indicated a possible anti-debugging technique which was investigated and is further discussed in Section 3.3.2.

```
35001A41 Access violation when reading [00000000]
76F363B0 New thread with ID 00001298 created
35001A41 Access violation when reading [00000000]
35001A41 Access violation when reading [00000000]
35001A41 Access violation when reading [00000000]
35001A41 Access violation when reading [00000000]
35001A41 Access violation when reading [00000000]
35001A41 Access violation when reading [00000000]
35001A41 Access violation when reading [00000000]
35001A41 Access violation when reading [00000000]
35001A41 Access violation when reading [00000000]
35001A41 Access violation when reading [00000000]
35001A41 Exception C000041D
Debugged program was unable to process exception
Thread 000016A4 terminated, exit code C000041D (-1073740771.)
Thread 0000172C terminated, exit code C000041D (-1073740771.)
Thread 00000048 terminated, exit code C000041D (-1073740771.)
35000000 Module C:\Users\user\Desktop\Samples\3\180f82bbedb03dc29328e32e054069870a1e65078b78b2120a84c96aaed7d843.exe
74C30000 Module C:\Windows\System32\WS2_32.dll
00400000 Unload C:\Users\user\Desktop\Samples\3\180f82bbedb03dc29328e32e054069870a1e65078b78b2120a84c96aaed7d843.exe
Process terminated, exit code C000041D (-1073740771.)
```

Figure 2-28 Access violation during debugging

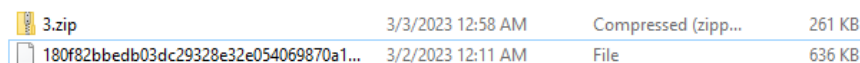
3 RESULTS

3.1 STATIC ANALYSIS

The results of static analysis firstly reveal that the investigated malware sample is the Ryuk ransomware.

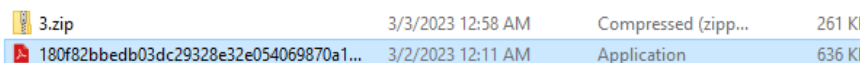
As discussed in Section 2.2.2, the file is a portable executable. Utilising this finding in conjunction with PEiD concludes that the sample is not packed and that the code is compiled with Microsoft Visual C++.

An additional discovery during this stage is the Adobe icon that the application uses which can be observed after renaming the file to end with “.exe”. This is an attempt of masquerading as a PDF file to trick a potential victim into executing the malware. Figure 3-1 and Figure 3-2 showcase the sample file icon before and after renaming.



Name	Date modified	Type	Size
3.zip	3/3/2023 12:58 AM	Compressed (zipp...	261 KB
180f82bbedb03dc29328e32e054069870a1...	3/2/2023 12:11 AM	File	636 KB

Figure 3-1 Initial file appearance in File Explorer



Name	Date modified	Type	Size
3.zip	3/3/2023 12:58 AM	Compressed (zipp...	261 KB
180f82bbedb03dc29328e32e054069870a1...	3/2/2023 12:11 AM	Application	636 KB

Figure 3-2 Application icon after renaming it

Further investigation of the PE file reveals the compilation time being 2:51:01 UTC on February 11, 2021 and the file name, *RecurseExec.exe*, with the description of “*RecurseExec MFC Application*”. The entropy of 6.236, which measures the randomness in data and tends to be high for complex malware, falls within the range that legitimate files are also usually in of 4.8 – 7.2 (Practical Security Analytics, no date). This is another detail that increases the stealth of this ransomware.

Ten dynamic linked libraries can be observed as imports of the executable, one of them being a driver file. The driver file, *WINSPOOL.DRV*, contains methods used by the Graphics Device Interface and by applications, to interact with the Print Spooler, which stores print jobs in the computer's memory. The imported functions, *OpenPrinterA* and *ClosePrinter*, retrieve a handle of a specified printer and close the printer object respectively. *DocumentPropertiesA* displays printer-configuration property sheet or retrieves/modifies printer initialization information. This could indicate that the malware attempts to print on any printers that are on the same network as the infected machine. Cases where ransom notes are printed have been reported in the past (Abrams, 2020).

Many functions from *KERNEL32.dll*, which carries out memory management, input/output operations, and thread/process creation, among others, were used by the sample. Notable instances include *FindFirstFileA* and *FindNextFileA* for enumerating directories, *CreateProcess* for creating processes, *Sleep* for time-based evasion, *CreateFile* for creating/opening files, and functions for memory allocation, such as *HeapAlloc*, *GlobalAlloc*, *LocalAlloc*, and *VirtualAlloc*.

Additionally, *EnumSystemLocalesA*, which can be used to avoid infecting systems of a certain region, and *isDebuggerPresent*, which determines whether a process is being debugged as an anti-debugging measure, are used from this library.

Next, *USER32.dll*, which is used for manipulating elements of the Windows user interface, and *GDI32.dll*, for performing drawing functions for output devices such as printers, can be observed. The presence of these libraries is a further implication of the malware having some printing functionality.

A further notable imported DLL is *ADVAPI32.dll*. The ransomware performs file encryption with *CryptImportKey*, *CryptEncrypt*, and *CryptAcquireContextW* functions from this DLL. It is also used by the Windows Registry. Functions such as *RegCreateKeyA*, *RegOpenKeyA*, *RegQueryValueExA*, and *RegSetValueExA* are used to perform operations with Windows Registry keys.

From the remaining DLLs, *SHELL32.dll* contains functions for opening web pages and files, *SHLWAPI.dll* contains further registry-related functions and functions for URL and UNC path usage. Lastly, *ole32.dll*, *OLEAUT32.dll*, and *oleacc.dll* are related to Object Linking and Embedding operations.

The Strings output provided additional information on the ransomware's functionality with copyright lines from utilities that this executable employs. The first one, "*Copyright (c) 1992-2004 by P.J. Plauger, licensed by Dinkumware, Ltd. ALL RIGHTS RESERVED*", at position 0003A948 in the output (Appendix B – Strings) is related to Microsoft Visual C++ being used as Dinkumware provides the C++ standard library that ships with Microsoft Visual C++.

Another string, "*A Kamal Shankar Quick Tool - Recursive Executer*", at position 0007B742 is a reference to a program that recursively executes tools that normally only operate in the directory in which they are called from. The malware possibly utilises this to recursively enumerate and encrypt directories within the file system.

Additional results include functions from the imported libraries which were discussed earlier and the error code at position 0007C1E2 which contains the string "*Could not start print job*" which is a further indicator that the malware might be attempting to print something.

Furthermore, the string "*RSA2*" indicates that the RSA cryptosystem is in use. Like many ransomware families, Ryuk encrypts files with two encryption algorithms – symmetric and asymmetric. Files are encrypted with the symmetric algorithm and the symmetric encryption key is encrypted with the asymmetric public key (Manocha, 2022). "*RSA2*" being present in the executable suggests that the asymmetric algorithm in use is RSA. In these scenarios, the RSA public key comes shipped with the ransomware while the symmetric algorithms encryption key is generated during runtime. The RSA private key, however, is possessed by the threat actor and provided to the victim when the ransom is paid.

Lastly, the strings output includes references to libraries that did not appear in the imported library list such as *ntdll.dll* (positions 0002E2B8 and 0002E50C), which contains Windows NT kernel functions. The reason for this is the library getting indirectly loaded by other imported DLLs to obtain additional functions required to perform tasks.

3.2 DYNAMIC ANALYSIS

When running the executable, three other executables were added to the directory it was executed from. The file names of the generated executables changed when running the malware in other instances and appeared to be randomly generated, however, the first of them always ended with “-rep” while the other two ended with “-lan”. The ransomware then advanced to encrypt the system, which was indicated by files now ending with a .RYK extension and a dropped HTML README file in each directory (Figure 3-3 and Figure 3-4).





 180f82bbedb03dc29328e32e054069870a1...	3/2/2023 12:11 AM	Application	636 KB
 CNzMJpduwrep.exe	3/2/2023 12:11 AM	Application	636 KB
 hYRWwaKxylan.exe	3/2/2023 12:11 AM	Application	636 KB
 JlnUXoSDolan.exe	3/2/2023 12:11 AM	Application	636 KB

Figure 3-3 Three new executables in the entry directory








Name	Date modified	Type	Size
 My Music	2/27/2023 12:49 AM	File folder	
 My Pictures	2/27/2023 12:49 AM	File folder	
 My Videos	2/27/2023 12:49 AM	File folder	
 WindowsPowerShell	2/27/2023 10:55 PM	File folder	
 config.xml.RYK	4/7/2023 3:35 PM	RYK File	3 KB
 desktop.ini	2/27/2023 12:49 AM	Configuration sett...	1 KB
 RyukReadMe.html	4/7/2023 3:35 PM	Microsoft Edge H...	2 KB

Figure 3-4 An encrypted file ending with .RYK and an HTML README file in the current user's home directory

The HTML file displayed the contents seen in Figure 3-5. Pressing the “Contact” button displayed an alert box with instructions to access an onion site and fill out a form with a given password (Figure 3-6). The link and password did not change upon running the malware another time.



Ryuk

balance of shadow universe

Figure 3-5 RyukReadMe.html

This page says

INSTRUCTION:

1. Download tor browser.
2. Open link through tor browser: <http://piesa6sapybbrz63pqmmwdzyc5fp73b3uya5cpli6pp5jpswndiu44id.onion>
3. Fill the form, your password: 5GqsR1ewcO

We will contact you shortly.
Always send files for test decryption.



Figure 3-6 Contact button prompt

Additionally, after the malware had been running for enough time to have encrypted most of the user files and/or changed values needed for the normal function of the infected machine, the recycle bin functionality of Windows started issuing warnings about it being corrupted (Figure 3-7).

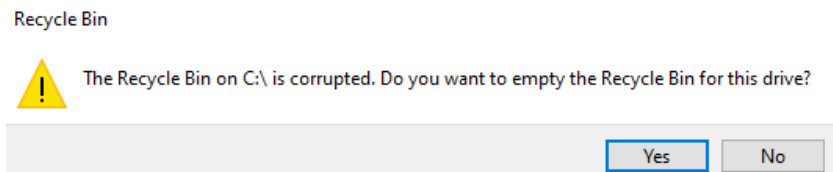


Figure 3-7 Recycle bin warning

When one of the 3 executables that were created by the original malware sample was launched, it repeated the entire process of making new executables and then encrypting files while the previously run application never stopped as a process (Figure 3-8).

180f82bbedb03dc29328e32...		95,996 K	38,508 K	7048	RecurseExec	MFC Application
HNIxMOMPrep.exe		93,952 K	6,952 K	4224	RecurseExec	MFC Application
zUWbxivDlan.exe	19.80	96,512 K	6,376 K	752	RecurseExec	MFC Application
JRRORoGhxlان.exe	10.66	94,116 K	7,144 K	1192	RecurseExec	MFC Application
HNIxMOMPrep.exe	14.47	94,904 K	20,620 K	22792	RecurseExec	MFC Application
KJDOXMjnPrep.exe		94,164 K	10,216 K	22260	RecurseExec	MFC Application
UKJYHGfYhlan.exe		2,264 K	9,552 K	22516	RecurseExec	MFC Application
TxpTlhOYlan.exe		2,340 K	9,612 K	24056	RecurseExec	MFC Application
icacls.exe	8.38	1,384 K	4,304 K	22740		Microsoft Corporation
conhost.exe	12.95	6,924 K	14,668 K	24508	Console Window Host	Microsoft Corporation

Figure 3-8 A newly created executable repeating the encryption process.

From the processes started by the malware which were observable from Process Monitor and Process Explorer, conhost.exe is related to the Command Prompt and acts as a host to the console window. Net and net1.exe are used to enable IPv6. The most significant finding is the use of icacls.exe. This executable is used for file and directory access control permissions. The command issued by the ransomware, `icacls "C:*" /grant Everyone:F/T/C/Q`, grants everyone full access to the entire C drive. The *T*, *C*, and *Q* options are used to apply this command to subdirectories of the starting directory, ignore any errors, and suppress success messages respectively. This command allowed the malware to have full access to directories and files on the infected system to encrypt them. Additionally, the use of threads could be observed to quickly execute the enumeration and encryption process of the filesystem.

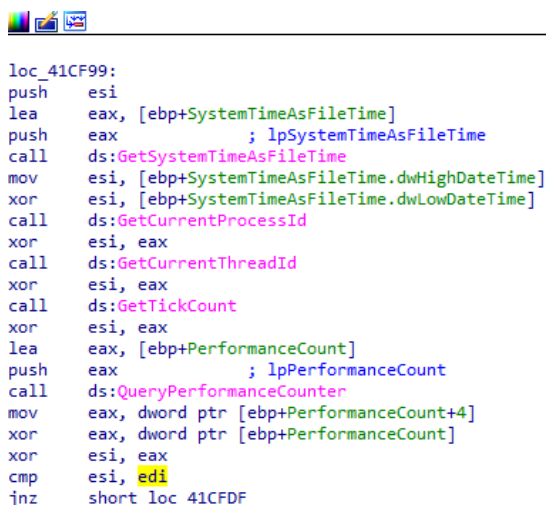
When comparing the infected machines registry before and after executing the ransomware, Regshot identified 15 deleted keys and 32 deleted values. In addition, 62 new keys and 913 new values were added, and 162 values were edited. Notably, despite the ransomware creating new files in each directory, these changes did not appear in the comparison even when redoing the process. This influences the accuracy of the results as further insight into how the filesystem was changed by the malware cannot be obtained.

Lastly, the malware exhibited some networking functionality. All observed IP addresses (224.0.0.22, 224.0.0.251, and 239.255.255.250) are within the multicast range which is used for network discovery. The use of the Echo protocol for addresses within the multicast range indicates the possibility of the ransomware attempting to find other hosts to further spread across the network after infecting a single node. As discussed in Section 3.1, the compilation time of this sample is February 2021, which corresponds with the time sources report Ryuk starting to exhibit the capability to spread over a network after gaining initial access to a single host (Manocha, 2022) which further explains the exhibited behaviour.

3.3 CODE ANALYSIS

3.3.1 Static Analysis

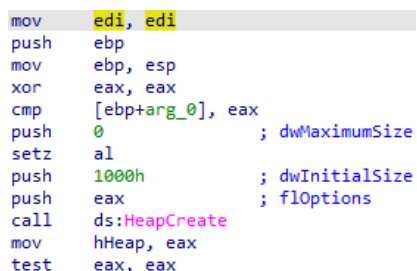
Following the function calls from the starting position first reveals the malware initially enumerating current system time, process and thread IDs, and tick and performance counts (Figure 3-9).



```
loc_41CF99:
push     esi
lea     eax, [ebp+SystemTimeAsFileTime]
push     eax          ; lpSystemTimeAsFileTime
call    ds:GetSystemTimeAsFileTime
mov     esi, [ebp+SystemTimeAsFileTime.dwHighDateTime]
xor     esi, [ebp+SystemTimeAsFileTime.dwLowDateTime]
call    ds:GetCurrentProcessId
xor     esi, eax
call    ds:GetCurrentThreadId
xor     esi, eax
call    ds:GetTickCount
xor     esi, eax
lea     eax, [ebp+PerformanceCount]
push     eax          ; lpPerformanceCount
call    ds:QueryPerformanceCounter
mov     eax, dword ptr [ebp+PerformanceCount+4]
xor     eax, dword ptr [ebp+PerformanceCount]
xor     esi, eax
cmp     esi, edi
jnz     short loc_41CFDF
```

Figure 3-9 Enumeration commands used by the executable

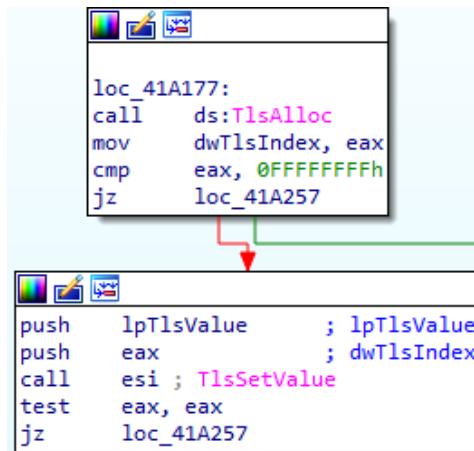
Afterward, the use of memory allocation functions can also be observed as seen in Figure 3-10.



```
mov     edi, edi
push    ebp
mov     ebp, esp
xor     eax, eax
cmp     [ebp+arg_0], eax
push    0          ; dwMaximumSize
setz   al
push    1000h      ; dwInitialSize
push    eax        ; flOptions
call    ds:HeapCreate
mov     hHeap, eax
test   eax, eax
```

Figure 3-10 Memory allocation with HeapCreate

Subsequentially, memory allocation for threads with Thread Local Storage can be observed. *TlsAlloc* assigns a thread index in the Thread Local Storage while *TlsSetValue* stores a value in the storage slot with this index (Figure 3-11). On several instances throughout the code, thread creation functions can be encountered repeatedly as this ransomware sample uses threads to efficiently enumerate and encrypt the filesystem.

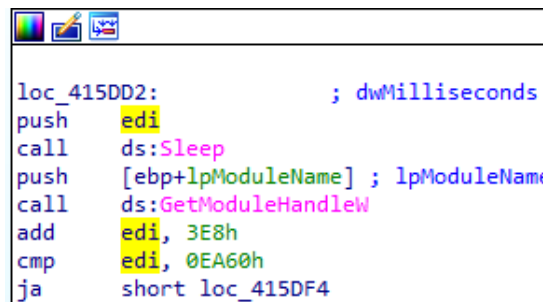


```
loc_41A177:
call  ds:TlsAlloc
mov   dwTlsIndex, eax
cmp   eax, 0FFFFFFFh
jz    loc_41A257

push  lpTlsValue ; lpTlsValue
push  eax ; dwTlsIndex
call  esi ; TlsSetValue
test  eax, eax
jz    loc_41A257
```

Figure 3-11 Thread Local Storage commands

In a function called after the Thread Local Storage functions, the use of *Sleep* can be observed (Figure 3-12) as an evasion technique that delays execution.



```
loc_415DD2: ; dwMilliseconds
push  edi
call  ds:Sleep
push  [ebp+lpModuleName] ; lpModuleName
call  ds:GetModuleHandleW
add   edi, 3E8h
cmp   edi, 0EA60h
ja    short loc_415DF4
```

Figure 3-12 Sleep being called

When progressing further some error checking (Figure 3-13), followed by anti-debugging (Figure 3-14) is performed. These functions and other related error-checking and anti-debugging function calls can be regularly encountered throughout the code.



```
push  offset aProgramNameUnk ; "<program name unknown>"
push  2FBh
push  esi
call  sub_4160FF
add   esp, 0Ch
test  eax, eax
jz    short loc_41C55D
```

Figure 3-13 Error handling invalid file names (indicated by the string)



Figure 3-14 Checking for debuggers and terminating the process

Further advancement into statically analysing the code involved looking up specific function calls to grasp their role in the code. Figure 3-15 displays a command and arguments passed to it used for file opening. This command is used together with a call to a procedure `sub_401490` which enumerates the directory the opened file is in to discover other files.

```

; int __stdcall sub_401770(LPCSTR lpString2, int, int, int, int, int, int, int, LPCSTR lpFileName, int)
sub_401770 proc near

lpString2= dword ptr 4
arg_4= dword ptr 8
arg_8= dword ptr 0Ch
arg_C= dword ptr 10h
arg_10= dword ptr 14h
arg_14= dword ptr 18h
arg_18= dword ptr 1Ch
lpFileName= dword ptr 20h
arg_20= dword ptr 24h

mov     eax, [esp+arg_8]
mov     edx, [esp+arg_14]
push    esi
mov     esi, ecx
mov     ecx, [esp+4+arg_C]
push    0 ; hTemplateFile
push    80h ; 'e' ; dwFlagsAndAttributes
push    4 ; dwCreationDisposition
push    0 ; lpSecurityAttributes
mov     [esi+4], eax
mov     eax, [esp+14h+arg_18]
push    3 ; dwShareMode
mov     [esi+18h], eax
mov     eax, [esp+18h+lpFileName]
mov     [esi+8], ecx
mov     ecx, [esp+18h+arg_10]
mov     [esi+1Ch], edx
mov     edx, [esp+18h+arg_20]
push    40000000h ; dwDesiredAccess
push    eax ; lpFileName
mov     dword ptr [esi], offset off_42E524
mov     [esi+20h], ecx
mov     [esi+0Ch], eax
mov     [esi+14h], edx
call    ds:CreateFileA

```

Figure 3-15 Command with arguments

The `sub_401490` procedure initially finds the first file of the current directory (Figure 3-16) and then continues across the directory until the last file (Figure 3-17).

```

loc_4015CC:
lea  edx, [esp+370h+FindFileData] ; Load Effective Address
push edx                               ; lpFindFileData
lea  eax, [esp+374h+String1] ; Load Effective Address
push eax                               ; lpFileName
call ds:FindFirstFileA ; Indirect Call Near Procedure
mov  [esp+370h+hFindFile], eax
cmp  eax, 0FFFFFFFh ; Compare Two Operands
jz   loc_401726 ; Jump if Zero (ZF=1)

```

Figure 3-16 First file of the directory identified

```

loc_401703:
mov  edx, [esp+370h+hFindFile]
lea  ecx, [esp+370h+FindFileData] ; Load Effective Address
push ecx                               ; lpFindFileData
push edx                               ; hFindFile
call ds:FindNextFileA ; Indirect Call Near Procedure
test  eax, eax                         ; Logical Compare
jnz  loc_4015F0 ; Jump if Not Zero (ZF=0)

loc_4015F0:
mov  eax, [esp+370h+hFindFile]
push eax                               ; hFindFile
call ds:FindClose ; Indirect Call Near Procedure

```

Figure 3-17 Finding other files in the current directory and close

Additionally, strings indicating that operations on the current directory have been finished and signs of subdirectory enumeration can be seen in Figure 3-18. This code likely relates to the recursive execution tool identified in Section 3.1.

```

lea  ecx, [esp+370h+String] ; Load Effective Address
push ecx
push offset aFinishedOperat_0 ; "Finished operating in the current direc"...
push offset byte_43B5C0 ; LPSTR
call edi ; wsprintfA ; Indirect Call Near Procedure
add  esp, 0Ch ; Add
push 24h ; '$' ; uType
push offset aSubDirectoryOp ; "Sub directory operation query"
push offset byte_43B5C0 ; lpText
push 0 ; hWnd
call ds:MessageBoxA ; Indirect Call Near Procedure
cmp  eax, 7 ; Compare Two Operands
jz   short loc_401726 ; Jump if Zero (ZF=1)

```

Figure 3-18 Messages relating to the state of operations in the current working directory.

An interesting finding is the string which appears right before encryption-related functions are called (Figure 3-19). While not a public key itself, it might be related to the RSA public key that comes shipped with the malware being loaded (discussed in Section 3.1).

```

push 1 ; phProv
push offset a2Snrkwkzszpupi ; "^2?SnrwkZSzuPI"
call sub_401AF0

```

Figure 3-19 String value in code before encryption function is called

Figure 3-20 and Figure 3-21 display the encryption functionality of this ransomware. *CryptAcquireContext* is first called to obtain a handle to a particular key container. Then *CryptImportKey* is called to for acquiring cryptographic keys and lastly, the file is encrypted with *FileEncrypt*.

```

push  0F000000h ; dwFlags
push  1         ; dwProvType
push  ebx      ; szProvider
push  ebx      ; szContainer
lea   eax, [esp+24h+phProv]
push  eax     ; phProv
call  edi ; CryptAcquireContextW
test  eax, eax
jz    loc_401BD6

loc_401B48:
mov   edx, [esp+14h+phProv]
mov   edi, ds:CryptImportKey
lea   ecx, [esp+14h+phKey]
push  ecx     ; phKey
push  ebx     ; dwFlags
push  ebx     ; hPubKey
push  134h    ; dwDataLen
push  offset pbData ; pbData
push  edx     ; hProv
mov   [esp+2Ch+phKey], ebx
call  edi ; CryptImportKey
test  eax, eax
jz    short loc_401BD6

```

Figure 3-20 *CryptAcquireContextW* and *CryptImportKey* called

```

loc_401BDF:
mov   eax, [esp+14h+pdwDataLen]
mov   ecx, [eax]
mov   edx, [esp+14h+pbData]
push  ecx     ; dwBufLen
push  eax     ; pdwDataLen
mov   eax, [esp+1Ch+hKey]
push  edx     ; pbData
push  ebx     ; dwFlags
push  1       ; Final
push  ebx     ; hHash
push  eax     ; hKey
call  ds:CryptEncrypt
pop   edi
test  eax, eax
pop   ebx
setnz al
pop   esi
add   esp, 8

```

Figure 3-21 Encryption function called

Lastly, the memory that was allocated at the beginning of the execution is freed (Figure 3-22).

```

push  eax     ; dwTlsIndex
call  ds:TlsFree

loc_411258:
mov   eax, [esi+10h]
test  eax, eax
jz    short loc_411279

push  eax     ; pMem
call  ds:GlobalHandle
mov   edi, eax
push  edi     ; hMem
call  ds:GlobalUnlock
push  edi     ; hMem
call  ds:GlobalFree

```

Figure 3-22 Memory being freed

3.3.2 Dynamic Analysis

Dynamic analysis first reveals all the DLLs used by the malicious application and additional DLLs for function utility being imported before the program entry point is reached (Figure 3-23).

```

File 'C:\Users\user\Desktop\Samples\3\180f82bbdb03dc29328e32e054069870a1e65078b78b2120a84c96aaed7d843.exe'
00415B0C New process with ID 000004C4 created
76F363B0 Main thread with ID 000015A4 created
New thread with ID 0000172C created
00400000 Module C:\Users\user\Desktop\Samples\3\180f82bbdb03dc29328e32e054069870a1e65078b78b2120a84c96aaed7d843.exe
72F60000 Module C:\Windows\SYSTEM32\PROPSYS.dll
73030000 Module C:\Windows\SYSTEM32\WINSPPOOL.DRV
73A90000 Module C:\Windows\SYSTEM32\apphelp.dll
73BB0000 Module C:\Windows\SYSTEM32\IPHLPAPI.DLL
746A0000 Module C:\Windows\System32\CRYPTBASE.dll
746B0000 Module C:\Windows\System32\SspiCli.dll
746D0000 Module C:\Windows\System32\KERNELBASE.dll
748D0000 Module C:\Windows\System32\win32u.dll
74960000 Module C:\Windows\System32\wcrbase.dll
74A90000 Module C:\Windows\System32\powprof.dll
74AE0000 Module C:\Windows\System32\ole32.dll
74BE0000 Module C:\Windows\System32\shlwapi.dll
74D90000 Module C:\Windows\System32\GDI32.dll
74DC0000 Module C:\Windows\System32\gdi32full.dll
74F40000 Module C:\Windows\System32\cfgmgr32.dll
74F80000 Module C:\Windows\System32\combase.dll
75200000 Module C:\Windows\System32\SHELL32.dll
757D0000 Module C:\Windows\System32\msvcp_win.dll
75850000 Module C:\Windows\System32\msvort.dll
75910000 Module C:\Windows\System32\kernel.appcore.dll
75920000 Module C:\Windows\System32\bcrypt.dll
75950000 Module C:\Windows\System32\USER32.dll
75B70000 Module C:\Windows\System32\profapi.dll
Invalid or compressed Image Export Directory
75B90000 Module C:\Windows\System32\windows.storage.dll
762A0000 Module C:\Windows\System32\sechost.dll
76320000 Module C:\Windows\System32\shcore.dll
763C0000 Module C:\Windows\System32\UMPDC.dll
76430000 Module C:\Windows\System32\cryptsp.dll
76450000 Module C:\Windows\System32\OLEAUT32.dll
76A80000 Module C:\Windows\System32\ADVAPI32.dll
76C40000 Module C:\Windows\System32\RPCRT4.dll
76D90000 Module C:\Windows\System32\KERNEL32.DLL
76E70000 Module C:\Windows\System32\bcryptPrimitives.dll
76EE0000 Module C:\Windows\SYSTEM32\ntdll.dll
76F363B0 New thread with ID 00000D48 created
00415B0C Program entry point
  
```

Figure 3-23 DLLs being loaded before the program entry point

In addition to the imported libraries which appear in the imports of the portable executable, encryption-related libraries such as bcrypt.dll, bcryptPrimitives.dll, CRYPTBASE.dll, and cryptsp.dll are being imported.

As discussed in Section 2.4.2, an access violation kept being encountered by the debugging process and later the process terminated entirely. Malware code often utilises access violations and exception handling to its advantage as an anti-debugging measure which is suspected to be the case with this sample. Yason (2007) states that some malware purposefully does not handle exceptions when a debugger is present and passes them to it as second chance exceptions, while they would be handled and execution would continue if no debugger was detected.

The exception is encountered after the use of two anti-debugging functions. The first one is the ntdll libraries *NtQueryInformationProcess* function (Figure 3-24) which retrieves information about the current process, including whether it is being debugged from its *ProcessDebugPort* value. Afterward, the second function, *IsDebuggerPresent* from KERNEL32.dll, can be seen being accessed via the FS segment (Figure 3-25). It can be concluded that after confirming that a debugger is present, the malware performs the discussed anti-debugging technique of not handling exceptions.

350019F2	01B8 90906A04	ADD DWORD PTR DS:[EAX+46A9090],EDI	
350019F8	8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
350019FB	8B15 E0060235	MOV EDX,DWORD PTR DS:[350206E0]	ntdll.ZwQueryInformationProcess
35001A01	EB 06	JMP SHORT 180f82 1.35001A09	

Figure 3-24 NtQueryInformationProcess being called

747E3D1F	CC	INT3	
747E3D20	64:A1 30000000	MOV EAX,DWORD PTR FS:[30]	
747E3D26	0FB640 02	MOVZX EAX,BYTE PTR DS:[EAX+2]	

Figure 3-25 IsDebuggerPresent being called

4 DISCUSSION

4.1 GENERAL DISCUSSION

The tested sample was identified as the Ryuk ransomware which first appeared in August 2018 and has been known to target large organizations, in the healthcare, government, financial, and publishing sectors in addition to targeting critical infrastructure (SentinelOne, no date). It is typically delivered through phishing campaigns as a malicious email attachment. Once it infects a system, it encrypts the files and demands payment in exchange for a decryption key. In 2020, CrowdStrike's Global Threat Report listed Ryuk as responsible for three of the top 10 largest ransom payments demanded that year, ranging from 5.3 to 12.5 million USD (Trend Micro, no date).

The main indicators of compromise that the system has been hit by Ryuk are the encrypted files which end with a .RYK extension and the ransom notes in every directory. The malicious executable can also be found in the running processes even after it finishes actively enumerating and encrypting the filesystem. Additionally, a spike in system resource use is apparent when it is actively executing.

The undertaken analysis helped in understanding the specifics of how this malware operates. It was discovered that this malware recursively enumerates the filesystem, uses `icacls.exe` to obtain full file permissions in the system, and then encrypts it. To further decrease the runtime of this process, Ryuk creates a significant number of threads to parallelise these operations. The encryption likely follows the outline many ransomware families utilise and uses a combination of symmetric and asymmetric algorithms, where a file is first encrypted by a symmetric algorithm followed by its key being encrypted by the asymmetric algorithm's public key, which comes shipped with the malware, while the private key is in the possession of the ransomware group. This was further confirmed by the string "RSA2", corresponding to the RSA cryptosystem, being present in the malicious executable. Furthermore, the malicious executable uses an Adobe icon to trick a potential victim into executing it.

Countermeasures for Ryuk, and ransomware altogether, include investing in anti-virus software and keeping systems up to date with the latest patches applied. Monitoring network processes is also a crucial step in identifying whether a network has been compromised, especially if the specific malware strain persists in the system for some time before beginning to encrypt it. Regularly backing up critical data and storing it correctly (i.e., not on the same network) is also important, as it allows for the possibility to recover files without paying the ransom, therefore minimising both financial and intellectual property losses. Additionally, it is important for users to be aware of, recognize, and report phishing attempts to help in preventing the initial infection.

4.2 CONCLUSIONS

This project aimed to perform malware analysis of a malware sample and was successful in meeting the objectives of identifying it and recognising its main characteristics, components, and impacts on a computer system. The methodology steps outlined in *Practical Malware Analysis* were successfully applied to this scenario and static, dynamic, and code analysis techniques were performed on the sample. However, there are several aspects of this investigation that could have been more thorough. This involves

the dynamic code analysis stage which could have been executed fully after identifying solutions to the encountered obstacles. Furthermore, an even more detailed look at the disassembled binary would have provided an even better insight into the full functionality of Ryuk. Registry analysis and the identification of the symmetric encryption algorithm in use would also have benefited the overall quality of this project. These and other suggested improvements are further discussed in Section 4.3.

Overall, the analysis of this sample of Ryuk ransomware reveals its highly dangerous encryption and network propagation capabilities and the severe impacts it can have on a system which in turn cause massive financial and intellectual property losses. It further highlights the role of malware analysis in developing effective countermeasures against emerging threats. By following a structured methodology to gain a comprehensive understanding of the capabilities and impacts of malicious payloads, the obtained expertise can be used to effectively develop and implement countermeasures. Additionally, it is important to take proactive measures for preventing and detecting malware attacks. Backup maintenance, regular monitoring of processes, implementation of strong security controls and software, and user training all contribute to decreasing the risk of infection and the severity of malware attacks.

4.3 FUTURE WORK

Future investigative work relating to this ransomware sample mainly requires a more in-depth look at the disassembled code. This would include further static analysis in a disassembler and a continuation of dynamic analysis by bypassing the discussed anti-debugging techniques. To bypass the use of *NtQueryInformationProcess*, a breakpoint can be set where this function returns, and when this happens, the return value can be manipulated. This can be done manually or with a script. Additionally, a plugin for OllyDbg that injects a code that manipulates the return value of *NtQueryInformationProcess* can be used to patch this. A similar approach can be used to bypass the use of *IsDebuggerPresent*.

Additionally, further registry analysis could be completed to see what operations the malware performed on it, including whether any processes were disabled or enabled. Next, memory analysis could also be performed on the .vmem and .vmss files of the virtual machine used for this investigation. This would comprise of using the Volatility framework on the prepared memory images and reveal whether any process hollowing is performed as a persistence technique on the system.

Possible printing and networking functionality was also observed for this strain of the Ryuk ransomware. This could be further explored to understand this malware's full impacts on a network of more than one host. Testing the network propagation capabilities of this malware would involve setting up another Windows host on the closed testing network and assessing the executed malicious application's effects on it.

Lastly, the symmetric encryption algorithm this malware uses could be fully identified by analysing the code and imported functions and an investigation could be attempted into the onion link mentioned in the README files instructions to obtain insight into how the ransomware grouping behind Ryuk operates, however, the site referenced in this sample could no longer be active.

REFERENCES

- Abrams, L., 2020. *Egregor ransomware print bombs printers with ransom notes*. [Online]
Available at: <https://www.bleepingcomputer.com/news/security/egregor-ransomware-print-bombs-printers-with-ransom-notes/>
[Accessed 26 April 2023].
- A, M. K., 2018. *Learning Malware Analysis*. Birmingham: Packt Publishing.
- Baker, K., 2022. *Malware Analysis*. [Online]
Available at: <https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/>
[Accessed 1 April 2023].
- Fleck, A., 2022. *Cybercrime Expected To Skyrocket in Coming Years*. [Online]
Available at: <https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/>
[Accessed 1 April 2023].
- Gibson, D., 2011. *SSCP Systems Security Certified Practitioner All-in-One Exam Guide*. New York: McGraw-Hill.
- Kacherginsky, P., 2017. *FLARE VM: The Windows Malware Analysis Distribution You've Always Needed!*. [Online]
Available at: <https://www.mandiant.com/resources/blog/flare-vm-the-windows-malware>
[Accessed 11 April 2023].
- Kleymenov, A. & Thabet, A., 2019. *Mastering Malware Analysis*. Birmingham: Packt Publishing.
- Malwarebytes, no date. *Malware*. [Online]
Available at: <https://www.malwarebytes.com/malware>
[Accessed 1 April 2023].
- Manocha, H., 2022. *Ryuk Ransomware: History, Timeline, And Adversary Simulation*. [Online]
Available at: <https://fourcore.io/blogs/ryuk-ransomware-simulation-mitre-ttp>
[Accessed 30 April 2023].
- N-able, 2019. *Malware Analysis Overview*. [Online]
Available at: <https://www.n-able.com/blog/malware-analysis-steps>
[Accessed 22 April 2023].
- Practical Security Analytics, no date. *Threat Hunting with File Entropy*. [Online]
Available at: <https://practicalsecurityanalytics.com/file-entropy/>
[Accessed 28 April 2023].
- SentinelOne, no date. *What Is Ryuk Ransomware?*. [Online]
Available at: <https://www.sentinelone.com/cybersecurity-101/ryuk-ransomware/>
[Accessed 30 April 2023].
- Sikorski, M. & Honig, A., 2012. *Practical Malware Analysis*. San Francisco: No Starch Press.

Trend Micro, no date. *What Is RYUK Ransomware?*. [Online]

Available at: https://www.trendmicro.com/en_gb/what-is/ransomware/ryuk-ransomware.html

[Accessed 30 April 2023].

Yason, M. V., 2007. *The Art of Unpacking*. [Online]

Available at: <https://www.blackhat.com/presentations/bh-usa-07/Yason/Whitepaper/bh-usa-07-yason-WP.pdf>

[Accessed 28 April 2023].

APPENDICES

APPENDIX A – IMPORTED FUNCTIONS

wsprintfA	SetFocus	LockResource
lstrlenA	SetFilePointer	LocalReAlloc
lstrcpynA	SetErrorMode	LocalFree
lstrcpyA	SetCursor	LocalAlloc
lstrcmpW	SetBkColor	LoadResource
lstrcmpA	SetActiveWindow	LoadLibraryA
lstrcatA	SendMessageA	LoadIconA
WritePrivateProfileStringA	SendDlgItemMessageA	LoadCursorA
WriteFile	SelectObject	LoadBitmapA
WriteConsoleW	ScreenToClient	LeaveCriticalSection
WriteConsoleA	ScaleWindowExtEx	LCMapStringW
WindowFromPoint	ScaleViewportExtEx	LCMapStringA
WinHelpA	SaveDC	IsWindowVisible
WideCharToMultiByte	SHGetPathFromIDListA	IsWindowEnabled
WaitForSingleObject	SHGetMalloc	IsWindow
VirtualFree	SHBrowseForFolderA	IsValidLocale
VirtualAlloc	RtlUnwind	IsValidCodePage
ValidateRect	RestoreDC	IsIconic
UpdateWindow	RemovePropA	IsDialogMessageA
UnregisterClassA	ReleaseDC	IsDebuggerPresent
UnhookWindowsHookEx	RegisterWindowMessageA	InterlockedIncrement
UnhandledExceptionFilter	RegisterClassA	InterlockedExchange
TranslateMessage	RegSetValueExA	InterlockedDecrement
TlsSetValue	RegQueryValueExA	InitializeCriticalSectionAndSpinCount
TlsGetValue	RegQueryValueA	InitializeCriticalSection
TlsFree	RegOpenKeyExA	HeapSize
TlsAlloc	RegOpenKeyA	HeapReAlloc
TextOutA	RegEnumKeyA	HeapFree
TerminateProcess	RegDeleteKeyA	HeapCreate
TabbedTextOutA	RegCreateKeyExA	HeapAlloc
SystemParametersInfoA	RegCloseKey	GrayStringA
Sleep	RectVisible	GlobalUnlock
SizeofResource	ReadFile	GlobalReAlloc
ShowWindow	RaiseException	GlobalLock
SetWindowsHookExA	QueryPerformanceCounter	GlobalHandle
SetWindowTextA	PtVisible	GlobalGetAtomNameA
SetWindowPos	PtInRect	GlobalFree
SetWindowLongA	PostQuitMessage	GlobalFlags
SetWindowExtEx	PostMessageA	GlobalFindAtomA
SetViewportOrgEx	PeekMessageA	GlobalDeleteAtom
SetViewportExtEx	PathRemoveFileSpecW	GlobalAlloc
SetUnhandledExceptionFilter	PathFindFileNameA	GlobalAddAtomA
SetTextColor	PathFindExtensionA	GetWindowThreadProcessId
SetStdHandle	OpenPrinterA	GetWindowTextLengthA
SetPropA	OffsetViewportOrgEx	GetWindowTextA
SetMenuItemBitmaps	MultiByteToWideChar	GetWindowRect
SetMenu	MulDiv	GetWindowPlacement
SetMapMode	ModifyMenuA	GetWindowLongA
SetLastError	MessageBoxA	GetWindow
SetHandleCount	MapWindowPoints	GetVersionExA
SetForegroundWindow	LresultFromObject	GetUserDefaultLCID

GetTopWindow	GetClassInfoExA	CheckMenuItem
GetTickCount	GetClassInfoA	CallWindowProcA
GetSystemTimeAsFileTime	GetCapture	CallNextHookEx
GetSystemMetrics	GetCPLInfo	BeginPaint
GetSysColorBrush	GetActiveWindow	AdjustWindowRectEx
GetSysColor	GetACP	9 (VariantClear)
GetSubMenu	FreeResource	8 (BSTR_UserUnmarshal)
GetStringTypeW	FreeLibrary	12 (VariantChangeType)
GetStringTypeA	FreeEnvironmentStringsW	
GetStockObject	FreeEnvironmentStringsA	
GetStdHandle	FormatMessageA	
GetStartupInfoA	FlushFileBuffers	
GetPropA	FindResourceA	
GetProcAddress	FindNextFileA	
GetParent	FindFirstFileA	
GetObjectA	FindClose	
GetOEMCP	ExtTextOutA	
GetNextDlgTabItem	ExitProcess	
GetModuleHandleW	Escape	
GetModuleHandleA	EnumSystemLocalesA	
GetModuleFileNameW	EnumResourceLanguagesA	
GetModuleFileNameA	EnterCriticalSection	
GetMessageTime	EndPaint	
GetMessagePos	EndDialog	
GetMessageA	EnableWindow	
GetMenuState	EnableMenuItem	
GetMenuItemID	DuplicateHandle	
GetMenuItemCount	DrawTextExA	
GetMenuCheckMarkDimensions	DrawTextA	
GetMenu	DrawIcon	
GetLocaleInfoW	DocumentPropertiesA	
GetLocaleInfoA	DispatchMessageA	
GetLastError	DestroyWindow	
GetLastActivePopup	DestroyMenu	
GetKeyState	DeleteObject	
GetForegroundWindow	DeleteDC	
GetFocus	DeleteCriticalSection	
GetFileType	DefWindowProcA	
GetEnvironmentStringsW	CryptImportKey	
GetEnvironmentStrings	CryptEncrypt	
GetDlgItem	CryptAcquireContextW	
GetDlgItemID	CreateWindowExA	
GetDeviceCaps	CreateStdAccessibleObject	
GetDesktopWindow	CreateProcessA	
GetDC	CreatePipe	
GetCursorPos	CreateFileA	
GetCurrentThreadId	CreateDialogIndirectParamA	
GetCurrentThread	CreateBitmap	
GetCurrentProcessId	CopyRect	
GetCurrentProcess	ConvertDefaultLocale	
GetConsoleOutputCP	CompareStringA	
GetConsoleMode	CoUninitialize	
GetConsoleCP	CoTaskMemFree	
GetCommandLineA	CoInitializeEx	
GetClipboard	CoCreateInstance	
GetClientRect	ClosePrinter	
GetClassNameA	CloseHandle	
GetClassLongA	ClientToScreen	

APPENDIX B – STRINGS OUTPUT

Note: Invalid strings, i.e., non-string byte sequences that have been interpreted as strings by the Strings utility, have been removed from this output.

File: 180f82bbedb03dc29328e32e054069870a1e65078b78b2120a84c96aaed7d843
MD5: a563c50c5fa0fd541248acaf72cc4e7d
Size: 650752

Ascii Strings:

```
-----  
0000004D !This program cannot be run in DOS mode.  
000000D0 RichI  
000001E8 .text  
0000020F `.rdata  
00000237 @.data  
00000260 .src  
0002D928 CloseHandle  
0002D934 ReadFile error!  
0002D944 Close handle error!  
0002D958 Duplicate handle error 2!  
0002D974 Duplicate handle error!  
0002D98C Stdout pipe creation error!  
0002D9B0 Finished operating in the current directory "%s".  
0002D9E3 Will I continue into the (sub)directory(s) ?  
0002DA1C Sub directory operation query  
0002DA40 Finished operating in the current directory "%s".  
0002DA73 Will I continue into the subdirectory(s) ?  
0002DB9C bad allocation  
0002DE78 Win32 Executables(*.exe)|*.exe||  
0002DEA0 RedirectedStream  
0002DEB8 You have not filled up essential entries.  
0002DEE3 These values are essential for me to function properly.  
0002DF1C Try again.  
0002DF28 Invalid field entries  
0002DF40 Task Completed.  
0002DF50 Recursive Execution completed sucessfully  
0002DF80 ios_base::eofbit set  
0002DF98 ios_base::failbit set  
0002DFB0 ios_base::badbit set  
0002DFC8 Here you can specify the (sub)directory under which to start recursing.  
0002E150 Enter the "current directory" environment to pass to the program. It's recommended to enter "<>" to indicate the  
current directory being recursed.  
0002E1E4 Leave it blank to operate in root directory too  
0002E214 A value of -1 implies Infinite wait state  
0002E240 Enter "<>" (without the quote  
0002E25D s) where you want me to substitute the current directory into ..  
0002E2A0 Fuck Def  
0002E2AC 8192  
0002E2CC CWinApp  
0002E2D4 Settings  
0002E2E0 PreviewPages  
0002E378 DeactivateActCtx  
0002E38C ActivateActCtx  
0002E39C ReleaseActCtx  
0002E3AC CreateActCtxA  
0002E3BC KERNEL32
```


0002E3C8 Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
0002E404 NoRun
0002E40C NoDrives
0002E418 RestrictRun
0002E424 NoNetConnectDisconnect
0002E43C NoRecentDocsHistory
0002E450 NoClose
0002E458 Software\Microsoft\Windows\CurrentVersion\Policies\Network
0002E494 NoEntireNetwork
0002E4A4 Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
0002E4E0 NoPlacesBar
0002E4EC NoBackButton
0002E4FC NoFileMru
0002E50C ntdll.dll
0002E518 GetSystemDefaultUILanguage
0002E534 GetUserDefaultUILanguage
0002E550 kernel32.dll
0002E560 %s%s.dll
0002E62C %s (%s:%d)
0002E638 %s (%s:%d)
0002E648 Exception thrown in destructor
0002E668 f:\dd\vctools\vc7libs\ship\atlmfc\src\mfccore.cpp
0002E6A0 CCmdTarget
0002E7A4 CWinThread
0002E850 Software\Classes\
0002E864 Software\
0002E870 CDialog
0002EA00 Edit
0002EAD0 COleException
0002EB18 DISPLAY
0002EB20 CInvalidArgException
0002EB38 CNotSupportedException
0002EB50 CMemoryException
0002EB64 CSimpleException
0002EB78 CException
0002EC80 CWnd
0002EC90 AfxWnd90s
0002EC9C AfxControlBar90s
0002ECB0 AfxMDIFrame90s
0002ECC0 AfxFrameOrView90s
0002ECD4 AfxOleControl90s
0002ECE8 AfxOldWndProc423
0002ED20 EnumDisplayDevicesA
0002ED34 GetMonitorInfoA
0002ED44 EnumDisplayMonitors
0002ED58 MonitorFromPoint
0002ED6C MonitorFromRect
0002ED7C MonitorFromWindow
0002ED90 GetSystemMetrics
0002EDA4 USER32
0002F194 InitCommonControls
0002F1A8 InitCommonControlsEx
0002F1C0 HtmlHelpA
0002F1CC hhctrl.ocx
0002F2CB F#32768
0002F2D8 f:\dd\vctools\vc7libs\ship\atlmfc\include\afxwin2.inl
0002F5E8 commctrl_DragListMsg
0002F600 CreateActCtxW

0002F638 comctl32.dll
0002F650 comdlg32.dll
0002F668 shell32.dll
0002F67C CEdit
0002F6C0 CGdiObject
0002F6CC CPaintDC
0002F6DC CUserException
0002F6EC CResourceException
0002F8D4 f:\dd\vctools\vc7libs\ship\atlmfc\include\afxwin1.inl
0002F90C CFileDialog
0002FADE p4GetOpenFileNameA
0002FAF4 GetSaveFileNameA
0002FCFC SHCreateItemFromParsingName
0002FD18 Shell32.dll
0002FD24 CToolTipCtrl
0002FE9C tooltips_class32
0002FF30 CObject
0002FF38 Delete
0002FF40 NoRemove
0002FF4C ForceRemove
0002FFA8 software
0002FFB4 combobox
0002FFC8 f:\dd\vctools\vc7libs\ship\atlmfc\src\mfc\auxdata.cpp
00030010 System
00030018 CMenu
00030054 CMapPtrToPtr
00030094 CArchiveException
000300E0 CCommonDialog
00030160 commdlg_SetRGBColor
00030174 commdlg_help
00030184 commdlg_ColorOK
00030194 commdlg_FileNameOK
000301A8 commdlg_ShareViolation
000301C0 commdlg_LBSelChangedNotify
000301DC CMapStringToPtr
00030218 .INI
00030220 .HLP
00030228 .CHM
00030230 NotifyWinEvent
00030240 user32.dll
00030254 %2\CLSID
00030260 %2\Insertable
00030270 %2\protocol\StdFileEditing\verb\0
00030292 &Edit
00030298 %2\protocol\StdFileEditing\server
000302C0 CLSID\%1
000302CC CLSID\%1\ProgID
000302E0 CLSID\%1\InprocHandler32
000302F9 ole32.dll
00030304 CLSID\%1\LocalServer32
00030320 CLSID\%1\Verb\0
00030330 &Edit,0,2
0003033C CLSID\%1\Verb\1
0003034C &Open,0,2
00030358 CLSID\%1\Insertable
00030370 CLSID\%1\AuxUserType\2
0003038C CLSID\%1\AuxUserType\3
000303A8 CLSID\%1\DefaultIcon

000303BD %3,%7
 000303C4 CLSID\%1\MiscStatus
 000303DC CLSID\%1\InProcServer32
 000303F8 CLSID\%1\DocObject
 00030410 %2\DocObject
 00030420 CLSID\%1\Printable
 00030434 CLSID\%1\DefaultExtension
 0003044E %9, %8
 000305DC CByteArray
 000305F8 CObArray
 00030628 CPtrArray
 00030694 Unknown exception
 000306D4 CorExitProcess
 00030718 HeapQueryInformation
 00030754 bad exception
 00030764 EncodePointer
 00030790 DecodePointer
 000307A0 FlsFree
 000307A8 FlsSetValue
 000307B4 FlsGetValue
 000307C0 FlsAlloc
 000307CC LC_TIME
 000307D4 LC_NUMERIC
 000307E0 LC_MONETARY
 000307EC LC_CTYPE
 000307F8 LC_COLLATE
 00030804 LC_ALL
 00030877 !"#%&'()*+,-./0123456789;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
 000308EC runtime error
 00030900 TLOSS error
 00030910 SING error
 00030920 DOMAIN error
 00030930 R6034
 00030937 An application has made an attempt to load the C runtime library incorrectly.
 00030985 Please contact the application's support team for more information.
 000309D0 R6033
 000309D7 - Attempt to use MSIL code from this assembly during native code initialization
 00030A27 This indicates a bug in your application. It is most likely the result of calling an MSIL-compiled (/clr) function from a native constructor or from DllMain.
 00030AC8 R6032
 00030ACF - not enough space for locale information
 00030B00 R6031
 00030B07 - Attempt to initialize the CRT more than once.
 00030B37 This indicates a bug in your application.
 00030B64 R6030
 00030B6B - CRT not initialized
 00030B84 R6028
 00030B8B - unable to initialize heap
 00030BAC R6027
 00030BB3 - not enough space for lowio initialization
 00030BE4 R6026
 00030BEB - not enough space for stdio initialization
 00030C1C R6025
 00030C23 - pure virtual function call
 00030C44 R6024
 00030C4B - not enough space for _onexit/atexit table
 00030C7C R6019
 00030C83 - unable to open console device

00030CA8 R6018
00030CAF - unexpected heap error
00030CCC R6017
00030CD3 - unexpected multithread lock error
00030CFC R6016
00030D03 - not enough space for thread data
00030D2A This application has requested the Runtime to terminate it in an unusual way.
00030D78 Please contact the application's support team for more information.
00030DC0 R6009
00030DC7 - not enough space for environment
00030DEC R6008
00030DF3 - not enough space for arguments
00030E18 R6002
00030E1F - floating point support not loaded
00030E48 Microsoft Visual C++ Runtime Library
00030E78 <program name unknown>
00030E90 Runtime Error!
00030EA0 Program:
00030F38 (null)
00031016 GAsProcessorFeaturePresent
00031034 SunMonTueWedThuFriSat
0003104C JanFebMarAprMayJunJulAugSepOctNovDec
00031074 Complete Object Locator'
00031090 Class Hierarchy Descriptor'
000310B0 Base Class Array'
000310C4 Base Class Descriptor at (
000310E0 Type Descriptor'
000310F4 `local static thread guard'
00031110 `managed vector copy constructor iterator'
0003113C `vector vbase copy constructor iterator'
00031168 `vector copy constructor iterator'
0003118C `dynamic atexit destructor for '
000311B0 `dynamic initializer for '
000311CC `eh vector vbase copy constructor iterator'
000311F8 `eh vector copy constructor iterator'
00031220 `managed vector destructor iterator'
00031248 `managed vector constructor iterator'
00031270 `placement delete[] closure'
00031290 `placement delete closure'
000312AC `omni callsig'
000312BC delete[]
000312C8 new[]
000312D0 `local vftable constructor closure'
000312F4 `local vftable'
00031304 `RTTI
00031310 `udt returning'
00031320 `copy constructor closure'
0003133C `eh vector vbase constructor iterator'
00031364 `eh vector destructor iterator'
00031384 `eh vector constructor iterator'
000313A8 `virtual displacement map'
000313C4 `vector vbase constructor iterator'
000313E8 `vector destructor iterator'
00031408 `vector constructor iterator'
00031428 `scalar deleting destructor'
00031448 `default constructor closure'
00031468 `vector deleting destructor'
00031488 `vbase destructor'

0003149C `string'
000314A8 `local static guard'
000314C0 `typeof'
000314CC `vcall'
000314D4 `vhtable'
000314E0 `vftable'
00031564 operator
00031588 delete
00031590 new
00031598 __unaligned
000315A4 __restrict
000315B0 __ptr64
000315B8 __clrcall
000315C4 __fastcall
000315D0 __thiscall
000315DC __stdcall
000315E8 __pascal
000315F4 __cdecl
000315FC __based(
00031D38 !"#\$%&'()*+,-./0123456789;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
00031EB8 !"#\$%&'()*+,-./0123456789;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`ABCDEFGHIJKLMNopqrstuvwxyz{|}~
00031F98 HH:mm:ss
00031FA4 dddd, MMMM dd, yyyy
00031FB8 MM/dd/yy
00031FCC December
00031FD8 November
00031FE4 October
00031FEC September
00031FF8 August
00032000 July
00032008 June
00032010 April
00032018 March
00032020 February
0003202C January
00032064 Saturday
00032070 Friday
00032078 Thursday
00032084 Wednesday
00032090 Tuesday
00032098 Monday
000320A0 Sunday
000320C4 united-states
000320D4 united-kingdom
000320E4 trinidad & tobago
000320F8 south-korea
00032104 south-africa
00032114 south korea
00032120 south africa
00032130 slovak
00032138 puerto-rico
00032144 pr-china
00032150 pr china
00032160 new-zealand
0003216C hong-kong
00032178 holland
00032180 great britain
00032190 england

00032198 czech
000321A0 china
000321A8 britain
000321B0 america
000321C4 swiss
000321CC swedish-finland
000321DC spanish-venezuela
000321F0 spanish-uruguay
00032200 spanish-puerto rico
00032214 spanish-peru
00032224 spanish-paraguay
00032238 spanish-panama
00032248 spanish-nicaragua
0003225C spanish-modern
0003226C spanish-mexican
0003227C spanish-honduras
00032290 spanish-guatemala
000322A4 spanish-el salvador
000322B8 spanish-ecuador
000322C8 spanish-dominican republic
000322E4 spanish-costa rica
000322F8 spanish-colombia
0003230C spanish-chile
0003231C spanish-bolivia
0003232C spanish-argentina
00032340 portuguese-brazilian
00032358 norwegian-nynorsk
0003236C norwegian-bokmal
00032380 norwegian
0003238C italian-swiss
0003239C irish-english
000323AC german-swiss
000323BC german-luxembourg
000323D0 german-lichtenstein
000323E4 german-austrian
000323F4 french-swiss
00032404 french-luxembourg
00032418 french-canadian
00032428 french-belgian
00032438 english-usa
00032444 english-us
00032450 english-uk
0003245C english-trinidad y tobago
00032478 english-south africa
00032490 english-nz
0003249C english-jamaica
000324AC english-ire
000324B8 english-caribbean
000324CC english-can
000324D8 english-belize
000324E8 english-aus
000324F4 english-american
00032508 dutch-belgian
00032518 chinese-traditional
0003252C chinese-singapore
00032540 chinese-simplified
00032554 chinese-hongkong
00032568 chinese

00032578 canadian
00032584 belgian
0003258C australian
00032598 american-english
000325AC american english
000325C0 american
000328B0 Norwegian-Nynorsk
000328C4 GetProcessWindowStation
000328DC GetUserObjectInformationA
000328F8 GetLastActivePopup
0003290C GetActiveWindow
0003291C MessageBoxA
00032928 USER32.DLL
00032934 1#QNAN
0003293C 1#INF
00032944 1#IND
0003294C 1#SNAN
00032954 CONOUT\$\n
000329A0 string too long
000329B0 invalid string position
00032AB4 bad cast
00032AE5 =L9o<\n
00032B00 OLEACC.dll
00036A3A CreateStdAccessibleObject
00036A56 LresultFromObject
00036FAE CloseHandle
00036FBC lstrlenA
00036FC8 WriteFile
00036FD4 GetLastError
00036FE4 ReadFile
00036FF0 TerminateProcess
00037004 WaitForSingleObject
0003701A CreateProcessA
0003702C DuplicateHandle
0003703E GetCurrentProcess
00037052 CreatePipe
00037060 lstrcpyA
0003706C FindClose
00037078 FindNextFileA
00037088 lstrcmpA
00037094 FindFirstFileA
000370A6 lstrcatA
000370B2 lstrcpynA
000370BE SetFilePointer
000370D0 CreateFileA
000370DE VirtualAlloc
000370EE GetProcAddress
00037100 GetModuleHandleA
00037114 FreeLibrary
00037122 GlobalAlloc
00037130 GlobalLock
0003713E InterlockedExchange
00037154 sizeofResource
00037166 LockResource
00037176 LoadResource
00037186 FindResourceA
00037196 CompareStringA
000371A8 WideCharToMultiByte

000371BE LoadLibraryA
000371CE GetLocaleInfoA
000371E0 GetModuleFileNameA
000371F6 EnumResourceLanguagesA
00037210 ConvertDefaultLocale
00037228 GetCurrentThreadId
0003723E GetCurrentThread
00037252 GlobalDeleteAtom
00037266 GlobalAddAtomA
00037278 SetLastError
00037288 GetCurrentProcessId
0003729E FreeResource
000372AE GlobalFree
000372BC GlobalUnlock
000372CC MulDiv
000372D6 MultiByteToWideChar
000372EC LocalFree
000372F8 FormatMessageA
0003730A GetVersionExA
0003731A lstrcmpW
00037326 GlobalFindAtomA
00037338 GlobalGetAtomNameA
0003734E GetModuleFileNameW
00037364 InterlockedDecrement
0003737C WritePrivateProfileStringA
0003739A GlobalFlags
000373A8 LocalAlloc
000373B6 LeaveCriticalSection
000373CE TlsGetValue
000373DC EnterCriticalSection
000373F4 GlobalReAlloc
00037404 GlobalHandle
00037414 InitializeCriticalSection
00037430 TlsAlloc
0003743C TlsSetValue
0003744A LocalReAlloc
0003745A DeleteCriticalSection
00037472 TlsFree
0003747C InterlockedIncrement
00037494 FlushFileBuffers
000374A8 GetModuleHandleW
000374BC GetCPInfo
000374C8 GetOEMCP
000374D4 SetErrorMode
000374E4 RtlUnwind
000374F0 RaiseException
00037502 GetCommandLineA
00037514 GetStartupInfoA
00037526 HeapAlloc
00037532 HeapFree
0003753E Sleep
00037546 ExitProcess
00037554 HeapReAlloc
00037562 HeapSize
0003756E UnhandledExceptionFilter
0003758A SetUnhandledExceptionFilter
000375A8 IsDebuggerPresent
000375BC GetACP

000375C6 IsValidCodePage
000375D8 GetStdHandle
000375E8 FreeEnvironmentStringsA
00037602 GetEnvironmentStrings
0003761A FreeEnvironmentStringsW
00037634 GetEnvironmentStringsW
0003764E SetHandleCount
00037660 GetFileType
0003766E HeapCreate
0003767C VirtualFree
0003768A QueryPerformanceCounter
000376A4 GetTickCount
000376B4 GetSystemTimeAsFileTime
000376CE InitializeCriticalSectionAndSpinCount
000376F6 LCMaPStringA
00037706 LCMaPStringW
00037716 GetStringTypeA
00037728 GetStringTypeW
0003773A GetUserDefaultLCID
00037750 EnumSystemLocalesA
00037766 IsValidLocale
00037776 GetLocaleInfoW
00037788 GetConsoleCP
00037798 GetConsoleMode
000377AA SetStdHandle
000377BA WriteConsoleA
000377CA GetConsoleOutputCP
000377E0 WriteConsoleW
000377EE KERNEL32.dll
000377FE MessageBoxA
0003780C wsprintfA
00037818 DrawIcon
00037824 SendMessageA
00037834 IsIconic
00037840 GetClientRect
00037850 EnableWindow
00037860 LoadIconA
0003786C GetSystemMetrics
00037880 PostQuitMessage
00037892 PostMessageA
000378A2 CheckMenuItem
000378B2 EnableMenuItem
000378C4 GetMenuState
000378D4 ModifyMenuA
000378E2 GetParent
000378EE GetFocus
000378FA LoadBitmapA
00037908 GetMenuCheckMarkDimensions
00037926 SetMenuItemBitmaps
0003793C ValidateRect
0003794C GetCursorPos
0003795C PeekMessageA
0003796C GetKeyState
0003797A IsWindowVisible
0003798C GetActiveWindow
0003799E DispatchMessageA
000379B2 TranslateMessage
000379C6 GetMessageA

000379D4 CallNextHookEx
000379E6 SetWindowsHookExA
000379FA SetCursor
00037A06 IsWindowEnabled
00037A18 GetLastActivePopup
00037A2E GetWindowLongA
00037A40 GetWindowThreadProcessId
00037A5C EndDialog
00037A68 GetNextDlgTabItem
00037A7C GetDlgItem
00037A8A IsWindow
00037A96 DestroyWindow
00037AA6 CreateDialogIndirectParamA
00037AC4 SetActiveWindow
00037AD6 GetDesktopWindow
00037AEA GetSubMenu
00037AF8 GetMenuItemCount
00037B0C GetMenuItemID
00037B1C GetWindow
00037B28 GetWindowRect
00037B38 GetWindowPlacement
00037B4E SystemParametersInfoA
00037B66 SetWindowPos
00037B76 SetWindowLongA
00037B88 GetMenu
00037B92 CallWindowProcA
00037BA4 DefWindowProcA
00037BB6 GetDlgItemID
00037BC6 PtInRect
00037BD2 CopyRect
00037BDE ScreenToClient
00037BF0 AdjustWindowRectEx
00037C06 GetSysColor
00037C14 RegisterClassA
00037C26 GetClassInfoA
00037C36 GetClassInfoExA
00037C48 CreateWindowExA
00037C5A UpdateWindow
00037C6A SetForegroundWindow
00037C80 SetMenu
00037C8A MapWindowPoints
00037C9C GetMessagePos
00037CAC GetMessageTime
00037CBE UnhookWindowsHookEx
00037CD4 GetTopWindow
00037CE4 GetForegroundWindow
00037CFA GetWindowTextA
00037D0C GetWindowTextLengthA
00037D24 SetFocus
00037D30 RemovePropA
00037D3E GetPropA
00037D4A SetPropA
00037D56 GetClassNameA
00037D66 GetClassLongA
00037D76 GetCapture
00037D84 WinHelpA
00037D90 SendDlgItemMessageA
00037DA6 RegisterWindowMessageA

00037DC0 IsDialogMessageA
00037DD4 SetWindowTextA
00037DE6 ShowWindow
00037DF4 TabbedTextOutA
00037E06 DrawTextA
00037E12 DrawTextExA
00037E20 GrayStringA
00037E2E ClientToScreen
00037E40 GetDC
00037E48 ReleaseDC
00037E54 BeginPaint
00037E62 EndPaint
00037E6E WindowFromPoint
00037E80 LoadCursorA
00037E8E GetSysColorBrush
00037EA2 DestroyMenu
00037EB0 UnregisterClassA
00037EC2 USER32.dll
00037ED0 CreateBitmap
00037EE0 GetDeviceCaps
00037EF0 GetClipBox
00037EFE SetTextColor
00037F0E SetBkColor
00037F1C GetObjectA
00037F2A SaveDC
00037F34 RestoreDC
00037F40 SetMapMode
00037F4E DeleteObject
00037F5E PtVisible
00037F6A RectVisible
00037F78 TextOutA
00037F84 ExtTextOutA
00037F92 Escape
00037F9C SelectObject
00037FAC SetViewportOrgEx
00037FC0 OffsetViewportOrgEx
00037FD6 SetViewportExtEx
00037FEA ScaleViewportExtEx
00038000 SetWindowExtEx
00038012 ScaleWindowExtEx
00038026 DeleteDC
00038032 GetStockObject
00038042 GDI32.dll
0003804E ClosePrinter
0003805E DocumentPropertiesA
00038074 OpenPrinterA
00038082 WINSPOOL.DRV
00038092 CryptEncrypt
000380A2 CryptImportKey
000380B4 CryptAcquireContextW
000380CC RegCloseKey
000380DA RegQueryValueExA
000380EE RegOpenKeyExA
000380FE RegDeleteKeyA
0003810E RegEnumKeyA
0003811C RegOpenKeyA
0003812A RegQueryValueA
0003813C RegCreateKeyExA

0003814E RegSetValueExA
0003815E ADVAPI32.dll
0003816E SHGetPathFromIDListA
00038186 SHBrowseForFolderA
0003819C SHGetMalloc
000381A8 SHELL32.dll
000381B6 PathFindExtensionA
000381CC PathFindFileNameA
000381E0 PathRemoveFileSpecW
000381F4 SHLWAPI.dll
00038202 CoTaskMemFree
00038212 CoUninitialize
00038224 CoCreateInstance
00038238 CoInitializeEx
00038248 ole32.dll
00038252 OLEAUT32.dll
00038408 .?AVCGetFileList@@
00038424 .?AVCRecurseExecApp@@@
00038444 .?AVCWinApp@@
0003845C .?AVCWinThread@@
00038478 .?AVCCmdTarget@@@
00038494 .?AVCObject@@
000384A8 ^?SnrwkZSzpuPI
000384C8 RSA2
000384ED HN:D
000384FF xLu5
00038545 #WER
0003859E 1.HKe
0003864C .?AVbad_alloc@std@@
00038668 .?AVexception@std@@@
00038684 .?AVCEdit@@
00038698 .?AVCWnd@@
000386AC .?AVCRecurseExecDlg@@@
000386CC .?AVCDialog@@
000386E4 .?AVruntime_error@std@@@
00038704 .?AVfailure@ios_base@std@@@
000387B8 .PAVCException@@
000387E0 .?AVCCmdUI@@@
000387F8 .PAVCMemoryException@@@
00038818 .?AVCOleException@@@
00038834 .?AVCException@@@
00038850 .PAVColeException@@@
0003886C .PAVCObject@@@
00038884 .PAX
00038894 .PAVCSimpleException@@@
000388B4 .PAVCNotSupportedException@@@
000388DC .PAVCInvalidArgException@@@
00038900 .?AVCSimpleException@@@
00038920 .?AVCMemoryException@@@
00038940 .?AVCNotSupportedException@@@
00038968 .?AVCInvalidArgException@@@
00038BF4 .?AVXAccessible@CWnd@@@
00038C14 .?AVXAccessibleServer@CWnd@@@
00038C3C .?AVCTestCmdUI@@@
00038C58 .?AV_AFX_HTMLHELP_STATE@@@
00038C7C .?AVCNoTrackObject@@@
00038C9C .PAVCUserException@@@
00038CC0 .?AV?SIAccessibleProxyImpl@VCAccessibleProxy@ATL@@@ATL@@@

00038D04 .?AUIAccessible@@
 00038D20 .?AUIDispatch@@
 00038D38 .?AUIUnknown@@
 00038D50 .?AUIAccessibleProxy@@
 00038D70 .?AV?\$CMFCComObject@VCAccessibleProxy@ATL@@@
 00038DA8 .?AVCAccessibleProxy@ATL@@
 00038DD0 .?AV?\$CCComObjectRootEx@VCComSingleThreadModel@ATL@@@ATL@@
 00038E14 .?AVCComObjectRootBase@ATL@@
 00038E3C .?AUIOleWindow@@
 00038E58 .?AV_AFX_THREAD_STATE@@
 00038E78 .?AVAFX_MODULE_THREAD_STATE@@
 00038EA0 .?AVAFX_MODULE_STATE@@
 00038EC0 .?AVCDllIsolationWrapperBase@@
 00038EE8 .?AVCComCtlWrapper@@
 00038F08 .?AVCComDlgWrapper@@
 00038F28 .?AVCShellWrapper@@
 00038F44 .?AV_AFX_BASE_MODULE_STATE@@
 00038F6C .?AVCAfxStringMgr@@
 00038F88 .?AUIAtIStringMgr@ATL@@
 00038FA8 .?PAVCResourceException@@
 00038FCC .?AVCResourceException@@
 00038FF0 .?AVCUserException@@
 00039010 .?AVCGdiObject@@
 0003902C .?AVCDC@@
 00039040 .?AVCPaintDC@@
 00039098 .?AVCCCommonDialog@@
 000390B4 .?AVXFileDialogEvents@CFileDialog@@
 000390E0 .?AUIFileDialogEvents@@
 00039100 .?AVXFileDialogControlEvents@CFileDialog@@
 00039134 .?AUIFileDialogControlEvents@@
 0003915C .?AVCFileDialog@@
 00039178 .?AVCToolTipCtrl@@
 00039194 .?AUCThreadData@@
 000391B0 .?AVCHandleMap@@
 000391CC .?AVCMenu@@
 000391E0 .?AVCMapPtrToPtr@@
 000391FC .?PAVCArchiveException@@
 0003921C .?AVCArchiveEx
 0003922A ception@@
 0003923C .?AVCMapStringToPtr@@
 0003925C .?AVCObArray@@
 0003927C Apartment
 00039288 Both
 00039290 Free
 000392C4 .?AVCByteArray@@
 000392FC .?AV?\$CArray@W4LoadArrayObjType@CArchive@@@ABW412@@@
 00039338 .?AVCPtrArray@@
 00039354 .?AVtype_info@@
 0003938C .?AVbad_cast@std@@
 0003954C .?AVbad_exception@std@@
 000396CE abcdefghijklmnopqrstuvwxyz
 000396EE ABCDEFGHIJKLMNOPQRSTUVWXYZ
 000398D9 abcdefghijklmnopqrstuvwxyz
 000398F9 ABCDEFGHIJKLMNOPQRSTUVWXYZ
 0003A6EC .?AVlogic_error@std@@
 0003A70C .?AVlength_error@std@@
 0003A72C .?AVout_of_range@std@@
 0003A754 .?AVfacet@locale@std@@

```

0003A774 .?AUctype_base@std@@
0003A794 .?AVios_base@std@@
0003A7B0 .?AV?$_losb@H@std@@
0003A7CC .?AV?$basic_ostream@DU?$char_traits@D@std@@@std@@
0003A808 .?AV?$basic_ios@DU?$char_traits@D@std@@@std@@
0003A840 .?AV?$ctype@D@std@@
0003A85C .?AV?$basic_streambuf@DU?$char_traits@D@std@@@std@@
0003A898 .?AV?$basic_filebuf@DU?$char_traits@D@std@@@std@@
0003A8D4 .?AVcodecvt_base@std@@
0003A8F4 .?AV?$codecvt@DDH@std@@
0003A91C .?AV_Locimp@locale@std@@
0003A948 Copyright (c) 1992-2004 by P.J. Plauger, licensed by Dinkumware, Ltd. ALL RIGHTS RESERVED.
0009EC2C <assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
0009EC77 <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
0009ECAE <security>
0009ECBF <requestedPrivileges>
0009ECDC <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
0009ED3C </requestedPrivileges>
0009ED5A </security>
0009ED6B </trustInfo>
0009ED7B
</assembly>PAPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDI
NGXXPADDINGPADDINGXXPADDINGPADDINGX

```

Unicode Strings:

```

-----
00014137 jjjjj
0002E2B8 NTDLL.dll
0002EDAC accParent
0002EDC0 accChildCount
0002EDDC accChild
0002EDF0 accName
0002EE00 accValue
0002EE14 accDescription
0002EE34 accRole
0002EE44 accState
0002EE58 accHelp
0002EE68 accHelpTopic
0002EE84 accKeyboardShortcut
0002EEAC accFocus
0002EEC0 accSelection
0002EEDC accDefaultAction
0002EF00 accSelect
0002EF14 accLocation
0002EF2C accNavigate
0002EF44 accHitTest
0002EF5C accDoDefaultAction
000306E4 mscoree.dll
000306FC kernel32.dll
00030774 KERNEL32.DLL
00030F28 (null)
00031890 ((((( H
00031A92 h((( H
00031B90 H
0007B742 A Kamal Shankar Quick Tool - Recursive Executer
0007B7A8 MS Sans Serif
0007B804 Cancel
0007B850 Program options

```

0007B8B4 Redirect STDIO
0007B8F0 Check2
0007B91C Confirm new entry
0007B940 Check this if you want the program to ask for confirmation everytime it enters a new (sub)directory..
0007BA2C Execution Options
0007BA94 &Browse..
0007BAC8 Select the program you want to execute
0007BB58 Select the starting directory
0007BBB8 Browse ..
0007BC0C Executable arguments
0007BC78 Directory Wildcard
0007BCDC Timeout (ms)
0007BD34 Current Dir Value
0007BD7C MS Shell Dlg
0007BDAE &New
0007BE0E Cancel
0007BE36 &Help
0007BE5E MS Shell Dlg
0007BE7A Open
0007BE84 Save As
0007BE94 All Files (*.*)
0007BEB4 Untitled
0007BECA an unnamed file
0007BF00 &Hide
0007BF2A No error message is available.#Attempted an unsupported operation.\$A required resource was unavailable.
0007BFFA Out of memory.
0007C018 An unknown error has occurred.!Encountered an improper argument.
0007C0AE Incorrect filename.
0007C0D6 Failed to open document.
0007C108 Failed to save document.
0007C13A Save changes to %1? Failed to create empty document.
0007C1A4 The file is too large to open.
0007C1E2 Could not start print job.
0007C218 Failed to launch help.
0007C246 Internal application error.
0007C27E Command failed.)Insufficient memory to perform operation.PSystem registry entries have been removed and the INI file (if any) was deleted.BNot all of the system registry entries (or INI file) were removed.FThis program requires the file %s, which was not found on this system.tThis program is linked to the missing export %s in the file %s. This machine may have an incompatible version of %s.
0007C596 Enter an integer.
0007C5BA Enter a number.#Enter an integer between %1 and %2.!Enter a number.# between %1 and %2.!Enter no more than %1 characters.
0007C6AA Select a button.#Enter an integer between 0 and 255.
0007C714 Enter a positive integer.
0007C748 Enter a date and/or time.
0007C77C Enter a currency.
0007C7A0 Enter a GUID.
0007C7BC Enter a time.
0007C7D8 Enter a date.
0007C7FA Unexpected file format.O%1
0007C830 Cannot find this file.
0007C85E Verify that the correct path and file name are given.
0007C8CA Destination disk drive is full.5Unable to read from %1, it is opened by someone else.AUnable to write to %1, it is read-only or opened by someone else.1Encountered an unexpected error while reading %1.1Encountered an unexpected error while writing %1.
0007CAD6 %1: %2
0007CAE4 Continue running script?
0007CB16 Dispatch exception: %1

0007CB78 #Unable to read write-only property.#Unable to write read-only property.
0007CC0C #Unable to load mail system support.
0007CC56 Mail system DLL is invalid.!Send Mail failed to send message.
0007CCEE No error occurred.-An unknown error occurred while accessing %1.
0007CD70 %1 was not found.
0007CD94 %1 contains an incorrect path.8Could not open %1 because there are too many open files.
0007CE44 Access to %1 was denied.0An incorrect file handle was associated with %1.8Could not remove %1 because it is the current directory.2Could not create %1 because the directory is full.
0007CFB0 Seek failed on %14Encountered a hardware I/O error while accessing %1.3Encountered a sharing violation while accessing %1.3Encountered a locking violation while accessing %1.
0007D10E Disk full while accessing %1.\$Attempted to access %1 past its end.
0007D196 No error occurred.-An unknown error occurred while accessing %1.%Attempted to write to the reading %1.\$Attempted to access %1 past its end.&Attempted to read from the writing %1.
0007D2FC %1 has a bad format."%1 contained an unexpected object. %1 contains an incorrect schema.
0007D3BE pixels
0007D3EC Uncheck
0007D3FC Check
0007D408 Mixed
0009E91E VS_VERSION_INFO
0009E97A StringFileInfo
0009E99E 040904B0
0009E9B6 CompanyName
0009E9D6 FileDescription
0009E9F8 RecurseExec MFC Application
0009EA36 FileVersion
0009EA50 1, 0, 0, 1
0009EA6E InternalName
0009EA88 RecurseExec
0009EAA6 LegalCopyright
0009EAC4 Copyright (C) 2004
0009EAF2 LegalTrademarks
0009EB1A OriginalFilename
0009EB3C RecurseExec.EXE
0009EB62 ProductName
0009EB7C RecurseExec Application
0009EBB2 ProductVersion
0009EBD0 1, 0, 0, 1
0009EBEE VarFileInfo
0009EC0E Translation

APPENDIX C – REGSHOT COMPARISON RESULTS

Regshot 1.9.1 x64 Unicode (beta r321)

Comments:

Datetime: 2023-04-25 13:39:20, 2023-04-25 13:55:29

Computer: DESKTOP-14QC1L8, DESKTOP-14QC1L8

Username: user, user

Keys deleted: 15

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\8a535587-09dd-40c5-947a-851dce1b5177
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1168
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\348
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3488
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4532
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6268
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6336
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6404
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6456
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\8a535587-09dd-40c5-947a-851dce1b5177
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000030188
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000170332
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Search\JumplistData

Keys added: 62

HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-18_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-19_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-20_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\S-1-5-21-2169232433-3398496680-935370409-1000_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\WLIDSVC_HWID_HardwareUpdate_OutOfTolerance
HKLM\SOFTWARE\Microsoft\IdentityCRL\ThrottleCache\WLIDSVC_{DF60E2DF-88AD-4526-AE21-83D130EF0F68}
HKLM\SOFTWARE\Microsoft\RADAR\HeapLeakDetection\DiagnosedApplications\Procmon64.exe
HKLM\SOFTWARE\Microsoft\Wbem\Transports\Decoupled\Client
HKLM\SOFTWARE\Microsoft\Wbem\Transports\Decoupled\Client\{07D286B5-CFF0-4020-AE6C-C1984298126E}
HKLM\SOFTWARE\Microsoft\Wbem\Transports\Decoupled\Client\{28E1A4B7-A839-4DEF-BFCD-139F94FDEADD}
HKLM\SOFTWARE\Microsoft\Wbem\Transports\Decoupled\Client\{4BAFBEA3-DD7F-4F90-AA63-1F362B11CBD6}
HKLM\SOFTWARE\Microsoft\Wbem\Transports\Decoupled\Client\{6A372444-ED79-4648-BBB5-598A90C9C1D8}
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Creative\S-1-5-21-2169232433-3398496680-935370409-1000\133269037093887185
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Creative\S-1-5-21-2169232433-3398496680-935370409-1000\133269037102788429
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1536
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\272
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4420
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Multimedia\Audio Compression Manager

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Multimedia\Audio Compression Manager\MSACM
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Multimedia\Audio Compression Manager\Priority v4.00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Multimedia\msacm.imaadpcm
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Multimedia\msacm.msgsm610
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000010350
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000010568
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000200CA
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000002034A
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000002056A
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000003044A
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000003057A
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000004045C
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000040470
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000040524
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000503BE
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000050468
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000050524
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000602B6
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000060468
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000008034E
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000009034E

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000C03B2

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000D03B2

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000E03B2

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000F034E

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000F03B2

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000F0512

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000013034E

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000350346

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\Microsoft.ScreenSketch_8wekyb3d8bbwe!App

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\ClientTelemetry

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\ClientTelemetry\WAMAccounts

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows NT\CurrentVersion\HostActivityManager\CommitHistory\Microsoft.ScreenSketch_8wekyb3d8bbwe!App

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AM\AM\UI

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AM\UI\App

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AM\UI\App\V1

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AM\UI\App\V1\LU

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AM\AM\UI

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AM\UI\App

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AU\App\V1
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AU\App\V1\LU

Values deleted: 32

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\BITS\PerfMMFileName: "Global\MMF_BITS902d2bba-4b5a-4f05-925d-10b2533e2fce"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1168\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1168\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1168\CreationTime: 0x01D9777A56CEE3FF
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\348\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\348\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\348\CreationTime: 0x01D9777AFABB2D50
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3488\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3488\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3488\CreationTime: 0x01D9777AD8831EF5
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4532\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4532\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4532\CreationTime: 0x01D9777B366DF4FD
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6268\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6268\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6268\CreationTime: 0x01D9777A4E3FD429
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6336\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6336\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6336\CreationTime: 0x01D9777A8164BAFE
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6404\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6404\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6404\CreationTime: 0x01D9777A4E85A0D1
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6456\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6456\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6456\CreationTime: 0x01D9777A59E1A5C7
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults\LastRun\RunIsInProgressOrCrashed: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\VolatileNotifications\41C64E6DA3937055: 01 00 04 80 44 00 00 00
50 00 00 00 00 00 00 00 14 00 00 00 02 00 30 00 02 00 00 00 00 00 14 00 03 00 00 00 01 01 00 00 00 00 05 12 00 00 00 00 00
14 00 00 00 01 00 01 01 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 05 12 00 00 00
20 00 00 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\VolatileNotifications\41C64E6DA3842055: 01 00 04 80 44 00 00 00
50 00 00 00 00 00 00 00 14 00 00 00 02 00 30 00 02 00 00 00 00 00 14 00 03 00 00 00 01 01 00 00 00 00 05 12 00 00 00 00
14 00 00 00 01 00 01 01 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 05 12 00 00 00
20 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000030
188\VirtualDesktop: 10 00 00 00 30 30 44 56 61 15 42 70 9E 4B 5D 47 A4 E5 16 EE C6 77 D5 DB
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000170
332\VirtualDesktop: 10 00 00 00 30 30 44 56 61 15 42 70 9E 4B 5D 47 A4 E5 16 EE C6 77 D5 DB
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Search\JumplistData\windows.immersivecontrolpanel_cw5n1h2txyewy!mic
rosoft.windows.immersivecontrolpanel: 0x01D9777AC5300D7F
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Search\JumplistData\MSEdge: 0x01D9777B0B00C0D3

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Creative\S-1-5-21-2169232433-3398496680-935370409-1000\133269037102788429\portraitImage:
"C:\Users\user\AppData\Local\Packages\Microsoft.Windows.ContentDeliveryManager_cw5n1h2txyewy\LocalState\Assets\0c5c81e222bc1c7505cadda6beb5d679a4a394341ad0c6bef26039431cecd5e2"
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LogonUI\Creative\S-1-5-21-2169232433-3398496680-935370409-1000\133269037102788429\showImageOnSecureLock: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1536\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1536\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1536\CreationTime: 0x01D9777D377E3293
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\272\Terminator: "WerCrashReportFatal"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\272\Reason: 0x00000001
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\272\CreationTime: 0x01D9777D602ECA04
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4420\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4420\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4420\CreationTime: 0x01D9777D5EB677E8
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults\LastRun\RunEndTimestamp: 0x01D9777D80ACD7C5
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults\LastRun\ErrorCode: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults\LastRun\EnterpriseErrorCode: 0x00000000
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults\LastRun\ComponentWhichCausedErrorCode: ""
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults\LastRun\ErroredComponents: ""
HKLM\SOFTWARE\WOW6432Node\Microsoft\EdgeUpdate\UsageStats\Daily\Counts\winhttp_status_secure_failure: 08 00 00 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSource6Flags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSource6Width: 0x00000400
HKLM\SYSTEM\ControlSet001\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSource6Height: 0x00000300
HKLM\SYSTEM\ControlSet001\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSource6X: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\DefaultSettings.BitsPerPel: 0x00000020
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\DefaultSettings.XResolution: 0x00000400
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\DefaultSettings.YResolution: 0x00000300
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\DefaultSettings.VRefresh: 0x00000001
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\DefaultSettings.Flags: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\DefaultSettings.XPanning: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\DefaultSettings.YPanning: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\DefaultSettings.Orientation: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\DefaultSettings.FixedOutput: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\Attach.RelativeX: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\Attach.RelativeY: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\DefaultSettings.DriverExtra: FE FF FF FF FE FF FF FF 15 00 00 00 04 00 00 00 00 00 00 02 00 00 00

HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\Attach.RelativeY: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\DefaultSettings.DriverExtra: FE FF FF FF FE FF FF FF 15 00 00 00 04 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.BitsPerPel: 0x00000020
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.XResolution: 0x00000400
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.YResolution: 0x00000300
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.VRefresh: 0x00000001
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.Flags: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.XPanning: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.YPanning: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.Orientation: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.FixedOutput: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\Attach.RelativeX: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\Attach.RelativeY: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.DriverExtra: FE FF FF FF FE FF FF FF 15 00 00 00 04 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSource6Flags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSource6Width: 0x00000400
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSource6Height: 0x00000300
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSource6X: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSource6Flags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSource6Width: 0x00000400
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSource6Height: 0x00000300
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSource6X: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0002\VidPNSource6Flags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0002\VidPNSource6Width: 0x00000400
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0002\VidPNSource6Height: 0x00000300
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0002\VidPNSource6X: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0002\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0003\VidPNSource6Flags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0003\VidPNSource6Width: 0x00000400
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0003\VidPNSource6Height: 0x00000300

HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0003\VidPNSource6X: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0003\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0004\VidPNSource6Flags:
0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0004\VidPNSource6Width:
0x00000400
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0004\VidPNSource6Height:
0x00000300
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0004\VidPNSource6X: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0004\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0005\VidPNSource6Flags:
0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0005\VidPNSource6Width:
0x00000400
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0005\VidPNSource6Height:
0x00000300
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0005\VidPNSource6X: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0005\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\VidPNSource6Flags:
0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\VidPNSource6Width:
0x00000400
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\VidPNSource6Height:
0x00000300
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\VidPNSource6X: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\VidPNSource6Flags:
0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\VidPNSource6Width:
0x00000400
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\VidPNSource6Height:
0x00000300
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\VidPNSource6X: 0x00000000
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSource6Flags:
0x00000003
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSource6Width:
0x00000400
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSource6Height:
0x00000300
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSource6X: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-
BD247E05F284}\0001\DefaultSettings.BitsPerPel: 0x00000020
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-
BD247E05F284}\0001\DefaultSettings.XResolution: 0x00000400
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-
BD247E05F284}\0001\DefaultSettings.YResolution: 0x00000300
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-
BD247E05F284}\0001\DefaultSettings.VRefresh: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-
BD247E05F284}\0001\DefaultSettings.Flags: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-
BD247E05F284}\0001\DefaultSettings.XPanning: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-
BD247E05F284}\0001\DefaultSettings.YPanning: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-
BD247E05F284}\0001\DefaultSettings.Orientation: 0x00000000

HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\DefaultSettings.YPanning: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\DefaultSettings.Orientation: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\DefaultSettings.FixedOutput: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\Attach.RelativeX: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\Attach.RelativeY: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\DefaultSettings.DriverExtra: FE FF FF FF FE FF FF FF 15 00 00 00 04 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.BitsPerPel: 0x00000020
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.XResolution: 0x00000400
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.YResolution: 0x00000300
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.VRefresh: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.Flags: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.XPanning: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.YPanning: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.Orientation: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.FixedOutput: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\Attach.RelativeX: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\Attach.RelativeY: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\DefaultSettings.DriverExtra: FE FF FF FF FE FF FF FF 15 00 00 00 04 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSource6Flags: 0x00000003
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSource6Width: 0x00000400
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSource6Height: 0x00000300
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSource6X: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSource6Flags: 0x00000003
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSource6Width: 0x00000400
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSource6Height: 0x00000300
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSource6X: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSource6Y: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0002\VidPNSource6Flags: 0x00000003

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@C:\Windows\System32\ieframe.dll,-912: "HTML Document"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\diagtrack.dll,-3001: "Connected User Experiences and Telemetry"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@windows.storage.dll,-34583: "Saved Pictures"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@windows.storage.dll,-21824: "Camera Roll"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@C:\Program Files\Common Files\system\wab32res.dll,-10100: "Contacts"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@C:\Windows\System32\ieframe.dll,-12385: "Favorites Bar"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@windows.storage.dll,-21825: "3D Objects"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@C:\Windows\System32\Windows.UI.Immersive.dll,-38304: "Public Account Pictures"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-15: "Balanced"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-14: "Automatically balances performance with energy consumption on capable hardware."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-13: "High performance"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-12: "Favors performance, but may use more energy."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-11: "Power saver"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-10: "Saves energy by reducing your computer's performance where possible."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\AJRouter.dll,-1: "Routes AllJoyn messages for the local AllJoyn clients. If this service is stopped the AllJoyn clients that do not have their own bundled routers will be unable to run."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\Alg.exe,-113: "Provides support for 3rd party protocol plug-ins for Internet Connection Sharing"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\appidsvc.dll,-101: "Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\appinfo.dll,-101: "Facilitates the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to launch applications with the additional administrative privileges they may require to perform desired user tasks."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@appmgmts.dll,-3251: "Processes installation, removal, and enumeration requests for software deployed through Group Policy. If the service is disabled, users will be unable to install, remove, or enumerate software deployed through Group Policy. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\AppReadiness.dll,-1001: "Gets apps ready for use the first time a user signs in to this PC and when adding new apps."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\AppVClient.exe,-101: "Manages App-V users and virtual applications"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\appxdeploymentserver.dll,-2: "Provides infrastructure support for deploying Store applications. This service is started on demand and if disabled Store applications will not be deployed to the system, and may not function properly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\assignedaccessmanagersvc.dll,-101: "AssignedAccessManager Service supports kiosk experience in Windows."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\AudioEndpointBuilder.dll,-205: "Manages audio devices for the Windows Audio service. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\audiosrv.dll,-201: "Manages audio for Windows-based programs. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\autotimesvc.dll,-7: "This service sets time based on NITZ messages from a Mobile Network"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\AxInstSV.dll,-104: "Provides User Account Control validation for the installation of ActiveX controls from the Internet and enables management of ActiveX control installation based on Group Policy settings. This service is started on demand and if disabled the installation of ActiveX controls will behave according to default browser settings."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\bdesvc.dll,-101: "BDESVC hosts the BitLocker Drive Encryption service. BitLocker Drive Encryption provides secure startup for the operating system, as well as full volume encryption for OS, fixed or removable volumes. This service allows BitLocker to prompt users for various actions related to their volumes when mounted, and unlocks volumes automatically without user interaction. Additionally, it stores recovery information to Active Directory, if available, and, if necessary, ensures the most recent recovery certificates are used. Stopping or disabling the service would prevent users from leveraging this functionality."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\bfe.dll,-1002: "The Base Filtering Engine (BFE) is a service that manages firewall and Internet Protocol security (IPsec) policies and implements user mode filtering. Stopping or disabling the BFE service will significantly reduce the security of the system. It will also result in unpredictable behavior in IPsec management and firewall applications."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\bisrv.dll,-101: "Windows infrastructure service that controls which background tasks can run on the system."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\BTAGService.dll,-102: "Service supporting the audio gateway role of the Bluetooth Handsfree Profile."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\BthAvctpSvc.dll,-102: "This is Audio Video Control Transport Protocol service"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\bthserv.dll,-102: "The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already installed Bluetooth devices to fail to operate properly and prevent new devices from being discovered or associated."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\CapabilityAccessManager.dll,-2: "Provides facilities for managing UWP apps access to app capabilities as well as checking an app's access to specific app capabilities"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\cdpsvc.dll,-101: "This service is used for Connected Devices Platform scenarios"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\certprop.dll,-12: "Copies user certificates and root certificates from smart cards into the current user's certificate store, detects when a smart card is inserted into a smart card reader, and, if needed, installs the smart card Plug and Play minidriver."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ClipSVC.dll,-104: "Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled applications bought using Windows Store will not behave correctly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@comres.dll,-948: "Manages the configuration and tracking of Component Object Model (COM)+-based components. If the service is stopped, most COM+-based components will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\coremessaging.dll,-2: "Manages communication between system components."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\cryptsvc.dll,-1002: "Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be installed; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Automatic Root Certificate Update Service, which retrieves root certificates from Windows Update and enable scenarios such as SSL. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\cscsvc.dll,-201: "The Offline Files service performs maintenance activities on the Offline Files cache, responds to user logon and logoff events, implements the internals of the public API, and dispatches interesting events to those interested in Offline Files activities and changes in cache state."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@combase.dll,-5013: "The DCOMLAUNCH service launches COM and DCOM servers in response to object activation requests. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the DCOMLAUNCH service running."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\defragsvc.dll,-102: "Helps the computer run more efficiently by optimizing files on storage drives."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\das.dll,-101: "Enables pairing between the system and wired or wireless devices."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\umpnpgm.dll,-101: "Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\DevQueryBroker.dll,-101: "Enables apps to discover devices with a background task"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\dhcpcore.dll,-101: "Registers and updates IP addresses and DNS records for this computer. If this service is stopped, this computer will not receive dynamic IP addresses and DNS updates. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\DiagSvc\DiagnosicsHub.StandardCollector.ServiceRes.dll,-1001: "Diagnostics Hub Standard Collector Service. When running, this service collects real time ETW events and processes them."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\DiagSvc.dll,-101: "Executes diagnostic actions for troubleshooting support"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\diagtrack.dll,-3002: "The Connected User Experiences and Telemetry service enables features that support in-application and connected user experiences. Additionally, this service manages the event driven collection and transmission of diagnostic and usage information (used to improve the experience and quality of the Windows Platform) when the diagnostics and usage privacy option settings are enabled under Feedback and Diagnostics."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\dispbroker.desktop.dll,-102: "Manages the connection and configuration of local and remote displays"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\Microsoft.Graphics.Display.DisplayEnhancementService.dll,-1001: "A service for managing display enhancement such as brightness control."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\Windows.Internal.Management.dll,-101: "Performs Device Enrollment Activities for Device Management"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\dmwappushsvc.dll,-201: "Routes Wireless Application Protocol (WAP) Push messages received by the device and synchronizes Device Management sessions"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\dnsapi.dll,-102: "The DNS Client service (dnscache) caches Domain Name System (DNS) names and registers the full computer name for this computer. If the service is stopped, DNS names will continue to be resolved. However, the results of DNS name queries will not be cached and the computer's name will not be registered. If the service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\dot3svc.dll,-1103: "The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\dps.dll,-501: "The Diagnostic Policy Service enables problem detection, troubleshooting and resolution for Windows components. If this service is stopped, diagnostics will no longer function."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\DeviceSetupManager.dll,-1001: "Enables the detection, download and installation of device-related software. If this service is disabled, devices may be configured with outdated software, and may not work correctly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\dssvc.dll,-10002: "Provides data brokering between applications."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\dusmsvc.dll,-2: "Network data usage, data limit, restrict background data, metered networks."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\eapsvc.dll,-2: "The Extensible Authentication Protocol (EAP) service provides network authentication in such scenarios as 802.1x wired and wireless, VPN, and Network Access Protection (NAP). EAP also provides application programming interfaces (APIs) that are used by network access clients, including wireless and VPN clients, during the authentication process. If you disable this service, this computer is prevented from accessing networks that require EAP authentication."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\efssvc.dll,-101: "Provides the core file encryption technology used to store encrypted files on NTFS file system volumes. If this service is stopped or disabled, applications will be unable to access encrypted files."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\embeddedmodesvc.dll,-202: "The Embedded Mode service enables scenarios related to Background Applications. Disabling this service will prevent Background Applications from being activated."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@EnterpriseAppMgmtSvc.dll,-2: "Enables enterprise application management."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wevtvc.dll,-201: "This service manages events and event logs. It supports logging events, querying events, subscribing to events, archiving event logs, and managing event metadata. It can display events in both XML and plain text format. Stopping this service may compromise security and reliability of the system."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@comres.dll,-2451: "Supports System Event Notification Service (SENS), which provides automatic distribution of events to subscribing Component Object Model (COM) components. If the service is stopped, SENS will close and will not be able to provide logon and logoff notifications. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\fxsresm.dll,-122: "Enables you to send and receive faxes, utilizing fax resources available on this computer or on the network."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\fdpHost.dll,-101: "The FDPHOST service hosts the Function Discovery (FD) network discovery providers. These FD providers supply network discovery services for the Simple Services Discovery Protocol (SSDP) and Web Services – Discovery (WS-D) protocol. Stopping or disabling the FDPHOST service will disable network discovery for these protocols when using FD. When this service is unavailable, network services using FD and relying on these discovery protocols will be unable to find network devices or resources."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\fdrespub.dll,-101: "Publishes this computer and resources attached to this computer so they can be discovered over the network. If this service is stopped, network resources will no longer be published and they will not be discovered by other computers on the network."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\fhsvc.dll,-102: "Protects user files from accidental loss by copying them to a backup location"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\FntCache.dll,-101: "Optimizes performance of applications by caching commonly used font data. Applications will start this service if it is not already running. It can be disabled, though doing so will degrade application performance."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\PresentationHost.exe,-3310: "Optimizes performance of Windows Presentation Foundation (WPF) applications by caching commonly used font data. WPF applications will start this service if it is not already running. It can be disabled, though doing so will degrade the performance of WPF applications."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\FrameServer.dll,-101: "Enables multiple clients to access video frames from camera devices."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@gpapi.dll,-113: "The service is responsible for applying settings configured by administrators for the computer and users through the Group Policy component. If the service is disabled, the settings will not be applied and applications and components will not be manageable through Group Policy. Any components or applications that depend on the Group Policy component might not be functional if the service is disabled."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\GraphicsPerfSvc.dll,-101: "Graphics performance monitor service"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\hidserv.dll,-102: "Activates and maintains the use of hot buttons on keyboards, remote controls, and other multimedia devices. It is recommended that you keep this service running."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\hvhostsvc.dll,-101: "Provides an interface for the Hyper-V hypervisor to provide per-partition performance counters to the host operating system."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\tetheringservice.dll,-4098: "Provides the ability to share a cellular data connection with another device."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ikeext.dll,-502: "The IKEEXT service hosts the Internet Key Exchange (IKE) and Authenticated Internet Protocol (AuthIP) keying modules. These keying modules are used for authentication and key exchange in Internet Protocol security (IPsec). Stopping or disabling the IKEEXT service will disable IKE and AuthIP key exchange with peer computers. IPsec is typically configured to use IKE or AuthIP; therefore, stopping or disabling the IKEEXT service might result in an IPsec failure and might compromise the security of the system. It is strongly recommended that you have the IKEEXT service running."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\InstallService.dll,-201: "Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled then installations will not function properly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\iphlpvc.dll,-501: "Provides tunnel connectivity using IPv6 transition technologies (6to4, ISATAP, Port Proxy, and Teredo), and IP-HTTPS. If this service is stopped, the computer will not have the enhanced connectivity benefits that these technologies offer."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\ipxlatcfg.dll,-501: "Configures and enables translation from v4 to v6 and vice versa"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@keyiso.dll,-101: "The CNG key isolation service is hosted in the LSA process. The service provides key process isolation to private keys and associated cryptographic operations as required by the Common Criteria. The service stores and uses long-lived keys in a secure process complying with Common Criteria requirements."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@comres.dll,-2947: "Coordinates transactions between the Distributed Transaction Coordinator (MSDTC) and the Kernel Transaction Manager (KTM). If it is not needed, it is recommended that this service remain stopped. If it is needed, both MSDTC and KTM will start this service automatically. If this service is disabled, any MSDTC transaction interacting with a Kernel Resource Manager will fail and any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\srvc.dll,-101: "Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wkssvc.dll,-101: "Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\lfsvc.dll,-2: "This service monitors the current location of the system and manages geofences (a geographical location with associated events). If you turn off this service, applications will be unable to use or receive notifications for geolocation or geofences."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\licensemanagersvc.dll,-201: "Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled then content acquired through the Microsoft Store will not function properly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ltdres.dll,-2: "Creates a Network Map, consisting of PC and device topology (connectivity) information, and metadata describing each PC and device. If this service is disabled, the Network Map will not function properly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\lmhsvc.dll,-102: "Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients on the network, therefore enabling users to share files, print, and log on to the network. If this service is stopped, these functions might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\lsm.dll,-1002: "Core Windows Service that manages local user sessions. Stopping or disabling this service will result in system instability."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\LanguageOverlayServer.dll,-101: "Provides infrastructure support for deploying and configuring localized Windows resources. This service is started on demand and, if disabled, additional Windows languages will not be deployed to the system, and Windows may not function properly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\moshost.dll,-101: "Windows service for application access to downloaded maps. This service is started on-demand by application accessing downloaded maps. Disabling this service will prevent apps from accessing maps."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\FirewallAPI.dll,-23091: 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6E 00 64 00 65 00 72 00 20 00 46 00 69 00 72 00 65 00 77 00 61 00 6C 00 6C 00 20 00 68 00 65 00 6C 00 70 00 73 00 20 00 70 00 72 00 6F 00 74 00 65 00 63 00 74 00 20 00 79 00 6F 00 75 00 72 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 20 00 62 00 79 00 20 00 70 00 72 00 65 00 76 00 65 00 6E 00 74 00 69 00 6E 00 67 00 20 00 75 00 6E 00 61 00 75 00 74 00 68 00 6F 00 72 00 69 00 7A 00 65 00 64 00 20 00 75 00 73 00 65 00 72 00 73 00 20 00 66 00 72 00 6F 00 6D 00 20 00 67 00 61 00 69 00 6E 00 69 00 6E 00 67 00 20 00 61 00 63 00 63 00 65 00 73 00 73 00 20 00 74 00 6F 00 20 00 79 00 6F 00 75 00 72 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 20 00 74 00 68 00 72 00 6F 00 75 00 67 00 68 00 20 00 74 00 68 00 65 00 20 00 49 00 6E 00 74 00 65 00 72 00 6E 00 65 00 74 00 20 00 6F 00 72 00 20 00 61 00 20 00 6E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 2E 00 00 00 00 00

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@comres.dll,-2798: "Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will fail. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\iscsidsc.dll,-5001: "Manages Internet SCSI (iSCSI) sessions from this computer to remote iSCSI target devices. If this service is stopped, this

computer will not be able to login or access iSCSI targets. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\msimg.dll,-32: "Adds, modifies, and removes applications provided as a Windows Installer (*.msi, *.msp) package. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\NaturalAuth.dll,-101: "Signal aggregator service, that evaluates signals based on time, network, geolocation, bluetooth and cdf factors. Supported features are Device Unlock, Dynamic Lock and Dynamo MDM policies"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ncasvc.dll,-3008: "Provides DirectAccess status notification for UI components"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ncbservice.dll,-501: "Brokers connections that allow Windows Store Apps to receive notifications from the internet."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\NcdAutoSetup.dll,-101: "Network Connected Devices Auto-Setup service monitors and installs qualified devices that connect to a qualified network. Stopping or disabling this service will prevent Windows from discovering and installing qualified network connected devices automatically. Users can still manually add network connected devices to a PC through the user interface."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\netlogon.dll,-103: "Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\netman.dll,-110: 4D 00 61 00 6E 00 61 00 67 00 65 00 73 00 20 00 6F 00 62 00 6A 00 65 00 63 00 74 00 73 00 20 00 69 00 6E 00 20 00 74 00 68 00 65 00 20 00 4E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 20 00 61 00 6E 00 64 00 20 00 44 00 69 00 61 00 6C 00 2D 00 55 00 70 00 20 00 43 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 73 00 20 00 66 00 6F 00 6C 00 64 00 65 00 72 00 2C 00 20 00 69 00 6E 00 20 00 77 00 68 00 69 00 63 00 68 00 20 00 79 00 6F 00 75 00 20 00 63 00 61 00 6E 00 20 00 76 00 69 00 65 00 77 00 20 00 62 00 6F 00 74 00 68 00 20 00 6C 00 6F 00 63 00 61 00 6C 00 20 00 61 00 72 00 65 00 61 00 20 00 6E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 20 00 61 00 6E 00 64 00 20 00 72 00 65 00 6D 00 6F 00 74 00 65 00 20 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 73 00 2E 00 00 00 00 00

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\netprofmsvc.dll,-203: 49 00 64 00 65 00 6E 00 74 00 69 00 66 00 69 00 65 00 73 00 20 00 74 00 68 00 65 00 20 00 6E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 73 00 20 00 74 00 6F 00 20 00 77 00 68 00 69 00 63 00 68 00 20 00 74 00 68 00 65 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 20 00 68 00 61 00 73 00 20 00 63 00 6F 00 6E 00 6E 00 65 00 65 00 74 00 65 00 64 00 2C 00 20 00 63 00 6F 00 6C 00 6C 00 65 00 63 00 74 00 73 00 20 00 61 00 6E 00 64 00 20 00 73 00 74 00 6F 00 72 00 65 00 73 00 20 00 70 00 72 00 6F 00 70 00 65 00 72 00 74 00 69 00 65 00 73 00 20 00 66 00 6F 00 72 00 20 00 74 00 68 00 65 00 73 00 65 00 20 00 6E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 73 00 2C 00 20 00 61 00 6E 00 64 00 20 00 6E 00 6F 00 74 00 69 00 66 00 69 00 65 00 73 00 20 00 61 00 70 00 70 00 6C 00 69 00 63 00 61 00 74 00 69 00 6F 00 6E 00 73 00 20 00 77 00 68 00 65 00 6E 00 20 00 74 00 68 00 65 00 73 00 65 00 2

0 00 70 00 72 00 6F 00 70 00 65 00 72 00 74 00 69 00 65 00 73 00 20 00 63 00 68 00 61 00 6E 00 67 00 65 00 2E 00 00 00 00 00

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\NetSetupSvc.dll,-4: "The Network Setup Service manages the installation of network drivers and permits the configuration of low-level network settings. If this service is stopped, any driver installations that are in-progress may be cancelled."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll,-8200: "Provides ability to share TCP ports over the net.tcp protocol."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\NgcCtnrSvc.dll,-2: "Manages local user identity keys used to authenticate user to identity providers as well as TPM virtual smart cards. If this service is disabled, local user identity keys and TPM virtual smart cards will not be accessible. It is recommended that you do not reconfigure this service."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\ngcscv.dll,-101: "Provides process isolation for cryptographic keys used to authenticate to a user's associated identity providers. If this service is disabled, all uses and management of these keys will not be available, which includes machine logon and single-sign on for apps and websites. This service starts and stops automatically. It is recommended that you do not reconfigure this service."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\nlasvc.dll,-2: "Collects and stores configuration information for the network and notifies programs when this information is modified. If this service is stopped, configuration information might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\nsivc.dll,-201: "This service delivers network notifications (e.g. interface addition/deleting etc) to user mode clients. Stopping this service will cause loss of network connectivity. If this service is disabled, any other services that explicitly depend on this service will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\pnrpsvc.dll,-8005: "Provides identity services for the Peer Name Resolution Protocol (PNRP) and Peer-to-Peer Grouping services. If disabled, the Peer Name Resolution Protocol (PNRP) and Peer-to-Peer Grouping services may not function, and some applications, such as HomeGroup and Remote Assistance, may not function correctly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\p2psvc.dll,-8007: "Enables multi-party communication using Peer-to-Peer Grouping. If disabled, some applications, such as HomeGroup, may not function."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\pcasvc.dll,-2: "This service provides support for the Program Compatibility Assistant (PCA). PCA monitors programs installed and run by the user and detects known compatibility problems. If this service is stopped, PCA will not function properly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\peerdistsvc.dll,-9001: "This service caches network content from peers on the local subnet."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\PerceptionSimulation\PerceptionSimulationService.exe,-102: "Enables spatial perception simulation, virtual camera management and spatial input simulation."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\SysWow64\perfhost.exe,-1: "Enables remote users and 64-bit processes to query performance counters provided by 32-bit DLLs. If this service is stopped, only local users and 32-bit processes will be able to query performance counters provided by 32-bit DLLs."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\PhoneserviceRes.dll,-10001: 4D 00 61 00 6E 00 61 00 67 00 65 00 73 00 20 00 74 00 68 00 65 00 20 00 74 00 65 00 6C 00 65 00 70 00 68 00 6F 00 6E 00 79 00 20 00 73 00 74 00 61 00 74 00 65 00 20 00 6F 00 6E 00 20 00 74 00 68 00 65 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 00 00 00 00

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\pla.dll,-501: "Performance Logs and Alerts Collects performance data from local or remote computers based on preconfigured schedule parameters, then writes the data to a log or triggers an alert. If this service is stopped, performance information will not be collected. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\pnrpauto.dll,-8003: "This service publishes a machine name using the Peer Name Resolution Protocol. Configuration is managed via the netsh context 'p2p pnrp peer' "

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\pnrpsvc.dll,-8001: "Enables serverless peer name resolution over the Internet using the Peer Name Resolution Protocol (PNRP). If disabled, some peer-to-peer and collaborative applications, such as Remote Assistance, may not function."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\polstore.dll,-5011: "Internet Protocol security (IPsec) supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. This service enforces IPsec policies created through the IP Security Policies snap-in or the command-line tool "netsh ipsec". If you stop this service, you may experience network connectivity issues if your policy requires that connections use IPsec. Also,remote management of Windows Defender Firewall is not available when this service is stopped."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\umpo.dll,-101: "Manages power policy and power policy notification delivery."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll,-2: "This service opens custom printer dialog boxes and handles notifications from a remote print server or a printer. If you turn off this service, you won't be able to see printer extensions or notifications."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\profsvc.dll,-301: "This service is responsible for loading and unloading user profiles. If this service is stopped or disabled, users will no longer be able to successfully sign in or sign out, apps might have problems getting to users' data, and components registered to receive profile event notifications won't receive them."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\pushtoinstall.dll,-201: "Provides infrastructure support for the Microsoft Store. This service is started automatically and if disabled then remote installations will not function properly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\qwwave.dll,-2: "Quality Windows Audio Video Experience (qWave) is a networking platform for Audio Video (AV) streaming applications on IP home networks. qWave enhances AV streaming performance and reliability by ensuring network quality-of-service (QoS) for AV applications. It provides mechanisms for admission control, run time monitoring and enforcement, application feedback, and traffic prioritization."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\rasauto.dll,-201: "Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\rasmans.dll,-201: "Manages dial-up and virtual private network (VPN) connections from this computer to the Internet or other remote networks. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\mprdim.dll,-201: "Offers routing services to businesses in local area and wide area network environments."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@regsvc.dll,-2: "Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\RDXService.dll,-257: "The Retail Demo service controls device activity while the device is in retail demo mode."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\RMapi.dll,-1002: 52 00 61 00 64 00 69 00 6F 00 20 00 4D 00 61 00 6E 00 61 00 67 00 65 00 6D 00 65 00 6E 00 74 00 20 00 61 00 6E 00 64 00 20 00 41 00 69 00 72 00 70 00 6C 00 61 00 6E 00 65 00 20 00 4D 00 6F 00 64 00 65 00 20 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 00 00 00

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\RpcEpMap.dll,-1002: "Resolves RPC interfaces identifiers to transport endpoints. If this service is stopped or disabled, programs using Remote Procedure Call (RPC) services will not function properly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\Locator.exe,-3: "In Windows 2003 and earlier versions of Windows, the Remote Procedure Call (RPC) Locator service manages the RPC name service database. In Windows Vista and later versions of Windows, this service does not provide any functionality and is present for application compatibility."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@combase.dll,-5011: "The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activations requests, object exporter resolutions and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\samsrv.dll,-2: "The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\SCardSvr.dll,-5: "Manages access to smart cards read by this computer. If this service is stopped, this computer will be unable to read smart cards. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\ScDeviceEnum.dll,-101: "Creates software device nodes for all smart card readers accessible to a given session. If this service is disabled, WinRT APIs will not be able to enumerate smart card readers."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\schedsvc.dll,-101: "Enables a user to configure and schedule automated tasks on this computer. The service also hosts multiple Windows system-critical tasks. If this service is stopped or disabled, these tasks will not be run at their scheduled times. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\certprop.dll,-14: "Allows the system to be configured to lock the user desktop upon smart card removal."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\sdrsvc.dll,-102: "Provides Windows Backup and Restore capabilities."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\seclogon.dll,-7000: "Enables starting processes under alternate credentials. If this service is stopped, this type of logon access will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\SecurityHealthAgent.dll,-1001: "Windows Security Service handles unified device protection and health information"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\SEMgrSvc.dll,-1002: "Manages payments and Near Field Communication (NFC) based secure elements."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\Sens.dll,-201: "Monitors system events and notifies subscribers to COM+ Event System of these events."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%ProgramFiles%\Windows Defender Advanced Threat Protection\MsSense.exe,-1002: "Windows Defender Advanced Threat Protection service helps protect against advanced threats by monitoring and reporting security events that happen on the computer."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\SensorDataService.exe,-102: "Delivers data from a variety of sensors"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\sensorservice.dll,-1001: "A service for sensors that manages different sensors' functionality. Manages Simple Device Orientation (SDO) and History for sensors. Loads the SDO sensor that reports device orientation changes. If this service is stopped or disabled, the SDO sensor will not be loaded and so auto-rotation will not occur. History collection from Sensors will also be stopped."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\sensrsvc.dll,-1001: "Monitors various sensors in order to expose data and adapt to system and user state. If this service is stopped or disabled, the display brightness will not adapt to lighting conditions. Stopping this service may affect other system functionality and features as well."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\SessEnv.dll,-1027: "Remote Desktop Configuration service (RDCS) is responsible for all Remote Desktop Services and Remote Desktop related configuration and session maintenance activities that require SYSTEM context. These include per-session temporary folders, RD themes, and RD certificates."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\SgrmBroker.exe,-101: "Monitors and attests to the integrity of the Windows platform."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ipnathlp.dll,-107: "Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\SharedRealitySvc.dll,-101: "This service is used for Spatial Perception scenarios"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\shsvcs.dll,-12289: "Provides notifications for AutoPlay hardware events."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\Windows.SharedPC.AccountManager.dll,-101: "Manages profiles and accounts on a SharedPC configured device"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\smphost.dll,-101: "Host service for the Microsoft Storage Spaces management provider. If this service is stopped or disabled, Storage Spaces cannot be managed."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\SmsRouterSvc.dll,-10002: "Routes messages based on rules to appropriate clients."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@firewallapi.dll,-50324: 52 00 65 00 63 00 65 00 69 00 76 00 65 00 73 00 20 00 74 00 72 00 61 00 70 00 20 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 73 00 20 00 67 00 65 00 6E 00 65 00 72 00 61 00 74 00 65 00 64 00 20 00 62 00 79 00 20 00 6C 00 6F 00 63 00 61 00 6C 00 20 00 6F 00 72 00 20 00 72 00 65 00 6D 00 6F 00 74 00 65 00 20 00 53 00 69 00 6D 00 70 00 6C 00 65 00 20 00 4E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 20 00 4D 00 61 00 6E 00 61 00 67 00 65 00 6D 00 65 00 6E 00 74 00 20 00 50 00 72 00 6F 00 74 00 6F 00 63 00 6F 00 6C 00 20 00 28 00 53 00 4E 00 4D 00 50 00 29 00 20 00 61 00 67 00 65 00 6E 00 74 00 73 00 20 00 61 00 6E 00 64 00 20 00 66 00 6F 00 72 00 77 00 61 00 72 00 64 00 73 00 20 00 74 00 68 00 65 00 20 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 73 00 20 00 74 00 6F 00 20 00 53 00 4E 00 4D 00 50 00 20 00 6D 00 61 00 6E 00 61 00 67 00 65 00 6D 00 65 00 6E 00 74 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 73 00 20 00 72 00 75 00 6E 00 6E 00 69 00 6E 00 67 00 20 00 6F 00 6E 00 20 00 74 00 68 00 69 00 73 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 20 00 66 00 6E 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 62 00 61 00 73 00 20 00 69 00 73 00 20 00 73 00 74 00 6F 00 70 00 70 00 65 00 64 00 2C 00 20 00 53 00 4E 00 4D 00 50 00 2D 00 62 00 61 00 73 00 65 00 64 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 73 00 20 00 6F 00 6E 00 20 00 74 00 68 00 69 00 73 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 20 00 77 00 69 00 6C 00 6C 00 20 00 6E 00 6F 00 74 00 20 00 72 00 65 00 63 00 65 00 69 00 76 00 65 00 20 00 53 00 4E 00 4D 00 50 00 20 00 74 00 72 00 61 00 70 00 20 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 73 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 64 00 2C 00 20 00 61 00 6E 00 79 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 64 00 2C 00 20 00 61 00 6E 00 79 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 65 00 78 00 70 00 6C 00 69 00 63 00 69 00 74 00 6C 00 79 00 20 00 64 00 65 00 70 00 65 00 6E 00 64 00 20 00 6F 00 6E 00 20 00 69 00 74 00 20 00 77 00 69 00 6C 00 6C 00 20 00 66 00 61 00 69 00 6C 00 20 00 74 00 6F 00 20 00 73 00 74 00 61 00 72 00 74 00 2E 00 00 00 00 00

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\spectrum.exe,-102: "Enables spatial perception, spatial input, and holographic rendering."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\spoolsv.exe,-2: "This service spools print jobs and handles interaction with the printer. If you turn off this service, you won't be able to print or see your printers."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\spssvc.exe,-100: "Enables the download, installation and enforcement of digital licenses for Windows and Windows applications. If the service is disabled,

the operating system and licensed applications may run in a notification mode. It is strongly recommended that you not disable the Software Protection service."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\ssdpsrv.dll,-101: 44 00 69 00 73 00 63 00 6F 00 76 00 65 00 72 00 73 00 20 00 6E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 65 00 64 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 61 00 6E 00 64 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 75 00 73 00 65 00 20 00 74 00 68 00 65 00 20 00 53 00 53 00 44 00 50 00 20 00 64 00 69 00 73 00 63 00 6F 00 76 00 65 00 72 00 79 00 20 00 70 00 72 00 6F 00 74 00 6F 00 63 00 6F 00 6C 00 2C 00 20 00 73 00 75 00 63 00 68 00 20 00 61 00 73 00 20 00 55 00 50 00 6E 00 50 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 2E 00 20 00 41 00 6C 00 73 00 6F 00 20 00 61 00 6E 00 6E 00 6F 00 75 00 6E 00 63 00 65 00 73 00 20 00 53 00 53 00 44 00 50 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 61 00 6E 00 64 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 72 00 75 00 6E 00 6E 00 69 00 6E 00 67 00

20 00 6F 00 6E 00 20 00 74 00 68 00 65 00 20 00 6C 00 6F 00 63 00 61 00 6C 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 73 00 74 00 6F 00 70 00 70 00 65 00 64 00 2C 00 20 00 53 00 53 00 44 00 50 00 2D 00 62 00 61 00 73 00 65 00 64 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 77 00 69 00 6C 00 6C 00 20 00 6E 00 6F 00 74 00 20 00 62 00 65 00 20 00 64 00 69 00 73 00 63 00 6F 00 76 00 65 00 72 00 65 00 64 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 64 00 2C 00 20 00 61 00 6E 00 79 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 65 00 78 00 70 00 6C 00 69 00 63 00 69 00 74 00 6C 00 79 00 20 00 64 00 65 00 70 00 65 00 6E 00 64 00 20 00 6F 00 6E 00 20 00 69 00 74 00 20 00 77

00 69 00 6C 00 6C 00 20 00 66 00 61 00 69 00 6C 00 20 00 74 00 6F 00 20 00 73 00 74 00 61 00 72 00 74 00 2E 00 20 00 00 00 00 00 HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\sstpsvc.dll,-201: "Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\windows.staterepository.dll,-2: "Provides required infrastructure support for the application model."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wiaservc.dll,-10: "Provides image acquisition services for scanners and cameras"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\StorSvc.dll,-101: "Provides enabling services for storage settings and external storage expansion"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\svsvc.dll,-102: "Verifies potential file system corruptions."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\swprv.dll,-102: "Manages software-based volume shadow copies taken by the Volume Shadow Copy service. If this service is stopped, software-based volume shadow copies cannot be managed. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\sysmain.dll,-1001: "Maintains and improves system performance over time."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\SystemEventsBrokerServer.dll,-1002: "Coordinates execution of background work for WinRT application. If this service is stopped or disabled, then background work might not be triggered."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\TabSvc.dll,-101: "Enables Touch Keyboard and Handwriting Panel pen and ink functionality"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\tapisrv.dll,-10101: "Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer and, through the LAN, on servers that are also running the service."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\termstrv.dll,-267: "Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service. To prevent remote use of this computer, clear the checkboxes on the Remote tab of the System properties control panel item."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\themeservice.dll,-8193: "Provides user experience theme management."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\TieringEngineService.exe,-701: "Optimizes the placement of data in storage tiers on all tiered storage spaces in the system."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\TimeBrokerServer.dll,-1002: "Coordinates execution of background work for WinRT application. If this service is stopped or disabled, then background work might not be triggered."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\tokenbroker.dll,-101: "This service is used by Web Account Manager to provide single-sign-on to apps and services."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\trkws.dll,-2: "Maintains links between NTFS files within a computer or across computers in a network."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\MitigationClient.dll,-104: "Enables automatic mitigation for known problems by applying recommended troubleshooting. If stopped, your device will not get recommended troubleshooting for problems on your device."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\tzautoupdate.dll,-201: "Automatically sets the system time zone."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\AgentService.exe,-101: "Provides support for application and OS settings roaming"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\umrdp.dll,-1001: "Allows the redirection of Printers/Drives/Ports for RDP connections"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\upnphost.dll,-214: 41 00 6C 00 6C 00 6F 00 77 00 73 00 20 00 55 00 50 00 6E 00 50 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 6F 00 20 00 62 00 65 00 20 00 68 00 6F 00 73 00 74 00 65 00 64 00 20 00 6F 00 6E 00 20 00 74 00 68 00 69 00 73 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 73 00 74 00 6F 00 70 00 70 00 65 00 64 00 2C 00 20 00 61 00 6E 00 79 00 20 00 68 00 6F 00 73 00 74 00 65 00 64 00 20 00 55 00 50 00 6E 00 50 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 77 00 69 00 6C 00 6C 00 20 00 73 00 74 00 6F 00 70 00 20 00 66 00 75 00 6E 00 63 00 74 00 69 00 6F 00 6E 00 69 00 6E 00 67 00 20 00 61 00 6E 00 64 00 20 00 6E 00 6F 00 20 00 61 00 64 00 64 00 69 00 74 00 69 00 6F 00 6E 00 61 00 6C 00 20 00 68 00 6F 00 73 00 74 00 65 00 64 00 20 00 64 00 65 00 64 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 64 00 2C 00 20 00 61 00 6E 00 79 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 65 00 78 00 70 00 6C 00 69 00 63 00 69 00 74 00 6C 00 79 00 20 00 64 00 65 00 70 00 65 00 6E 00 64 00 20 00 6F 00 6E 00 20 00 69 00 74 00 20 00 77 00 69 00 6C 00 6C 00 20 00 66 00 61 00 69 00 6C 00 20 00 74 00 6F 00 20 00 73 00 74 00 61 00 72 00 74 00 2E 00 00 00 00 00

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\usermgr.dll,-101: "User Manager provides the runtime components required for multi-user interaction. If this service is stopped, some applications may not operate correctly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\vac.dll,-201: "Hosts spatial analysis for Mixed Reality audio simulation."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\vaultsvc.dll,-1004: "Provides secure storage and retrieval of credentials to users, applications and security service packages."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\vds.exe,-112: "Provides management services for disks, volumes, file systems, and storage arrays."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-802: "Provides an interface for the Hyper-V host to interact with specific services running inside the virtual machine."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-102: "Monitors the state of this virtual machine by reporting a heartbeat at regular intervals. This service helps you identify running virtual machines that have stopped responding."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-202: "Provides a mechanism to exchange data between the virtual machine and the operating system running on the physical computer."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvext.dll,-602: "Provides a platform for communication between the virtual machine and the operating system running on the physical computer."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-302: "Provides a mechanism to shut down the operating system of this virtual machine from the management interfaces on the physical computer."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-402: "Synchronizes the system time of this virtual machine with the system time of the physical computer."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-902: "Provides a mechanism to manage virtual machine with PowerShell via VM session without a virtual network."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvext.dll,-502: "Coordinates the communications that are required to use Volume Shadow Copy Service to back up applications and data on this virtual machine from the operating system on the physical computer."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\vssvc.exe,-101: "Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\w32time.dll,-201: "Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\WalletService.dll,-1001: "Hosts objects used by clients of the wallet"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\Windows.WARP.JITService.dll,-101: "Provides a JIT out of process service for WARP when running with ACG enabled."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wbengine.exe,-105: "The WBENGINE service is used by Windows Backup to perform backup and recovery operations. If this service is stopped by a user, it may cause the currently running backup or recovery operation to fail. Disabling this service may disable backup and recovery operations using Windows Backup on this computer."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wbiosvc.dll,-101: "The Windows biometric service gives client applications the ability to capture, compare, manipulate, and store biometric data without gaining direct access to any biometric hardware or samples. The service is hosted in a privileged SVCHOST process."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wcmSvc.dll,-4098: "Makes automatic connect/disconnect decisions based on the network connectivity options currently available to the PC and enables management of network connectivity based on Group Policy settings."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wcnscvc.dll,-4: 57 00 43 00 4E 00 43 00 53 00 56 00 43 00 20 00 68 00 6F 00 73 00 74 00 73 00 20 00 74 00 68 00 65 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 43 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 20 00 4E 00 6F 00 77 00 20 00 43 00 6F 00 6E 00 66 00 69 00 67 00 75 00 72 00 61 00 74 00 69 00 6F 00 6E 00 20 00 77 00 68 00 69 00 63 00 68 00 20 00 69 00 73 00 20 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 27 00 73 00 20 00 49 00 6D 00 70 00 6C 00 65 00 6D 00 65 00 6E 00 74 00 61 00 74 00 69 00 6F 00 6E 00 20 00 6F 00 66 00 20 00 57 00 69 00 72 00 65 00 6C 00 65 00 73 00 73 00 20 00 50 00 72 00 6F 00 74 00 65 00 63 00 74 00 65 00 64 00 20 00 53 00 65 00 74 00 75 00 70 00 20 00 28 00 57 00 50 00 53 00 29 00 20 00 70 00 72 00 6F 00 74 00 6F 00 63 00 6F 00 6C 00 2E 00 20 00 54 00 68 00 69 00 73 00 20 00 69 00 73 00 20 00 75 00 73 00 65 00 64 00 20 00 74 00 6F 00 20 00 63 00 6

F 00 6E 00 66 00 69 00 67 00 75 00 72 00 65 00 20 00 57 00 69 00 72 00 65 00 6C 00 65 00 73 00 73 00 20 00 4C 00 41 00 4E 00 20 00 73 00 65 00 74 00 74 00 69 00 6E 00 67 00 73 00 20 00 66 00 6F 00 72 00 20 00 61 00 6E 00 20 00 41 00 63 00 63 00 65 00 73 00 73 00 20 00 50 00 6F 00 69 00 6E 00 74 00 20 00 28 00 41 00 50 00 29 00 20 00 6F 00 72 00 20 00 61 00 20 00 57 00 69 00 72 00 65 00 6C 00 65 00 73 00 73 00 20 00 44 00 65 00 76 00 69 00 63 00 65 00 2E 00 20 00 54 00 68 00 65 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 73 00 74 00 61 00 72 00 74 00 65 00 64 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 6D 00 61 00 74 00 69 00 63 00 61 00 6C 00 6C 00 79 00 20 00 61 00 73 00 20 00 6E 00 65 00 65 00 64 00 65 00 64 00 2E 00 00 00 00 00

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wdi.dll,-503: "The Diagnostic Service Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local Service context. If this service is stopped, any diagnostics that depend on it will no longer function."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wdi.dll,-501: "The Diagnostic System Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local System context. If this service is stopped, any diagnostics that depend on it will no longer function."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-242: "Helps guard against intrusion attempts targeting known and newly discovered vulnerabilities in network protocols"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\weclnt.dll,-101: 45 00 6E 00 61 00 62 00 6C 00 65 00 73 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 2D 00 62 00 61 00 73 00 65 00 64 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 73 00 20 00 74 00 6F 00 20 00 63 00 72 00 65 00 61 00 74 00 65 00 2C 00 20 00 61 00 63 00 63 00 65 00 73 00 73 00 2C 00 20 00 61 00 6E 00 64 00 20 00 6D 00 6F 00 64 00 69 00 66 00 79 00 20 00 49 00 6E 00 74 00 65 00 72 00 6E 00 65 00 74 00 2D 00 62 00 61 00 73 00 65 00 64 00 20 00 66 00 69 00 6C 00 65 00 73 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 74 00 6F 00 70 00 70 00 65 00 64 00 2C 00 20 00 74 00 68 00 65 00 73 00 65 00 20 00 66 00 75 00 6E 00 63 00 74 00 69 00 6F 00 6E 00 73 00 20 00 77 00 69 00 6C 00 6C 00 20 00 66 00 61 00 69 00 6C 00 20 00 74 00 6F 00 20 00 73 00 74 00 61 00 72 00 74 00 2E 00 00 00 00 00

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\weclnt.dll,-201: "This service manages persistent subscriptions to events from remote sources that support WS-Management protocol. This includes

Windows Vista event logs, hardware and IPMI-enabled event sources. The service stores forwarded events in a local Event Log. If this service is stopped or disabled event subscriptions cannot be created and forwarded events cannot be accepted."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wephostsvc.dll,-101: "Windows Encryption Provider Host Service brokers encryption related functionalities from 3rd Party Encryption Providers to processes that need to evaluate and apply EAS policies. Stopping this will compromise EAS compliancy checks that have been established by the connected Mail Accounts"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wercplsupport.dll,-100: "This service provides support for viewing, sending and deletion of system-level problem reports for the Problem Reports and Solutions control panel."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wersvc.dll,-101: "Allows errors to be reported when programs stop working or responding and allows existing solutions to be delivered. Also allows logs to be generated for diagnostic and repair services. If this service is stopped, error reporting might not work correctly and results of diagnostic services and repairs might not be displayed."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wfdscnmgsvcs.dll,-9001: "Manages connections to wireless services, including wireless display and docking."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wiarpc.dll,-1: "Launches applications associated with still image acquisition events."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-240: "Helps protect users from malware and other potentially unwanted software"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\winhttp.dll,-101: "WinHTTP implements the client HTTP stack and provides developers with a Win32 API and COM Automation component for sending HTTP requests and receiving responses. In addition, WinHTTP provides support for auto-discovering a proxy configuration via its implementation of the Web Proxy Auto-Discovery (WPAD) protocol."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\wbem\wmisvc.dll,-204: "Provides a common interface and object model to access management information about operating system, devices, applications and services. If this service is stopped, most Windows-based software will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\wsmsvc.dll,-102: "Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web services protocol used for remote software and hardware management. The WinRM service listens on the network for WS-Management requests and processes them. The WinRM Service needs to be configured with a listener using winrm.cmd command line tool or through Group Policy in order for it to listen over the network. The WinRM service provides access to WMI data and enables event collection. Event collection and subscription to events require that the service is running. WinRM messages use HTTP and HTTPS as transports. The WinRM service does not depend on IIS but is preconfigured to share a port with IIS on the same machine. The WinRM service reserves the /wsman URL prefix. To prevent conflicts with IIS, administrators should ensure that any websites hosted on IIS do not use the /wsman URL prefix."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\flightsettings.dll,-104: "Provides infrastructure support for the Windows Insider Program. This service must remain enabled for the Windows Insider Program to work."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wlansvc.dll,-258: "The WLANSVC service provides the logic required to configure, discover, connect to, and disconnect from a wireless local area network (WLAN) as defined by IEEE 802.11 standards. It also contains the logic to turn your computer into a software access point so that other devices or computers can connect to your computer wirelessly using a WLAN adapter that can support this. Stopping or disabling the WLANSVC service will make all WLAN adapters on your computer inaccessible from the Windows networking UI. It is strongly recommended that you have the WLANSVC service running if your computer has a WLAN adapter."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wldisvc.dll,-101: "Enables user sign-in through Microsoft account identity services. If this service is stopped, users will not be able to logon to the computer with their Microsoft account."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\lpasvc.dll,-1001: "This service provides profile management for subscriber identity modules"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\Windows.Management.Service.dll,-101: "Performs management including Provisioning and Enrollment activities"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\wbem\wmiapsrv.exe,-111: "Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service only runs when Performance Data Helper is activated."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-102: "Shares Windows Media Player libraries to other networked players and media devices using Universal Plug and Play"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\workfolderssvc.dll,-101: "This service syncs files with the Work Folders server, enabling you to use the files on any of the PCs and devices on which you've set up Work Folders."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\WpcRefreshTask.dll,-101: "Enforces parental controls for child accounts in Windows. If this service is stopped or disabled, parental controls may not be enforced."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wpdbusenum.dll,-101: "Enforces group policy for removable mass-storage devices. Enables applications such as Windows Media Player and Image Import Wizard to transfer and synchronize content using removable mass-storage devices."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wpnservice.dll,-2: "This service runs in session 0 and hosts the notification platform and connection provider which handles the connection between the device and WNS server."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wscsvc.dll,-201: "The WSCSVC (Windows Security Center) service monitors and reports security health settings on the computer. The health settings include firewall (on/off), antivirus (on/off/out of date), antispyware (on/off/out of date), Windows Update (automatically/manually download and install updates), User Account Control (on/off), and Internet settings (recommended/not recommended). The service provides COM APIs for independent software vendors to register and record the state of their products to the Security Center service. The Security and Maintenance UI uses the service to provide systray alerts and a graphical view of the security health states in the Security and Maintenance control panel. Network Access Protection (NAP) uses the service to report the security health states of clients to the NAP Network Policy Server to make network quarantine decisions. The service also has a public API that allows external consumers to programmatically retrieve the aggregated security health state of the system."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\SearchIndexer.exe,-104: "Provides content indexing, property caching, and search results for files, e-mail, and other content."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wwansvc.dll,-258: "This service manages mobile broadband (GSM & CDMA) data card/embedded module adapters and connections by auto-configuring the networks. It is strongly recommended that this service be kept running for best user experience of mobile broadband devices."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\XblAuthManager.dll,-101: "Provides authentication and authorization services for interacting with Xbox Live. If this service is stopped, some applications may not operate correctly."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\XblGameSave.dll,-101: "This service syncs save data for Xbox Live save enabled games. If this service is stopped, game save data will not upload to or download from Xbox Live."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\xboxgipsvc.dll,-101: "This service manages connected Xbox Accessories."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\XboxNetApiSvc.dll,-101: "This service supports the Windows.Networking.XboxLive application programming interface."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\AarSvc.dll,-101: "Runtime for activating conversational agent applications"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\BcastDVRUserService.dll,-101: "This user service is used for Game Recordings and Live Broadcasts"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\Microsoft.Bluetooth.UserService.dll,-102: "The Bluetooth user service supports proper functionality of Bluetooth features relevant to each user session."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\CaptureService.dll,-101: "Enables optional screen capture functionality for applications that call the Windows.Graphics.Capture API."

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\cbdhsvc.dll,-101: "This user service is used for Clipboard scenarios"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\cdpusersvc.dll,-101: "This user service is used for Connected Devices Platform scenarios"

HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ConsentUxClient.dll,-101: "Allows ConnectUX and PC Settings to Connect and Pair with WiFi displays and Bluetooth devices."

HKU\DEFAULT\Software\Classes\Local
Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\CredentialEnrollmentManager.exe,-101: "Credential Enrollment
Manager"
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\deviceaccess.dll,-108:
"Enables apps to pair devices"
HKU\DEFAULT\Software\Classes\Local
Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\Windows.Devices.Picker.dll,-1007: "This user service is used for
managing the Miracast, DLNA, and DIAL UI"
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\DevicesFlowBroker.dll,-
104: "Allows ConnectUX and PC Settings to Connect and Pair with WiFi displays and Bluetooth devices."
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\MessagingService.dll,-
101: "Service supporting text messaging and related functionality."
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\APHostRes.dll,-10001:
"This service synchronizes mail, contacts, calendar and various other user data. Mail and other applications dependent on this
functionality will not work properly when this service is not running."
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\UserDataAccessRes.dll,-
15000: 49 00 6E 00 64 00 65 00 78 00 65 00 73 00 20 00 63 00 6F 00 6E 00 74 00 61 00 63 00 74 00 20 00 64 00 61 00 74 00 61
00 20 00 66 00 6F 00 72 00 20 00 66 00 61 00 73 00 74 00 20 00 63 00 6F 00 6E 00 74 00 61 00 63 00 74 00 20 00 73 00 65 00 61
00 72 00 63 00 68 00 69 00 6E 00 67 00 2E 00 20 00 49 00 66 00 20 00 79 00 6F 00 75 00 20 00 73 00 74 00 6F 00 70 00 20 00 6F
00 72 00 20 00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63
00 65 00 2C 00 20 00 63 00 6F 00 6E 00 74 00 61 00 63 00 74 00 73 00 20 00 6D 00 69 00 67 00 68 00 74 00 20 00 62 00 65 00 20
00 6D 00 69 00 73 00 73 00 69 00 6E 00 67 00 20 00 66 00 72 00 6F 00 6D 00 20 00 79 00 6F 00 75 00 72 00 20 00 73 00 65 00 61
00 72 00 63 00 68 00 20 00 72 00 65 00 73 00 75 00 6C 00 74 00 73 00 2E 00 00 00 00 00
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\PrintWorkflowService.dll,-
101: "Print Workflow"
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\UserDataAccessRes.dll,-
10002: 48 00 61 00 6E 00 64 00 6C 00 65 00 73 00 20 00 73 00 74 00 6F 00 72 00 61 00 67 00 65 00 20 00 6F 00 66 00 20 00 73
00 74 00 72 00 75 00 63 00 74 00 75 00 72 00 65 00 64 00 20 00 75 00 73 00 65 00 72 00 20 00 64 00 61 00 74 00 61 00 2C 00 20
00 69 00 6E 00 63 00 6C 00 75 00 64 00 69 00 6E 00 67 00 20 00 63 00 6F 00 6E 00 74 00 61 00 63 00 74 00 20 00 69 00 6E 00 66
00 6F 00 2C 00 20 00 63 00 61 00 6C 00 65 00 6E 00 64 00 61 00 72 00 73 00 2C 00 20 00 6D 00 65 00 73 00 73 00 61 00 67 00 65
00 73 00 2C 00 20 00 61 00 6E 00 64 00 20 00 6F 00 74 00 68 00 65 00 72 00 20 00 63 00 6F 00 6E 00 74 00 65 00 6E 00 74 00 2E
00 20 00 49 00 66 00 20 00 79 00 6F 00 75 00 20 00 73 00 74 00 6F 00 70 00 20 00 6F 00 72 00 20 00 64 00 69 00 73 00 61 00 62
00 6C 00 65 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 2C 00 20 00 61 00 70 00 70 00 73
00 20 00
74 00 68 00 61 00 74 00 20 00 75 00 73 00 65 00 20 00 74 00 68 00 69 00 73 00 20 00 64 00 61 00 74 00 61 00 20 00 6D 00 69
00 67 00 68 00 74 00 20 00 6E 00 6F 00 74 00 20 00 77 00 6F 00 72 00 6B 00 20 00 63 00 6F 00 72 00 72 00 65 00 63 00 74 00 6C
00 79 00 2E 00 00 00 00 00
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\UserDataAccessRes.dll,-
14000: 50 00 72 00 6F 00 76 00 69 00 64 00 65 00 73 00 20 00 61 00 70 00 70 00 73 00 20 00 61 00 63 00 63 00 65 00 73 00 73
00 20 00 74 00 6F 00 20 00 73 00 74 00 72 00 75 00 63 00 74 00 75 00 72 00 65 00 64 00 20 00 75 00 73 00 65 00 72 00 20 00 64
00 61 00 74 00 61 00 2C 00 20 00 69 00 6E 00 63 00 6C 00 75 00 64 00 69 00 6E 00 67 00 20 00 63 00 6F 00 6E 00 74 00 61 00 63
00 74 00 20 00 69 00 6E 00 66 00 6F 00 2C 00 20 00 63 00 61 00 6C 00 65 00 6E 00 64 00 61 00 72 00 73 00 2C 00 20 00 6D 00 65
00 73 00 73 00 61 00 67 00 65 00 73 00 2C 00 20 00 61 00 6E 00 64 00 20 00 6F 00 74 00 68 00 65 00 72 00 20 00 63 00 6F 00 6E
00 74 00 65 00 6E 00 74 00 2E 00 20 00 49 00 66 00 20 00 79 00 6F 00 75 00 20 00 73 00 74 00 6F 00 70 00 20 00 6F 00 72 00 20
00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 2C
00 20 00
61 00 70 00 70 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 75 00 73 00 65 00 20 00 74 00 68 00 69 00 73 00 20 00 64 00 61
00 74 00 61 00 20 00 6D 00 69 00 67 00 68 00 74 00 20 00 6E 00 6F 00 74 00 20 00 77 00 6F 00 72 00 6B 00 20 00 63 00 6F 00 72
00 72 00 65 00 63 00 74 00 6C 00 79 00 2E 00 00 00 00 00
HKU\DEFAULT\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\WpnUserService.dll,-2:
"This service hosts Windows notification platform which provides support for local and push notifications. Supported
notifications are tile, toast and raw."
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Multimedia\msacm.imaadpcm\MaxRTEncodeSetting: 0x00000006
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Multimedia\msacm.imaadpcm\MaxRTDecodeSetting: 0x00000006
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Multimedia\msacm.msgsm610\MaxRTEncodeSetting: 0x00000004

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\MrtCache\C:%5CProgram Files%5CWindowsApps%5CMicrosoft.ScreenSketch_10.2008.2277.0_x64__8wekyb3d8bbwe%5Cmicrosoft.system.package.meta data%5CS-1-5-21-2169232433-3398496680-935370409-1000-MergedResources-1.pri\1d94a4e31595da\fae8ab0e@\{Microsoft.ScreenSketch_10.2008.2277.0_x64__8wekyb3d8bbwe?ms-resource://Microsoft.ScreenSketch/Resources/AppDescription}: "Snip & Sketch"

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\MrtCache\C:%5CWindows%5CSystemApps%5CShellExperienceHost_cw5n1h2txyewy%5Cresources.pri\1d57cbad338cb4e\4a01460c8@\{Microsoft.Windows.ShellExperienceHost_10.0.18362.387_neutral_neutral_cw5n1h2txyewy?ms-resource://Microsoft.Windows.ShellExperienceHost/resources/AppDescription}: "Windows Shell Experience Host"

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\windows.storage.dll,-9012: "Computer"

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AU\App\V1\LU\PCT: 0x01D9777B93CE1585

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AU\App\V1\LU\PTT: 0x01D9777BBADED3C6

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1398x788x96(1).x: 0xFFFFFFFF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1398x788x96(1).y: 0xFFFFFFFF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MaxPos1398x788x96(1).x: 0xFFFFFFFF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MaxPos1398x788x96(1).y: 0xFFFFFFFF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1398x788x96(1).left: 0x000000E7

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1398x788x96(1).top: 0x00000063

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1398x788x96(1).right: 0x0000055A

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1398x788x96(1).bottom: 0x000002BB

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\MrtCache\C:%5CProgram Files%5CWindowsApps%5CMicrosoft.ScreenSketch_10.2008.2277.0_x64__8wekyb3d8bbwe%5Cmicrosoft.system.package.meta data%5CS-1-5-21-2169232433-3398496680-935370409-1000-MergedResources-1.pri\1d94a4e31595da\fae8ab0e@\{Microsoft.ScreenSketch_10.2008.2277.0_x64__8wekyb3d8bbwe?ms-resource://Microsoft.ScreenSketch/Resources/AppDescription}: "Snip & Sketch"

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\MrtCache\C:%5CWindows%5CSystemApps%5CShellExperienceHost_cw5n1h2txyewy%5Cresources.pri\1d57cbad338cb4e\4a01460c8@\{Microsoft.Windows.ShellExperienceHost_10.0.18362.387_neutral_neutral_cw5n1h2txyewy?ms-resource://Microsoft.Windows.ShellExperienceHost/resources/AppDescription}: "Windows Shell Experience Host"

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\windows.storage.dll,-9012: "Computer"

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AU\App\V1\LU\PCT: 0x01D9777B93CE1585

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.ScreenSketch_8wekyb3d8bbwe\HAM\AU\App\V1\LU\PTT: 0x01D9777BBADED3C6

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1398x788x96(1).x: 0xFFFFFFFF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MinPos1398x788x96(1).y: 0xFFFFFFFF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MaxPos1398x788x96(1).x: 0xFFFFFFFF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\MaxPos1398x788x96(1).y: 0xFFFFFFFF

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
 Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1398x788x96(1).left: 0x000000E7
 HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
 Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1398x788x96(1).top: 0x00000063
 HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
 Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1398x788x96(1).right: 0x0000055A
 HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
 Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\WinPos1398x788x96(1).bottom: 0x000002BB
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@C:\Windows\System32\ieframe.dll,-912: "HTML
 Document"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\diagtrack.dll,-3001:
 "Connected User Experiences and Telemetry"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@windows.storage.dll,-34583: "Saved Pictures"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@windows.storage.dll,-21824: "Camera Roll"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@C:\Program Files\Common Files\system\wab32res.dll,-
 10100: "Contacts"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@C:\Windows\System32\ieframe.dll,-12385: "Favorites
 Bar"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@windows.storage.dll,-21825: "3D Objects"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@C:\Windows\System32\Windows.UI.Immersive.dll,-
 38304: "Public Account Pictures"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-15:
 "Balanced"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-14:
 "Automatically balances performance with energy consumption on capable hardware."
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-13: "High
 performance"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-12: "Favors
 performance, but may use more energy."
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-11: "Power
 saver"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\powrprof.dll,-10: "Saves
 energy by reducing your computer's performance where possible."
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\AJRouter.dll,-1: "Routes
 AllJoyn messages for the local AllJoyn clients. If this service is stopped the AllJoyn clients that do not have their own bundled
 routers will be unable to run."
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\Alg.exe,-113: "Provides
 support for 3rd party protocol plug-ins for Internet Connection Sharing"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\appidsvc.dll,-101:
 "Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced."
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\appinfo.dll,-101: "Facilitates
 the running of interactive applications with additional administrative privileges. If this service is stopped, users will be unable to
 launch applications with the additional administrative privileges they may require to perform desired user tasks."
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@appmgmts.dll,-3251: "Processes installation, removal,
 and enumeration requests for software deployed through Group Policy. If the service is disabled, users will be unable to install,
 remove, or enumerate software deployed through Group Policy. If this service is disabled, any services that explicitly depend on
 it will fail to start."
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\AppReadiness.dll,-1001:
 "Gets apps ready for use the first time a user signs in to this PC and when adding new apps."
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\AppVClient.exe,-101:
 "Manages App-V users and virtual applications"
 HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\appxdeploymentserver.dll,-
 2: "Provides infrastructure support for deploying Store applications. This service is started on demand and if disabled Store
 applications will not be deployed to the system, and may not function properly."
 HKU\S-1-5-18\Software\Classes\Local
 Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\assignedaccessmanagersvc.dll,-101: "AssignedAccessManager
 Service supports kiosk experience in Windows."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\AudioEndpointBuilder.dll,-205: "Manages audio devices for the Windows Audio service. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\audiosrv.dll,-201: "Manages audio for Windows-based programs. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\autotimesvc.dll,-7: "This service sets time based on NITZ messages from a Mobile Network"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\AxInstSV.dll,-104: "Provides User Account Control validation for the installation of ActiveX controls from the Internet and enables management of ActiveX control installation based on Group Policy settings. This service is started on demand and if disabled the installation of ActiveX controls will behave according to default browser settings."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\bdesvc.dll,-101: "BDESVC hosts the BitLocker Drive Encryption service. BitLocker Drive Encryption provides secure startup for the operating system, as well as full volume encryption for OS, fixed or removable volumes. This service allows BitLocker to prompt users for various actions related to their volumes when mounted, and unlocks volumes automatically without user interaction. Additionally, it stores recovery information to Active Directory, if available, and, if necessary, ensures the most recent recovery certificates are used. Stopping or disabling the service would prevent users from leveraging this functionality."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\bfe.dll,-1002: "The Base Filtering Engine (BFE) is a service that manages firewall and Internet Protocol security (IPsec) policies and implements user mode filtering. Stopping or disabling the BFE service will significantly reduce the security of the system. It will also result in unpredictable behavior in IPsec management and firewall applications."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\bisrv.dll,-101: "Windows infrastructure service that controls which background tasks can run on the system."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\BTAGService.dll,-102: "Service supporting the audio gateway role of the Bluetooth Handsfree Profile."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\BthAvctpSvc.dll,-102: "This is Audio Video Control Transport Protocol service"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\bthserv.dll,-102: "The Bluetooth service supports discovery and association of remote Bluetooth devices. Stopping or disabling this service may cause already installed Bluetooth devices to fail to operate properly and prevent new devices from being discovered or associated."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\CapabilityAccessManager.dll,-2: "Provides facilities for managing UWP apps access to app capabilities as well as checking an app's access to specific app capabilities"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\cdpsvc.dll,-101: "This service is used for Connected Devices Platform scenarios"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\certprop.dll,-12: "Copies user certificates and root certificates from smart cards into the current user's certificate store, detects when a smart card is inserted into a smart card reader, and, if needed, installs the smart card Plug and Play minidriver."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ClipSVC.dll,-104: "Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled applications bought using Windows Store will not behave correctly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@comres.dll,-948: "Manages the configuration and tracking of Component Object Model (COM)+-based components. If the service is stopped, most COM+-based components will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\coremessaging.dll,-2: "Manages communication between system components."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\cryptsvc.dll,-1002: "Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows new programs to be installed; Protected Root Service, which adds and removes Trusted Root Certification Authority certificates from this computer; and Automatic Root Certificate Update Service, which retrieves root certificates from Windows Update and enable scenarios such as SSL. If this service is stopped, these management services will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\cscsvc.dll,-201: "The Offline Files service performs maintenance activities on the Offline Files cache, responds to user logon and logoff events, implements the internals of the public API, and dispatches interesting events to those interested in Offline Files activities and changes in cache state."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@combase.dll,-5013: "The DCOMLAUNCH service launches COM and DCOM servers in response to object activation requests. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the DCOMLAUNCH service running."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\defragsvc.dll,-102: "Helps the computer run more efficiently by optimizing files on storage drives."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\das.dll,-101: "Enables pairing between the system and wired or wireless devices."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\umpnpgmgr.dll,-101: "Enables a computer to recognize and adapt to hardware changes with little or no user input. Stopping or disabling this service will result in system instability."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\DevQueryBroker.dll,-101: "Enables apps to discover devices with a background task"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\dhcpcore.dll,-101: "Registers and updates IP addresses and DNS records for this computer. If this service is stopped, this computer will not receive dynamic IP addresses and DNS updates. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\DiagSvc\DiagnosicsHub.StandardCollector.ServiceRes.dll,-1001: "Diagnostics Hub Standard Collector Service. When running, this service collects real time ETW events and processes them."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\DiagSvc.dll,-101: "Executes diagnostic actions for troubleshooting support"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\diagtrack.dll,-3002: "The Connected User Experiences and Telemetry service enables features that support in-application and connected user experiences. Additionally, this service manages the event driven collection and transmission of diagnostic and usage information (used to improve the experience and quality of the Windows Platform) when the diagnostics and usage privacy option settings are enabled under Feedback and Diagnostics."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\dispbroker.desktop.dll,-102: "Manages the connection and configuration of local and remote displays"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\Microsoft.Graphics.Display.DisplayEnhancementService.dll,-1001: "A service for managing display enhancement such as brightness control."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\Windows.Internal.Management.dll,-101: "Performs Device Enrollment Activities for Device Management"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\dmwappushsvc.dll,-201: "Routes Wireless Application Protocol (WAP) Push messages received by the device and synchronizes Device Management sessions"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\dnsapi.dll,-102: "The DNS Client service (dnscache) caches Domain Name System (DNS) names and registers the full computer name for this computer. If the service is stopped, DNS names will continue to be resolved. However, the results of DNS name queries will not be cached and the computer's name will not be registered. If the service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\dot3svc.dll,-1103: "The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\dps.dll,-501: "The Diagnostic Policy Service enables problem detection, troubleshooting and resolution for Windows components. If this service is stopped, diagnostics will no longer function."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\DeviceSetupManager.dll,-1001: "Enables the detection, download and installation of device-related software. If this service is disabled, devices may be configured with outdated software, and may not work correctly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\dssvc.dll,-10002: "Provides data brokering between applications."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\dusmsvc.dll,-2: "Network data usage, data limit, restrict background data, metered networks."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\eapsvc.dll,-2: "The Extensible Authentication Protocol (EAP) service provides network authentication in such scenarios as 802.1x wired and wireless, VPN, and Network Access Protection (NAP). EAP also provides application programming interfaces (APIs) that are used by

network access clients, including wireless and VPN clients, during the authentication process. If you disable this service, this computer is prevented from accessing networks that require EAP authentication."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\efssvc.dll,-101: "Provides the core file encryption technology used to store encrypted files on NTFS file system volumes. If this service is stopped or disabled, applications will be unable to access encrypted files."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\embeddedmodesvc.dll,-202: "The Embedded Mode service enables scenarios related to Background Applications. Disabling this service will prevent Background Applications from being activated."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@EnterpriseAppMgmtSvc.dll,-2: "Enables enterprise application management."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wevtvc.dll,-201: "This service manages events and event logs. It supports logging events, querying events, subscribing to events, archiving event logs, and managing event metadata. It can display events in both XML and plain text format. Stopping this service may compromise security and reliability of the system."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@comres.dll,-2451: "Supports System Event Notification Service (SENS), which provides automatic distribution of events to subscribing Component Object Model (COM) components. If the service is stopped, SENS will close and will not be able to provide logon and logoff notifications. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\fxsresm.dll,-122: "Enables you to send and receive faxes, utilizing fax resources available on this computer or on the network."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\fdpHost.dll,-101: "The FDPHOST service hosts the Function Discovery (FD) network discovery providers. These FD providers supply network discovery services for the Simple Services Discovery Protocol (SSDP) and Web Services – Discovery (WS-D) protocol. Stopping or disabling the FDPHOST service will disable network discovery for these protocols when using FD. When this service is unavailable, network services using FD and relying on these discovery protocols will be unable to find network devices or resources."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\fdrespub.dll,-101: "Publishes this computer and resources attached to this computer so they can be discovered over the network. If this service is stopped, network resources will no longer be published and they will not be discovered by other computers on the network."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\fhsvc.dll,-102: "Protects user files from accidental loss by copying them to a backup location"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\FntCache.dll,-101: "Optimizes performance of applications by caching commonly used font data. Applications will start this service if it is not already running. It can be disabled, though doing so will degrade application performance."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\PresentationHost.exe,-3310: "Optimizes performance of Windows Presentation Foundation (WPF) applications by caching commonly used font data. WPF applications will start this service if it is not already running. It can be disabled, though doing so will degrade the performance of WPF applications."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\FramerServer.dll,-101: "Enables multiple clients to access video frames from camera devices."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@gpapi.dll,-113: "The service is responsible for applying settings configured by administrators for the computer and users through the Group Policy component. If the service is disabled, the settings will not be applied and applications and components will not be manageable through Group Policy. Any components or applications that depend on the Group Policy component might not be functional if the service is disabled."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\GraphicsPerfSvc.dll,-101: "Graphics performance monitor service"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\hidserv.dll,-102: "Activates and maintains the use of hot buttons on keyboards, remote controls, and other multimedia devices. It is recommended that you keep this service running."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\hvhostsvc.dll,-101: "Provides an interface for the Hyper-V hypervisor to provide per-partition performance counters to the host operating system."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\tetheringservice.dll,-4098: "Provides the ability to share a cellular data connection with another device."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ikeext.dll,-502: "The IKEEXT service hosts the Internet Key Exchange (IKE) and Authenticated Internet Protocol (AuthIP) keying modules. These keying modules are used for authentication and key exchange in Internet Protocol security (IPsec). Stopping or disabling the IKEEXT service will disable IKE and AuthIP key exchange with peer computers. IPsec is typically configured to use IKE or AuthIP; therefore, stopping or disabling the IKEEXT service might result in an IPsec failure and might compromise the security of the system. It is strongly recommended that you have the IKEEXT service running."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\InstallService.dll,-201: "Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled then installations will not function properly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\iphlpvc.dll,-501: "Provides tunnel connectivity using IPv6 transition technologies (6to4, ISATAP, Port Proxy, and Teredo), and IP-HTTPS. If this service is stopped, the computer will not have the enhanced connectivity benefits that these technologies offer."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\ipxlatcfg.dll,-501: "Configures and enables translation from v4 to v6 and vice versa"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@keyiso.dll,-101: "The CNG key isolation service is hosted in the LSA process. The service provides key process isolation to private keys and associated cryptographic operations as required by the Common Criteria. The service stores and uses long-lived keys in a secure process complying with Common Criteria requirements."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@comres.dll,-2947: "Coordinates transactions between the Distributed Transaction Coordinator (MSDTC) and the Kernel Transaction Manager (KTM). If it is not needed, it is recommended that this service remain stopped. If it is needed, both MSDTC and KTM will start this service automatically. If this service is disabled, any MSDTC transaction interacting with a Kernel Resource Manager will fail and any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\srvc.dll,-101: "Supports file, print, and named-pipe sharing over the network for this computer. If this service is stopped, these functions will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wkssvc.dll,-101: "Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\lfsvc.dll,-2: "This service monitors the current location of the system and manages geofences (a geographical location with associated events). If you turn off this service, applications will be unable to use or receive notifications for geolocation or geofences."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\licensemanagersvc.dll,-201: "Provides infrastructure support for the Microsoft Store. This service is started on demand and if disabled then content acquired through the Microsoft Store will not function properly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ltdres.dll,-2: "Creates a Network Map, consisting of PC and device topology (connectivity) information, and metadata describing each PC and device. If this service is disabled, the Network Map will not function properly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\lmhsvc.dll,-102: "Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients on the network, therefore enabling users to share files, print, and log on to the network. If this service is stopped, these functions might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\lsm.dll,-1002: "Core Windows Service that manages local user sessions. Stopping or disabling this service will result in system instability."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\LanguageOverlayServer.dll,-101: "Provides infrastructure support for deploying and configuring localized Windows resources. This service is started on demand and, if disabled, additional Windows languages will not be deployed to the system, and Windows may not function properly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\moshost.dll,-101: "Windows service for application access to downloaded maps. This service is started on-demand by application accessing downloaded maps. Disabling this service will prevent apps from accessing maps."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\FirewallAPI.dll,-23091: 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6E 00 64 00 65 00 72 00 20 00 46 00 69 00 72 00 65 00 77 00 61 00 6C 00 6C 00 20 00 68 00 65 00 6C 00 70 00 73 00 20 00 70 00 72 00 6F 00 74 00 65 00 63 00 74 00 20 00 79 00 6F 00 75 00 72 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 20 00 62 00 79 00 20 00 70 00 72 00 65 00 76 00 65 00 6E 00 74 00 69 00 6E 00 67 00 20 00 75 00 6E 00 61 00 75 00 74 00 68 00 6F 00 72 00 69 00 7A 00 65 00 64 00 20 00 75 00 73 00 65 00 72 00 73 00 20 00 66 00 72 00 6F 00 6D 00 20 00 67 00 61 00 69 00 6E 00 69 00 6E 00 67 00 20 00 61 00 63 00 63 00 65 00 73 00 73 00 20 00 74 00 6F 00 20 00 79 00 6F 00 75 00 72 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 20 00 74 00 68 00 72 00 0F 00 75 00 67 00 68 00 20 00 74 00 68 00 65 00 20 00 49 00 6E 00 74 00 65 00 72 00 6E 00 65 00 74 00 20 00 6F 00 72 00 20 00 61 00 20 00 6E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 2E 00 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@comres.dll,-2798: "Coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. If this service is stopped, these transactions will fail. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\iscsidsc.dll,-5001: "Manages Internet SCSI (iSCSI) sessions from this computer to remote iSCSI target devices. If this service is stopped, this computer will not be able to login or access iSCSI targets. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\msimsg.dll,-32: "Adds, modifies, and removes applications provided as a Windows Installer (*.msi, *.msp) package. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\NaturalAuth.dll,-101: "Signal aggregator service, that evaluates signals based on time, network, geolocation, bluetooth and cdf factors. Supported features are Device Unlock, Dynamic Lock and Dynamo MDM policies"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ncasvc.dll,-3008: "Provides DirectAccess status notification for UI components"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ncbservice.dll,-501: "Brokers connections that allow Windows Store Apps to receive notifications from the internet."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\NcdAutoSetup.dll,-101: "Network Connected Devices Auto-Setup service monitors and installs qualified devices that connect to a qualified network. Stopping or disabling this service will prevent Windows from discovering and installing qualified network connected devices automatically. Users can still manually add network connected devices to a PC through the user interface."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\netlogon.dll,-103: "Maintains a secure channel between this computer and the domain controller for authenticating users and services. If this service is stopped, the computer may not authenticate users and services and the domain controller cannot register DNS records. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\netman.dll,-110: 4D 00 61 00 6E 00 61 00 67 00 65 00 73 00 20 00 6F 00 62 00 6A 00 65 00 63 00 74 00 73 00 20 00 69 00 6E 00 20 00 74 00 68 00 65 00 20 00 4E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 20 00 61 00 6E 00 64 00 20 00 44 00 69 00 61 00 6C 00 2D 00 55 00 70 00 20 00 43 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 73 00 20 00 66 00 6F 00 6C 00 64 00 65 00 72 00 2C 00 20 00 69 00 6E 00 20 00 77 00 68 00 69 00 63 00 68 00 20 00 79 00 6F 00 75 00 20 00 63 00 61 00 6E 00 20 00 76 00 69 00 65 00 77 00 20 00 62 00 6F 00 74 00 68 00 20 00 6C 00 6F 00 63 00 61 00 6C 00 20 00 61 00 72 00 65 00 61 00 20 00 6E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 20 00 61 00 6E 00 64 00 20 00 72 00 65 00 6D 00 6F 00 74 00 65 00 20 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 69 00 6F 00 6E 00 73 00 2E 00 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\netprofmsvc.dll,-203: 49 00 64 00 65 00 6E 00 74 00 69 00 66 00 69 00 65 00 73 00 20 00 74 00 68 00 65 00 20 00 6E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 73 00 20 00 74 00 6F 00 20 00 77 00 68 00 69 00 63 00 68 00 20 00 74 00 68 00 65 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 20 00 68 00 61 00 73 00 20 00 63 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 65 00 64 00 2C 00 20 00 63 00 6F 00 6C 00 6C 00 65 00 63 00 74 00 73 00 20 00 61 00 6E 00 64 00 20 00 73 00 74 00 6F 00 72 00 65 00 73 00 20 00 70 00 72 00 6F 00 70 00 65 00 72 00 74 00 69 00 65 00 73 00 20 00 66 00 6F 00 72 00 20 00 74 00 68 00 65 00 73 00 65 00 20 00 6E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 73 00 2C 00 20 00 61 00 6E 00 64 00 20 00 6E 00 6F 00 74 00 69 00 66 00 69 00 65 00 73 00 20 00 61 00 70 00 70 00 6C 00 69 00 63 00 61 00 74 00 69 00 6F 00 6E 00 73 00 20 00 77 00 68 00 65 00 6E 00 20 00 74 00 68 00 65 00 73 00 65 00 2

0 00 70 00 72 00 6F 00 70 00 65 00 72 00 74 00 69 00 65 00 73 00 20 00 63 00 68 00 61 00 6E 00 67 00 65 00 2E 00 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\NetSetupSvc.dll,-4: "The Network Setup Service manages the installation of network drivers and permits the configuration of low-level network settings. If this service is stopped, any driver installations that are in-progress may be cancelled."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\Microsoft.NET\Framework64\v4.0.30319\ServiceModelInstallRC.dll,-8200: "Provides ability to share TCP ports over the net.tcp protocol."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\NgcCtnrSvc.dll,-2: "Manages local user identity keys used to authenticate user to identity providers as well as TPM virtual smart cards. If this service is disabled, local user identity keys and TPM virtual smart cards will not be accessible. It is recommended that you do not reconfigure this service."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\ngcsvc.dll,-101: "Provides process isolation for cryptographic keys used to authenticate to a user's associated identity providers. If this service is disabled, all uses and management of these keys will not be available, which includes machine logon and single-sign on for apps and websites. This service starts and stops automatically. It is recommended that you do not reconfigure this service."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\nlasvc.dll,-2: "Collects and stores configuration information for the network and notifies programs when this information is modified. If this service is stopped, configuration information might be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\nsisvc.dll,-201: "This service delivers network notifications (e.g. interface addition/deleting etc) to user mode clients. Stopping this service will cause loss of network connectivity. If this service is disabled, any other services that explicitly depend on this service will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\pnrpsvc.dll,-8005: "Provides identity services for the Peer Name Resolution Protocol (PNRP) and Peer-to-Peer Grouping services. If disabled, the Peer Name Resolution Protocol (PNRP) and Peer-to-Peer Grouping services may not function, and some applications, such as HomeGroup and Remote Assistance, may not function correctly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\p2psvc.dll,-8007: "Enables multi-party communication using Peer-to-Peer Grouping. If disabled, some applications, such as HomeGroup, may not function."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\pcasvc.dll,-2: "This service provides support for the Program Compatibility Assistant (PCA). PCA monitors programs installed and run by the user and detects known compatibility problems. If this service is stopped, PCA will not function properly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\peerdistsvc.dll,-9001: "This service caches network content from peers on the local subnet."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\PerceptionSimulation\PerceptionSimulationService.exe,-102: "Enables spatial perception simulation, virtual camera management and spatial input simulation."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\SysWow64\perfhost.exe,-1: "Enables remote users and 64-bit processes to query performance counters provided by 32-bit DLLs. If this service is stopped, only local users and 32-bit processes will be able to query performance counters provided by 32-bit DLLs."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\PhonereserviceRes.dll,-10001: 4D 00 61 00 6E 00 61 00 67 00 65 00 73 00 20 00 74 00 68 00 65 00 20 00 74 00 65 00 6C 00 65 00 70 00 68 00 6F 00 6E 00 79 00 20 00 73 00 74 00 61 00 74 00 65 00 20 00 6F 00 6E 00 20 00 74 00 68 00 65 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\pla.dll,-501: "Performance Logs and Alerts Collects performance data from local or remote computers based on preconfigured schedule parameters, then writes the data to a log or triggers an alert. If this service is stopped, performance information will not be collected. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\pnrpauto.dll,-8003: "This service publishes a machine name using the Peer Name Resolution Protocol. Configuration is managed via the netsh context 'p2p pnrp peer' "

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\pnrpsvc.dll,-8001: "Enables serverless peer name resolution over the Internet using the Peer Name Resolution Protocol (PNRP). If disabled, some peer-to-peer and collaborative applications, such as Remote Assistance, may not function."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\polstore.dll,-5011: "Internet Protocol security (IPsec) supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection. This service enforces IPsec policies created through the IP Security Policies snap-in or the command-line tool "netsh ipsec". If you stop this service, you may experience network connectivity issues if your policy requires that connections use IPsec. Also,remote management of Windows Defender Firewall is not available when this service is stopped."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\umpo.dll,-101: "Manages power policy and power policy notification delivery."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll,-2: "This service opens custom printer dialog boxes and handles notifications from a remote print server or a printer. If you turn off this service, you won't be able to see printer extensions or notifications."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\profsvc.dll,-301: "This service is responsible for loading and unloading user profiles. If this service is stopped or disabled, users will no longer be able to successfully sign in or sign out, apps might have problems getting to users' data, and components registered to receive profile event notifications won't receive them."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\pushtoinstall.dll,-201: "Provides infrastructure support for the Microsoft Store. This service is started automatically and if disabled then remote installations will not function properly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\qwwave.dll,-2: "Quality Windows Audio Video Experience (qWave) is a networking platform for Audio Video (AV) streaming applications on IP home networks. qWave enhances AV streaming performance and reliability by ensuring network quality-of-service (QoS) for AV applications. It provides mechanisms for admission control, run time monitoring and enforcement, application feedback, and traffic prioritization."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\rasauto.dll,-201: "Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\rasmans.dll,-201: "Manages dial-up and virtual private network (VPN) connections from this computer to the Internet or other remote networks. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\mprdim.dll,-201: "Offers routing services to businesses in local area and wide area network environments."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%Systemroot%\system32\regsvc.dll,-2: "Enables remote users to modify registry settings on this computer. If this service is stopped, the registry can be modified only by users on this computer. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\RDService.dll,-257: "The Retail Demo service controls device activity while the device is in retail demo mode."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\RMapi.dll,-1002: 52 00 61 00 64 00 69 00 6F 00 20 00 4D 00 61 00 6E 00 61 00 67 00 65 00 6D 00 65 00 6E 00 74 00 20 00 61 00 6E 00 64 00 20 00 41 00 69 00 72 00 70 00 6C 00 61 00 6E 00 65 00 20 00 4D 00 6F 00 64 00 65 00 20 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\RpcEpMap.dll,-1002: "Resolves RPC interfaces identifiers to transport endpoints. If this service is stopped or disabled, programs using Remote Procedure Call (RPC) services will not function properly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\Locator.exe,-3: "In Windows 2003 and earlier versions of Windows, the Remote Procedure Call (RPC) Locator service manages the RPC name service database. In Windows Vista and later versions of Windows, this service does not provide any functionality and is present for application compatibility."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@combase.dll,-5011: "The RPCSS service is the Service Control Manager for COM and DCOM servers. It performs object activations requests, object exporter resolutions and distributed garbage collection for COM and DCOM servers. If this service is stopped or disabled, programs using COM or DCOM will not function properly. It is strongly recommended that you have the RPCSS service running."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\samsrv.dll,-2: "The startup of this service signals other services that the Security Accounts Manager (SAM) is ready to accept requests. Disabling this service will prevent other services in the system from being notified when the SAM is ready, which may in turn cause those services to fail to start correctly. This service should not be disabled."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\SCardSvr.dll,-5: "Manages access to smart cards read by this computer. If this service is stopped, this computer will be unable to read smart cards. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\ScDeviceEnum.dll,-101: "Creates software device nodes for all smart card readers accessible to a given session. If this service is disabled, WinRT APIs will not be able to enumerate smart card readers."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\schedsvc.dll,-101: "Enables a user to configure and schedule automated tasks on this computer. The service also hosts multiple Windows system-critical tasks. If this service is stopped or disabled, these tasks will not be run at their scheduled times. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\certprop.dll,-14: "Allows the system to be configured to lock the user desktop upon smart card removal."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\sdrsvc.dll,-102: "Provides Windows Backup and Restore capabilities."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\seclogon.dll,-7000: "Enables starting processes under alternate credentials. If this service is stopped, this type of logon access will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\SecurityHealthAgent.dll,-1001: "Windows Security Service handles unified device protection and health information"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\SEMgrSvc.dll,-1002: "Manages payments and Near Field Communication (NFC) based secure elements."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\Sens.dll,-201: "Monitors system events and notifies subscribers to COM+ Event System of these events."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%ProgramFiles%\Windows Defender Advanced Threat Protection\MsSense.exe,-1002: "Windows Defender Advanced Threat Protection service helps protect against advanced threats by monitoring and reporting security events that happen on the computer."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\SensorDataService.exe,-102: "Delivers data from a variety of sensors"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\sensorservice.dll,-1001: "A service for sensors that manages different sensors' functionality. Manages Simple Device Orientation (SDO) and History for sensors. Loads the SDO sensor that reports device orientation changes. If this service is stopped or disabled, the SDO sensor will not be loaded and so auto-rotation will not occur. History collection from Sensors will also be stopped."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\sensrsvc.dll,-1001: "Monitors various sensors in order to expose data and adapt to system and user state. If this service is stopped or disabled, the display brightness will not adapt to lighting conditions. Stopping this service may affect other system functionality and features as well."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\SessEnv.dll,-1027: "Remote Desktop Configuration service (RDCS) is responsible for all Remote Desktop Services and Remote Desktop related configuration and session maintenance activities that require SYSTEM context. These include per-session temporary folders, RD themes, and RD certificates."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\SgrmBroker.exe,-101: "Monitors and attests to the integrity of the Windows platform."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ipnathlp.dll,-107: "Provides network address translation, addressing, name resolution and/or intrusion prevention services for a home or small office network."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\SharedRealitySvc.dll,-101: "This service is used for Spatial Perception scenarios"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\shsvcs.dll,-12289: "Provides notifications for AutoPlay hardware events."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\Windows.SharedPC.AccountManager.dll,-101: "Manages profiles and accounts on a SharedPC configured device"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\smphost.dll,-101: "Host service for the Microsoft Storage Spaces management provider. If this service is stopped or disabled, Storage Spaces cannot be managed."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\SmsRouterSvc.dll,-10002: "Routes messages based on rules to appropriate clients."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@firewallapi.dll,-50324: 52 00 65 00 63 00 65 00 69 00 76 00 65 00 73 00 20 00 74 00 72 00 61 00 70 00 20 00 6D 00 65 00 73 00 61 00 67 00 65 00 73 00 20 00 67 00 65 00 6E 00 65 00 72 00 61 00 74 00 65 00 64 00 20 00 62 00 79 00 20 00 6C 00 6F 00 63 00 61 00 6C 00 20 00 6F 00 72 00 20 00 72 00 65 00 6D 00 6F 00 74 00 65 00 20 00 53 00 69 00 6D 00 70 00 6C 00 65 00 20 00 4E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 20 00 4D 00 61 00 6E 00 61 00 67 00 65 00 6D 00 65 00 6E 00 74 00 20 00 50 00 72 00 6F 00 74 00 6F 00 63 00 6F 00 6C 00 20 00 28 00 53 00 4E 00 4D 00 50 00 29 00 20 00 61 00 67 00 65 00 6E 00 74 00 73 00 20 00 61 00 6E 00 64 00 20 00 66 00 6F 00 72 00 77 00 61 00 72 00 64 00 73 00 20 00 74 00 68 00 65 00 20 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 73 00 20 00 74 00 6F 00 20 00 53 00 4E 00 4D 00 50 00 20 00 6D 00 61 00 6E 00 61 00 67 00 65 00 6D 00 65 00 6E 00 74 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 73 00 20 00 72 00 75 00 6E 00 6E 00 69 00 6E 00 67 00 20 00 6F 00 6E 00 20 00 74 00 68 00 69 00 73 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 73 00 74 00 6F 00 70 00 70 00 65 00 64 00 2C 00 20 00 53 00 4E 00 4D 00 50 00 2D 00 62 00 61 00 73 00 65 00 64 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 73 00 20 00 6F 00 6E 00 20 00 74 00 68 00 69 00 73 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 20 00 77 00 69 00 6C 00 6C 00 20 00 6E 00 6F 00 74 00 20 00 72 00 65 00 63 00 65 00 69 00 76 00 65 00 20 00 53 00 4E 00 4D 00 50 00 20 00 74 00 72 00 61 00 70 00 20 00 6D 00 65 00 73 00 73 00 61 00 67 00 65 00 73 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 64 00 2C 00 20 00 61 00 6E 00 79 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 65 00 78 00 70 00 6C 00 69 00 63 00 69 00 74 00 6C 00 79 00 20 00 64 00 65 00 70 00 65 00 6E 00 64 00 20 00 6F 00 6E 00 20 00 69 00 74 00 20 00 77 00 69 00 6C 00 6C 00 20 00 66 00 61 00 69 00 6C 00 20 00 74 00 6F 00 20 00 73 00 74 00 61 00 72 00 74 00 2E 00 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\spectrum.exe,-102: "Enables spatial perception, spatial input, and holographic rendering."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\spoolsv.exe,-2: "This service spools print jobs and handles interaction with the printer. If you turn off this service, you won't be able to print or see your printers."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\spssvc.exe,-100: "Enables the download, installation and enforcement of digital licenses for Windows and Windows applications. If the service is disabled,

the operating system and licensed applications may run in a notification mode. It is strongly recommended that you not disable the Software Protection service."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\ssdpsrv.dll,-101: 44 00 69 00 73 00 63 00 6F 00 76 00 65 00 72 00 73 00 20 00 6E 00 65 00 74 00 77 00 6F 00 72 00 6B 00 65 00 64 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 61 00 6E 00 64 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 75 00 73 00 65 00 20 00 74 00 68 00 65 00 20 00 53 00 53 00 44 00 50 00 20 00 64 00 69 00 73 00 63 00 6F 00 76 00 65 00 72 00 79 00 20 00 70 00 72 00 6F 00 74 00 6F 00 63 00 6F 00 6C 00 2C 00 20 00 73 00 75 00 63 00 68 00 20 00 61 00 73 00 20 00 55 00 50 00 6E 00 50 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 2E 00 20 00 41 00 6C 00 73 00 6F 00 20 00 61 00 6E 00 6E 00 6F 00 75 00 6E 00 63 00 65 00 73 00 20 00 53 00 53 00 44 00 50 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 61 00 6E 00 64 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 72 00 75 00 6E 00 6E 00 69 00 6E 00 67 00

20 00 6F 00 6E 00 20 00 74 00 68 00 65 00 20 00 6C 00 6F 00 63 00 61 00 6C 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 73 00 74 00 6F 00 70 00 70 00 65 00 64 00 2C 00 20 00 53 00 53 00 44 00 50 00 2D 00 62 00 61 00 73 00 65 00 64 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 77 00 69 00 6C 00 6C 00 20 00 6E 00 6F 00 74 00 20 00 62 00 65 00 20 00 64 00 69 00 73 00 63 00 6F 00 76 00 65 00 72 00 65 00 64 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 64 00 2C 00 20 00 61 00 6E 00 79 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 65 00 78 00 70 00 6C 00 69 00 63 00 69 00 74 00 6C 00 79 00 20 00 64 00 65 00 70 00 65 00 6E 00 64 00 20 00 6F 00 6E 00 20 00 69 00 74 00 20 00 77 00 69 00 6C 00 6C 00 20 00 66 00 61 00 69 00 6C 00 20 00 74 00 6F 00 20 00 73 00 74 00 61 00 72 00 74 00 2E 00 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\sstpsvc.dll,-201: "Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\windows.staterepository.dll,-2: "Provides required infrastructure support for the application model."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wiaservc.dll,-10: "Provides image acquisition services for scanners and cameras"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\StorSvc.dll,-101: "Provides enabling services for storage settings and external storage expansion"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\svsvc.dll,-102: "Verifies potential file system corruptions."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\swprv.dll,-102: "Manages software-based volume shadow copies taken by the Volume Shadow Copy service. If this service is stopped, software-based volume shadow copies cannot be managed. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\sysmain.dll,-1001: "Maintains and improves system performance over time."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\SystemEventsBrokerServer.dll,-1002: "Coordinates execution of background work for WinRT application. If this service is stopped or disabled, then background work might not be triggered."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\TabSvc.dll,-101: "Enables Touch Keyboard and Handwriting Panel pen and ink functionality"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\tapisrv.dll,-10101:

"Provides Telephony API (TAPI) support for programs that control telephony devices on the local computer and, through the LAN, on servers that are also running the service."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\termsrv.dll,-267: "Allows users to connect interactively to a remote computer. Remote Desktop and Remote Desktop Session Host Server depend on this service. To prevent remote use of this computer, clear the checkboxes on the Remote tab of the System properties control panel item."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\themeservice.dll,-8193: "Provides user experience theme management."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\TieringEngineService.exe,-701: "Optimizes the placement of data in storage tiers on all tiered storage spaces in the system."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%windir%\system32\TimeBrokerServer.dll,-1002: "Coordinates execution of background work for WinRT application. If this service is stopped or disabled, then background work might not be triggered."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\tokenbroker.dll,-101: "This service is used by Web Account Manager to provide single-sign-on to apps and services."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\trkws.dll,-2: "Maintains links between NTFS files within a computer or across computers in a network."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\MitigationClient.dll,-104: "Enables automatic mitigation for known problems by applying recommended troubleshooting. If stopped, your device will not get recommended troubleshooting for problems on your device."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\tzautoupdate.dll,-201: "Automatically sets the system time zone."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\AgentService.exe,-101: "Provides support for application and OS settings roaming"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\umrdp.dll,-1001: "Allows the redirection of Printers/Drives/Ports for RDP connections"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\upnphost.dll,-214: 41 00 6C 00 6C 00 6F 00 77 00 73 00 20 00 55 00 50 00 6E 00 50 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 6F 00 20 00 62 00 65 00 20 00 68 00 6F 00 73 00 74 00 65 00 64 00 20 00 6F 00 6E 00 20 00 74 00 68 00 69 00 73 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 73 00 74 00 6F 00 70 00 70 00 65 00 64 00 2C 00 20 00 61 00 6E 00 79 00 20 00 68 00 6F 00 73 00 74 00 65 00 64 00 20 00 55 00 50 00 6E 00 50 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 77 00 69 00 6C 00 6C 00 20 00 73 00 74 00 6F 00 70 00 20 00 66 00 75 00 6E 00 63 00 74 00 69 00 6F 00 6E 00 69 00 6E 00 67 00 20 00 61 00 6E 00 64 00 20 00 6E 00 6F 00 20 00 61 00 64 00 64 00 69 00 74 00 69 00 6F 00 6E 00 61 00 6C 00 20 00 68 00 6F 00 73 00 74 00 65 00 64 00 20 00 64 00 65 00 76 00 69 00 63 00 65 00 73 00 20 00 63 00 61 00 6E 00 20 00 62 00 65 00 20 00 61 00 64 00 64 00 65 00 64 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 64 00 2C 00 20 00 61 00 6E 00 79 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 65 00 78 00 70 00 6C 00 69 00 63 00 69 00 74 00 6C 00 79 00 20 00 64 00 65 00 70 00 65 00 6E 00 64 00 20 00 6F 00 6E 00 20 00 69 00 74 00 20 00 77 00 69 00 6C 00 6C 00 20 00 66 00 61 00 69 00 6C 00 20 00 74 00 6F 00 20 00 73 00 74 00 61 00 72 00 74 00 2E 00 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\usermgr.dll,-101: "User Manager provides the runtime components required for multi-user interaction. If this service is stopped, some applications may not operate correctly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\vac.dll,-201: "Hosts spatial analysis for Mixed Reality audio simulation."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\vaultsvc.dll,-1004: "Provides secure storage and retrieval of credentials to users, applications and security service packages."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\vds.exe,-112: "Provides management services for disks, volumes, file systems, and storage arrays."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-802: "Provides an interface for the Hyper-V host to interact with specific services running inside the virtual machine."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-102: "Monitors the state of this virtual machine by reporting a heartbeat at regular intervals. This service helps you identify running virtual machines that have stopped responding."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-202: "Provides a mechanism to exchange data between the virtual machine and the operating system running on the physical computer."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvcext.dll,-602: "Provides a platform for communication between the virtual machine and the operating system running on the physical computer."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-302: "Provides a mechanism to shut down the operating system of this virtual machine from the management interfaces on the physical computer."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-402: "Synchronizes the system time of this virtual machine with the system time of the physical computer."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvc.dll,-902: "Provides a mechanism to manage virtual machine with PowerShell via VM session without a virtual network."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\icsvcext.dll,-502: "Coordinates the communications that are required to use Volume Shadow Copy Service to back up applications and data on this virtual machine from the operating system on the physical computer."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\vssvc.exe,-101: "Manages and implements Volume Shadow Copies used for backup and other purposes. If this service is stopped, shadow copies will be unavailable for backup and the backup may fail. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\w32time.dll,-201: "Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\WalletService.dll,-1001: "Hosts objects used by clients of the wallet"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\Windows.WARP.JITService.dll,-101: "Provides a JIT out of process service for WARP when running with ACG enabled."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wbengine.exe,-105: "The WBENGINE service is used by Windows Backup to perform backup and recovery operations. If this service is stopped by a user, it may cause the currently running backup or recovery operation to fail. Disabling this service may disable backup and recovery operations using Windows Backup on this computer."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wbiosvc.dll,-101: "The Windows biometric service gives client applications the ability to capture, compare, manipulate, and store biometric data without gaining direct access to any biometric hardware or samples. The service is hosted in a privileged SVCHOST process."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wcmshvc.dll,-4098: "Makes automatic connect/disconnect decisions based on the network connectivity options currently available to the PC and enables management of network connectivity based on Group Policy settings."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wcnscvc.dll,-4: 57 00 43 00 4E 00 43 00 53 00 56 00 43 00 20 00 68 00 6F 00 73 00 74 00 73 00 20 00 74 00 68 00 65 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 20 00 43 00 6F 00 6E 00 6E 00 65 00 63 00 74 00 20 00 4E 00 6F 00 77 00 20 00 43 00 6F 00 6E 00 66 00 69 00 67 00 75 00 72 00 61 00 74 00 69 00 6F 00 6E 00 20 00 77 00 68 00 69 00 63 00 68 00 20 00 69 00 73 00 20 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 27 00 73 00 20 00 49 00 6D 00 70 00 6C 00 65 00 6D 00 65 00 6E 00 74 00 61 00 74 00 69 00 6F 00 6E 00 20 00 6F 00 66 00 20 00 57 00 69 00 72 00 65 00 6C 00 65 00 73 00 73 00 20 00 50 00 72 00 6F 00 74 00 65 00 63 00 74 00 65 00 64 00 20 00 53 00 65 00 74 00 75 00 70 00 20 00 28 00 57 00 50 00 53 00 29 00 20 00 70 00 72 00 6F 00 74 00 6F 00 63 00 6F 00 6C 00 2E 00 20 00 54 00 68 00 69 00 73 00 20 00 69 00 73 00 20 00 75 00 73 00 65 00 64 00 20 00 74 00 6F 00 20 00 63 00 6F 00 6E 00 66 00 69 00 67 00 75 00 72 00 65 00 20 00 57 00 69 00 72 00 65 00 6C 00 65 00 73 00 73 00 20 00 4C 00 41 00 4E 00 20 00 73 00 65 00 74 00 74 00 69 00 6E 00 67 00 73 00 20 00 66 00 6F 00 72 00 20 00 61 00 6E 00 20 00 41 00 63 00 63 00 65 00 73 00 73 00 20 00 50 00 6F 00 69 00 6E 00 74 00 20 00 28 00 41 00 50 00 29 00 20 00 6F 00 72 00 20 00 61 00 20 00 57 00 69 00 72 00 65 00 6C 00 65 00 73 00 73 00 20 00 44 00 65 00 76 00 69 00 63 00 65 00 2E 00 20 00 54 00 68 00 65 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 73 00 74 00 61 00 72 00 74 00 65 00 64 00 20 00 70 00 72 00 6F 00 67 00 67 00 72 00 61 00 6D 00 6D 00 61 00 74 00 69 00 63 00 61 00 6C 00 6C 00 79 00 20 00 61 00 73 00 20 00 6E 00 65 00 65 00 64 00 65 00 64 00 2E 00 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wdi.dll,-503: "The Diagnostic Service Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local Service context. If this service is stopped, any diagnostics that depend on it will no longer function."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\wdi.dll,-501: "The Diagnostic System Host is used by the Diagnostic Policy Service to host diagnostics that need to run in a Local System context. If this service is stopped, any diagnostics that depend on it will no longer function."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-242: "Helps guard against intrusion attempts targeting known and newly discovered vulnerabilities in network protocols"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\webclnt.dll,-101: 45 00 6E 00 61 00 62 00 6C 00 65 00 73 00 20 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 2D 00 62 00 61 00 73 00 65 00 64 00 20 00 70 00 72 00 6F 00 67 00 72 00 61 00 6D 00 73 00 20 00 74 00 6F 00 20 00 63 00 72 00 65 00 61 00 74 00 65 00 2C 00 20 00 61 00 63 00 63 00 65 00 73 00 73 00 2C 00 20 00 61 00 6E 00 64 00 20 00 6D 00 6F 00 64 00 69 00 66 00 79 00 20 00 49 00 6E 00 74 00 65 00 72 00 6E 00 65 00 74 00 2D 00 62 00 61 00 73 00 65 00 64 00 20 00 66 00 69 00 6C 00 65 00 73 00 2E 00 20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 73 00 74 00 6F 00 70 00 70 00 65 00 64 00 2C 00 20 00 74 00 68 00 65 00 73 00 65 00 20 00 66 00 75 00 6E 00 63 00 74 00 69 00 6F 00 6E 00 73 00 20 00 77 00 69 00 6C 00 6C 00 20 00 66 00 61 00 69 00 6C 00 20 00 74 00 6F 00 20 00 63 00 00

20 00 49 00 66 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 20 00 69 00 73 00 20 00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 64 00 2C 00 20 00 61 00 6E 00 79 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 65 00 78 00 70 00 6C 00 69 00 63 00 69 00 74 00 6C 00 79 00 20 00 64 00 65 00 70 00 65 00 6E 00 64 00 20 00 6F 00 6E 00 20 00 69 00 74 00 20 00 77 00 69 00 6C 00 6C 00 20 00 66 00 61 00 69 00 6C 00 20 00 74 00 6F 00 20 00 73 00 74 00 61 00 72 00 74 00 2E 00 00 00 00 00

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\weclnt.dll,-201: "This service manages persistent subscriptions to events from remote sources that support WS-Management protocol. This includes

Windows Vista event logs, hardware and IPMI-enabled event sources. The service stores forwarded events in a local Event Log. If this service is stopped or disabled event subscriptions cannot be created and forwarded events cannot be accepted."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wepostsvc.dll,-101: "Windows Encryption Provider Host Service brokers encryption related functionalities from 3rd Party Encryption Providers to processes that need to evaluate and apply EAS policies. Stopping this will compromise EAS compliancy checks that have been established by the connected Mail Accounts"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wercplsupport.dll,-100: "This service provides support for viewing, sending and deletion of system-level problem reports for the Problem Reports and Solutions control panel."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wersvc.dll,-101: "Allows errors to be reported when programs stop working or responding and allows existing solutions to be delivered. Also allows logs to be generated for diagnostic and repair services. If this service is stopped, error reporting might not work correctly and results of diagnostic services and repairs might not be displayed."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wfdscnmgsvc.dll,-9001: "Manages connections to wireless services, including wireless display and docking."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wiarpc.dll,-1: "Launches applications associated with still image acquisition events."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%ProgramFiles%\Windows Defender\MpAsDesc.dll,-240: "Helps protect users from malware and other potentially unwanted software"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\winhttp.dll,-101: "WinHTTP implements the client HTTP stack and provides developers with a Win32 API and COM Automation component for sending HTTP requests and receiving responses. In addition, WinHTTP provides support for auto-discovering a proxy configuration via its implementation of the Web Proxy Auto-Discovery (WPAD) protocol."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wbem\wmisvc.dll,-204: "Provides a common interface and object model to access management information about operating system, devices, applications and services. If this service is stopped, most Windows-based software will not function properly. If this service is disabled, any services that explicitly depend on it will fail to start."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wsmsvc.dll,-102: "Windows Remote Management (WinRM) service implements the WS-Management protocol for remote management. WS-Management is a standard web services protocol used for remote software and hardware management. The WinRM service listens on the network for WS-Management requests and processes them. The WinRM Service needs to be configured with a listener using winrm.cmd command line tool or through Group Policy in order for it to listen over the network. The WinRM service provides access to WMI data and enables event collection. Event collection and subscription to events require that the service is running. WinRM messages use HTTP and HTTPS as transports. The WinRM service does not depend on IIS but is preconfigured to share a port with IIS on the same machine. The WinRM service reserves the /wsman URL prefix. To prevent conflicts with IIS, administrators should ensure that any websites hosted on IIS do not use the /wsman URL prefix."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\flightsettings.dll,-104: "Provides infrastructure support for the Windows Insider Program. This service must remain enabled for the Windows Insider Program to work."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wlansvc.dll,-258: "The WLANSVC service provides the logic required to configure, discover, connect to, and disconnect from a wireless local area network (WLAN) as defined by IEEE 802.11 standards. It also contains the logic to turn your computer into a software access point so that other devices or computers can connect to your computer wirelessly using a WLAN adapter that can support this. Stopping or disabling the WLANSVC service will make all WLAN adapters on your computer inaccessible from the Windows networking UI. It is strongly recommended that you have the WLANSVC service running if your computer has a WLAN adapter."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wlidsvc.dll,-101: "Enables user sign-in through Microsoft account identity services. If this service is stopped, users will not be able to logon to the computer with their Microsoft account."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\lpasvc.dll,-1001: "This service provides profile management for subscriber identity modules"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\Windows.Management.Service.dll,-101: "Performs management including Provisioning and Enrollment activities"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wbem\wmiapsrv.exe,-111: "Provides performance library information from Windows Management Instrumentation (WMI) providers to clients on the network. This service only runs when Performance Data Helper is activated."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-102: "Shares Windows Media Player libraries to other networked players and media devices using Universal Plug and Play"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\workfoldersvc.dll,-101: "This service syncs files with the Work Folders server, enabling you to use the files on any of the PCs and devices on which you've set up Work Folders."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\WpcRefreshTask.dll,-101: "Enforces parental controls for child accounts in Windows. If this service is stopped or disabled, parental controls may not be enforced."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wpdbusenum.dll,-101: "Enforces group policy for removable mass-storage devices. Enables applications such as Windows Media Player and Image Import Wizard to transfer and synchronize content using removable mass-storage devices."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\wpnservice.dll,-2: "This service runs in session 0 and hosts the notification platform and connection provider which handles the connection between the device and WNS server."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wscsvc.dll,-201: "The WSCSVC (Windows Security Center) service monitors and reports security health settings on the computer. The health settings include firewall (on/off), antivirus (on/off/out of date), antispyware (on/off/out of date), Windows Update (automatically/manually download and install updates), User Account Control (on/off), and Internet settings (recommended/not recommended). The service provides COM APIs for independent software vendors to register and record the state of their products to the Security Center service. The Security and Maintenance UI uses the service to provide systray alerts and a graphical view of the security health states in the Security and Maintenance control panel. Network Access Protection (NAP) uses the service to report the security health states of clients to the NAP Network Policy Server to make network quarantine decisions. The service also has a public API that allows external consumers to programmatically retrieve the aggregated security health state of the system."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\SearchIndexer.exe,-104: "Provides content indexing, property caching, and search results for files, e-mail, and other content."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\System32\wwansvc.dll,-258: "This service manages mobile broadband (GSM & CDMA) data card/embedded module adapters and connections by auto-configuring the networks. It is strongly recommended that this service be kept running for best user experience of mobile broadband devices."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\XblAuthManager.dll,-101: "Provides authentication and authorization services for interacting with Xbox Live. If this service is stopped, some applications may not operate correctly."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\XblGameSave.dll,-101: "This service syncs save data for Xbox Live save enabled games. If this service is stopped, game save data will not upload to or download from Xbox Live."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\xboxgipsvc.dll,-101: "This service manages connected Xbox Accessories."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%systemroot%\system32\XboxNetApiSvc.dll,-101: "This service supports the Windows.Networking.XboxLive application programming interface."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\AarSvc.dll,-101: "Runtime for activating conversational agent applications"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\BcastDVRUserService.dll,-101: "This user service is used for Game Recordings and Live Broadcasts"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\Microsoft.Bluetooth.UserService.dll,-102: "The Bluetooth user service supports proper functionality of Bluetooth features relevant to each user session."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\CaptureService.dll,-101: "Enables optional screen capture functionality for applications that call the Windows.Graphics.Capture API."

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\cbdhsvc.dll,-101: "This user service is used for Clipboard scenarios"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\cdpusersvc.dll,-101: "This user service is used for Connected Devices Platform scenarios"

HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\ConsentUxClient.dll,-101: "Allows ConnectUX and PC Settings to Connect and Pair with WiFi displays and Bluetooth devices."

HKU\S-1-5-18\Software\Classes\Local
Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\CredentialEnrollmentManager.exe,-101: "Credential Enrollment
Manager"
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\deviceaccess.dll,-108:
"Enables apps to pair devices"
HKU\S-1-5-18\Software\Classes\Local
Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\Windows.Devices.Picker.dll,-1007: "This user service is used for
managing the Miracast, DLNA, and DIAL UI"
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\DevicesFlowBroker.dll,-
104: "Allows ConnectUX and PC Settings to Connect and Pair with WiFi displays and Bluetooth devices."
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\MessagingService.dll,-101:
"Service supporting text messaging and related functionality."
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\APHostRes.dll,-10001: "This
service synchronizes mail, contacts, calendar and various other user data. Mail and other applications dependent on this
functionality will not work properly when this service is not running."
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\UserDataAccessRes.dll,-
15000: 49 00 6E 00 64 00 65 00 78 00 65 00 73 00 20 00 63 00 6F 00 6E 00 74 00 61 00 63 00 74 00 20 00 64 00 61 00 74 00 61
00 20 00 66 00 6F 00 72 00 20 00 66 00 61 00 73 00 74 00 20 00 63 00 6F 00 6E 00 74 00 61 00 63 00 74 00 20 00 73 00 65 00 61
00 72 00 63 00 68 00 69 00 6E 00 67 00 2E 00 20 00 49 00 66 00 20 00 79 00 6F 00 75 00 20 00 73 00 74 00 6F 00 70 00 20 00 6F
00 72 00 20 00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 20 00 74 00 68 00 69 00 73 00 65 00 72 00 76 00 69 00 63
00 65 00 2C 00 20 00 63 00 6F 00 6E 00 74 00 61 00 63 00 74 00 73 00 20 00 6D 00 69 00 67 00 68 00 74 00 20 00 62 00 65 00 20
00 6D 00 69 00 73 00 73 00 69 00 6E 00 67 00 20 00 66 00 72 00 6F 00 6D 00 20 00 79 00 6F 00 75 00 72 00 20 00 73 00 65 00 61
00 72 00 63 00 68 00 20 00 72 00 65 00 73 00 75 00 6C 00 74 00 73 00 2E 00 00 00 00 00
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\PrintWorkflowService.dll,-
101: "Print Workflow"
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\UserDataAccessRes.dll,-
10002: 48 00 61 00 6E 00 64 00 6C 00 65 00 73 00 20 00 73 00 74 00 6F 00 72 00 61 00 67 00 65 00 20 00 6F 00 66 00 20 00 73
00 74 00 72 00 75 00 63 00 74 00 75 00 72 00 65 00 64 00 20 00 75 00 73 00 65 00 72 00 20 00 64 00 61 00 74 00 61 00 2C 00 20
00 69 00 6E 00 63 00 6C 00 75 00 64 00 69 00 6E 00 67 00 20 00 63 00 6F 00 6E 00 74 00 61 00 63 00 74 00 20 00 69 00 6E 00 66
00 6F 00 2C 00 20 00 63 00 61 00 6C 00 65 00 6E 00 64 00 61 00 72 00 73 00 2C 00 20 00 6D 00 65 00 73 00 73 00 61 00 67 00 65
00 73 00 2C 00 20 00 61 00 6E 00 64 00 20 00 6F 00 74 00 68 00 65 00 72 00 20 00 63 00 6F 00 6E 00 74 00 65 00 6E 00 74 00 2E
00 20 00 49 00 66 00 20 00 79 00 6F 00 75 00 20 00 73 00 74 00 6F 00 70 00 20 00 6F 00 72 00 20 00 64 00 69 00 73 00 61 00 62
00 6C 00 65 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 2C 00 20 00 61 00 70 00 70 00 73
00 20 00
74 00 68 00 61 00 74 00 20 00 75 00 73 00 65 00 20 00 74 00 68 00 69 00 73 00 20 00 64 00 61 00 74 00 61 00 20 00 6D 00 69
00 67 00 68 00 74 00 20 00 6E 00 6F 00 74 00 20 00 77 00 6F 00 72 00 6B 00 20 00 63 00 6F 00 72 00 72 00 65 00 63 00 74 00 6C
00 79 00 2E 00 00 00 00 00
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\UserDataAccessRes.dll,-
14000: 50 00 72 00 6F 00 76 00 69 00 64 00 65 00 73 00 20 00 61 00 70 00 70 00 73 00 20 00 61 00 63 00 63 00 65 00 73 00 73
00 20 00 74 00 6F 00 20 00 73 00 74 00 72 00 75 00 63 00 74 00 75 00 72 00 65 00 64 00 20 00 75 00 73 00 65 00 72 00 20 00 64
00 61 00 74 00 61 00 2C 00 20 00 69 00 6E 00 63 00 6C 00 75 00 64 00 69 00 6E 00 67 00 20 00 63 00 6F 00 6E 00 74 00 61 00 63
00 74 00 20 00 69 00 6E 00 66 00 6F 00 2C 00 20 00 63 00 61 00 6C 00 65 00 6E 00 64 00 61 00 72 00 73 00 2C 00 20 00 6D 00 65
00 73 00 73 00 61 00 67 00 65 00 73 00 2C 00 20 00 61 00 6E 00 64 00 20 00 6F 00 74 00 68 00 65 00 72 00 20 00 63 00 6F 00 6E
00 74 00 65 00 6E 00 74 00 2E 00 20 00 49 00 66 00 20 00 79 00 6F 00 75 00 20 00 73 00 74 00 6F 00 70 00 20 00 6F 00 72 00 20
00 64 00 69 00 73 00 61 00 62 00 6C 00 65 00 20 00 74 00 68 00 69 00 73 00 20 00 73 00 65 00 72 00 76 00 69 00 63 00 65 00 2C
00 20 00
61 00 70 00 70 00 73 00 20 00 74 00 68 00 61 00 74 00 20 00 75 00 73 00 65 00 20 00 74 00 68 00 69 00 73 00 20 00 64 00 61
00 74 00 61 00 20 00 6D 00 69 00 67 00 68 00 74 00 20 00 6E 00 6F 00 74 00 20 00 77 00 6F 00 72 00 6B 00 20 00 63 00 6F 00 72
00 72 00 65 00 63 00 74 00 6C 00 79 00 2E 00 00 00 00 00
HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\64\52C64B7E\@%SystemRoot%\system32\WpnUserService.dll,-2:
"This service hosts Windows notification platform which provides support for local and push notifications. Supported
notifications are tile, toast and raw."

Values modified: 162

HKLM\SOFTWARE\Microsoft\Multimedia\Audio\Journal\Render: 53 00 57 00 44 00 5C 00 4D 00 4D 00 44 00 45 00 56 00 41 00
50 00 49 00 5C 00 7B 00 30 00 2E 00 30 00 2E 00 30 00 2E 00 30 00 30 00 30 00 30 00 30 00 30 00 7D 00 2E 00 7B 00

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SystemProtectedUserData\S-1-5-21-2169232433-3398496680-935370409-1000\AnyoneRead\ScaleFactors\ScaleFactors: 76 85 0C 62 7D 77 D9 01 64 00 00 00 00 00 00 08 F6 EB 02 00 00 00 00 D0 B6 41 03 00 00 00 00

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUPProvider\StartTime: 0x01D9777B4A95BD34

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\VFUPProvider\StartTime: 0x01D9777D86C840A7

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\WOSC>LastRefreshAttempted: 0x01D9777A90F346D2

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Wosc\Client\Persistent\ClientState\WOSC>LastRefreshAttempted: 0x01D9777D8785CD99

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\AuxJsonOutputFileCreationTime_20H1: 0x01D94B0586EE2941

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\AuxJsonOutputFileCreationTime_20H1: 0x01D9777D7B509AEA

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser>LastOnlineTime: 0x01D94B058A05B6EF

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser>LastOnlineTime: 0x01D9777D80ACD7C5

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults>LastRun\RunStartTimestamp: 0x01D94B0D5B1AFEE8

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults>LastRun\RunStartTimestamp: 0x01D9777C8BDB2587

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults>LastSuccessfulFromEnterprisePerspectiveRun\RunStartTimestamp: 0x01D94B0578CAF538

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults>LastSuccessfulFromEnterprisePerspectiveRun\RunStartTimestamp: 0x01D9777C8BDB2587

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults>LastSuccessfulFromEnterprisePerspectiveRun\RunEndTimestamp: 0x01D94B058A05B6EF

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults>LastSuccessfulFromEnterprisePerspectiveRun\RunEndTimestamp: 0x01D9777D80ACD7C5

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults>LastSuccessfulRun\RunStartTimestamp: 0x01D94B0578CAF538

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults>LastSuccessfulRun\RunStartTimestamp: 0x01D9777C8BDB2587

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults>LastSuccessfulRun\RunEndTimestamp: 0x01D94B058A05B6EF

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Appraiser\RunResults>LastSuccessfulRun\RunEndTimestamp: 0x01D9777D80ACD7C5

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\AvTracking\History\TimeStamp: 0x01D94AFFB00115C7

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\AvTracking\History\TimeStamp: 0x01D9777D86FAD8B3

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\ClientTelemetry\GentelLastMonthlyRun: 0x01D94A4687512673

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\ClientTelemetry\GentelLastMonthlyRun: 0x01D9777D34E31957

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CompatMarkers\20H1\TimestampEpochString: "1677541509"

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CompatMarkers\20H1\TimestampEpochString: "1682430884"

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CompatMarkers\20H1\Timestamp: 0x01D94B05870603F8

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\CompatMarkers\20H1\Timestamp: 0x01D9777D7D8CFEC5

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\GeneralMarkers\UNV\TimestampEpochString: "1677459476"

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\GeneralMarkers\UNV\TimestampEpochString:
"1682430762"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\GeneralMarkers\UNV\Timestamp:
0x01D94A4687512673
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\GeneralMarkers\UNV\Timestamp:
0x01D9777D34E31957
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Shared\CompatMarkers\20H1\UtcSyncId:
"{EE297293-7D50-43EF-945E-4CE0553A65EE}"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Shared\CompatMarkers\20H1\UtcSyncId:
"{134FEB10-B545-4E68-9A95-11D4DE39E803}"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Shared\CompatMarkers\20H1\checksum: 3C 3D 13
F2 36 F2 E2 A3 B0 E1 A7 C9 C3 AC E0 99 7E 21 75 3E 21 00 5F 07 12 08 5B 8D FA E6 52 95
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Shared\CompatMarkers\20H1\checksum: 1E 7D 0B
32 C3 4A BE 03 FC 4E 23 F9 7F F7 BF B0 73 78 70 D9 F9 C1 50 B9 82 41 7D CD EF 07 CF D3
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Shared\GeneralMarkers\UNV\UtcSyncId:
"{07018ED5-F333-45D5-A9FD-B54DA788C38D}"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Shared\GeneralMarkers\UNV\UtcSyncId:
"{D6C7ABBD-CE5D-4BAB-9C94-8F350FCD9C22}"
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Shared\GeneralMarkers\UNV\checksum: 63 26 35
77 4A 6A F8 50 01 51 8E B9 EB 30 69 35 1B 91 0C 96 3D 82 C9 67 FA 4F 8C D1 D8 30 AC B6
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Shared\GeneralMarkers\UNV\checksum: 5A 73 CA
E9 98 D2 8C F4 7D 09 66 00 E9 DA E0 D6 B9 A6 3E DC 2D AD CB F3 69 9B 2E 7F 54 5D 33 57
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Shared\TargetVersionUpgradeExperienceIndicators\20H1\UtcSyncId: "{9322C375-664E-
446F-8168-ABAD7DE5815D}"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Shared\TargetVersionUpgradeExperienceIndicators\20H1\UtcSyncId: "{8F700127-7F47-
43D1-9A4D-AD660668C48B}"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Shared\TargetVersionUpgradeExperienceIndicators\20H1\checksum: D7 32 80 7E 79 4D E3
96 0E 84 BA 10 41 CA BF 3F 81 FC 7F 15 A4 BF 9A 48 9F 8E 38 1D B3 DA 0A A8
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Shared\TargetVersionUpgradeExperienceIndicators\20H1\checksum: 70 ED 13 12 12 D7 66
48 2D 01 2B 2B 1E DE EE 43 43 73 F6 E7 3E 8D 9C 1A 1D 15 FE 36 E2 5B 2A 4A
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Shared\TargetVersionUpgradeExperienceIndicators\UNV\UtcSyncId: "{EE6341DE-E33A-
4502-8E59-5B9087BC1B0F}"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Shared\TargetVersionUpgradeExperienceIndicators\UNV\UtcSyncId: "{D4AEE974-8683-
4715-8DE3-28FA75D442C7}"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Shared\TargetVersionUpgradeExperienceIndicators\UNV\checksum: 8D 1A D8 38 5A 9B C1
6A 9A 39 E1 39 27 3F F6 18 AA 2C FC A5 4A 18 52 D0 BC A7 58 7B 2F 1F E0 73
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Shared\TargetVersionUpgradeExperienceIndicators\UNV\checksum: 7F 0D 67 08 92 E1 36
DF 8B 56 CE 14 E7 50 CF 6B 29 85 22 79 2C 70 2A 95 BE 7B 92 02 CD 75 A5 82
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\20H1\GenTelRunTimestamp:
"133220150929189461"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\20H1\GenTelRunTimestamp:
"133269041379947407"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\20H1\TimestampEpochString: "1677541510"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\20H1\TimestampEpochString: "1682430889"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\20H1\Timestamp: 0x01D94B0587D56C19

HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\20H1\Timestamp: 0x01D9777D80941BE3
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\UNV\GenTelRunTimestamp:
"133220150929189461"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\UNV\GenTelRunTimestamp:
"133269041379947407"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\UNV\TimestampEpochString: "1677541509"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\UNV\TimestampEpochString: "1682430884"
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\UNV\Timestamp: 0x01D94B0586FA1285
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\TargetVersionUpgradeExperienceIndicators\UNV\Timestamp: 0x01D9777D7D8D516D
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\LastNormalRun:
0x01D94B05788F60AF
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\TelemetryController\LastNormalRun:
0x01D9777C6B064AC5
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75: 9C 01 00 00 00 00 00 00 04
00 04 00 01 00 04 00 01 01 00 00 02 12 F8 00 A5 AD CF 00 CD AD 05 01 DB B4 EF 00 27 01 02 00 00 00 01 A6 37 01 01 BF 1E 01
01 CF 2A 01 02 12 F8 00 02 83 8B 00 02 99 66 00 03 AA 2B 01 04 93 1A 01 05 61 0F 01 05 D4 7F 00 08 8D 42 01 09 92 F8 00 09
EF 7D 00 0C E9 C2 00 0D 37 C6 00 0D 78 79 00 0D A1 81 00 0D D3 F9 00 0E 01 3E 01 0E BA CD 00 0F 05 DE 00 10 96 86 00 12 E5
F8 00 13 E9 78 00 15 8A A2 00 15 B6 25 01 15 CE EB 00 19 C0 E2 00 1B 42 78 00 1B F5 EF 00 1B F6 0B 00 1C 8F CF 00 1C 95 5C 00
1C A7 21 01 1E 1F 51 01 1E 8D 52 00 1F 4E A8 00 20 18 F2 00 21 77 7A 00 24 AC C7 00 25 3A D5 00 27 69 12 01 27 DB 21 01 27
E8 CF 00 28 A1 1B 01 29 45 01 01 2A 68 A9 00 2A B7 22 01 2A B8 5E 01 2A C7 DE 00 2B 24 99 00 2C 3D 81 00 2C D8 42 01 2D D8
F4 00 2E 80 1D 01 2F 34 FB 00 2F 39 D5 00 30 50 25 01 31 17 5D 00 31 48 4F 00 32 57 A4 00 36 E9 D2 00 39 D3 79 00 3A 35 D8
00 3A 5D E3 00 3B CE 3
4 01 3C B3 52 00 3D 7F E6 00 3D E7 43 00 3E 33 83 00 3E A5 FA 00 3F 9A C7 00 40 56 F1 00 40 A5 6A 00 40 B0 2A 01 41 99 0F 01
41 A8 76 00 42 1D 0B 01 42 26 4A 00 42 B3 AE 00 44 B9 07 01 46 1D 0B 01 46 48 B6 00 46 79 D1 00 46 C2 21 01 48 C2 4F 00 48
F9 A6 00 49 EA B7 00 4A AA 81 00 4C 37 FA 00 4C 41 B4 00 4C A7 70 00 4E 12 24 01 4E BF 72 00 4E E7 C1 00 4F 14 C2 00 4F D5
EC 00 50 34 A5 00 52 9F 4A 01 52 A7 AA 00 52 D3 16 00 54 7A 52 00 54 B7 DC 00 56 0A 85 00 57 AD 12 01 58 0B D0 00 59 53 94
00 5A 5E B5 00 5B 3A F5 00 5C 59 7F 00 5E 65 27 01 60 47 8F 00 60 D7 D3 00 61 13 24 01 63 96 77 00 64 D4 19 01 65 A6 9E 00
65 D3 68 00 66 8F D3 00 6C 52 0D 01 6E 07 7F 00 6F B3 11 01 6F BD A9 00 70 2A 07 01 71 05 28 01 71 40 A3 00 71 66 0E 01 72
3C 12 00 72 6E 4A 00 72 9B 37 01 74 77 AD 00 74 D6 20 01 75 17 34 01 75 A3 7E 00 75 AB 0A 01 78 2D B0 00 78 EF 64 00 79 2D
4F 01 79 9C 39 00 7B 45 D5 00 7B 9F EB 00 7B A8 D1 00 7E 31 1A 01 7E 62 C1 00 7F 88 CA 00 80 CB 42 01 81 06 95 00 82 25 1D
01 82 27 73 00
83 60 A9 00 83 D7 5C 00 83 F1 60 00 84 4D 26 01 84 E6 83 00 85 12 4A 00 85 50 AE 00 86 7B 06 01 87 92 17 01 87 92 21 01 87
DE 83 00 89 97 F5 00 89 AC 11 01 8A 80 93 00 8A FA E3 00 8B 4E 1D 01 8B 51 88 00 8B EE F2 00 8D 94 1D 01 8E 25 60 01 8E 78
A2 00 90 48 1F 01 90 D5 D0 00 91 23 D3 00 92 A1 67 01 93 86 61 00 95 9B 51 00 96 5D D2 00 97 6A B6 00 97 74 8D 00 97 F6 C4
00 98 BF 37 01 9A 4E 96 00 9B 2B DB 00 9B 4D 87 00 9C A4 EB 00 9C E0 A8 00 9D 9D 92 00 9E BB 0D 01 A0 86 61 00 A0 CD 71 00
A1 89 C7 00 A2 05 06 00 A2 2E 1E 01 A3 9D 22 01 A3 E7 15 01 A4 58 02 00 A5 AD CF 00 A6 44 A6 00 A6 E9 B3 00 A7 36 A8 00 A7
B8 AD 00 AD 73 BF 00 AD D4 EC 00 AE 5C D2 00 B1 CE 98 00 B2 91 DD 00 B2 AA 21 01 B3 92 FB 00 B5 61 0D 01 B6 21 C9 00 B8 02
97 00 B9 1A F3 00 BA F9 E9 00 BB 8E 8B 00 BB AE 7E 00 BC 6E B4 00 BC D2 2A 01 BC FA 8D 00 BD 38 8F 00 BD 53 98 00 BE 0C AC
00 BE FD 22 01 BF 8E CE 00 C0 46 AD 00 C2 61 0B 01 C3 3E A3 00 C3 6D 81 00 C3 99 F3 00 C4 66 27 01 C5 35 C9 00 C5 68 DE 00
C7 0B C2 00 C8
46 4E 00 C9 26 2D 01 C9 38 97 00 C9 53 F1 00 CA 23 B7 00 CA 99 CE 00 CB 74 DA 00 CC 49 56 00 CD AD 05 01 CD BD 8C 00 CF 74
AA 00 CF D9 35 00 D0 17 56 00 D0 72 5B 00 D0 D0 EF 00 D1 9A 7B 00 D1 D2 A7 00 D2 A9 2B 01 D3 82 61 00 D3 C7 AF 00 D3 E8
8D 00 D6 F6 DE 00 D9 07 24 01 D9 3D AA 00 DA BB D8 00 DA FF 0E 00 DD 1B 19 01 DE 3C DA 00 E0 62 38 01 E0 86 23 01 E1 7E
8C 00 E1 9A D3 00 E2 1B 56 00 E4 2A 5E 00 E4 69 C9 00 E5 4C 27 01 E7 A4 D9 00 E8 9A FD 00 E8 9E FA 00 E9 8C 0A 01 EC B9 22
01 EF 79 8B 00 F0 E0 B6 00 F1 7D 5F 00 F1 FC 60 00 F2 B4 FA 00 F3 08 DB 00 F3 28 21 01 F3 67 04 01 F3 8B B5 00 F4 3D 77 00 F5
48 B1 00 F5 50 0D 01 F5 57 2A 01 F6 30 8E 00 F7 12 5E 00 F7 D3 6F 00 F7 ED 6A 00 F8 FE 82 00 F9 77 8C 00 FA 38 17 01 FB 08 06
01 FD B0 D9 00 02 00 03 00 00 00 7D 98 C5 00 83 06 1B 01 A9 00 06 00 00 00 00 47 F1 00 02 A4 15 01 04 92 1E 01 05 2A D1 00
05 37 C6 00 06 A3 17 01 08 58 71 00 08 CE 23 01 08 F0 28 01 0A 29 D8 00 0B FF 5C 00 0C 4C BC 00 0C 5C 22 01 0C 77 1A 01 0D
9A 03 01 0E 4D 7
E 00 0E 9D 19 01 0F BA 9E 00 11 0F AA 00 13 19 83 00 14 AA FD 00 15 40 28 01 15 9A DB 00 19 C3 98 00 1A FA 99 00 1D 49 12
01 22 D3 89 00 24 20 29 01 24 6F 16 00 25 BE 17 01 27 A2 A2 00 28 0C 0E 01 28 8B B4 00 29 00 D8 00 2C 21 D7 00 2D 85 BA 00

2D B1 A3 00 2E 68 A9 00 32 55 1E 01 32 56 AE 00 34 B3 77 00 34 BB EF 00 37 22 C7 00 37 F8 1D 01 3F 1C EA 00 42 7F 7A 00 42
93 80 00 42 C4 6A 00 42 FA 58 00 43 AB 21 01 48 C6 F5 00 4C 29 FB 00 4C AF 71 00 50 A4 30 01 52 22 13 01 52 54 FE 00 52 D7
1F 01 53 D8 8F 00 55 5F 2A 01 56 B7 22 01 59 E5 D3 00 5B C7 F7 00 5C C0 05 01 5C E1 7D 00 5E 42 C4 00 5F 6C DC 00 63 3E 99
00 63 63 81 00 65 6D 24 01 65 7F 0E 01 67 68 A7 00 69 D2 81 00 6B 01 10 01 6E 7B 8C 00 70 BF 19 01 70 E8 25 01 73 D3 A7 00
74 10 1B 01 76 41 8E 00 77 BB 2B 01 78 7F E1 00 7A 22 26 01 7B 7C C2 00 7B B8 5E 01 7C 22 B8 00 7C 78 A4 00 82 E6 F4 00 84
68 0B 01 8A D2 D2 00 8C 3B D3 00 8F 3C F3 00 91 3C 08 01 91 50 8A 00 91 67 C8 00 91 96 22 01 91 D3 A3 00 92 82 71 00 92 C4
14 01 93 69 C7 00
96 39 0B 01 96 51 62 01 99 69 8A 00 9B 56 A4 00 9B CE 5C 00 9C 40 27 01 9D 9F A0 00 9F 60 C3 00 9F 8F 6E 00 9F C8 CA 00 A0
2A AB 00 A0 AD 1C 01 A0 B5 0A 01 A1 D7 B3 00 A2 A6 F8 00 A3 36 FB 00 A3 C4 E2 00 A3 F7 6A 00 A5 04 03 01 A5 22 A4 00 A5 8F
60 00 A6 38 DA 00 A8 CF 27 01 A9 B2 DB 00 AF EF C9 00 B0 75 5E 00 B4 89 22 01 B6 51 5D 00 B7 E2 BF 00 BA 14 65 00 BC 8A A7
00 BD C3 98 00 BF F1 A9 00 C2 21 D1 00 C4 5F 7F 00 C5 C0 05 01 C8 2B FC 00 C9 77 D7 00 C9 D7 CA 00 CC C1 01 01 CC EF EF 00
D0 D3 22 01 D0 FE 62 00 D1 58 96 00 D3 30 1C 01 D6 B7 9A 00 D9 E6 FC 00 DA 19 D7 00 DA D8 7E 00 DC 1C 62 00 DC 30 D1 00
DD EB 26 01 DF D5 22 01 E6 19 9B 00 E6 B9 2B 01 E9 8A A7 00 E9 D1 F5 00 EA B9 4F 00 ED 0C AD 00 F0 0E 4E 01 F0 3A DD 00 F3
9E D3 00 F4 06 28 01 F4 AD 7A 00 F4 C8 2F 01 F5 51 F9 00 F6 D9 EC 00 F8 07 1A 01 F8 71 9A 00 FA 67 CB 00 0B 00 40 01 00 00
02 12 F8 00 2D D8 F4 00 4B 11 B4 00 74 D6 20 01 7B A8 D1 00 8A FA E3 00 9F 27 FF 00 A3 9D 22 01 A5 AD CF 00 CD AD 05 01 DB
B4 EF 00 03 00 41
01 00 00 2A 68 A9 00 2A B7 22 01 3A 5D E3 00 01 00 42 01 00 00 27 69 12 01 01 00 43 01 00 00 C0 EC 7C 00 01 00 44 01 00 00
7E 31 1A 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC1C75: AE 01 00 00 00 00 00 00 04
00 04 00 01 00 04 00 01 01 00 00 02 12 F8 00 A5 AD CF 00 CD AD 05 01 DB B4 EF 00 31 01 02 00 00 00 01 31 8E 00 01 A6 37 01
01 BF 1E 01 01 CF 2A 01 02 12 F8 00 02 83 8B 00 02 99 66 00 03 AA 2B 01 04 93 1A 01 05 61 0F 01 05 D4 7F 00 08 8D 42 01 09
92 F8 00 09 EF 7D 00 0C 35 84 00 0C E9 C2 00 0D 37 C6 00 0D 78 79 00 0D A1 81 00 0D D3 F9 00 0E 01 3E 01 0E BA CD 00 0F 05
DE 00 10 96 86 00 12 E5 F8 00 13 E9 78 00 15 8A A2 00 15 B6 25 01 15 CE EB 00 19 C0 E2 00 1B 42 78 00 1B B8 3C 01 1B F5 EF
00 1B F6 0B 00 1C 8F CF 00 1C 95 5C 00 1C A7 21 01 1E 1F 51 01 1E 8D 52 00 1F 4E A8 00 20 18 F2 00 21 77 7A 00 24 AC C7 00
25 3A D5 00 27 69 12 01 27 DB 21 01 27 E8 CF 00 28 A1 1B 01 29 45 01 01 2A 68 A9 00 2A B7 22 01 2A B8 5E 01 2A C7 DE 00 2B
24 99 00 2C 3D 81 00 2C D8 42 01 2D D8 F4 00 2E 80 1D 01 2F 34 FB 00 2F 39 D5 00 30 50 25 01 31 17 5D 00 31 48 4F 00 32 57
A4 00 36 E9 D2 00 39 D3 7
9 00 3A 35 D8 00 3A 5D E3 00 3B CE 34 01 3C B3 52 00 3D 7F E6 00 3D E7 43 00 3E 33 83 00 3E A5 FA 00 3F 9A C7 00 40 56 F1 00
40 A5 6A 00 40 B0 2A 01 41 99 0F 01 41 A8 76 00 42 1D 0B 01 42 26 4A 00 42 B3 AE 00 44 30 7C 00 44 B9 07 01 46 1D 0B 01 46
48 B6 00 46 79 D1 00 46 C2 21 01 48 C2 4F 00 48 F9 A6 00 49 EA B7 00 4A AA 81 00 4C 37 FA 00 4C 41 B4 00 4C A7 70 00 4E 12
24 01 4E BF 72 00 4E E7 C1 00 4F 14 C2 00 4F D5 EC 00 50 34 A5 00 52 9F 4A 01 52 A7 AA 00 52 D3 16 00 54 7A 52 00 54 B7 DC
00 56 0A 85 00 57 AD 12 01 58 0B D0 00 58 20 18 01 58 41 0D 01 59 53 94 00 5A 5E B5 00 5B 3A F5 00 5C 59 7F 00 5E 65 27 01
60 47 8F 00 60 D7 D3 00 61 13 24 01 63 96 77 00 64 D4 19 01 65 A6 9E 00 65 D3 68 00 66 8F D3 00 6C 52 0D 01 6E 07 7F 00 6F
B3 11 01 6F BD A9 00 70 2A 07 01 71 05 28 01 71 40 A3 00 71 66 0E 01 72 3C 12 00 72 6E 4A 00 72 9B 37 01 74 77 AD 00 74 D6
20 01 75 17 34 01 75 A3 7E 00 75 AB 0A 01 78 2D B0 00 78 EF 64 00 79 2D 4F 01 79 9C 39 00 7B 45 D5 00 7B 9F EB 00 7B A8 D1
00 7E 31 1A 01
7E 62 C1 00 7F 88 CA 00 80 CB 42 01 81 06 95 00 82 25 1D 01 82 27 73 00 83 60 A9 00 83 D7 5C 00 83 F1 60 00 84 4D 26 01 84
E6 83 00 85 12 4A 00 85 50 AE 00 86 7B 06 01 87 92 17 01 87 92 21 01 87 DE 83 00 89 97 F5 00 89 AC 11 01 8A 80 93 00 8A FA
E3 00 8B 4E 1D 01 8B 51 88 00 8B EE F2 00 8D 94 1D 01 8E 25 60 01 8E 78 A2 00 90 48 1F 01 90 D5 D0 00 91 23 D3 00 92 A1 67
01 93 86 61 00 95 9B 51 00 95 E1 DB 00 96 5D D2 00 97 6A B6 00 97 74 8D 00 97 F6 C4 00 98 BF 37 01 9A 4E 96 00 9B 2B DB 00
9B 4D 87 00 9C A4 EB 00 9C E0 A8 00 9D 9D 92 00 9E BB 0D 01 A0 86 61 00 A0 CD 71 00 A1 89 C7 00 A2 05 06 00 A2 2E 1E 01 A3
9D 22 01 A3 E7 15 01 A4 58 02 00 A4 BA 37 01 A5 AD CF 00 A6 44 A6 00 A6 E9 B3 00 A7 36 A8 00 A7 B8 AD 00 AD 4F F8 00 AD 73
BF 00 AD D4 EC 00 AE 5C D2 00 B1 CE 98 00 B2 91 DD 00 B2 AA 21 01 B3 92 FB 00 B5 61 0D 01 B6 21 C9 00 B8 02 97 00 B9 1A F3
00 BA F9 E9 00 BB 8E 8B 00 BB AE 7E 00 BC 6E B4 00 BC D2 2A 01 BC FA 8D 00 BD 38 8F 00 BD 53 98 00 BE 0C AC 00 BE FD 22 01
BF 8E CE 00 C0
46 AD 00 C2 61 0B 01 C3 3E A3 00 C3 6D 81 00 C3 99 F3 00 C4 66 27 01 C5 35 C9 00 C5 68 DE 00 C7 0B C2 00 C8 46 4E 00 C9 26
2D 01 C9 38 97 00 C9 53 F1 00 CA 23 B7 00 CA 99 CE 00 CB 74 DA 00 CC 49 56 00 CD AD 05 01 CD BD 8C 00 CF 74 AA 00 CF D9 35
00 D0 17 56 00 D0 72 5B 00 D0 D0 EF 00 D1 9A 7B 00 D1 D2 A7 00 D2 A9 2B 01 D3 82 61 00 D3 C7 AF 00 D3 E8 8D 00 D6 F6 DE
00 D9 07 24 01 D9 3D AA 00 DA BB D8 00 DA FF 0E 00 DD 1B 19 01 DE 3C DA 00 E0 62 38 01 E0 86 23 01 E1 7E 8C 00 E1 9A D3 00
E2 1B 56 00 E4 2A 5E 00 E4 69 C9 00 E5 4C 27 01 E7 A4 D9 00 E8 9A FD 00 E8 9E FA 00 E9 8C 0A 01 EC B9 22 01 EF 79 8B 00 F0
E0 B6 00 F1 7D 5F 00 F1 FC 60 00 F2 B4 FA 00 F3 08 DB 00 F3 28 21 01 F3 3A 38 01 F3 67 04 01 F3 8B B5 00 F4 3D 77 00 F5 48 B1
00 F5 50 0D 01 F5 57 2A 01 F6 30 8E 00 F7 12 5E 00 F7 D3 6F 00 F7 ED 6A 00 F8 FE 82 00 F9 77 8C 00 FA 38 17 01 FB 08 06 01 FD
B0 D9 00 02 00 03 00 00 00 7D 98 C5 00 83 06 1B 01 B5 00 06 00 00 00 00 47 F1 00 02 A4 15 01 04 92 1E 01 05 2A D1 00 05 37
C6 00 06 A3 1
7 01 08 58 71 00 08 CE 23 01 08 F0 28 01 0A 29 D8 00 0B FF 5C 00 0C 4C BC 00 0C 5C 22 01 0C 77 1A 01 0D 9A 03 01 0E 4D 7E 00
0E 9D 19 01 0F BA 9E 00 11 0F AA 00 13 19 83 00 14 AA FD 00 15 40 28 01 15 9A DB 00 19 C3 98 00 1A FA 99 00 1D 49 12 01 22
D3 89 00 24 20 29 01 24 6F 16 00 25 BE 17 01 27 A2 A2 00 28 0C 0E 01 28 8B B4 00 29 00 D8 00 2C 21 D7 00 2D 85 BA 00 2D B1
A3 00 2E 68 A9 00 31 C2 E1 00 32 55 1E 01 32 56 AE 00 34 B3 77 00 34 BB EF 00 37 22 C7 00 37 F8 1D 01 39 5E A7 00 3F 1C EA

00 42 7F 7A 00 42 93 80 00 42 C4 6A 00 42 FA 58 00 43 AB 21 01 48 C6 F5 00 4C 29 FB 00 4C AF 71 00 50 20 18 01 50 8F C4 00
50 A4 30 01 52 22 13 01 52 54 FE 00 52 D7 1F 01 53 D8 8F 00 55 5F 2A 01 56 B7 22 01 59 E5 D3 00 5B C7 F7 00 5C C0 05 01 5C
E1 7D 00 5E 42 C4 00 5F 6C DC 00 61 F5 E3 00 63 3E 99 00 63 63 81 00 65 6D 24 01 65 7F 0E 01 67 68 A7 00 69 D2 81 00 6B 01
10 01 6E 7B 8C 00 70 BF 19 01 70 E8 25 01 73 D3 A7 00 74 10 1B 01 76 41 8E 00 77 BB 2B 01 78 7F E1 00 7A 22 26 01 7B 7C C2
00 7B B8 5E 01
7C 22 B8 00 7C 78 A4 00 7E 86 DF 00 82 E6 F4 00 84 68 0B 01 84 E7 1C 01 8A D2 D2 00 8C 3B D3 00 8F 3C F3 00 91 3C 08 01 91
50 8A 00 91 67 C8 00 91 96 22 01 91 D3 A3 00 92 82 71 00 92 C4 14 01 93 69 C7 00 96 39 0B 01 96 51 62 01 99 69 8A 00 9B 56
A4 00 9B CE 5C 00 9C 40 27 01 9D 9F A0 00 9F 60 C3 00 9F 8F 6E 00 9F C8 CA 00 A0 2A AB 00 A0 AD 1C 01 A0 B5 0A 01 A1 D7 B3
00 A2 A6 F8 00 A3 36 FB 00 A3 C4 E2 00 A3 F7 6A 00 A5 04 03 01 A5 22 A4 00 A5 8F 60 00 A6 38 DA 00 A8 CF 27 01 A9 A4 C2 00
A9 B2 DB 00 AF EF C9 00 B0 75 5E 00 B4 89 22 01 B6 51 5D 00 B7 E2 BF 00 BA 14 65 00 BC 8A A7 00 BD C3 98 00 BF F1 A9 00 C2
21 D1 00 C4 5F 7F 00 C5 C0 05 01 C8 2B FC 00 C9 77 D7 00 C9 D7 CA 00 CC C1 01 01 CC EF EF 00 D0 40 27 01 D0 D3 22 01 D0 FE
62 00 D1 58 96 00 D2 E4 19 01 D3 30 1C 01 D6 B7 9A 00 D9 E6 FC 00 DA 19 D7 00 DA D8 7E 00 DC 1C 62 00 DC 30 D1 00 DD EB
26 01 DF D5 22 01 E6 19 9B 00 E6 B9 2B 01 E9 8A A7 00 E9 D1 F5 00 EA B9 4F 00 ED 0C AD 00 F0 0E 4E 01 F0 3A DD 00 F3 9E D3
00 F4 06 28 01 F4
74 5E 00 F4 AD 7A 00 F4 C8 2F 01 F5 51 F9 00 F6 D9 EC 00 F8 07 1A 01 F8 71 9A 00 FA 67 CB 00 FE 5B FE 00 0B 00 40 01 00 00 02
12 F8 00 2D D8 F4 00 4B 11 B4 00 74 D6 20 01 7B A8 D1 00 8A FA E3 00 9F 27 FF 00 A3 9D 22 01 A5 AD CF 00 CD AD 05 01 DB B4
EF 00 03 00 41 01 00 00 2A 68 A9 00 2A B7 22 01 3A 5D E3 00 01 00 42 01 00 00 27 69 12 01 01 00 43 01 00 00 C0 EC 7C 00 01
00 44 01 00 00 7E 31 1A 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: 11 02 00 00 00 00 00 00 04
00 04 00 01 02 06 00 00 00 00 10 00 00 00 0D 78 79 00 02 00 00 00 6B 50 7E 00 07 00 00 00 87 DE 83 00 06 00 00 00 99 CB
DC 00 2C 01 00 00 A1 9F 5E 00 02 00 00 00 DB B4 EF 00 07 00 01 00 00 00 06 00 00 00 18 7D C7 00 01 00 00 00 3D D7 34 01 31
01 00 00 56 73 7D 00 0B 00 00 00 6B 50 7E 00 01 00 00 00 90 D5 D0 00 05 00 00 00 98 29 B7 00 0B 00 00 00 E6 C5 31 00 01 00
04 00 00 00 3E 00 00 00 1A 9C B2 00 02 00 05 00 00 00 02 00 00 00 4F 87 1A 01 0A 00 00 00 9F C8 CA 00 02 00 64 00 00 00 03
00 00 00 42 1D 0B 01 06 00 00 00 46 1D 0B 01 07 00 65 00 00 00 35 00 00 00 1C 95 5C 00 0E 00 00 00 65 A6 9E 00 07 00 00 00
90 D5 D0 00 0B 00 00 00 9C A6 B4 00 C1 00 00 00 A2 05 06 00 EC 13 00 00 E6 C5 31 00 5E 01 00 00 F0 E0 B6 00 02 00 66 00 00
00 4B 00 00 00 65 A6 9E 00 5F 00 00 00 A2 05 06 00 01 00 67 00 00 00 0A 00 00 00 A2 05 06 00 02 00 68 00 00 00 0B 00 00 00
A2 05 06 00 01 00 00 00 B
C 6E B4 00 01 00 69 00 00 00 90 06 00 00 65 A6 9E 00 01 00 6B 00 00 00 07 00 00 00 65 A6 9E 00 01 00 70 00 00 00 06 00 00 00
65 A6 9E 00 01 00 72 00 00 00 8E 00 00 00 A2 05 06 00 01 00 73 00 00 00 36 00 00 00 65 A6 9E 00 01 00 77 00 00 00 07 00 00 00
65 A6 9E 00 01 00 7D 00 00 00 39 00 00 00 65 A6 9E 00 01 00 7F 00 00 00 40 00 00 00 65 A6 9E 00 01 00 97 00 00 00 10 00 00
00 BE B3 EF 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Notifications\Data\418A073AA3BC3475: 2B 02 00 00 00 00 00 00 04
00 04 00 01 02 06 00 00 00 00 12 00 00 00 0D 78 79 00 02 00 00 00 6B 50 7E 00 08 00 00 00 87 DE 83 00 06 00 00 00 99 CB
DC 00 47 01 00 00 A1 9F 5E 00 02 00 00 00 DB B4 EF 00 07 00 01 00 00 00 06 00 00 00 18 7D C7 00 02 00 00 00 3D D7 34 01 47
01 00 00 56 73 7D 00 0B 00 00 00 6B 50 7E 00 01 00 00 00 90 D5 D0 00 05 00 00 00 98 29 B7 00 0B 00 00 00 E6 C5 31 00 01 00
04 00 00 00 45 00 00 00 1A 9C B2 00 02 00 05 00 00 00 03 00 00 00 4F 87 1A 01 0A 00 00 00 9F C8 CA 00 02 00 64 00 00 00 04
00 00 00 42 1D 0B 01 08 00 00 00 46 1D 0B 01 07 00 65 00 00 00 35 00 00 00 1C 95 5C 00 0E 00 00 00 65 A6 9E 00 07 00 00 00
90 D5 D0 00 0B 00 00 00 9C A6 B4 00 C8 00 00 00 A2 05 06 00 DA 15 00 00 E6 C5 31 00 AD 01 00 00 F0 E0 B6 00 02 00 66 00 00
00 5B 00 00 00 65 A6 9E 00 5F 00 00 00 A2 05 06 00 01 00 67 00 00 00 11 00 00 00 A2 05 06 00 02 00 68 00 00 00 4D 00 00 00
A2 05 06 00 01 00 00 00 B
C 6E B4 00 01 00 69 00 00 00 27 08 00 00 65 A6 9E 00 01 00 6B 00 00 00 07 00 00 00 65 A6 9E 00 01 00 70 00 00 00 06 00 00 00
65 A6 9E 00 01 00 72 00 00 00 9E 00 00 00 A2 05 06 00 01 00 73 00 00 00 40 00 00 00 65 A6 9E 00 01 00 77 00 00 00 07 00 00 00
65 A6 9E 00 01 00 7D 00 00 00 43 00 00 00 65 A6 9E 00 01 00 7F 00 00 00 4A 00 00 00 65 A6 9E 00 01 00 97 00 00 00 12 00 00
00 BE B3 EF 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{1F4A5ADF-5C8A-4B1C-803C-
0970754DD23C}\DynamicInfo: 03 00 00 00 DC 16 F0 DE 87 4A D9 01 D2 AD E9 90 7A 77 D9 01 00 00 00 00 E7 2E 07 80 15 F2 F7
90 7A 77 D9 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{1F4A5ADF-5C8A-4B1C-803C-
0970754DD23C}\DynamicInfo: 03 00 00 00 DC 16 F0 DE 87 4A D9 01 A2 B9 6E 87 7D 77 D9 01 00 00 00 00 8F 2F 07 80 06 E7 8E
87 7D 77 D9 01
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{47597417-F213-4654-ADFC-
210B08F967A6}\DynamicInfo: 03 00 00 00 88 15 0F DF 87 4A D9 01 38 9B 5C E8 F9 4A D9 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{47597417-F213-4654-ADFC-
210B08F967A6}\DynamicInfo: 03 00 00 00 88 15 0F DF 87 4A D9 01 7F 0B 15 62 7D 77 D9 01 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00

HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows Search\Gather\Windows\SystemIndex\NewClientID: 0x00000012
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{0547A34B-7D7D-47B5-8407-EA3BC28D8AA2}: "95752304"
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows Search\UsnNotifier\Windows\Catalogs\SystemIndex\{0547A34B-7D7D-47B5-8407-EA3BC28D8AA2}: "279726440"
HKLM\SYSTEM\ControlSet001\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\ControlSet001\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\GraphicsDrivers\Configuration\NOEDID_15AD_0405_00000000_000F0000_0^20ED182961F2CFDB3A2D28C95A99744F\Timestamp: 0x01D9777A2EC04D5F
HKLM\SYSTEM\ControlSet001\Control\GraphicsDrivers\Configuration\NOEDID_15AD_0405_00000000_000F0000_0^20ED182961F2CFDB3A2D28C95A99744F\Timestamp: 0x01D9777D5A497F24
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\DefaultSettings.DriverExtra: FE FF FF FF FE FF FF FF 15 00 00 00 04 00 00 00 00 00 00 06 00 00 00
HKLM\SYSTEM\ControlSet001\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\DefaultSettings.DriverExtra: FE FF FF FF FE FF FF FF 15 00 00 00 04 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0002\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0002\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0003\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0003\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0004\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0004\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0005\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0005\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0006\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\ControlSet001\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0007\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\SequenceNumber: 0x00000027
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\SequenceNumber: 0x00000028
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Microsoft.Windows.Cortana_cw5n1h2txyewy: 50 2D BB FA 7A 77 D9 01 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Microsoft.Windows.Cortana_cw5n1h2txyewy: 1F 9E A2 70 7D 77 D9 01 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\InputApp_cw5n1h2txyewy: 63 45 14 E3 E2 4D D9 01 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00

HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\InputApp_cw5n1h2txywy: E6 E3 E2 96 7B 77 D9 01 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\windows.immersivecontrolpanel_cw5n1h2txywy: 87 75 D5 C4 7A 77 D9 01 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\windows.immersivecontrolpanel_cw5n1h2txywy: 6F 63 8C 37 7D 77 D9 01 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Device\HarddiskVolume3\Users\user\AppData\Local\Temp\Procmon64.exe: 39 3B 5A 43 7B 77 D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2169232433-3398496680-935370409-1000\Device\HarddiskVolume3\Users\user\AppData\Local\Temp\Procmon64.exe: AA 26 33 8C 7D 77 D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-90-0-1\SequenceNumber: 0x00000011
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-90-0-1\SequenceNumber: 0x00000029
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-90-0-1\Device\HarddiskVolume3\Windows\System32\dwm.exe: E2 CF 06 43 7A 77 D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-90-0-1\Device\HarddiskVolume3\Windows\System32\dwm.exe: AC 77 75 63 7D 77 D9 01 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\ControlSet001\Services\BITS\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\BITS\Start: 0x00000003
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4d36e968-e325-11ce-bfc1-08002be10318}\0000\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\CurrentControlSet\Control\GraphicsDrivers\Configuration\NOEDID_15AD_0405_00000000_000F0000_0^20ED182961F2CFDB3A2D28C95A99744F\Timestamp: 0x01D9777A2EC04D5F
HKLM\SYSTEM\CurrentControlSet\Control\GraphicsDrivers\Configuration\NOEDID_15AD_0405_00000000_000F0000_0^20ED182961F2CFDB3A2D28C95A99744F\Timestamp: 0x01D9777D5A497F24
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\DefaultSettings.DriverExtra: FE FF FF FF FE FF FF FF 15 00 00 00 04 00 00 00 00 00 00 00 06 00 00 00
HKLM\SYSTEM\CurrentControlSet\Control\UnitedVideo\CONTROL\VIDEO\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\DefaultSettings.DriverExtra: FE FF FF FF FE FF FF FF 15 00 00 00 04 00 00 00 00 00 00 00 02 00 00 00
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0000\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0001\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0002\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0002\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0003\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0003\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0004\VidPNSourceOfFlags: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0004\VidPNSourceOfFlags: 0x00000003
HKLM\SYSTEM\CurrentControlSet\Control\Video\{1309DFA1-B67B-11ED-A14C-BD247E05F284}\0005\VidPNSourceOfFlags: 0x00000002

ae14481203ce}\$\$windows.data.unifiedtile.localstartvolatiletilepropertiesmap\Current\Data: 02 00 00 00 82 A3 DD 51 7B 77 D9
01 00 00 00 00 43 42 01 00 0D 12 0A 0B 1A 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 43 00 4D 00 44
00 45 00 52 00 5C 00 43 00 4D 00 44 00 45 00 52 00 2E 00 45 00 58 00 45 00 C7 0A 43 39 9F 3A C5 14 01 C6 1E A0 BB 98 94 EA
AD D3 EC 01 00 36 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 52 00 45 00 47 00 53 00 48 00 4F 00 54
00 2D 00 58 00 36 00 34 00 2D 00 55 00 4E 00 49 00 43 00 4F 00 44 00 45 00 5C 00 52 00 45 00 47 00 53 00 48 00 4F 00 54 00
2D 00 58 00 36 00 34 00 2D 00 55 00 4E 00 49 00 43 00 4F 00 44 00 45 00 2E 00 45 00 58 00 45 00 C7 0A 8A B5 9A 3A C5 14 04
C6 1E A0 96 EA 8E B5 EF DD EC 01 00 23 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 0
0 53 00 59 00 53 00 49 00 4E 00 54 00 45 00 52 00 4E 00 41 00 4C 00 53 00 5C 00 50 00 52 00 4F 00 43 00 45 00 58 00 50 00 2E
00 45 00 58 00 45 00 C7 0A 18 3A 21 3A C5 14 02 C6 1E B0 AF D0 E8 B3 EF DD EC 01 00 23 57 00 7E 00 43 00 3A 00 5C 00 54 00
4F 00 4F 00 4C 00 53 00 5C 00 53 00 59 00 53 00 49 00 4E 00 54 00 45 00 52 00 4E 00 41 00 4C 00 53 00 5C 00 50 00 52 00 4F 00
43 00 4D 00 4F 00 4E 00 2E 00 45 00 58 00 45 00 C7 0A 3A 59 20 3A C5 14 02 C6 1E F0 92 A6 8E B4 EF DD EC 01 00 40 57 00 7E
00 4D 00 49 00 43 00 52 00 4F 00 53 00 4F 00 46 00 54 00 2E 00 41 00 55 00 54 00 4F 00 47 00 45 00 4E 00 45 00 52 00 41 00 54
00 45 00 44 00 2E 00 7B 00 43 00 42 00 46 00 34 00 36 00 39 00 39 00 39 00 2D 00 41 00 45 00 45 00 38 00 2D 00 45 00 43 00
41 00 41 00 2D 00 37 00 36 00 41 00 38 00 2D 00 38 00 41 00 30 00 31 00 43 00 46 00 43 00 31 00 36 00 34 00 36 00 30 00 7D
00 C7 0A 9F 7F 23 3A C5 14 02 C6 1E 90 CC C4 9B B0 EF DD EC 01 00 1C 57 00 7E 00 4D 00 49 00 43 00 52 00 4F 00 53 00 4F 00
46 00 54
00 2E 00 57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 2E 00 45 00 58 00 50 00 4C 00 4F 00 52 00 45 00 52 00 C7 0A 8B C4 FB 3C
C5 14 07 C6 1E D0 E2 BD DC E0 AE D3 EC 01 00 08 57 00 7E 00 4D 00 53 00 45 00 44 00 47 00 45 00 C7 0A AB EE 22 3B C5 14 02
C6 1E F0 98 D3 AB B3 EF DD EC 01 00 30 57 00 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00
45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31
00 39 00 38 00 42 00 37 00 7D 00 5C 00 43 00 4D 00 44 00 2E 00 45 00 58 00 45 00 C7 0A F9 4D 37 3B C5 14 03 C6 1E 80 8B F7
C8 B2 EF DD EC 01 00 34 57 00 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D
00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00
42 00 37 00 7D 00 5C 00 4E 00 4F 00 54 00 45 00 50 00 41 00 44 00 2E 00 45 00 58 00 45 00 C7 0A 19 AF 99 3C C5 14 02 C6 1E
B0 CB AE D9 D4
E1 D2 EC 01 00 43 57 00 7E 00 7B 00 36 00 44 00 38 00 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41 00 46 00 30 00 2D 00 34
00 34 00 34 00 42 00 2D 00 38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 37 00 33 00 46 00 30 00 32 00 32 00 30 00 30 00
45 00 7D 00 5C 00 49 00 44 00 41 00 20 00 46 00 52 00 45 00 45 00 57 00 41 00 52 00 45 00 20 00 37 00 2E 00 36 00 5C 00 49 00
44 00 41 00 36 00 34 00 2E 00 45 00 58 00 45 00 C7 0A 41 26 A5 3A C5 14 01 C6 1E 90 C1 85 88 ED AD D3 EC 01 00 40 57 00 7E
00 7B 00 36 00 44 00 38 00 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41 00 46 00 30 00 2D 00 34 00 34 00 34 00 42 00 2D 00
38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 37 00 33 00 46 00 30 00 32 00 32 00 30 00 30 00 45 00 7D 00 5C 00 57 00 49
00 52 00 45 00 53 00 48 00 41 00 52 00 4B 00 5C 00 57 00 49 00 52 00 45 00 53 00 48 00 41 00 52 00 4B 00 2E 00 45 00 58 00 45
00 C7 0A 5C D6 24 3A C5 14 02 C6 1E D0 E9 AE A0 B2 EF DD EC 01 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\CloudStore\Store\Cache\DefaultAccount\%de\$ab38e29e-5064-4a27-bea8-
ae14481203ce}\$\$windows.data.unifiedtile.localstartvolatiletilepropertiesmap\Current\Data: 02 00 00 00 D5 5B F4 2B 7D 77 D9
01 00 00 00 00 43 42 01 00 0D 12 0A 0B 1A 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 43 00 4D 00 44
00 45 00 52 00 5C 00 43 00 4D 00 44 00 45 00 52 00 2E 00 45 00 58 00 45 00 C7 0A 36 56 8C 3A C5 14 01 C6 1E A0 BB 98 94 EA
AD D3 EC 01 00 36 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 00 52 00 45 00 47 00 53 00 48 00 4F 00 54
00 2D 00 58 00 36 00 34 00 2D 00 55 00 4E 00 49 00 43 00 4F 00 44 00 45 00 5C 00 52 00 45 00 47 00 53 00 48 00 4F 00 54 00
2D 00 58 00 36 00 34 00 2D 00 55 00 4E 00 49 00 43 00 4F 00 44 00 45 00 2E 00 45 00 58 00 45 00 C7 0A E1 8F 98 3B C5 14 04
C6 1E A0 96 EA 8E B5 EF DD EC 01 00 23 57 00 7E 00 43 00 3A 00 5C 00 54 00 4F 00 4F 00 4C 00 53 00 5C 0
0 53 00 59 00 53 00 49 00 4E 00 54 00 45 00 52 00 4E 00 41 00 4C 00 53 00 5C 00 50 00 52 00 4F 00 43 00 45 00 58 00 50 00 2E
00 45 00 58 00 45 00 C7 0A 3A 25 24 3A C5 14 02 C6 1E B0 AF D0 E8 B3 EF DD EC 01 00 23 57 00 7E 00 43 00 3A 00 5C 00 54 00
4F 00 4F 00 4C 00 53 00 5C 00 53 00 59 00 53 00 49 00 4E 00 54 00 45 00 52 00 4E 00 41 00 4C 00 53 00 5C 00 50 00 52 00 4F 00
43 00 4D 00 4F 00 4E 00 2E 00 45 00 58 00 45 00 C7 0A 3A 25 24 3A C5 14 02 C6 1E F0 92 A6 8E B4 EF DD EC 01 00 40 57 00 7E
00 4D 00 49 00 43 00 52 00 4F 00 53 00 4F 00 46 00 54 00 2E 00 41 00 55 00 54 00 4F 00 47 00 45 00 4E 00 45 00 52 00 41 00 54
00 45 00 44 00 2E 00 7B 00 43 00 42 00 46 00 34 00 36 00 39 00 39 00 39 00 2D 00 41 00 45 00 45 00 38 00 2D 00 45 00 43 00
41 00 41 00 2D 00 37 00 36 00 41 00 38 00 2D 00 38 00 41 00 30 00 31 00 43 00 46 00 43 00 31 00 36 00 34 00 36 00 30 00 7D
00 C7 0A 60 FB 45 3B C5 14 02 C6 1E 90 CC C4 9B B0 EF DD EC 01 00 1C 57 00 7E 00 4D 00 49 00 43 00 52 00 4F 00 53 00 4F 00
46 00 54
00 2E 00 57 00 49 00 4E 00 44 00 4F 00 57 00 53 00 2E 00 45 00 58 00 50 00 4C 00 4F 00 52 00 45 00 52 00 C7 0A 5D BA 17 3D
C5 14 07 C6 1E D0 E2 BD DC E0 AE D3 EC 01 00 08 57 00 7E 00 4D 00 53 00 45 00 44 00 47 00 45 00 C7 0A 08 65 34 3B C5 14 02
C6 1E F0 98 D3 AB B3 EF DD EC 01 00 30 57 00 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00
45 00 37 00 2D 00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31
00 39 00 38 00 42 00 37 00 7D 00 5C 00 43 00 4D 00 44 00 2E 00 45 00 58 00 45 00 C7 0A 47 E1 67 3B C5 14 03 C6 1E 80 8B F7
C8 B2 EF DD EC 01 00 34 57 00 7E 00 7B 00 31 00 41 00 43 00 31 00 34 00 45 00 37 00 37 00 2D 00 30 00 32 00 45 00 37 00 2D
00 34 00 45 00 35 00 44 00 2D 00 42 00 37 00 34 00 34 00 2D 00 32 00 45 00 42 00 31 00 41 00 45 00 35 00 31 00 39 00 38 00

9926F41749EA)\Count\{6Q809377-6NS0-4440-8957-N3773S02200R}\Jverfunex\Jverfunex.rkr: 00 00 00 00 01 00 00 00 04 00 00
00 39 15 01 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00
00 80 BF FF FF FF FF D0 B4 0B 24 7B 77 D9 01 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA)\Count\:\Hfref\hfre\NccQngn\Ybpny\Grzc\cebprkc64.rkr: 00 00 00 00 00 00 00 00 00 00 00 11 05 00 00 00
00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00
FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA)\Count\:\Hfref\hfre\NccQngn\Ybpny\Grzc\cebprkc64.rkr: 00 00 00 00 00 00 00 00 04 00 00 00 45 05 02 00 00
00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF
FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA)\Count\:\Hfref\hfre\NccQngn\Ybpny\Grzc\Cebpzba64.rkr: 00 00 00 00 00 00 00 00 01 00 00 00 64 0C 00 00 00
00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF
FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA)\Count\:\Hfref\hfre\NccQngn\Ybpny\Grzc\Cebpzba64.rkr: 00 00 00 00 00 00 00 00 05 00 00 00 A8 B3 05 00 00
00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF
FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA)\Count\:\Gbbyf\Ertfubg-k64-Havpbqr\Ertfubg-k64-Havpbqr.rkr: 00 00 00 00 02 00 00 00 01 00 00 00 A9 0A 01
00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00
FF FF FF 20 8B DA 51 7B 77 D9 01 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-
9926F41749EA)\Count\:\Gbbyf\Ertfubg-k64-Havpbqr\Ertfubg-k64-Havpbqr.rkr: 00 00 00 00 02 00 00 00 05 00 00 00 4A DF 02
00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00
FF FF FF 20 8B DA 51 7B 77 D9 01 00 00 00 00
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Group
Policy\PolicyApplicationState\PolicyState: 0x00000000
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Microsoft\Windows\CurrentVersion\Group
Policy\PolicyApplicationState\PolicyState: 0x00000000
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\QuietHoursTelemetryLastRun: 0D 03 FC 63 00 00 00
00
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Notifications\Settings\QuietHoursTelemetryLastRun: 7C D8 47 64 00 00 00
00
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Search\InstalledWin32AppsRevision: "{B898FCEC-846E-4AA8-9957-
A79C6836A635}"
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Search\InstalledWin32AppsRevision: "{52EAE5EF-DF92-4ECB-8426-
444C8A67DE5D}"
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Search\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppsConstraintIndex\
LatestConstraintIndexFolder:
"C:\Users\user\AppData\Local\Packages\Microsoft.Windows.Cortana_cw5n1h2txyewy\LocalState\ConstraintIndex\Apps_{316a5
7f0-09ff-4d5a-8c53-c7cf23778cd2}"
HKU\S-1-5-21-2169232433-3398496680-935370409-
1000\Software\Microsoft\Windows\CurrentVersion\Search\Microsoft.Windows.Cortana_cw5n1h2txyewy\AppsConstraintIndex\
LatestConstraintIndexFolder:

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AU\App\V
1\LU\PCT: 0x01D9777B966E0E1D

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AU\App\V
1\LU\ICT: 0x01D94D6E69AE558F

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AU\App\V
1\LU\ICT: 0x01D9777B96E53FC9

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AU\App\V
1\LU\ITT: 0x01D94D6E69BCA362

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AU\App\V
1\LU\ITT: 0x01D9777B96F3924E

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ContentDeliveryManager
_cw5n1h2txyewy\HAM\AU\App\V1\LU\PCT: 0x01D9777AD67DE092

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ContentDeliveryManager
_cw5n1h2txyewy\HAM\AU\App\V1\LU\PCT: 0x01D9777BAE8B9981

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ContentDeliveryManager
_cw5n1h2txyewy\HAM\AU\App\V1\LU\PTT: 0x01D9777AD8A1A297

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ContentDeliveryManager
_cw5n1h2txyewy\HAM\AU\App\V1\LU\PTT: 0x01D9777BB04A9B4C

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyew
y\HAM\AU\CortanaUI\V1\LU\ITT: 0x01D94DE2E2DFD179

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyew
y\HAM\AU\CortanaUI\V1\LU\ITT: 0x01D9777A5D837BE1

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyew
y\HAM\AU\CortanaUI\V1\LU\PTT: 0x01D9777AFABC1118

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyew
y\HAM\AU\CortanaUI\V1\LU\PTT: 0x01D9777D5EBEA10C

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw
5n1h2txyewy\HAM\AU\App\V1\LU\ICT: 0x01D9777AD679607F

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw
5n1h2txyewy\HAM\AU\App\V1\LU\ICT: 0x01D9777B975D5359

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw
5n1h2txyewy\HAM\AU\App\V1\LU\ITT: 0x01D9777ADA88ED4E

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw
5n1h2txyewy\HAM\AU\App\V1\LU\ITT: 0x01D9777B9AF47283

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\windows.immersivecontrolpanel_cw5n1h2tx
yewy\HAM\AU\microsoft.windows.immersivecontrolpanel\V1\LU\PTT: 0x01D94F38BB74DBC4

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\windows.immersivecontrolpanel_cw5n1h2tx
yewy\HAM\AU\microsoft.windows.immersivecontrolpanel\V1\LU\PTT: 0x01D9777D37912CB4

HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx: 03 00 00 00 00 00 00 02 00 00 00 01 00 00 00 FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-1000\Software\Classes\Local
Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx: 01 00 00 00 00 00 00 03 00 00 00 02 00 00 00 FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AUI\App\V
1\LU\PCT: 0x01D94D6E69967DBA
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AUI\App\V
1\LU\PCT: 0x01D9777B966E0E1D
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AUI\App\V
1\LU\ICT: 0x01D94D6E69AE558F
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AUI\App\V
1\LU\ICT: 0x01D9777B96E53FC9
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AUI\App\V
1\LU\ITT: 0x01D94D6E69BCA362
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\InputApp_cw5n1h2txyewy\HAM\AUI\App\V
1\LU\ITT: 0x01D9777B96F3924E
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ContentDeliveryManager
_cw5n1h2txyewy\HAM\AUI\App\V1\LU\PCT: 0x01D9777AD67DE092
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ContentDeliveryManager
_cw5n1h2txyewy\HAM\AUI\App\V1\LU\PCT: 0x01D9777BAE8B9981
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ContentDeliveryManager
_cw5n1h2txyewy\HAM\AUI\App\V1\LU\PTT: 0x01D9777AD8A1A297
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ContentDeliveryManager
_cw5n1h2txyewy\HAM\AUI\App\V1\LU\PTT: 0x01D9777BB04A9B4C
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyew
y\HAM\AUI\CortanaUI\V1\LU\ITT: 0x01D94DE2E2DFD179
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyew
y\HAM\AUI\CortanaUI\V1\LU\ITT: 0x01D9777A5D837BE1
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyew
y\HAM\AUI\CortanaUI\V1\LU\PTT: 0x01D9777AFABC1118
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.Cortana_cw5n1h2txyew
y\HAM\AUI\CortanaUI\V1\LU\PTT: 0x01D9777D5EBEA10C
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw
5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 0x01D9777AD679607F
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw
5n1h2txyewy\HAM\AUI\App\V1\LU\ICT: 0x01D9777B975D5359
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw
5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 0x01D9777ADA88ED4E
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\Microsoft.Windows.ShellExperienceHost_cw
5n1h2txyewy\HAM\AUI\App\V1\LU\ITT: 0x01D9777B9AF47283

HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\windows.immersivecontrolpanel_cw5n1h2tx
yewy\HAM\AUI\microsoft.windows.immersivecontrolpanel\V1\LU\PTT: 0x01D94F38BB74DBC4
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\windows.immersivecontrolpanel_cw5n1h2tx
yewy\HAM\AUI\microsoft.windows.immersivecontrolpanel\V1\LU\PTT: 0x01D9777D37912CB4
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx: 03 00 00 00 00 00 00 00 02 00 00 00 01 00 00 00 FF FF FF FF
HKU\S-1-5-21-2169232433-3398496680-935370409-1000_Classes\Local
Settings\Software\Microsoft\Windows\Shell\BagMRU\2\MRUListEx: 01 00 00 00 00 00 00 00 03 00 00 00 02 00 00 00 FF FF FF FF

Total changes: 1184
