Health Information Compliance Alert

Cybersecurity: Feds See Spike in Ransomware Attacks

Caution: Your system may already be infected.

Not only are healthcare providers contending with a once-in-a-lifetime pandemic, but now they have to worry about spikes in ransomware attacks. New federal guidance suggests that HIPAA security is the critical key to thwarting digital mayhem.

Refresher: Though social engineering and mobile device management fails continue to be the top causes for data incidents in healthcare, malware and ransomware attacks are increasing at alarming rates. Cyber thugs hack networks, breach servers, and shut down systems - encrypting covered entities' (CEs) files while usurping private data and electronic protected health information (ePHI) - then demand a ransom in exchange for the remedy needed to decrypt the files.

Warning: On Oct. 28, the **Cybersecurity and Infrastructure Security Agency** (CISA), the **Federal Bureau of Investigation** (FBI), and the **Department of Health and Human Services** (HHS) issued a joint advisory alerting providers that they're on hackers' radar. The release details the "tactics, techniques, and procedures (TTPs) used by cybercriminals” to target the healthcare industry and "to infect systems with ransomware, notably Ryuk and Conti, for financial gain.”

In addition to this new concern, many providers are struggling mightily with the fiscal impact of the public health emergency (PHE) while conducting the lion's share of their daily business remotely due to coronavirus concerns. "The alert notes that responding to this threat will be particularly challenging for healthcare organizations during the COVID-19 pandemic, particularly those organizations currently experiencing surges in coronavirus cases,” explains attorney **Elizabeth F. Hodge** with **Akerman LLP** in a blog post.

Hodge adds, "Further, the alert acknowledges the reality that organizations will have to balance the risk posed by the pandemic against this new cyber threat when determining cybersecurity investments.”

Check Out the Threat Specifics

According to the advisory, "cyber actors” are utilizing TrickBot and BazarLoader malware to infect providers' IT systems. Once the hackers are in the system, they then deploy ransomware and havoc ensues.

Important: The three agencies also point out that TrickBot isn't new, but has actually been causing trouble on the malware scene since 2016. "What began as a banking trojan and descendant of Dyre malware, TrickBot now provides its operators a full suite of tools to conduct a myriad of illegal cyber activities. These activities include credential harvesting, mail exfiltration, cryptomining, point-of-sale data exfiltration, and the deployment of ransomware, such as Ryuk and Conti,” the advisory says. In fact, the report suggests TrickBot is likely already up and running in many providers' systems - and the organizations may be completely unaware of the infiltration.

"The alert warns those organizations that have indicators of a Trickbot network compromise to immediately back up and secure sensitive or proprietary data, as the infection may be an indicator of imminent ransomware attack,” Hodge says.

Register These 'Indicators of Compromise'

According to the feds, there are certain things that IT staff can look for that suggest TrickBot or Ryuk have infiltrated their systems. These "indicators of compromise" are a roadmap for IT management in identifying a data breach.

The alert breaks down some of the possible "indicators of compromise." Take a look at the details:

TrickBot: Once this malware infiltrates your system, it "copies itself as an executable file with a 12-character randomly generated file name (e.g. mfjdieks.exe)," the advisory says. The file is then placed in one of three directories related specifically to Microsoft Windows.

BazarLoader: This malware, along with BazarBackdoor, are considered the handiwork of TrickBot trojan creators; they began their chaotic rise in early 2020, infecting networks. "The loader and backdoor work closely together to achieve infection and communicate with the same [command and control] C2 infrastructure," mentions the brief.

Phishing emails are the modus operandi of these software programs, which are usually slipped in with mass email distributions. "Email received by a victim will contain a link to an actor-controlled Google Drive document or other free online filehosting solutions, typically purporting to be a PDF file. This document usually references a failure to create a preview of the document and contains a link to a URL hosting a malware payload in the form of a misnamed or multiple extension file," the feds caution. Like most social engineering tactics, the emails look legitimate because not only do they include the victims' names and information but also reference the names of confirmed business associates.

Ryuk: Since 2018, the ransomware has been "deployed as a payload" through TrickBot, the feds suggest. "While negotiating the victim network, Ryuk actors will commonly use commercial off-the-shelf products - such as Cobalt Strike and PowerShell Empire - in order to steal credentials," acknowledges the advisory. After mapping out their plan, the Ryuk hackers use "native tools... [like] PowerShell, Windows Management Instrumentation (WMI), Windows Remote Management, and Remote Desktop Protocol (RDP)" to move about the network and "shut down security applications," usurping the system, the joint report says.

Heed This Expert Advice

Although your first inclination might be to turn everything off, it's better to contain and keep the evidence intact should a criminal or forensic investigation ensue.

"When an organization finds out it has an incident such as ransomware, the temptation is to immediately power down the systems and wipe drives. In doing so, they may actually be destroying evidence that could be useful in investigating the incident," warns **Adam Kehler, CISSP,** principal consultant and healthcare practice lead with **Online Business Systems**.

Reminder: Preparation is key to repelling both malware and ransomware attacks. Remember, if your practice is the victim of a malicious hack, the first thing the **HHS Office for Civil Rights** (OCR) will look for is how you've assessed and managed your risks in compliance with the HIPAA Security Rule - and what you did after the fact. That's why thorough documentation of both your risks and mitigation tactics are crucial to reduce both cyber attacks and the OCR's wrath.

Resource: Find the joint advisory at: https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf.