®

Coronavirus Is Making Your IT Security Plans Sick

by Dice Staff
March 9, 2020
7 min read
CORONAVIRUS
COVID-19
CYBERSECURITY
PHISHING

The messages filtering into inboxes around the world seem legitimate enough. One might come from the World Health Organization, a well-respected part of the United Nations, while another bears the hallmarks of the U.S. Centers for Disease Control and Prevention. Each message warns about concerns over the novel coronavirus and offers advice about infection and what can be done to prevent it from spreading.

All it takes is a click on the embedded link to learn more.

And much like a virus, those emails and landing pages can lead to more severe problems down the road for those exposed. Since January, security researchers have been tracking a dizzying array of spam, phishing emails and outright fake news associated with the rise of coronavirus (COVID-19) as cybercriminals try to use the crisis to spread malware and steal login credentials from those seeking information.

Because cybercrooks have refined their techniques over the years, more phishing emails and malicious landing sites are now disguised using graphics and other details swiped from the legitimate websites of WHO and the CDC, security experts suggest.

“Their goal is to hide in plain sight with messages that users expect to see in their inbox and therefore blend into other legitimate business communications,” said Sherrod DeGrippo, a senior director for threat research and detection at security firm Proofpoint, which has been tracking about three or four of these malicious campaigns a day since February.

“The right brands and applications, the right time of day, the right request: We consider this social engineering at scale based on fear,” DeGrippo told Dice. “Organizations across the globe are sending out regular communications to employees and partners around protocol around coronavirus, which gives threat actors a place to mix in their malware lures among the legitimate informational messages being sent.”

As the coronavirus spreads to the United States, DeGrippo thinks that cybercriminals will begin adjusting their campaigns to fit that audience, including employees who might now work for home for several weeks to keep the virus from spreading throughout large corporations.

“This is a relatively new development. Because it’s new we haven’t yet seen attackers fold these developments into their theme ‘toolboxes,’” DeGrippo said. “But it’s reasonable to expect that they will soon.”

Keep Calm and IT On

In the two months that coronavirus has captured the public’s attention, cybercriminals have used the health crisis to spread various spam and phishing campaigns. In many cases, these lures help deliver malware, including various info stealers and, in some cases, Emotet, a one-time Trojan that is now used to spread other types of malware, including ransomware, while creating a botnet.

In recent days, researchers at Sophos picked-up on attackers attempting to plant TrickBot (another malware strain that can steal data or plant ransomware) in emails targeting Italy, where coronavirus has affected schools and other organizations. In this case, malicious Word documents attached to the email hide the malware.

Yet despite the rapid rise of these campaigns, security experts believe the best protection against spam and phishing is making sure the basics are covered. This includes identity and access management, secure remote access and endpoint protection, said Terrence Jackson, the CISO of Thycotic, a security firm based in Washington, D,C., who is responsible for the company’s own internal security posture.

This not only goes for staff that must show up for work at the office, but those employees who are now given the option to work from home.

“Preparing for the possibility of widespread telework should not be a huge cause of concern for the security team,” Jackson told Dice. “Companies may want to reiterate acceptable use policies and good cyber hygiene in preparation, but this should not be a cause of panic for security.”

An Ounce of Coronavirus Precaution

While following good cybersecurity practices and hygiene is essential, some CISOs and security officials say that organizations can use this time to try methods to stem the risk from various phishing and spam campaigns.

According to Rick Holland, CISO and vice president of strategy at San Francisco-based Digital Shadows, now is the time to conduct table-top exercises with key executives and business leaders to ensure that an organization is ready for what might lie ahead, including the possibility that many employees might work remotely for weeks or possibly months, which could subject them to phishing emails that are blocked at the office.

In addition, security leaders should check in with their SaaS providers to ensure that these firms have adequate security protections in place, Holland added. Finally, CISOs should check how on-premises applications interact with VPNs, and then check those connections so employees can access what they need while the software filters out spam and phishing emails.

“The more ‘cloud-friendly’ an organization is, the less pain they will feel when trying to set up a workforce to work remotely for a prolonged period,” Holland said. “You cannot replace legacy on-premises applications overnight, so increasing VPN capacity to accommodate more staff working remotely could be expensive. One of the unintended consequences of COVID-19 will likely be increased zero trust adoption that further embraces cloud services, eliminates VPNs, and enables employees to work from anywhere.”

Dice.com