ILLUSTRATION BY LJ DAVIDS

PREYING ON FEAR

CYBER CRIMINALS TAKE ADVANTAGE OF FEAR AND PUBLIC CONCERN TO EFFECTIVELY INFILTRATE ORGANIZATIONS. MANY OF THEM ARE NOW USING CORONAVIRUS-RELATED SCAMS TO DO SO. **BY MEGAN GATES**

WHEN PEOPLE ARE SCARED, they often want to learn more about the threat they are facing to gain a feeling of control. This is a normal human response. But there are ramifications for cybersecurity when bad actors exploit that response, as they have done during the coronavirus pandemic.

In late March 2020, analysts from KnowBe4—a security awareness training and simulated phishing platform—spotted a new phishing email trend that warned recipients they had been directly exposed to the virus through contact with a colleague, friend, or family member and urged recipients to print an attached Emergency Contact form to take with them to the nearest emergency clinic.

The email appeared to be sent from a hospital, which made it especially alarming and convincing.

"For the bad guys, this is a target-rich environment that preys on end users' fears and heightened emotions during this pandemic," said Eric Howes, principal lab researcher at KnowBe4. "Employees need to be extra cautious when it comes to any emails related to COVID-19, and they need to be trained and educated to expect them, accurately identify them, and handle them safely."

Unfortunately, the alert from KnowBe4 was not a one-off. Ever since the coronavirus outbreak began in China in December 2019 and became a pandemic in March 2020, cyber criminals have increasingly engaged in malicious activity to make a profit or gain access to information.

The World Health Organization (WHO) issued a warning in early 2020 that criminals were disguising themselves as the WHO in an attempt to steal money or sensitive information. Cyber actors were sending phishing emails, asking recipients for their usernames and passwords, to click on malicious links, or to open malicious attachments.

The U.S. Department of Justice (DOJ) also instructed U.S. attorneys to be on alert for frauds that preyed on those concerned about COVID-19.

"The pandemic is dangerous enough without wrongdoers seeking to profit from public panic and this sort of conduct cannot be tolerated," U.S. Attorney General William Barr said in a statement.

The FBI put out a public service announcement on 20 March, warning that it had seen an increase in scammers leveraging the COVID-19 pandemic. The Bureau advised citizens to be on the lookout for fake emails from the U.S. Centers for Disease Control and Preparedness (CDC) claiming to offer information on the virus, including links and attachments.

The FBI also warned the public to be cautious of anyone selling products that claimed to prevent, treat, diagnose, or cure COVID-19.

"Be alert to counterfeit products such as sanitizing products and personal protective equipment, including N95 respirator masks, goggles, full face shields, protective gowns, and gloves," the Bureau explained.

In a threat briefing in March, cybersecurity firm Crowdstrike said it first began to notice the trend of threat actors using coronavirus themes in their messaging in February 2020. MUMMY SPIDER, a

The pandemic is dangerous enough without wrongdoers seeking to profit from public panic.

financially motivated criminal attacker known for the Emotet malware, started using a coronavirus-related scheme to target Japanese victims, said Adam Meyers, vice president of threat intelligence for Crowdstrike.

"After a victim's email content has been stolen, MUMMY SPIDER identifies email threads by the subject line (e.g., Re:) and formulates a reply to the thread," according to Crowdstrike's Threat Intelligence Report. "This tactic increases the likelihood that a recipient will open a malicious attachment (or click a link) because the sender appears to be someone that they previously communicated with, and the subject line matches a prior conversation thread that they had with that person."

Then in early February, nation-state actors from North Korea and China began to use similar tactics, targeting South Korea, and India, Japan, Mongolia, the Philippines, Taiwan, and Vietnam, respectively.

North Korea's Velvet Chollima (the name Crowdstrike uses to refer to a North Korean nation-state threat actor) was specifically targeting individuals who spoke both Korean and English around the time that South Korea was being hit hard by the coronavirus.

"The timing lines up to when South Koreans would have been interested in anything related to coronavirus and more likely to open a document," Meyers explained.

Crowdstrike has also seen ransomware activity related to COVID-19. In the U.S. state of Illinois, the Champaign–Urbana Public Health District confirmed that its website was compromised by ransomware. The district notified the FBI and the U.S. Department of Homeland Security, according to *The News Gazette*, and was ultimately able to restore its website.

The ransomware attack, however, demonstrated how the trend of Big Game Hunting (BGH) will continue in 2020 and throughout the course of the pandemic. BGH refers to the trend of targeting institutions that need to have their operations up and running at all times—like a hospital or utility.

"This is concerning what we're seeing, and we're tracking it very closely," Meyers said.

These types of attacks spurred cybersecurity experts to team together to protect and respond to cyberthreats against healthcare services. The initiative, called Cyber Volunteers 19 (CV19) facilitates a volunteer matchmaking service to provide healthcare services access to a pool of cybersecurity experts, along with support for threat intelligence, security awareness, business continuity planning, and more. As of 17 March, CV19 said more than 1,000 people had indicated that they wanted to volunteer to help with the effort.

"Vast numbers of people are being affected by COVID-19, either directly or indirectly," wrote Sarah Smith, a security and resilience director, in a blog post for CV19. "It is vital to protect front-line healthcare services from buildings, facilities, and IT failures, to ensure people

THE DARK WEB

BY ERDAL OZKAYA AND RAFIQUL ISLAM. CRC Press; CRCpress.com; 266 pages; $59.95.

STEEPING ONESELF in *Inside the Dark Web* is akin to planning a first attempt at mountain climbing. A rising fear of a dangerous adventure yields to a growing appreciation for the Sherpas. The book's two authors acquit themselves as experienced guides to the cyber underworld and the field's relevance to law enforcement.

Although well-organized, the book is not an easy read, with sometimes unexplained technical jargon, often choppy sentence structure, and frequently overlapping and repetitive flow of material. Notably lacking is a glossary of significant cyber terms.

Still, the complexity of the territory may excuse such obstacles, and the reader soon encounters the various dimensions of the dark web. Of great use to students of cybersecurity are conclusions and summary sections, as well as questions at the end of most chapters.

Early in the book, readers are introduced to the dark web's threat landscape, the familiar range of narcotics trafficking, child pornography, terrorism, weapons, unconventional currency marketing, and other illegal activity. The authors explain where to find the dark web. It's not in the visible Web (about 4 percent of the World Wide Web) but in the deep web (the other 96 percent), which houses medical records, government files, and other sites that must be kept away from public eyes. The dark web is a subset of the deep web that is entirely made up of dark sites.

Dark websites are not indexed by search engines like Google; they are accessible only through special browsers such as Tor. The authors argue that Tor's original objective—to protect users' privacy and anonymity—was blighted by criminal exploitation of it.

The authors discuss content analysis, exploiting content logs, and forensics among other things. Like Sherpas, they lead the reader on an inside tour of a crime and threat target that is largely unfamiliar to security professionals. Much of the book may require a second or third reading, but the volume is an excellent reference.

REVIEWER: *James T. Dunne, CPP, is a member of the ASIS Communities for Global Terrorism, Political Instability, and International Crime, and for Information Technology Security. He is a senior analyst in the State Department's Bureau of Diplomatic Security. The views expressed here are those of the reviewer, and do not necessarily reflect those of the U.S. Department of State or the U.S. government.*

can get access to the care and support they need. By working together, we can enable the continuity and availability of these essential services."

To help mitigate the threat of these schemes against organizations, especially as increasing numbers of workers are logging into assets from home, Lance Spitzner, director of SANS Institute Security Awareness Program, said security professionals should focus on three areas: social engineering awareness, password policies, and updating systems.

"Our goal is to make security as simple as possible for people," Spitzner said in a webinar hosted by SANS on preparing workforces to go remote. "They're overwhelmed, and you might think [multi-factor authentication and virtual private networks] are simple—for a lot of people they are scary and confusing."

This is why Spitzner suggests partnering with the communications team to push out internal cybersecurity messaging to make employees aware of threats so they will know what to look for and—ideally—not fall for them.

Tonia Dudley, Cofense security solutions advisor and board member of the National Cyber Security Alliance, cautioned against using coronavirus themes in phishing simulation campaigns. Instead, organizations should focus on what to look for in phishing emails and basic security measures to take while working from home.

RANSOMWARE ATTACKS

In March 2020, ransomware attacks increased 148% over baseline levels from February 2020. Researchers found attacks spiked on days with significant news about COVID-19.

SOURCE: *Amid COVID-19, Global Orgs See a 148% Spike in Ransomware Attacks, Finance Industry Heavily Targeted,* VMware Carbon Black, April 2020

Spitzner also said organizations should communicate with staff about how to report suspicious activity or potential incidents.

"Approachable, empathetic, helpful—that's what we as the security team will have to be for our team during these difficult transitioning times," he said.

To further assist organizations making the transition to remote work, SANS also released a Work-from-Home Deployment Kit. The kit provides general information on how to identify common social engineering attacks, how to set up a secure Wi-Fi network, how to create a strong password, how to update devices that are not corporate issued, and how to talk to family members—who might also be using the same Wi-Fi network—about how to be safe online.

"Move quickly and secure that remote workforce. Decide what are the key behaviors to focus on," Spitzner said. "The toughest part is not deciding what to teach, but what to cut and what not to teach. Prioritize the fewest risks that have the greatest return on investment."

On the bright side, as people adjust to remote work—which may become the norm during the pandemic where drastic social distancing measures are called for—more individuals will become aware of the markers of a phishing email or fraudulent message, and security tools will get better at blocking them outright, says David London, senior director at The Chertoff Group, who focuses on cyber risk management and incident response planning.

"From an IT security perspective, their tools are getting smarter—their email filtering tools are constantly refining their rule sets and filtering to catch these emails before they hit a normal worker's inbox," he explains. "They'll be able to block more content in the future... and individuals will become more savvy about suspicious emails."

Over the next year as the world goes through periods of social distancing to mitigate coronavirus outbreaks, London says he's optimistic about organizations' ability to handle the transition.

"If this were to cycle through again, most organizations will be prepared," he explains. "From an overall IT infrastructure perspective, I have heard far less bad news around outages, lack of bandwidth, and platform functions—which is surprising given the massive increase of work from home participants." ▪

@ To read the reports mentioned in this article, visit SM Online.