HEPLERBROOM LLC

Cybersecurity in the COVID-19 Pandemic: Resources You Can Use

The global pandemic impacts virtually every aspect of life—including our physical and financial conditions and our relationships with others—in profound ways. Since time immemorial, criminals have used uncertain and disruptive events to prey on people. But we should be safer from security intrusions while social distancing in this stay-at-home, work-from-home era, right? Wrong. Today's online criminals are no exception. The frequency, intensity, and sophistication of cyber threats is increasing, and the focus is changing to individual attacks as well.

What is going on out there?

A few examples:

- **NETFLIX.** Scammers are focusing on people looking to stream content from Netflix during our imposed isolation. The number of cyberattacks performed by ersatz websites posing as Netflix has increased significantly during the ongoing coronavirus crisis. Phishing attacks by Netflix doppelgangers doubled, and many of the websites offer attractive payment options to steal user data and payment information.

- **CONSUMER AND BUSINESS FRAUD.** As of March 30, 2020, the FBI has reviewed in excess of 1,200 COVID-19 scam complaints. Modalities and targets include phishing campaigns on first responders, ransomware attacks on medical facilities, public and private entities with work-at-home users on remote telework and education platforms with software vulnerabilities, and fake COVID-19 websites that download malware on unsuspecting users' devices.

  At the Federal Trade Commission, coronavirus-related consumer complaints have doubled in the last week to 7,800. The explosion of scams includes robocalls, texts, and emails posing as government officials or businesses offering refunds for missed vacations or virus-testing kits. Scammers have posed as legitimate businesses selling coronavirus

treatments, charities funneling help to the infected, and officials from the Centers for Disease Control and Prevention, the Small Business Administration, and the World Health Organization, among others. Consider:

- A fake Costco text message offered "$110 goodies" as their stimulus package for completing a survey.
- An email scam, exhibiting the World Health Organization logo, click-baited with free access to consumer stimulus package information for various countries. "These economic benefits will allow you to take the necessary measures to limit person-to-person contact and slow the spread of COVID-19."
- A commercial email advertisement offered "Wholsal *(sic)* CSP Protective Masks."
- The public is interested in medical and public health information. A fake Johns Hopkins infection map comes loaded with a Java based malware kit.
- Attackers are focused on popular home routers with COVID-19-themed webpages carrying malicious infostealer payloads.
- The FTC calculates the average loss per consumer is approximately $600, or nearly $5 million nationwide in recent days alone.

- **COVID-19 DOMAINS.** Although estimates vary widely, during the last several weeks, between 30,000 and 100,000 new coronavirus-related domains were registered, of which thousands were malicious or questionable and under investigation.

- **THE ZOOM QUANDRY.** The private teleconferencing platform has grown exponentially as many new worldwide customers are using Zoom amid the coronavirus pandemic, including universities and K-12 school systems. Hackers are engaging in "Zoombombing" by accessing weak points to intrude into on-line conferences and disrupt them with offensive speech and images. Additionally, fake Zoom sites have proliferated. According to Check Point Research, over 1,700 new "Zoom" websites were registered since the coronavirus pandemic started, 25% over the past week, many of which contain malicious "Zoom" files targeting remote workers.

Zoom's privacy and security practices have come under increased scrutiny in recent weeks. The New York attorney general's office recently asked Zoom whether it had implemented any new security practices in response to the surge in traffic. On March 30 and 31, 2020, two Zoom subscribers sued Zoom in separate class-action lawsuits, accusing it of sharing user data with Facebook without permission, failing to provide end-to-end encryption, and overstating privacy protections in violation of the California Consumer Privacy Act ("CCPA" summarized here by TechTarget) and other state laws. The federal lawsuits, filed in the Northern District of California, allege Zoom failed to disclose that its iOS app was transmitting information about users' and their devices to Facebook.

Zoom's CEO acknowledged rapid growth impacted their security and privacy controls. Zoom then released a new version of its client for Apple mobile devices on Friday April 3, to remove the connection to Facebook, which users must install themselves. Before the update, the app informed Facebook about each user's IP address, advertising ID, mobile carrier, device model, iOS version, and time zone and language settings, among other data. Zoom is now cautioning users not to share publicly their meeting room codes (which are permanent) and to use password features and activate optional controls, including one that lets meeting hosts approve attendees before they join. Meanwhile, on Sunday, April 5, Zoom updated its privacy policy to be more transparent about what customer data it collects and how it uses that information. In a blog post announcing the changes, Zoom emphasized that it neither sells user data nor monitors the content of meetings held on its platform.

The perhaps ironic reward for transparency? A stock-drop class action lawsuit filed April 7, 2020, again in the Northern District of California federal court. The investor plaintiff claims that a precipitous drop in Zoom's share price resulted from media reports of the platform's security and privacy flaws. The company's shares closed down about 7.5% at $113.75 on Tuesday, losing nearly a third of their market value since a late March record high.

- **PHYSICAL PHISHING.** In a recent flash alert, the FBI identified a threat group using “gift cards, sweet faced teddy bears, and the post office to carry out a new physical phishing campaign directed to employees of target companies working in the Human Resources (HR), Information Technology (IT), or Executive Management (EM) roles.” Targets receive a new furry friend in the mail with a gift card, a malicious USB drive, and a fake letter purporting to be from the customer relations department of Best Buy. The scam entices victims to plug the malware-loaded USB drive into their computer with a letter that states: "Best Buy Company thanks you for being our regular customer for a long period of time, so we would like to send you a gift card in the amount of $50. You can spend it on any product from the list of items presented on a USB stick." If the recipient inserts the flash drive into their computer, it infects their device with a JavaScript backdoor or other malware. The USB device is typically a commercially available tool known as a "BadUSB" or "Bad Beetle USB" device. Schemes that use such malicious USBs are known as "Bash Bunny" attacks. Similar attacks, which rely on the victim's using a malicious USB stick that is in reality a malicious USB keyboard preloaded with keystrokes, are called "Rubber Ducky" attacks.
- **TARGETED, Persistent & Patient Attacks.** According to Symantec, targeted ransomware attacks increased 62% between 2017 and 2019. These attacks differ from random commodity ransomware attacks as the hackers use their extensive knowledge of system administration and common network security misconfigurations. Unlike “spray and pay campaigns,” these sophisticated hackers infiltrate a network, perform deep reconnaissance to learn your environment, adapt on the fly to disable or circumvent defensive measures, and perform privilege escalation and lateral movement activities based on security weaknesses and vulnerable services they discover in the network. They often stay active on networks and undetected for months (using networks’ available resources) before deploying the ransomware. Fileless attacks stay off disks to avoid detection, and attackers are exploiting weak authentication practices to gain entry and manipulate systems or machines to steal data and delete or disable back-ups. While this may happen with commodity ransomware as well, this advanced

persistence makes it more difficult to remediate as it is difficult to find them and identify all compromised email inboxes, credentials, end-points, or applications.

- **VPN ATTACKS.** Microsoft has also recently alerted several dozen hospitals in a "first of its kind notification" that their gateway and VPN appliances are vulnerable to ransomware groups actively scanning for exposed endpoints. Attackers are probing the internet for vulnerable systems, with VPNs currently in high demand as COVID-19 increases work-from-home data movement and communications. The malware structure seen in the new attacks aims to take advantage of vulnerable healthcare organizations already under extreme pressure dealing with infected patients. Ransomware attackers are targeting flaws in Citrix ADC, Citrix Gateway, and other enterprise secure remote communication software. It also appears that threat groups may have exploited vulnerabilities in the Pulse Security VPN. The National Cyber Security Centre (NCSC) and the NSA pushed out alerts last October that these products were being targeted by advanced persistent threat (APT) groups.
- **"WATERING HOLE" ATTACKS.** To set up a watering hole attack, cybercriminals observe or ascertain which sites are visited by particular groups of people and then compromise those sites with malware. In the case of Holy Water, affected websites are ones owned by personalities, public bodies, charities, and various organizations, with the attackers targeting people in a specific religious or ethnic group. When a user visits a compromised site, a piece of malicious JavaScript automatically loads to determine if this person is a potential target. If so, a second JavaScript piece loads a plugin that launches a fake Adobe Flash update popup window. Accepting the update downloads a malicious installer that sets up a backdoor exploit that gives the attacker full remote access to the infected computer, where they can change files and steal confidential information.
- **DATA BREACHES CONTINUE. MARRIOTT, AGAIN.** For the second time in less than 18 months, Marriott International has experienced a data breach. Marriott emailed a breach notice on March 31, 2020, to an estimated 5.2 million potentially affected guests. In February, Marriott first noticed that

two franchise employees' login credentials were used to access an abnormally high number of guest records. They believe the activity started in mid-January. The company confirmed that the login credentials were disabled, and it began an investigation, heightened its monitoring, began to inform and assist guests, and notified the relevant authorities, while simultaneously continuing its ongoing internal investigation. Marriott has set up dedicated call center resources with additional information and an option to enroll in IdentityWorks monitoring service free if guests enroll before June 30, 2020.

WHAT CAN BE DONE?

Following common-sense cyber hygiene practices can protect your personal and business data. In addition to other information and links to helpful third-party and government sites on our website and blog, consider taking these precautions:

COMMON SENSE CYBER HYGIENE FOR EVERYONE

- Protect yourself and particularly the elderly from exaggerated or false claims on pitches for COVID-19 tests, treatments, vaccines, protective devices, financial stimulus payments, debt or rent relief, and the like. Any legitimate government communication will have a verifiable address and/or telephone number.
- Hover your cursor over sender names on emails to see if the sender's email address is legitimate or matches the name or subject matter.
- Use legitimate anti-virus and anti-malware software to identify and block known malware from accessing your personal computer. (Norton by Symantec, McAfee, and Windows Defender are examples, but there are other choices.)
- Watch for spelling errors and uncommon syntax and grammar in emails or websites.
- Look out for files received via email from unknown senders, and be wary of unusual or urgent prompts for action you would not usually do.
- Use strong passwords and make sure you do not reuse passwords between different applications and accounts.
- For Zoom meetings, use the password feature, lock your meeting after invited guests access the meeting, and understand the meeting controls, especially

managing participants. (You may want to consider other available platforms, such as Microsoft Teams, Telehealth, Webex, and Skype.)

ADVANCED PROTECTIVE MEASURES FOR BUSINESS

- Comprehensive incident response procedures and subsequent network hardening are necessary. Do not skimp on your IT budget. Microsoft recommends:
  - Manage all internet-facing assets and install the latest security updates. Use threat and vulnerability management audits to check these assets regularly for vulnerabilities, misconfigurations, and suspicious activity.
  - Secure remote desktop access with Multi-Factor Authentication (MFA) or at least enable network-level authentication (NLA).
  - Maintain credential discipline and avoid the use of domain-wide, admin-level service accounts. Use strong randomized administrator credentials.
  - Monitor for brute-force attempts and check excessive failed authentication attempts.
  - Monitor for clearing of Event Logs, especially the Security Event log and PowerShell Operational logs.
  - Activate tamper protection features to stop attackers from disabling security services.
  - Determine where highly privileged accounts are logging on and exposing credentials. Monitor and investigate logon events (event ID 4624) for logon type attributes. Domain admin accounts and other accounts with high privilege should not be present on workstations.
  - Turn on cloud-delivered protection and automatic sample submission, such as those on Microsoft Defender ATP. These capabilities use artificial intelligence and machine learning to quickly identify and stop new and unknown threats at multiple points in the attack chain, before a ransomware payload is deployed.
  - Turn on attack surface reduction rules, including rules that block credential theft, ransomware activity, and suspicious use of PsExec and WMI. To address malicious activity initiated through weaponized Office documents, use rules that block advanced macro activity, executable content, process creation, and process injection initiated by Office applications. To assess the impact of these rules, deploy them in audit mode.

  - Turn on AMSI for Office VBA if you have Office 365.
  - Utilize the Windows Defender Firewall and your network firewall to prevent RPC and SMB communication among endpoints whenever possible to limit lateral movement and other attack activities.
- Take the FBI's advice and "carefully consider" video conferencing software, VoIP conference call systems, and other telework applications.
- Regardless of the COVID-19 environment, never use software from untrusted sources.
- Evaluate and check all vendors and business transaction participants for security compliance.
- Consider segmenting your data or establishing "demilitarized zones" (DMZs) between common and highly sensitive data.

The pandemic has generated a host of new information security threats as remote work environments with potential vulnerabilities have proliferated, and hackers have seized on the crisis as an opportunity to create new and more convincing and sophisticated forms of cyber-attacks and scams. There are no cookie cutter solutions. If you have questions or need assistance, please contact our HBCyberGroup.