PUBLICATION

Best Practices for Responding to the Threat of Ransomware

Authors: Alisa L. Chestler, Samuel Lanier Felker

June 15, 2016

Ransomware, a specialized form of malware used for extortion attempts, has been around the internet for more than a decade but now, because of a rash of recent attacks, has moved to the forefront as the most problematic cyber threat. According to Kaspersky Lab's *IT Threat Evolution in Q1 2016*, ransomware is the most significant issue for cybersecurity professionals in 2016 because new and more sophisticated forms of ransomware have appeared and there is a dramatic increase in reported attacks. In a just a two month period, three hospitals in the United States were publicly brought to their knees by criminal cyberattacks using various forms of ransomware. Hospitals are not the only victims; they are just the most public because of the nature of their operations.

The Recent Attacks

In early February, Hollywood Presbyterian Medical Center in Los Angeles made a $17,000 ransom payment in Bitcoins to a malware hacker who seized control of the hospital's computer systems and demanded money ransom as a condition to returning access. The cyber-attack occurred February 5, when hackers using malware infected the institution's computers, preventing hospital staff from being able to communicate from those devices. The malware locked key systems by encrypting files, rendering them unusable by staff. Without the decryption key from the hackers, the hospital had no access to its own systems. According to the CEO, "[t]he quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key." The hospital said it alerted authorities and was able to restore all its computer systems with the assistance of technology experts, but the episode lasted ten days. Early reporting indicated there was no evidence that any patient or employee information was subject to unauthorized access, however, only time will tell whether the hospital's security controls were robust enough to prevent such losses. Regardless of whether there was any data loss, one consequence is clear – the event disrupted operations and forced the hospital to return to pen and paper for its record-keeping for an extended period. The hackers are totally anonymous and there have been no reports of suspects.

On March 18, cybercriminals struck again. Methodist Hospital in Henderson, Kentucky, was attacked by the same malware called Locky, which encrypts all data on the infected system and deletes the originals, preventing health care providers from accessing patient files and otherwise using electronic web-based services. The malware reportedly came in as an attachment to a spam email and attempted to spread across the hospital's network from the infected computer that triggered the attack. The facility declared a state of emergency. After working over the weekend, the facility was able to report that its systems were "up and running." Methodist officials, however, said they did not pay the ransomware demand, rather administrators were able to restore the hospital's data from backups. Then in late March, MedStar Health, which operates ten hospitals and more than 250 outpatient clinics in Maryland and the Washington, D.C., area, reported being hit by malware that may be ransomware. MedStar posted on Facebook that its network, "was affected by a virus that prevents certain users from logging-in to our system," and that it acted quickly to take down all system interfaces to prevent the virus from spreading throughout the organization. Employees told the *Washington Post* that a pop-up screen appeared on their computers demanding payment in Bitcoin, a signature characteristic of ransomware. MedStar employees were unable to access email or patient records, though the clinics and facilities remained open. A few days later, MedStar reported on its Facebook page that, thanks to the hard work and determination of its IT team, their clinical and administrative systems were almost back online fully and that no patient information was compromised. MedStar will not disclose whether they paid the ransomware demand or were able to restore without paying the monetary demand.

Ransomware is a fast-growing problem for all organizations, not just hospitals.

Ransomware Threat Grows

Ransomware is a category of malware or malicious software which disables the functionality of a computer in some way. After infecting a computer, the ransomware program displays a screen message that demands payment, usually in Bitcoin in order to avoid traceability. Sometimes the scammers add pressure by including a countdown clock and threatening to destroy data unless payment is made by the deadline. The scam has evolved over time using various techniques to disable a computer, but the most recent evolution locks the computer display, disallowing any access to programs or encrypts files. The malware, in effect, holds the computer ransom as an extortion racket until payment is made. The hackers promise to then provide the "key" to unlock the computer and restore functionality.

These aggressive assaults generally begin in a similar manner to other types of malware. The user clicks on an infected pop-up advertisement, or on an innocent appearing link in an email and is thereby directed to an infected website. Unfortunately, even if a person does pay up, there is no guarantee the fraudsters will keep their end of the bargain and unlock the computer. The only reliable way to restore functionality is to remove the malware.

Initially seen in Russia and Eastern European countries in 2005, ransomware has spread throughout Europe and across the Atlantic to the United States and Canada. According to Symantec, this malware is highly profitable for criminals, with as many as 2.9 percent of compromised users paying out a conservative estimate of more than $5 million a year in "ransom" payments. It appears that ransomware attacks are on the rise, both against individual PCs and business networks, and recently law firms and even police stations have reported being victimized. The FBI issued an alert in June 2015 about the spread of ransomware schemes and identified CryptoWall as the most current and significant ransomware threat targeting U.S. individuals and businesses. Between April 2014 and June 2015, the FBI received almost 1,000 CryptoWall-related complaints with victims reporting losses totaling more than $18 million. *Fortune* Magazine also reports that ransomware attacks have soared in recent years and estimates that the CryptoWall malware alone had earned its developers more than $325 million in payments.

Responding to the Threat

So this leaves all organizations with the question, "What should we do to protect ourselves?" Here are a few high level suggestions:

1. Make sure employees know who to contact at any time – day or night – if they suspect they have been infected or have received a ransom demand. A timely response will limit the potential damage. Your help desk should be prepared to guide end users in disconnecting from the network as soon as possible. Employees may feel embarrassed when their computer becomes infected with malware, especially when they welcomed the attack by inadvertently clicking on a deceptive email link. Good training will ensure that such feelings do not deter employees from acting responsibly and immediately reporting a suspected attack.
2. Be ready for a ransomware attack by having a solid plan in place. Make sure that your documented Data Incident Policy and Procedure is current and contains the information you need to respond effectively and quickly. Have the emergency phone numbers and email for critical team members,

federal authorities and outside vendors – including technical forensic investigators and experienced breach-response legal counsel. Your Policy and Procedure should have decision trees for any event including a ransomware attack, a distributed denial-of-service (DDoS) attack or a breach of personal information.

3. Organizations must test their policies and procedures to ensure that they are appropriate, that all executives understand the implications of the decisions made and that employees understand the policies and procedures well enough to respond appropriately. We strongly recommend that you "bench test" your Policy and Procedure to make sure the plan works for your organization. Don't wait until trouble strikes.
4. Ensure that the organization's security program includes a detailed disaster recovery and business continuity program (DR/BC Program). These DR/BC Programs are not limited to planning for situations such as fires, earthquakes, floods and hurricanes – they should include the potential for a ransomware or DDoS attack. Organizations should have a good understanding of the latency for back up files and the ability to switch to another hot site or third-party location. The recovery points and objectives for the recovery should be known in advance. Important data should be regularly backed up and saved via unconnected storage solutions. When data is appropriately backed up, ransomware demands become less effective.
5. All organizations must continue to update operating system and security software on a regular and consistent basis. Investing in the right tools and protocols can be costly; however those costs should be evaluated with the new paradigm in mind – one in which your organization could be rendered paralyzed at the whim of a criminal.
6. Have a good understanding of information governance and its role in your comprehensive security program. While you may have a documented information security program in place, it may be missing key and critical pieces that could have been identified easily with a small investment in the development of an information governance program. Be vigilant and you will be ready if your organization is the next target of a malicious malware ransom attack.

For more information on how this issue may affect your business or related matters, contact Alisa Chestler, CIPP/US and Samuel L. Felker, or any member of Baker Donelson's Privacy and Information Security Team.