TREND MICRO | research

Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware

By Daniel Lunghi and Kenney Lu

APPENDIX

Indicators of Compromise (IoCs)

SHA-256 Hashes

SHA-256	Filename	Detection Name	Malware Family
0aef64991f9121a244c3f3bf7f5448bb8fb2c858bcf0ff26b3b663937af9ef40	c	HackTool.Linux.ReverseProxy.AA	Modified FRP
0e3cc4de26f59e4bee6760bdb1fb8cb9f48dc18aad1d8909c736a1a12841e1dd	thumb.db	Trojan.Win32.HYPERBRO.AA.enc	HyperBro
0e4becf70bb3c624b24d38f44bf92bd510f0ff718df2e3db8b71ef009189f072	DLPPREM32.DLL	Trojan.Win32.SYSUPDATE.BYY	SysUpdate
10ca2b47daaadb716b12a2b071de01e86c902e11263dc39e396be642adf369ce	config.data	TROJ_FRS.VSNTCT21	SysUpdate
15d404e03f1335a3e4a9e691a3f57b3765823249d5f28a23a728dab6f19cedc0	shjdh23423.bin	TROJ_ZBOTENC.ZCHE-A	Pandora rootkit
1ac0be7d289f2bbd00979069b9d3bf6ac76c0828c0ca7674ec791cdb463b8ff0	FPMMC.dll	TROJ_GEN.R002C0RLM20	SysUpdate
1b07b070eeec2744c7be733590a5694cd1ee9e967249a8efa50d3243468aa7b1		TROJ_GEN.R002C0DL420	HyperBro
244cc119ec1e77262f48dc5d2fc285ed4904b30b44ea28bf41f531cfb75cff99	mpsvc.dll	TROJ_FRS.VSNTCT21	Type 1
310524c47128a0095a923aea045db3b0bb999af41a77953667f2d812e6f08634	SETUPENGINE.hlp	Trojan.Win64.PANDORA.A.enc	Pandora rootkit
36fad80a5f328f487b20a3f5fc5f1902d50cbb1bd9167c44b66929a1288fc6f4	thinhostprobedll.dll	TROJ_GEN.R002C0DKU20	HyperBro
3e04eb55095ad6a45905564d91f2ab6500e07afcdf9d6c710d6166d4eef28185	Sosyal Güvenlik Reformu-Not-3.doc	TROJ_FRS.0NA103CT21	HyperBro
4123a19cda491f4d31a855e932b8b7afdcf3faf5b448f892da624c768205a289	Questions for Exit Interview_russian.doc	TROJ_FRS.0NA103CU21	SysUpdate
434cbc840f64033d64f76de7234afb05fddf582195c68bf8f786dd22daaa1c21	LIBVLC.dll	TROJ_FRS.VSNTAR21	SysUpdate
4f01ccf39dd17b3820b3ae2c650dab8d508254db6022b4aacf43d908e0fec678	SETUPENGINE.hlp	TROJ_FRS.VSNTCT21	Pandora rootkit
4f6987f39b14372d724086cbafc87de37d4b0f78491af93de1161f0b6ed413a7	thumb.dat	Trojan.Win32.HYPERBRO.AA.enc	HyperBro
4fce3d38e0a308088cd75c2ef1bb5aa312e83447d63a82f62839d3609a283b02	ASTEL.doc	TROJ_FRS.0NA103CU21	SysUpdate
52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7	vftrace.dll	Trojan.Win32.HYPERBRO.AB	HyperBro
5665fbb579e72e5b7a891389181c1cd9c6162bc684948483f1a0a685c134d848		Backdoor.Win32.HYPERBRO.END	HyperBro
5a98c49b4e5d980bc8078cbbd8899397e95a488234a87a12813fe437c585600f		Trojan.Win32.HYPERBRO.AA.enc	HyperBro
5d7ceaa3947d08636070f102772190ce7267d8f7d8e9fd58b29573b229de6599	DLPPREM32.bin	Trojan.Win32.SYSUPDATE.BYY.enc	SysUpdate
601a02b81e3bd134c2cf681ac03d696b446e10bf267b11b91517db1b233fec74	thumb.dat	Trojan.Win32.HYPERBRO.AA.enc	HyperBro

69f1914582f66ed216369d3a95842d58de9dffdbe8ae98712513c4ce142658ea	dummy_64.sys	Rootkit.Win64.HIDDEN.A	Hidden rootkit
6e1e74b0a064cc7d9aba8e485417632d7a55e0ff4ba9b078358ce9dd8b85ece4	SETUPENGINE.dll	TROJ_FRS.0NA103CT21	SysUpdate
734373b9d486c0a29a5b849f65cc060f461c471f318b61e122d813432a0bb752	mpsvc.dll	TROJ_FRS.0NA103CT21	Type 1
74780cd444b41d2fc8438f71528923d3ab297deed0fd1588d6d0c6707aecdc13	thumb.dat	Trojan.Win32.HYPERBRO.AA.enc	HyperBro
788bd34d3c5d12b9767f8ac5587f1970597c47fb06713a6070d430a593bb4945		TROJ_GEN.R002C0DKU20	HyperBro
7b007e0989e57e4507888cbb7ddd1c59002ba9e2071c36ac2e6d8e44648cda11	libgcj.vlc	Trojan.Win32.SYSUPDATE.BZA.enc	SysUpdate
7fa187c76316a428b0d0cecb8e5e12893a2b020fecde540246bb30d7f8868199	thumb.dat	Trojan.Win32.HYPERBRO.AA.enc	HyperBro
809aa69cd6c335f100baef5fa7897b153762e527bb811d2c570e8b3c7448f3b6	mpsvc.dll	TROJ_FRS.0NA103CT21	HyperBro
80fc8917c91c132e5274319013a4b659e435e8de8abf655cf3482798acb8650a	thumb.db	Trojan.Win32.HYPERBRO.AA.enc	HyperBro
83406f39147b01136bf9b3b88a1ec1a9339cd9d0cbcfa2a2583e3f97ad852287	thumb.dat	Trojan.Win32.HYPERBRO.AB.enc	HyperBro
9000ce3c0e01b6c80edb3af87aad8117513ce334135aa7d7b1c2afa067f4c4ab	sllauncherENU.dll	TROJ_GEN.R002C0DB321	HyperBro
900d6356e8a35f8fa6477cbc6a6bc79aa7a08c73773809965398b399d6833a5b	HiddenCLI.exe	Rootkit.Win64.HIDDEN.A	Hidden rootkit
91ac0dcb290f3d32a6607f2a21f0b2df4d413c3f44923bec8ce9466131dde8b0	SETUPENGINE.DLL	TROJ_FRS.VSNTDC21	Pandora rootkit
92bbcb5461ab5959e31f997a6df77995377d69f8077e43e5812fcbe9303d831c	mpsvc.dll	TROJ_FRS.0NA103CT21	HyperBro
942213df53d2c84a0efdd7c6a72ea4767cb4fa5f339bd86f7188be605818904e	thumb.dat	Trojan.Win32.HYPERBRO.AA.enc	HyperBro
999b1e31893d02dcef20a3846ad7e96153b0057b960488ad8b07c4d9c33d099e	LIBVLC.dll	TROJ_FRS.VSNTAR21	SysUpdate
9ae06dee8248c9e794e0ebae3274b25b280219068b73923783eb7dfea1358ec1		Trojan.Win32.HYPERBRO.AC	HyperBro
a4c7fe8278be79ce0bb0eca168412d5d25305dfc71b062af91e8cabbc8164783	data.res	Trojan.Win32.SYSUPDATE.BYY.enc	SysUpdate
a5d8cae9de9edf81d4898879b09c16d6afd12f1bdc320acdbc5c8a430831e55b	8.t	TROJ_FRS.0NA103CU21	SysUpdate
ab6998352fc0d745af94f02e42f8c3f061a99179fce2c890760f293f9744d1e8	GvG36a467C6Hkea	TROJ_FRS.VSNTCU21	SysUpdate
af31c16dcd54ee11d425eb3a579ad0606a05b36c0605cc16007f3d3c84d8e291	UPDSPAPI.dll	TROJ_ZBOT.ZCHE-A	Pandora rootkit
b39e2cf333b9f854bcdf993aa6c1f357d2a7042139e4c6ca47ed504090006a61		Trojan.Win32.SYSUPDATE.BZA.enc	SysUpdate
b945275314566e970c078316d9039171246b8ecbbe57cd424f1f486782d5aa61	thumb.dat	Backdoor.Win32.HYPERBRO.ENF.enc	HyperBro
d396eecf91cb35bc96d740e3d4aa7cac1143a98c3e185980731a48b1aad0bfd9	drv64.sys	Rootkit.Win64.PANDORA.A	Pandora rootkit
d40414b1173d59597ed1122361fe60303d3526f15320aede355c6ad9e7e239af	thinhostprobedll.dll	TROJ_GEN.R002C0DL420	HyperBro
d474198fd5ab7800cf00afbff16b258493529bc0e8451fb9382250a15ae29edb	utils.dll	TROJ_FRS.VSNTCT21	Hidden rootkit

e05e853cca1a8e9c8b1674f59c27b562887742f3110499f8ff38d0d287f0e7de		Trojan.Win32.SYSUPDATE.BZA.enc	SysUpdate
e123481468938fd56eeb506148db923033c3b1ed1d09088640fcf9031cd583c9	mpsvc.dll	TROJ_FRS.VSNTCT21	Type 1
e21360d6411ec9a719789e0f82dad5e380ee4a81faa3ebc072c8779e2a1da5ed	mpsvc.dll	TROJ_FRS.VSNTCT21	HyperBro
e657b213e87e1066de110cb4010e1c57250ebe46f08d2b9abc99a1b7c3e2d0dc	SETUPENGINE.DLL	TROJ_GEN.R03BC0WLB20	Pandora rootkit
e74056a729e004031b78007708bb98d759ff94b46866898c5a05d87013cd643c	vftrace.dll	Backdoor.Win32.HYPERBRO.ENF	HyperBro
ef51b08234488b6cb51eb949dff5b7421e9a040f73c10a40d5320dac561d944f		TROJ_FRS.0NA103CT21	SysUpdate
f944aa7f829f4129953e42026649179fc741def0dbd04d2cd5285501f8d4af5e		TROJ_FRS.VSNTDC21	Pandora rootkit
f9f3cdf8cca3cb138be71066314b1d6431de52a647b067efa87b2df7a9a3ae50	LIBVLC.hlp	Trojan.Win32.SYSUPDATE.BZA.enc	SysUpdate
fee067f6fe10f4d3f49fd082a2eb48619c4d43fc98bc689b3740cb862ff77d24		TROJ_GEN.R002C0DB321	HyperBro
92d53b227eac5ba0935726c86d8f0f456ab8429473bca4f68858448e92c6fade	HiddenService.exe	Rootkit.Win64.HIDDEN.A	Hidden rootkit
5cae9a425ed6a030390e7b104bf49836b0a1bdd86c0d345ce7a74b2207807459	Hidden.sys	TROJ_FRS.VSNTCT21	Hidden rootkit

SysUpdate URLs

URL	Category
139[.]59[.]81[.]253	C&C Server
34[.]93[.]247[.]126	C&C Server
45[.]142[.]214[.]188	C&C Server

HyperBro URLs

URL	Category
hxxp://35.187.148.253:443/api/v2/ajax	C&C Server
hxxps://89.35.178.105:443/api/v2/ajax	C&C Server
ns162[.]nsakadns[.]com:443/api/v2/ajax	C&C Server
104[.]209[.]198[.]177:443/api/v2/ajax	C&C Server
35[.]220[.]135[.]85:443/api/v2/ajax	C&C Server
47[.]75[.]49[.]32:443/api/v2/ajax	C&C Server
85[.]204[.]74[.]143:443/ajax	C&C Server
139[.]180[.]208[.]225:443/ajax	C&C Server
103[.]79[.]78[.]48	C&C Server
107[.]148[.]131[.]210:443/api/v2/ajax	C&C Server

Type 1 Malware URLs

URL	Category
settings-win[.]dyndns-office[.]com	C&C Server

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com