ARTICLE

COVID-19: New Cyber Threats

While we all adjust to the new world of social distancing and working remotely as a result of the coronavirus disease (COVID-19), it is important to not let our guard down when it comes to cyber risks. FTI Cybersecurity is here to help navigate this new normal and assist with our collective security.

Several new scams have emerged, including mass phishing and malware attacks involving emails designed to appear as legitimate messages from medical or health organizations. These emails contain malware-laden attachments designed to either harvest credentials or infect systems. The World Health Organization has released warnings about this threat.

Advanced Cyber Attacks

Concerningly, cyber criminals have upped their efforts beyond using a "spray and pray" approach typically seen with phishing emails. A recent threat involves distributing legitimate information regarding worldwide COVID-19 infection rates that secretly spreads malware to unknowing computers.

"In one scheme, an interactive dashboard of coronavirus infections and deaths produced by Johns Hopkins University is being used in malicious Web sites (and possibly spam emails) to spread password-stealing malware."[1]

Furthering the issue, Russian cyber criminals are selling a "coronavirus infection kit" that uses the Hopkins interactive map as part of a Java-based malware deployment scheme.[2] The use of real-time data and an interactive map makes the scam believable, especially when individuals are less guarded due to the uneasiness of dealing with a pandemic.

The Johns Hopkins interactive tracker is also used legitimately in a mobile application called "corona live" as a way to monitor the COVID-19 outbreak. Cyber criminals have developed a malicious app called "corona live 1.1," which tracks users' locations, grants access to photos and text messages, and records audio once downloaded.[3]

Cyber criminals are not restricted to just phishing/malware attacks. They have also developed a new strain of a common threat vector – ransomware.

Aptly named "CoronaVirus," this version of ransomware is spread using a fake web site that mimics the legitimate

services that WiseCleaner – software designed to optimize a computer's performance – offers.

Instead of simply encrypting files and blocking access to databases, this strain is designed to initially steal login credentials and cookie data, as well as gain access to cryptocurrency wallets. Once this information is captured by the attackers, a second file is downloaded to encrypt the machine's files.

Extra Precautions Needed

Cyber criminals are hoping that increased anxieties regarding COVID-19 will cause cybersecurity best practices to be forgotten. In times of uncertainty, it's easy to click on links at will, and not think twice about downloading an attachment, especially if it's labeled as new COVID-19 guidance.

It's worth revisiting these relevant tips from the Cybersecurity and Infrastructure Security Agency (CISA) on "avoiding social engineering and phishing attacks."

Furthering the issue of malicious actors taking advantage of COVID-19 fears is the significant number of individuals now working remotely and the increased cyber risks that this environment creates. Follow these recommendations to help mitigate risks from new threats and from working outside of the office.

- Use virtual private networks (VPN) and ensure the latest security patches are installed
- Provide IT security personnel with the resources they need to handle an increase in employees working remotely
- Implement multi-factor authentication on all devices, including VPN connections, for an additional layer of security
- Notify employees that phishing and malware attacks are increasing and what to look for (i.e. strange hyperlinks, misspelled words, unsolicited requests for personal information)
- Only download files from trusted sources

Best practices should always be followed when it comes to cybersecurity and data protection, and they should be especially leaned on when a singular topic has the attention of the world and distractions abound. Cyber criminals are relying on the opposite. Therefore, think twice, act once.

1,2. https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/
3. https://www.cnet.com/news/fake-coronavirus-tracking-apps-are-really-malware-that-stalks-its-users/

ANTHONY J. FERRANTE
Global Head of Cybersecurity,
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

DAVID DUNN
Managing Director, Cybersecurity
+1 267 507 2863
david.dunn@fticonsulting.com