Ransomware: A Primer

What it is, how it happens, and what to do about it

By Victor Hartman, JD, CPA, CFF, CFE, and Dr. Sridhar Ramamoorti, ACA, CPA/CITP/CFF/CGMA, CIA, CFE, CFSA, CGAP, CGFM, CRMA, CRP, MAFF

Healthcare IT is under attack by ruthless hackers willing to put patient care and EHR integrity at risk. Cyberthreats have increased significantly in the past year and there is no indication that it will slow. It is important to understand that on any day an attack can happen at your organization.

Your role is to help ensure an adequate defense exists, and that all employees are tuned in to how they could be used as inadvertent tools of hackers.

Victor Hartman is Principal of The Hartman Firm, LLC, specializing in forensic accounting and internal investigations. He was an FBI Special Agent serving as a Street Agent, Supervisory Special Agent and Chief Division Counsel. Victor is also an Adjunct Professor at Georgia State University and serves on Georgia Southern University's Forensic Accounting Advisory Board. You can reach Victor at (404) 369-0616 and Vic@hartmanfirm.com.

Dr. Sridhar Ramamoorti is an Associate Professor of Accounting and a Director of the Corporate Governance Center at Kennesaw State University. He has a unique, blended academic-practitioner background with over 30 years of experience in academia, auditing and consulting. You can reach Sridhar at (630) 347-9172 and Sri.Ramamoorti@gmail.com.

The healthcare industry in the United States faces a veritable tsunami of cyberthreats, the darkest of which may be ransomware. Consider the following scenario:

You are the practice administrator for a large medical office and a panicked nurse-practitioner rushes into your office. She is frantically trying to explain that her computer is not working and that she urgently needs a patient's electronic medical record because the doctor is preparing for an emergent surgery.

You quickly learn the computer is unresponsive because it has been locked and bitcoins are needed to pay a ransom to an anonymous hacker. What can you do?

This is not a futuristic scenario—such nightmarish demands are already with us, and are multiplying quickly. Indeed, a scenario similar to this can happen, not necessarily just in a hospital setting, but to any company, governmental organization or individual. But when it happens in the healthcare arena, quality of care and patient lives could be at risk. The problem is the fastest growing malware threat, known as ransomware.

Ransomware is a type of malware that infects a computer and restricts a user's access to the infected computer.[1] A variant known as crypto ransomware encrypts a user's data, making it nearly impossible to recover files and data without the decryption key. According to the Federal Bureau of Investigation (FBI), ransomware attacks have occurred more than 4,000 times daily since January 1, 2016—quadruple the approximately 1,000 attacks per day seen in 2015.[2]

In February 2016, Hollywood Presbyterian Medical Center paid a $17,000 ransom to a hacker who locked access to computer systems and prevented the hospital from sharing communications electronically.[3] Although Hollywood Presbyterian emphasized that patient care was not compromised, a hacker who can gain access to a network

[1] www.us-cert.gov/ncas/alerts/TA14-295A
[2] www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
[3] www.computerworld.com/article/3034721/healthcare-it/hollywood-hospital-ransomware-40-bitcoin-itbwcw.html

has the potential for inflicting catastrophic damage to a healthcare provider.

Hollywood Presbyterian is not alone, since the number of hospitals and other entities being hit with such attacks continues to grow. Indeed, on Saturday, November 26, 2016, the San Francisco Municipal Light Rail System was hacked, and a ransomware demand of $73,000 in bitcoin was made.[4]

Healthcare providers maintaining protected health information (PHI) face other daunting issues. Pursuant to the Health Insurance Portability and Accountability Act (HIPAA) regulations, if the attack is deemed a security incident, certain protocols may be required. Further, if the attack is deemed a breach, mandatory victim notification rules may require immediate disclosures.

How does this happen?

Hackers are always enhancing their tradecraft in an effort to get around a victim's defenses. Cybercriminals have even made it possible for fraudsters with few, if any, coding skills to launch attacks that lock up computer systems at small businesses, among other targets.

In an alarming development, groups of cybercriminals sell exploit kits, invisible web applications that deliver ransomware and other malware. Other criminals peddle payloads, the malware that is used to lock up files, or obfuscation services that make malware more difficult to detect.[5]

Nevertheless, victimization normally involves several steps, so there are opportunities to prevent the attack. Some ransomware may alert the victim of a demanded payment before the user can gain control of the compromised computer. Other variants may lock control of the user's screen. In these attacks, the victim can generally regain normal computer operations by deleting the malware and, in certain circumstances, removing and reinstalling the operating system.

Conversely, an effective crypto ransomware attack prevents any access to the data without the decryption key. This causes the victim to choose between paying the ransom or losing the data. More problematic, paying the ransom is no guarantee the hacker(s) will actually provide the encryption key. They may decide to ask for more.

Let's consider a crypto ransomware attack and its effect on the victim. Like any malware, the malicious code must first get introduced to a computer.

Questions to consider as an auditor

The Basics

1. How do ransomware extortionists gain access to health system computers?
2. What role can employee education play in preventing ransomware infections?
3. Are there steps health systems should be taking to reduce the risk of ransomware or to decrease its impact?
4. What can be learned from law enforcement's efforts to combat ransomware?
5. If your organization falls prey to ransomware, should you pay the ransom?
6. If you pay the ransom, how likely are you to receive the decryption key and be able to view your files?
7. What happens if you don't pay the ransom? Are your files lost forever?

[4] www.pcworld.com/article/3144996/security/san-franciscos-muni-transit-system-reportedly-hit-by-ransomware.html
[5] www.wsj.com/articles/ransomware-a-growing-threat-to-small-businesses-1429127403

Social engineering—exploiting the weakest link in computer security, the human being—is still the most common method of attack. The malware may be sent to thousands of potential victims in the form of spam. A user casually downloads an attachment from an email or clicks on a link in an innocuous-looking email and the malware gets into the computer. More sophisticated attacks target specific individuals in an organization.

Attacks have occurred more than 4,000 times daily since January 1, 2016.

Cybercriminals seem to have a dark sense of humor as well in order to increase victims' response rates to ransomware demands. The hackers sometimes will offer a *freemium* service, decrypting one or a few randomly selected files at no charge. Other ransomware schemes double the price of decryption after a couple of days to create a sense of urgency.[6]

A hacker can often find target information from a victim's own website. Other times, this information is learned by surfing social sites including Facebook and LinkedIn. Armed with this information, hackers can send clever emails enticing an unsuspecting employee to click on a malicious link or download the malware itself.

Other known methods include 'accidentally' dropping thumb drives in a corporate environment in the hope that some unsuspecting good Samaritan will pick it up and insert it into a USB port—and thus introduce malware. An employee spotting a thumb drive with the corporate logo in the company cafeteria is a vulnerable target.

A disgruntled employee can more easily gain access than an outsider.

Another significant vulnerability for the introduction of malware to the victim's system, either wittingly or unwittingly, is through third-party stakeholders like vendors and partners. An environment is only as strong as its weakest link, and these third parties should be required to follow the same stringent protocols required by the host company.

Finally, the threat of malicious insiders cannot be overlooked. A disgruntled employee or one just desiring to extort his (or her) employer can more easily gain access than an outsider.

The attempted introduction of malware into a computer presents an opportunity for the computer system to recognize the malware and stop it. Antivirus software that is updated in a timely manner is effective against known malware. However, when a skilled hacker creates new malware to exploit a previously unknown vulnerability, this "zero day attack" will enter the computer unimpeded because the malware is not recognized as malicious by the antivirus software.

Once crypto ransomware is live within the system, it will attempt to execute its next preprogrammed step. The malware will seek the hacker's command and control server in order to get the encryption key. Here again is an opportunity for the victim's defenses to detect an outbound communication and stop the attack.

One Russian cyberthreat group is reported to have used a Twitter feed as a communication protocol, using commands embedded in images through steganography.[7] The hacker receives communication from text embedded in photographs and then sends Tweets through the corporate feed.

The number of hospitals and other entities being hit with such attacks continues to grow.

When the malware is active in the victim's network, there are defenses that can detect the crypto ransomware, and this is especially true once encryption is initiated by the malware. Further, malware designers have learned to look for backup systems and files with recent updates as the prime place to initiate encryption to gain maximum damages before being detected.

At this point in the attack, the method of dealing with encrypted data will depend on a variety of factors. If the data has been backed up in a secure location, the victim

[6] *Ibid*

[7] www.documentcloud.org/documents/2186063-apt29-hammertoss-stealthy-tactics-define-a.html

can breathe a sigh of relief. The operating system can be reinstalled and the backed-up data used without major inconvenience or interruption.

If there is no data backup, the victim has to make a difficult decision. Questions to ask include:

1. Should the authorities be notified?
2. What is the value of the data?
3. In the case of medical data, is patient care an issue?
4. How much is the ransom?
5. What is the likelihood another ransom demand will be made despite a previous payment?
6. Would the ransom payment incentivize the hacker(s) to repeat the extortion activities against another victim?

These are difficult decisions and they should be made with the consultation and assistance of well-regarded experts. Upon discovery of the issue, management should promptly refer to their cyberincident response plan, if one exists. The plan should invoke the immediate engagement of a cyberincident response team that will include cyber forensic experts and legal counsel. After consultation with legal counsel, an assessment needs to be made of when to contact law enforcement and regulatory authorities.

Ransom demand

After encryption is complete, the victim is notified with a screen message advising that the files have been encrypted and a decryption key must be purchased to unlock the data.

The preferred method of payment is bitcoin due to the anonymity with which the hacker can receive payment. There may also be a countdown clock giving the victim a set number of hours to pay. One such variant, known as CryptoLocker, allows the victim 72 hours to pay with bitcoin. Lastly, there may also be a warning that removal of the malware will lead to destruction of the decryption key.

To pay or not

Like any ransom, no one wants to pay it. In a May 2016 presentation at the Center for Long-Term Cybersecurity at the University of California-Berkeley, FBI Cyber Division Assistant Director James Trainor said that he strongly advises companies not to pay. The reasoning behind the no-pay policy is that paying a ransom encourages bad actors to victimize others. An organization's ultimate decision to pay or not to pay must be very deliberate after considering the interests of all the stakeholders. In the case of healthcare providers, a patient that had no role in the attack could be potentially victimized by their caregiver's negligence.

An environment is only as strong as its weakest link.

In addition to ransomware, the malware may also contain other malicious code capable of recording keystrokes and stealing user names and passwords. Some variants will steal bank account details, and exploit information from social media to scam relatives and friends. When the malware attackers have this information, they can use it to cause severe damage ranging from identity theft to financial loss.

When computer credentials are stolen (access name and password), the hacker usually resells this stolen data to other cybercriminals online. Most importantly, this process from obtaining and selling credentials to hacking a victim's bank account may take many months.

HIPAA implications

As if these issues were not enough, HIPAA-covered entities have another set of issues to consider. Is a potential attack a security incident, breach, or something else? The appropriate answer for entity responders is that it is neither of these until a lawyer competent in this area says it is. Inaccurate internal misclassification and documentation of events may unnecessarily increase liability for an entity.

Upon discovery of the issue, management should promptly refer to their cyberincident response plan, if one exists.

A security incident is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.[8] The presence of malware on a covered entity's system is likely to be a security incident. If so, the entity must identify and respond to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate and document security incidents and their outcomes.[9]

[8] 45 CFR §§ 164.302
[9] 45 CFR §§ 164.308(a)(6)(ii)

The next issue to resolve is whether the event in question is a breach, thereby triggering mandatory notification requirements. Whether the event is a breach is a fact-specific determination. A breach under the HIPAA regulations is defined as the acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the information.[10]

FBI Cyber Division Assistant Director James Trainor strongly advises companies not to pay.

A hacker that has caused encryption of electronic protected health information (ePHI) will be presumed to be a breach because the ePHI disclosure was made to an unauthorized individual.[11]

However, this presumption is rebuttable if the entity demonstrates there is a low probability that the PHI has been compromised based on a risk of factors detailed in the regulations.[12] This last provision may save many providers that keep their ePHI encrypted. Again, this is a fact-dependent analysis that should be made by legal counsel.

If a breach is deemed to have occurred, the HIPAA regulation requires notification to the Health and Human Services Administration, to victims, and, when the number of victims exceeds 500, to the media.[13]

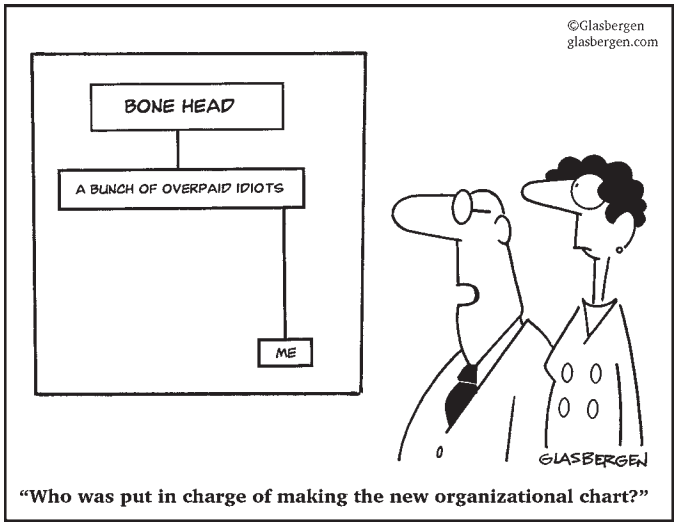
Conclusion

An effective crypto ransomware attack is a multistep process that gives its intended victim several opportunities to defend against it. Organizations need to start with a risk assessment to determine their unique vulnerabilities. Training is essential not only for network administrators, but for all computer users.

Social engineering continues to be one of the top risks, and the solution requires resource-intensive awareness training. Mandatory password changes every 90 days will help mitigate the risk of stolen credentials.

Network administrators must be following best practices, including software updates, implementation of resilient firewalls, monitoring all incoming and outgoing traffic. Assuming all else fails—and this should be a working assumption—your organization's data must be constantly backed up in a secure and redundant environment. **NP**

[10] CFR 164.402
[11] www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
[12] 164.402(2)
[13] 45 CFR 164.406-408



"Who was put in charge of making the new organizational chart?"