July 2021 | Volume 21, Issue No. 7

Briefings on HIPAA

Credit: Tashi-Delek. Image Source: www.gettyimages.com

In this Issue

CISA, FBI issue joint warning, mitigation tactics on TrickBot malware

by Dom Nicastro

The Cybersecurity and Infrastructure Security Agency (CISA) and FBI have observed continued targeting through spearphishing campaigns using TrickBot malware in North America, according to a *Joint Cybersecurity Advisory* published in March and updated in May.

The cybercrime actors lure victims, via phishing emails, with a traffic infringement phishing scheme to download TrickBot. TrickBot—first identified in 2016—is a Trojan (malware disguised as legitimate software) developed and operated by a sophisticated group of cybercrime actors. It is highly modular, multistage malware that provides its operators a full suite of tools to conduct a myriad of illegal cyber activities, according to the CISA and FBI.

In its advisory, the CISA and FBI offer several mitigation tactics, some of which we'll expand on and discuss in this article.

"The advisory recommends several mitigation measures. These mitigation measures include very fundamental tasks," says **Colin J. Zick,** partner and co-chair of the healthcare practice and privacy and data security practice and COVID-19 task force at Boston-based law firm Foley Hoag.

"Equally, or even more important, is the advisory's suggestion that employers provide social engineering and phishing training to employees, mandate reporting of all suspicious emails, flag external emails, and limit unnecessary services and lateral network communications," he adds. "Security is only as good as the weakest link, and these human factors are the weak link."

CISA and FBI recommendations for mitigation

The CISA and FBI recommend that anyone charged with defending a network—naturally, that includes HIPAA security officers—consider the following best practices to strengthen the security posture of their organization's systems, with system owners and administrators reviewing any configuration changes prior to implementation to avoid negative impacts:

- Adhere to the principle of least privilege.
- Consider drafting or updating a policy addressing suspicious emails that specifies users must report all suspicious emails to the security and/or IT departments.

hcpro

- Consider using application allow-list and deny-list technology on all assets to ensure that only authorized software executes on those assets, with all unauthorized software blocked from execution. Ensure that such technology only allows authorized, digitally signed scripts to run on a system.
- Disable the use of SMBv1 across the network and require at least SMBv2 to harden systems against network propagation modules used by TrickBot.
- Disable unnecessary services on agency workstations and servers.
- Enable a firewall on agency workstations configured to deny unsolicited connection requests.
- Enforce multifactor authentication (MFA).
- Implement a Domain-Based Message Authentication, Reporting & Conformance (DMARC) validation system.
- Implement an antivirus program and a formalized patch management process.
- Implement an intrusion detection system to detect C2 activity and other potentially malicious network activity.
- Implement filters at the email gateway and block suspicious IP addresses at the firewall.
- Implement Group Policy Object (GPO) and firewall rules.
- Limit unnecessary lateral communications between network hoses, segments, and devices.
- Maintain situational awareness of the latest threats and implement appropriate access control lists.
- Mark external emails with a banner denoting the email is from an external source to assist users in detecting spoofed emails.
- Monitor web traffic. Restrict user access to suspicious or risky sites.
- Provide social engineering and phishing training to employees.
- Segment and segregate networks and functions.

Training remains paramount

Richard Bailey, lead IT consultant at Orlando, Florida–based Atlantic.net, which provides HIPAA hosting solutions, says training is one of the best methods of defense against phishing attempts. Employees are the front line of the business, and training them on what to look for in phishing is essential.

"Learning how to spot a fake attachment, rogue email addresses, and URL—it doesn't take long to train the workforce to these threats, and even a little knowledge can bolster a business's defense," Bailey says. "Social engineering is a great tool to test your employees' ability to spot phishing attempts, but it's got to be done professionally and ethically."

Social engineering is the practice of centralized planning in an attempt to manage social change and regulate the future development and behavior of a society.

As for examples of unethical training, Bailey cites a case this year of a *British company whose social engineering* test backfired. West Midland Trains workers got an email from the payroll department of the British railroad company about a "one-off payment." It turned out to be a phishing email test, and it wasn't the best look for the company.

"This was a cynical and shocking stunt by West Midlands Trains, designed to trick employees who have been on the front line throughout this terrible pandemic," British TSSA General Secretary **Manuel Cortes** said in a statement. "They could and should have used any other pretext to test their internet security."

It's a group effort

Still, training employees is important—just in the right tact and context.

In the not-so-distant past, security awareness was mostly handled internally by the IT team or the most tech-savvy employee, according to **Steve Tcherchian,** chief information security officer at XYPRO, a Simi Valley, California–based cybersecurity company.

"This works when you're small," Tcherchian says. "But as the company grows, new hires come on board and this method won't be sustainable. Given that threats are continuously evolving and modernizing, you need a way to scale and automate this process. We had to consider the user experience, ease of use, automation, reporting, and metrics. And it was key for us to ensure we could certify the training."

Reporting and metrics can help identify gaps and areas for improvement, as well as measure multiple KPIs and adjust as needed.

© 2021 HCPro, a division of Simplify Compliance LLC.

Companies could also consider gamifying security training; this type of healthy competition engages everyone in the process, according to Tcherchian.

"For this to work, support is needed from the top down, meaning C-level (CEO, CISO, etc.)," Tcherchian says. "Trying to sell and implement security awareness modernization from the bottom up becomes a challenge, and a quick way to screw this up. This is easier if the business views the lack of employee security awareness as a business risk. Customers requiring this [to] be part of their vendors process also help add those necessary business drivers to ensure this gets attention and support at the highest levels."

Managing the email onslaught

CISA and FBI suggest policies addressing suspicious emails that specify users must report all such emails to the security or IT departments. They also encourage security teams to mark external emails with a banner denoting the email is from an external source to assist users in detecting spoofed emails.

"This tactic [is] already widely used within the enterprise," Bailey says. "Many businesses have office add-ons that provide a single-click reporting mechanism to report a suspicious email. Again, training about what to look for is critical."

Implement GPO and firewall rules

A Microsoft Group Policy Object (GPO) uses several protocols to create, read, update, and remove *GPOs*, according to Microsoft. Group Policy is a protocol that uses a document-centric approach to create, store, and associate policy settings. These settings are contained in GPOs to maintain various sets of behavior specifications.

"GPO is useful if configured correctly and if your estate is running Windows Server," Bailey says. "Simple rules such as disabling local admin can stop ransomware attacks in their tracks."

Enable software restriction policies, enforce Bitlocker encryption (featured in Microsoft Windows versions starting with Windows Vista), and create templates for locking down web browsers, Bailey adds.

"Firewall rules protect the physical gateway in and out of the network," he says. "At a minimum, a firewall should drop all traffic by default, and your network administrators should manage access in and out of the network."

Implement an antivirus program and a formalized patch management process

Antivirus (AV) is a mandatory requirement, but it cannot guarantee safety in every situation, according to Bailey. Some malware can bypass AV, especially if the virus definitions are not up to date.

"Patching your computer infrastructure is the best way to protect you," Bailey says. "Patch monthly, include operating system and application updates, and never run an end-of-life operating system."

Adhere to the principle of least privilege

Organizations must create access controls based upon the principle of least privilege, introduce strict access control management, and operate Privileged Access Management (PAM) for servers or databases that contain restricted information, Bailey says.

"This is usually a multifactor authentication service," he adds, "similar to what you might use for online banking."

Segment and segregate networks and functions

The CISA and FBI suggest limiting unnecessary lateral communications between network hoses, segments, and devices.

Network segmentation prevents a hacker from traversing the internal network once they gain unauthorized access to a network, Bailey says. It should be part of a well-defined Identity and Access Management (IAM), PAM, and AWS Key Management Service (KMS) strategy, creating the foundation to start building a zero-trust security platform.

"Bringing in assumed roles and permission-based access controls [pushes] the zero-trust methodology of 'trust no one, always authenticate,' " Bailey says.

We're seeking experts

Contact me and let me know your areas of expertise and interests in publishing or training.

– Steve Andrews
sandrews@hcpro.com

© 2021 HCPro, a division of Simplify Compliance LLC.

Enforce multifactor authentication

Experts have been preaching for years about the benefits of multifactor authentication (MFA). It's one of the biggest bangs for your buck in terms of cyber protection, yet the excuses for why it's not implemented never end, according to Tcherchian.

According to Microsoft, 99% of cyberattacks can be blocked by implementing MFA. MFA is an authentication method where a user is granted access only after successfully presenting two or more of the following pieces of information:

- Something you know (password)
- Something you have (security token)
- Something you are (biometrics)

"All it takes is one compromised account to one website to cause a ransomware attack to catapult a company negatively into the headlines," Tcherchian says. "With the unfortunate increase in COVID-19 phishing scams, there is no better time to implement multifactor authentication across your websites, applications, servers, and services. If we continue to delay, that time will pass and there will be no excuses left, only ransomware and companies that are going out of business."

MFA is now the standard, according to Bailey. In conjunction with a strong password policy, a secured virtual private network (VPN), and encryption, MFA is the de facto choice for securing all computer assets.

"MFA can be scaled easily, and MFA authentication software can be distributed—for example, to a user's mobile phone," Bailey says. "Securing infrastructure with MFA will create added protection. Each user will need not only a username and password, but also a PIN and a code generated from a mobile app, just like internet banking."

Disable unnecessary services on agency workstations and servers

All devices must undergo pre-build server hardening, during which the server is customized to required security standards.

Any host drivers and firmware should be updated to the required level to provide the best performance and security, and the base operating system needs to be configured for enhanced security.

"Turn off any unused system services, close potential security exploits, and optimize each platform," Bailey says. "This also [reduces] the footprint of the server."

One gaffe can be devastating

All it takes is one slip-up to cause a massive disruption. For example, the massive Colonial Pipeline ransomware hack was the result of a single compromised password. Hackers entered Colonial Pipeline's network through a VPN account, which was set up to allow employees to remotely access the network.

"The account was no longer in use at the time of the attack but could still be used to access Colonial's network," Zick says. "Had this network had multifactor authorization, the whole ordeal may have been avoided. Companies need to maintain good cyber hygiene, know where their endpoints are, where they lead to, and secure them." ■

More lessons in risk analysis, HIPAA security compliance in latest OCR resolution agreement

by Dom Nicastro

A clinical laboratory in May *agreed to pay $25,000* to the Office for Civil Rights (OCR) and implement a corrective action plan to settle potential HIPAA Security Rule violations. What happened?

Peachstate is a provider of diagnostic and laboratory-developed tests, including clinical and genetic testing services. OCR initiated a compliance review of Peachstate in December 2017 to determine its compliance with the HIPAA Privacy and Security rules. It found systemic noncompliance with the HIPAA Security Rule, including failures to conduct an enterprisewide risk analysis, implement risk management and audit controls, and maintain documentation of HIPAA Security Rule policies and procedures.

This stems from a January 2015 breach involving the U.S. Department of Veterans Affairs (VA) Telehealth Services Program managed by its business associate (BA), Authentidate Holding Corporation (AHC). The following year, AHC acquired Peachstate, and that's why OCR opened up its compliance review.

© 2021 HCPro, a division of Simplify Compliance LLC.