AHLA WEEKLY

2/21/2020

What Health Care Response Teams Need to Know About Ransomware

By Barry Mathis, PYA

Some executives at hospitals and health care companies may think that ransomware attacks are the work of a solo hacker sitting in his or her parents' basement. But ransomware is now a highly sophisticated endeavor run by organized crime rings. In some cases, they even employ psychologists who help determine which hospital employees are most likely to click on a phishing email to allow the initial infiltration.

These crime rings continue to prey on hospitals and health care organizations because of the bureaucratic way in which they respond to ransomware attacks. Instead of a "who's- on-first" response involving the hospital CEO, the compliance department, and the chief information security officer (CISO), it's advisable to *always* include the organization's general counsel in the response team to help coordinate and lead the effort.

Some cybersecurity insurance policies require the hospital to notify the insurer first. Be mindful of that when negotiating policy terms. The insurance company is likely to examine everything the organization should have done—but didn't—to prevent the attack.

The Shift to Behavioral-Based Safeguards

As recently as three years ago, many health care organizations relied on a data dictionary that contained the DNA of certain known viruses. Anti-malware software used the dictionary to quarantine files that looked suspicious. But viruses have become much more sophisticated. They now often operate in *Terminator*-like fashion, entering the system in pieces. First the "foot" penetrates the system, then the "arm," and so on. Once all the pieces are inside, they reassemble as the whole body and attack. There's no way that a data dictionary can prevent that.

The latest behavioral-based systems for detecting malware take a much different approach. They look for suspicious patterns—e.g., encrypting 300 directories in the last 300 CPU cycles. The protective software doesn't know exactly what's going on, but recognizes that it's bad and stops it, then notifies the system administrator. All the sleuthing is done at machine-level, requiring no human oversight.

Behavioral-based safeguards assume that the system *will* get infiltrated, no matter how much employee training the organization conducts and how many encrypting devices it installs. For a hospital with a large workforce, it's all but inevitable that one person every year will click on a phishing email or mistakenly provide a password.

One of the biggest data breaches in the entertainment industry occurred when the CEO responded to a phony email that read, "Please confirm your password." If a CEO can make that mistake, think about all of a hospital's new hires.

The Vocabulary of Ransomware

Here are some terms with which every ransomware response team should be familiar:

Payload—Malware, such as a worm or virus, which performs the malicious action (deleting data, sending spam, or encrypting data).

Encryption—Data that is scrambled using an encryption algorithm and encryption key.

Crypto Key—A string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa.

Key Logger—A software program that records keystrokes (e.g., a user's password).

Cryptocurrency—A digital currency using encryption techniques to regulate the generation currency and verify the transfer of funds.

Genealogy of Ransomware

The earliest known malware classified as "ransomware" was the PC Cyborg Trojan in 1989. The first ransom was for the now laughable amount of $189.

Extortionate ransomware didn't really become prominent until around 2005. This ransomware was initially limited to common office software like PDFs and Microsoft Word files. Later variants locked operating systems and master boot records, but a typical ransom was still in the $300 range.

The stakes increased dramatically when crypto ransomware began appearing around 2013. In these attacks, a user is tricked into launching malware that encrypts files before leaving a ransom note. The payment is via cryptocurrency.

By 2015, ransomware had become a full-fledged criminal enterprise. The targets shifted from individuals to businesses. In that year, there were 29 ransomware "families" detected. Within one year, that number had soared to 247 ransomware families—a 752% increase.

Today, there are many varieties of "lit fuse" ransomware strains that increase the ransom amount over time. In 2016 and 2017, ransomware attacks against businesses generated $1 billion.

Anatomy of Crypto Ransomware

Here is the typical sequence of a crypto ransomware attack:

Campaign—Bad actors use techniques, such as social engineering and weaponized tools, to identify the target's vulnerabilities.

Payload Delivery—The most common and effective method for delivering a payload is through email phishing. The most productive payloads are key loggers or weaponized websites. Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that his or her actions are being monitored.

Attack Coordination—Once the payload has reached its target, the crypto malware "phones home" to the bad actor, which generates the crypto key that gets embedded on the target server.

Crawl and Encrypt Files—The crypto software scans servers and shared drives for the types of files it will encrypt. Then it begins encrypting files, databases, and entire servers.

Extortion—The "ransom note" is most often found when technical support is troubleshooting problems caused by the encrypted files. To get the "key," a ransom must be paid.

Proactive Steps for Preventing Ransomware Attacks

Every hospital or health care organization should conduct an annual audit of its cybersecurity risk management program. The audit helps ensure that the organization has up-to-date behavioral-based safeguards in place—and that multi-factor authentication is used to prevent stolen passwords.

The audit team should work closely with the health care organization's general counsel to ensure that an in-house attorney is the point person for a rapid ransomware response. If the event rises to the level of breach notification, every person or department on the response team should have clear-cut responsibilities.

As crypto ransomware gets more sophisticated, it's imperative to respond quickly to every incident. For that reason, the response team, including the health care organization's attorney, CISO, and compliance team, should be proactive in understanding what they are up against.

Author

Barry Mathis is a consulting principal at PYA, P.C., a health care advisory firm with clients in all 50 states. He has nearly three decades of experience as a CIO, CTO, senior audit manager, and risk management consultant.