The other virus threat: Surge in COVID-themed cyberattacks
18 March 2020, by Rob Lever

Cyberattacks are preying on people's fears and anxieties about the coronavirus epidemic, security experts say.

It may look like an email from a supervisor with an attachment on the new "work from home policy." But it could be a cleverly designed scheme to hack into your network.

The abrupt move of millions of people to working remotely has sparked an unprecedented volume of attacks to trick people into giving up credentials to attackers, according to security researchers.

"We've never seen anything like this," said Sherrod DeGrippo, head of threat research for the security firm Proofpoint.

"We are seeing campaigns with message volumes up to hundreds of thousands which are leveraging this coronavirus."

The pandemic has created a perfect storm for cyberattacks, with millions of people working in unfamiliar, less secure circumstances and eager for information about the virus and new organizational policies being implemented.

This opens up a new avenue for malicious actors using phishing emails or "social engineering" to gain access or steal sensitive information.

"When someone is working form their home it is a similar threat profile as at an airport or a Starbucks, you just don't have that protection you might have in the workplace," DeGrippo said.

"And if we're at home with our family where we feel safe, you might see a family member hop on to do homework, and might not understand the security controls. Keeping mom's and dad's computer for mom and dad is the right thing to do."

With millions of people working from home, often on less secure devices, the risks of cyber intrusions and ransomware are likely to increase.

Preying on fear, sympathy

Tom Pendergast of the security and privacy training firm MediaPRO said many of the millions of people adjusting to the new landscape are unprepared for teleworking.

"It's one thing if people have been working remotely with equipment that has been properly configured,"
Pendergast said. "It's different for people who haven't had that experience."

Attackers are taking advantage of people's fears about COVID-19 with scare tactics to get people to click on malicious links or attachments, but also playing on sympathies with fake crowdfunding pages purported to be for people who have fallen ill, he added.

Pendergast said health care organizations are especially susceptible to schemes such as ransomware because "they are less likely to shut down their systems by refusing to pay."

This was highlighted with a major hospital in the Czech Republic hit with ransomware following an email campaign with a coronavirus "awareness" message, according to media reports.

"The COVID-19 scare has proven lucrative for cybercriminals in recent weeks as healthcare institutions scramble to test patients, treat the infected and protect their own staff from the contagion," said a blog post from Filip Truta of the security firm BitDefender.

"Healthcare infrastructures are highly susceptible to hacker attacks because of lax cybersecurity skills and safeguards."

**Stepped-up warnings**

The potential for costly cyberattacks has prompted warnings for stepped up vigilance.

The French public-private cybersecurity alliance this week warned businesses to be alert for faked emails related to purported orders or bank transfers, or phone calls aimed at obtained financial account information.

The US Department of Homeland Security issued an alert this month warning that the COVID epidemic has increased threats and that "cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information."

Hawaii’s attorney general Clare Connors advised residents to watch for fraudulent emails claiming to be from the Centers for Disease Control and Prevention or experts saying they have information about the virus.

"Scammers may still offer fake vaccines and other bogus medical products claiming to offer ‘cures’ for the virus," a statement from Connors’ office said.

DeGrippo said virtually all the cyber schemes related to the pandemic are financially motivated and added that "personally I find it depraved... it is taking humanity at its most vulnerable and trying to use that for financial gain."

She warned that the threats may evolve as attackers craft new scheme and techniques.

"I can see some attackers sending messages like, 'I'm in quarantine and need you to buy something for me,' or 'I need you to make this transfer of funds,'" she said.

"I think we'll see criminals leveraging the coronavirus to do more of that."

© 2020 AFP

Most of the COVID-themed cyberattacks appear to be financially motivated, researchers say