HEALTH TECH ACCESS ALLIANCE

March 6, 2020

Weaponizing Coronavirus to Infect Health IT Systems

Coronavirus & Ransomware?

Hackers are Weaponizing Coronavirus to Infect Health IT Systems

Unfortunately, threat actors are always looking for a vulnerability or weakness to create a data breach. Hackers use social engineering to take advantage of human emotions to trick people into taking the bait and opening emails, clicking on links, and compromising Health IT systems and Protected Health Information (PHI). The Department of Health and Human Services' Cybersecurity Coordination Center (CH3) recently alerted healthcare organizations and their staff that hackers are using Coronavirus phishing scams to trick health care workers into downloading ransomware and other viruses and malware onto their computers. This allows threat actors to hack into other areas of IT systems and steal patients' health information.

USA Today reported similar activities going on in Japan in the beginning of February, where hackers would send an email warning of Coronavirus becoming airborne and then tell the reader to click a link to "learn more". This would then download ransomware onto their computer or smartphone.

PC Magazine also reported at the end of

Top 5 Ways To Protect Against Coronavirus Attacks:

1. If you get an email mentioning Coronavirus, pause & check it carefully.
2. If an email that looks suspicious in any way, DO NOT OPEN IT--instead alert your IT services.
3. Be especially careful about emails that send you third-party links about Coronavirus. DO NOT CLICK ON THESE LINKS.
4. If you received an email, chances are someone else received it too. Alerting IT services can help isolate and remove threats before it's too late.
5. If you haven't received emails like this yet, don't think you won't see one soon. Stay vigilant so you won't be fooled and tempted to open or click on links that allow ransomware and malware attacks.

January, 2020, there was a similar scheme by hackers alerting Japanese citizens that there is a new strain of Coronavirus, again telling users to click the link to learn more. Besides stealing data, there have been multiple cases where organizations have experienced ransomware attacks. Threat actors have now moved to the U.S. Multiple organizations as well as individuals have been attacked.

In Wisconsin, NBC26 broke the news of scammers using Coronavirus "miracle cure" disinformation cons to sell users fake cures to the Coronavirus. The CDC and FDA both have alerted the public that no such cures exist at the time. However, pharmaceutical firms are working urgently on a treatment and vaccine for Coronavirus.

An audience hungry for information is an audience ripe for hacking attacks.

For information on the Coronavirus across the globe Johns Hopkins CCSE has a dashboard that tracks confirmed active and recovered cases of the Coronavirus.

The CDC and WHO provide regular Coronavirus updates to keep you informed of new developments.

Coronavirus Attacks

- *HHS recently warned healthcare organizations that hackers are using Coronavirus phishing scams to trick health care workers into downloading ransomware.*

- *Researchers at IBM X-Force identified campaigns where attackers sent infected email attachments disguised as instructions on Coronavirus. When opened, files silently installed an Emotet trojan.*

- *In Japan, emails were sent with supposed "new information" from what appeared to be legitimate disability welfare provider and a public health center clinic with a fake link about the Coronavirus that would download ransomware if clicked.*

- *Similarly, police in Britain are warning about frauds and email scams that have already tricked the British out of over $1,042,000 with fake "Centers for Disease Control & Prevention" or "WHO" links that lead to malicious websites and demands for payment.*

What does a Coronavirus phishing email look like?

While criminal hackers routinely use natural disasters and viral news topics to launch attacks, the coronavirus has the potential to affect healthcare providers directly because of their role in response to the virus.

Hackers prey on fear, curiosity, human error and our rush to get things done. Attackers use social media to "scope out" their target.

As a result, expect to see phishing emails posing as:

- Fedex, UPS, and Amazon, with messages about healthcare supplies

- Targeted attacks from suppliers saying goods cannot be delivered or will be delayed

- Urgent updates from government and global health agencies on how to avoid infection

- Emails that appear to be from other nonprofits and healthcare partners