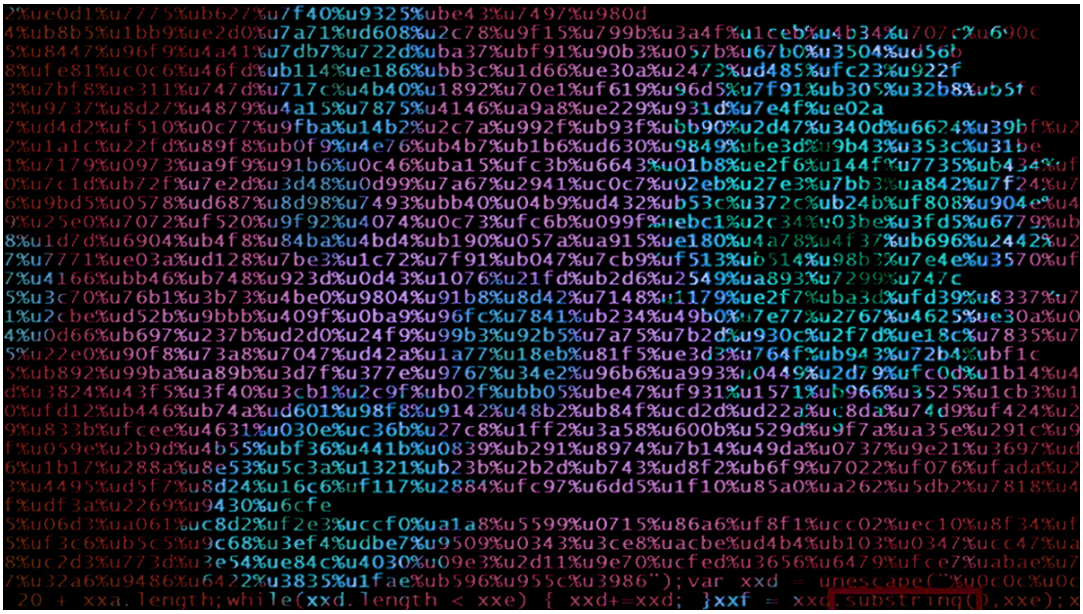
The Daily Swig
Cybersecurity news and views

Strategies for combating increased cyber threats tied to coronavirus

David Oberly 07 July 2020 at 16:09 UTC

Coronavirus | Cyber-attacks | Deep Dives

Although some countries are now emerging from lockdown, the precipitous rise in cyber-attacks tied to Covid-19 shows no sign of slowing, writes David Oberly



As the world grapples with the immediate public health and economic fallout of the Covid-19 pandemic, a related crisis has simultaneously emerged: a significant uptick in cyber-attacks seeking to exploit the global health emergency.

The novel coronavirus has created a perfect storm for cybercriminals, who have found a once-in-a-lifetime opportunity to cash in on the fear and panic gripping the world, as well as targeting companies and their workers with sophisticated cyber-attacks that integrate Covid-19 themes.

Consequently, businesses across all industries must take appropriate measures to effectively mitigate the threat posed by these enhanced cyber risks, which are expected to continue their upward trajectory for the duration of the pandemic.

The current threat landscape

Since the onset of the coronavirus crisis, cybercriminals have engaged in a concerted campaign of relentless, Covid-19-themed cyber-attacks designed to exploit the current crisis for a quick payday.

In particular, the most dangerous Covid-19 cyber threats that companies face today are phishing, business email compromise (BEC) scams, ransomware, and remote working vulnerabilities.

Phishing

Phishing involves fraudulent communications – most commonly emails – that appear to originate from a reputable source.

These messages are designed to trick recipients into doing a variety of things, including disclosing sensitive information, clicking on links that will inject malware into the recipient's device, or transferring money directly to cybercriminals.

Phishing scams have been prevalent since the start of the pandemic, as cybercrooks quickly seized the opportunity to exploit the fear, anxiety, and uncertainty generated by the health crisis, as well as the public's

Latest Posts

FireEye launches first public bug bounty program
Security vendor asks researchers to test core infrastructure

Fall in healthcare data breaches could be due to 'pandemic distraction'
Experts caution against drawing sanguin conclusions from latest US health department data

TinyMCE suffers big XSS flaw
Inadequate sanitization checks result in web security flaw in HTML text editor

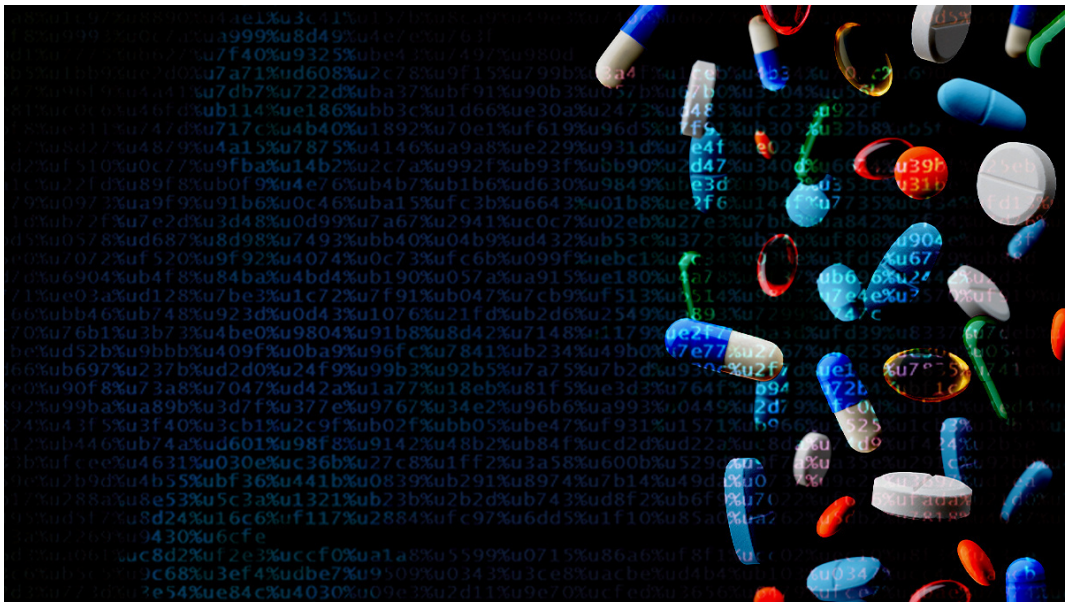
hunger for information about the virus.

RELATED Researchers identify new e-book phishing scam impersonating the WHO

Between the start of 2020 and the end of March alone, malicious phishing activity jumped a staggering 350%, according to data from Google. In April, the search giant reported that its Threat Analysis Group blocked 18 million Covid-19-themed phishing and malware emails per day.

Most of the coronavirus-themed phishing attacks to date have focused on impersonating major health organizations and offering fake Covid-19-related news.

Recently, however, cybercriminals have transitioned to impersonating popular tech platforms to mask their schemes, such as by sending fraudulent Zoom meeting invitations to deploy malware and spoofing Skype login pages to steal user credentials.



Coronavirus scammers have been impersonating healthcare organizations

BEC scams

BEC scams are specialized phishing attacks that involve tricking victims – often those who perform legitimate funds transfers – to make unauthorized wire transfers or send funds directly to cybercriminals.

While criminals have targeted company personnel with control over corporate financial accounts long before the current pandemic, they have added a new twist to their scams by including themes tied to Covid-19 – again, to leverage the fear, anxiety, and uncertainty that the world is experiencing.

READ MORE Coronavirus response: How security certification and training orgs are tackling the global disruption

Already a highly sophisticated scheme relying heavily on social engineering, the addition of Covid-19 themes has made this type of attack even more difficult to defend against during the current pandemic.

The rise in BEC scams has been so sharp that the FBI decided to issue two separate alerts warning businesses of the growing threat.

The US intelligence agency warns that cybercriminals are actively exploiting the uncertainty surrounding the Covid-19 pandemic to bolster the credibility of BEC scams, and advises businesses to anticipate an ongoing increase in BEC scams tied to the global health emergency.

Ransomware

Ransomware is a form of malicious malware that allows attackers to extort victims for financial gain by blocking access to files on infected networks until the victim pays a fee, or 'ransom'.

While hackers continue to leverage phishing scams to deploy ransomware, Remote Desktop Protocol (RDP) access attacks have become the most popular attack vector during the current pandemic – due in large part to the record number of employees now working from home.

Read more of the latest coronavirus-related security news

One of the most common ransomware attacks since Covid-19 spread rapidly beyond China's borders has been the use of a malicious Android app, which appears to offer users a real-time outbreak tracker, but also installs CovidLock ransomware when downloaded on a user's device.

A second common ransomware scheme has been the use of emails claiming to come from the Centers for Disease Control and Prevention (CDC) purporting to offer links to information on the virus, which also deploy malware when clicked.

Remote working

When employees were forced to work from home in the early stages of the pandemic, cybercriminals immediately turned their attention to exploiting the often-inadequate security postures and other unique vulnerabilities that result from remote working.

INSIGHT Coronavirus: How to work from home securely during a period of isolation

Remote working significantly enhances the threat of cyber incidents stemming from careless or negligent employees, who often fail to adhere to safe computing practices while working outside of the corporate security perimeter.

At the same time, remote working also enhances the risk of insider threats arising from malicious actors who intentionally misuse company data for financial gain or other personal benefit.

And if that wasn't enough, remote working also brings with it significant technical vulnerabilities, such as insufficiently secure connections.

How to defend against coronavirus-themed cyber threats

Taken together, cyber threats are at an all-time high. Fortunately, there are several actionable steps companies can take to minimize the risks posed by cyber-attacks that use Covid-19 themes or exploit new working practices.

Education and training: Workers must be trained in how to secure sensitive company data and neutralize attempted cyber-attacks, the most common attack scenarios, and avoid falling victim to Covid-19 cyber-scams.

Teleworking policies: With organizations obliged to continue remote working arrangements for the foreseeable future, companies should implement strong, comprehensive teleworking policies that address the security of company networks and data while employees work outside of the office. In particular, they should define the scope of permissible bring-your-own-device (BYOD) practices, and acceptable uses of company technology while working remotely.

Data backups: Organizations should complete backups of all data at regular intervals to eliminate the leverage that cybercriminals gain through a successful ransomware attack. Backups should be stored offsite and be tested routinely for data integrity and functionality.

Data monitoring: Organizations should monitor workers' use of electronic data, with an eye toward unusual activity – especially if data is being pulled off the company's network. Data monitoring can not only detect data leaks, but also discourage employees from taking unnecessary risks when accessing or handling company data.

Incident response/disaster recovery plans: Finally, companies should maintain incident response and disaster recovery plans that can be implemented immediately, with adequate resources, in the event of a data breach or cyber-attack. These plans should be periodically reviewed with input from key personnel to ensure that everyone is up to speed on their roles and responsibilities.

Security best practices

Ultimately, the precipitous rise in cyber-attacks tied to Covid-19 will continue apace – if not increase – for the duration of the global health crisis.

Now more than ever, businesses must consistently and aggressively apply security best practices to manage and defend against these burgeoning threats.

By implementing the best practices discussed above, companies can harden their human and technical cyber defenses – not just for the duration of the pandemic but also when Covid-19 is, mercifully, in our collective rear-view mirror.

YOU MIGHT ALSO LIKE Cybercrime report: Malware slingers riding the crest of the coronavirus pandemic

Coronavirus | Cyber-attacks | Deep Dives | US | Social Engineering | Healthcare | Policy and Legislation | Organizations | Data Breach | Cybercrime | Hacking News | Hacking Techniques | Network Security | Cloud Security | Education | Email Security | Ransomware | Malware | Mobile

David Oberly

@DavidJOberly

Related stories

FireEye launches first public bug bounty program

13 August 2020

Fall in healthcare data breaches could be due to 'pandemic distraction'

13 August 2020

TinyMCE suffers big XSS flaw

13 August 2020

US DoJ to shut down 300 fraudulent coronavirus websites

13 August 2020