allot
See. Control. Secure.

Threat Bulletin

COVID-19 Cyber Threats

April 2020

Cyber Threats – The Coronavirus Angle

On March 11, the World Health Organization (WHO) declared COVID-19 outbreak a pandemic, covering, at that time, over 110 countries and territories around the world. Many countries are currently in various states of lockdown. Universities are moving their classes online, businesses are going remote, and financial markets are suffering historic losses. The global pandemic is dramatically affecting almost every aspect of our lives. Cybersecurity is no exception.

As Covid-19 continues to spread across the globe and countries do their best to slow down the infection rate, hackers are taking advantage of the situation. Cybercriminals always closely follow the news agenda and are on the lookout for new themes and trending global topics to adjust their tactics. They are thrilled with the current global health crisis which provides them a perfect opportunity to capitalize on people's fears, concerns and general uncertainty.

Bad actors are using the pandemic to launch global phishing campaigns, distribute malware and collect personal user data, including financial data. Security researchers already report an unprecedented volume of coronavirus-themed cyberattacks - 80% of the current cyber threat landscape uses coronavirus themes in some way[1]. Proofpoint alone has seen over 500,000 messages, 300,000 malicious URLs, 200,000 malicious attachments with coronavirus themes across more than 140 campaigns. The numbers continue to grow by the minute.

Nearly every type of attack has been seen using the coronavirus theme. The most common include phishing, malicious attachments and apps, and malware-loaded websites.

COVID-19-Related Cyber Threats

Phishing

Online scammers were quick to exploit communal anxiety and craft convincing Covid-19-related emails in order to trick people into handing over their login credentials. Such emails typically appear to come from health authorities, such as the WHO (World Health Organization) or Center for Disease Control and Prevention (CDC), often claiming to contain information on how to protect yourself or offer new details about the disease. Other examples include all kinds of hooks: infected staff members, neighbors tested positive, recipient's exposure to the virus, stimulus payments, vaccines, charity donations, airline refunds, fake testing kits, and more.

Phishing attacks generally use two ways to make a victim visit the infected website: either an attachment opens it, or link in the email text redirects users to a fraudulent page where they are asked to fill in their credentials. In stressful and uncertain situations people are more prone to fall for these scams – they don't pay attention to small details and don't notice typos in URL address.

Malicious attachments

Apart from using email to "phish" for users' data, cybercriminals are also delivering malware to people's devices. Emails are disguised as coming from reliable sources such as Ministries of Health, Centers for Public Health or a local health organization. The email states that the file attached contains critical information about coronavirus to create the sense of urgency. Due to this, the target lowers their guard against potential cyberthreats and, most likely, will open the attachment and

[1] Proofpoint https://www.proofpoint.com/us/threat-insight/post/threat-snapshot-coronavirus-related-lures-comprise-more-80-percent-threat

eventually will get infected. Popular Trojans such as Trickbot and Lokibot have been seen to use this method of infection.

Malicious websites

In periods of disease outbreak, people naturally search online for the latest information and updates on how it might affect them, and what they can do to protect themselves and their families. Users have been regularly visiting COVID-19 dashboards and maps maintained by media and health authorities that track the spread of the virus, like the ones published by Johns Hopkins University or The New York Times.

Cybersecurity researchers have identified several fake COVID-19 tracker maps that infect victims' computers with malware when opened. To trick the users, these sites use a graphical interface almost identical to the design of reliable sources. They load a fully working online interactive map of coronavirus infected areas and claim to have real time data from the World Health Organization. The strategy of hackers is to make the users think the malicious site is actually a map, so that they will open it and spread it to their friends, helping it to go viral.

According to a recent study, coronavirus-themed websites are 50% more likely to be malicious than other websites[2]. Since January 2020, more than 4,000 domain names related to coronavirus have been registered globally — 3% of which are deemed to be "malicious," and 5% of which are described as "suspicious." As COVID-19 continues to spread and more apps and technologies are developed to monitor it, we will likely see an increase in coronavirus sites and malware going forward.

Malicious apps

Another lucrative target for cybercriminals is users' mobile phones. Multiple fake coronavirus tracking apps were seen spreading on app stores. A fake Android app delivers CovidLock ransomware which demands users pay up $100 in Bitcoin within 48 hours to unlock their phone. A supposed Lybia-based malware was spreading to Android phones via text promising to share data and stats about the coronavirus, but instead spies on users.

Zoom Attacks

New work-from-home practices, social distancing and government lockdowns have increased the demand for video conferencing apps. Platforms like Zoom are seeing huge spikes in usage as the COVID-19 pandemic keeps people under quarantine at home. With over 74,000 customers and 13 million monthly active users, Zoom is one of the most popular cloud-based enterprise communication platforms that offers chat, video and audio conferencing. Thanks to coronavirus,

[2] https://blog.checkpoint.com/2020/03/05/update-coronavirus-themed-domains-50-more-likely-to-be-malicious-than-other-domains/

Zoom has already added more users this year than in all of 2019[3]. Cybercriminals are taking advantage of its success by registering new fake "Zoom" domains and malicious "Zoom" executable files to trick people into downloading malware on their devices.

How to Protect Your Devices and Data

In these uncertain times, it is especially important to use good cyber hygiene and security best practices. By following these tips, you can protect yourself against coronavirus threats on the internet:

- As always, in times of stress and uncertainty, be vigilant for potential phishing attempts.
- Keep calm and don't trust emails that evoke strong emotions, a sense of urgency or that just seem suspicious.
- Visit only your local health authority's website for the latest official information.
- Think twice before downloading attachments or clicking links in any email or message, especially from someone you don't personally know.
- Do not provide your personal details in response to an email or on suspicious site.
- Always verify the web address of legitimate websites and manually type them into your browser. To get more tips on how to spot a phishing email and keep yourself safe, check out our Phishing Guide.
- Frequently back up files so they can be used to recover lost data in case of a ransomware infection.
- Avoid installing "free" apps from unofficial sources – other than Google Play or App Store.
- Check if your telecom provider offers a cybersecurity service that protects you on mobile and Wi-Fi networks by blocking various online threats, including those related to coronavirus.

Conclusion

No one knows or can predict when the coronavirus pandemic will be over. For many people around the world the current situation feels stressful, uncertain and unsettling, and it may stay this way for quite some time. People are now more vulnerable in every aspect of their lives and, naturally, more susceptible to online scams. As long as the COVID-19 pandemic remains front-page news, we will continue to see a huge amount of new cyberthreats leveraging the coronavirus theme to target users worldwide. Cybercriminals will adapt their campaigns and tools to shifting trends and news around the disease to make their activity even more profitable.

To protect their customers and combat the variety of cyberthreats out there, many telecom providers like Vodafone, Telefonica, and Hutchison Drei, are turning to network-based security which stops the attacks on the network-level before they even reach the user's device. In light of the coronavirus outbreak, this support is becoming more significant than ever before.

For more on how to protect your at-home subscribers, watch the Allot webinar:
"It's a New Reality: Cybersecure Your Customers at Home"**.**

[3] https://www.cnbc.com/2020/02/26/zoom-has-added-more-users-so-far-this-year-than-in-2019-bernstein.html