link. Now, for our second article in the series…

Threat Two: Ransomware – A Significant Cybersecurity Concern

By Samuel L. Felker, JD, CIPP/US, and Gina Greenwood, JD, CIPP/US

Over the past year, no information security threat has demanded more media and corporate attention than ransomware. The evolution of this threat from an ineffective nuisance to a sophisticated business model generating hundreds of millions of dollars for hackers has been impressive, to say the least, and the number and frequency of attacks are on the rise. Hospitals have been particularly vulnerable to ransomware attacks, but no one is immune from this hazard as hackers are targeting all sorts of businesses, as well as individuals. In this article, we will touch on the past, present and predicted future of ransomware attacks and provide insight regarding how to protect and defend an attack.

What is Ransomware?

Ransomware is a category of malware or malicious software that 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 threaten to destroy data unless payment is made by the deadline. Ransomware has evolved over time, using various techniques to disable a computer, but the most recent iteration either locks the computer display, disallowing any access to programs, or actually encrypts and/or removes files. The malware, in effect, holds the computer captive and demands a ransom be paid as a method of extortion. The hacker promises to provide the "key" to unlock the computer and restore functionality once payment is made. Ransomware generally infects IT systems in a similar manner as other types of malware. Commonly, the user clicks on an infected popup advertisement or on an infected link within an email and is directed to an infected website. To provide perspective about the scope of this problem, PhishMe recently reported that a staggering 93 percent of phishing emails were infected with ransomware in Q1 of 2016. With a simple click on a link or by opening an attachment, malware can enter the network, quickly infecting files and encrypting data.

If that isn't scary enough, ransomware hacking techniques are becoming more sophisticated and dangerous. According to Bill Dean, digital forensics expert and Senior Manager for LBMC Information Security, ransomware attacks often involve encryption with an "unbreakable" code to the entire system – including local user created files, local system backups (volume shadow copies), network shares to which the infected user account has modify rights (often causing major devastation) and any locally attached USB drives. In addition, an undocumented "feature" of most current ransomware variants is that cloud-based storage is also at risk. Cloud storage solutions often synchronize the local user files to the cloud provider. Dean warns that if the ransomware encrypts the local files that are to be synchronized, and there are not multiple versions in the cloud, the cloud-synchronized files will also be encrypted.

According to the Federal Trade Commission's recent guidance, linked here for convenience, ransomware

has quickly established itself as the predominant malware that threatens most organizations. The FTC reports that ransomware incidents have skyrocketed in the past year and several high-profile attacks on health care organizations highlight the challenges that ransomware poses. In February, an attack on a hospital in Southern California knocked out its network for more than a week, leaving staff without access to email and some patient data. The hospital ultimately paid a $17,000 ransom to restore access. Then, only a few weeks later, a hospital in Kentucky was hit with ransomware and its operations were disrupted for several days until data systems were restored. Reportedly, no ransom was paid. In April, another attack crippled the networks of ten Washington, D.C. area hospitals for nearly two weeks. But ransomware isn't just a health care problem – it affects businesses across industry sectors.

What is the Future of Ransomware?

By performing a detailed analysis of ransomware samples, Dean and his colleagues have determined that these attacks are currently geographically focused on certain countries. Additionally, due to the price tolerance (and likelihood of payment) of different countries, the amount of ransom fee demanded will actually vary based on the location and size of the system that is infected. Attackers also target the file types most likely to glean payment. Ransomware has become a big business indeed. Ransomware can be highly sophisticated with the ability to avoid detection, lie in wait, attack later, and extract and remove data – causing true data theft scenarios.

With the success that recent ransomware attacks have had, Dean said we can be assured that future enhancements will continue to be made by malicious hackers. While Dean said he hopes to be incorrect, below are some "features" that are likely to appear in future ransomware variants:

- **Support of Additional Operating Systems** – The Microsoft Windows operating systems are currently the primary target for ransomware attacks. With the market share that Apple OS X is gaining, this platform will likely be a future target.
- **Better Mobile Support** – While there have been some attempts at mobile support for ransomware, it has been weak at best. With users now storing more personal pictures and videos on mobile devices, this could be a feature addition by hackers to target consumers, likely leading to future app development.
- **More Targeted Attacks** – The majority of ransomware attacks today are "opportunistic" in that the infected user is part of a large phishing email distribution list or is inadvertently redirected to an infected ransomware distribution site while performing legitimate Internet surfing. In the future, the attacks may be more targeted with the goal of obtaining higher ransom opportunities. The attackers may even recruit disgruntled employees to assist in determining the critical files that are not being backed up, which would warrant much larger ransom payments. For their assistance, the insider would receive a portion of the ransom.
- **Easier Payment Methods** – Most ransomware variants today require payment in bitcoin, an untraceable Internet currency. The use of bitcoin for payment can be difficult for most people, as very few of us have bitcoin in an account today or know how to transact using it. To increase the likelihood of receiving a ransom payment, the bad guys know that they need to improve this transaction. For those victims that are return customers, maybe we will see a loyalty program with discounted rates on the future ransoms paid!

How to Respond to a Ransomware Attack

In recognition of this spreading menace, several U.S. governmental agencies have issued guidance on how to respond to a ransomware attack. Baker Donelson previously issued an alert on the HHS's Office of Civil Rights Ransomware Guidance, linked here for your convenience. In short, OCR basically opined that a

ransomware attack is a notifiable breach unless a HIPAA covered entity can prove otherwise, greatly raising the bar for forensic analysis of, response to and documentation of such security events. In addition to the FTC Guidance referenced earlier, the FBI also issued a Guidance in April, linked here for convenience.

Does It Make Sense to Pay the Ransom?

Clients frequently ask whether it make sense to pay the ransom. The FBI discourages victims from paying the ransom because payment doesn't guarantee your encrypted data will be returned, and in its view, payment encourages future criminal activity. In some cases, the attackers simply increase their demands once a victim expresses a willingness to pay. Despite the serious risks to consider before paying a ransom, businesses need to carefully evaluate all possible options in the event of a crippling ransomware attack that limits the organization's ability to function. Quite often the ransom amount is relatively small, as compared to the cost of business interruption, making ransom payment an appealing strategy. Of course, it is a strategy that should be discussed with counsel. The only reliable way to restore functionality is to remove all traces of the malware, which may prove to be a long and laborious process.

How to Defend Against Ransomware Attacks

There are currently no "silver bullets" to prevent ransomware infections. With hackers constantly modifying their methods and attack signatures, conventional controls – such as anti-virus software – are not enough. However, there are preventative measures that can be taken by organizations to build resilience against ransomware attacks. The FTC recommends:

- **Train and Educate Staff** – Implement education and awareness programs to train employees to exercise caution online and avoid phishing attacks. Use specific examples and send out weekly reminders.

- **Use Good Cyber Hygiene** – Practice good security by implementing basic cyber hygiene principles:
  - Assess the computers and devices connected to networks to proactively identify the scope of potential exposure to malware.
  - Identify technical measures that can mitigate risk, including endpoint security products, email authentication, intrusion prevention software and web browser protection.
  - Implement procedures to keep security current.
  - Update and patch third-party software to eliminate known vulnerabilities.

- **Create Backups** – Back up your data early and often. Well-prepared organizations with reliable backup systems may be able to restore systems from those backups with minimal data loss or business interruption. (These are the entities who are typically in a position to be able to refuse to pay the ransom).
  - Identify business-critical data in advance and establish regular and routine backups.
  - Keep backups disconnected from your network so that you can rely on them in the event of an attack.

- **Plan Ahead** – Prepare for an attack. Develop and test incident response and business continuity plans. We recommend your response plan detail attorneys, IT and forensic vendors and experienced law enforcement agents and their 24/7 cell phone numbers.

Additionally, in the unfortunate event of a ransomware attack, we recommend that businesses formally assess the damage after an attack by conducting a forensic examination. Be very careful not to allow

anyone to wipe the system clean. Your business will need to preserve the firewall, network and server logs as evidence of what happened. This is critical to be able to prove whether there was or was not a breach that requires reporting to consumers, the media and government.

For the detailed steps your organization can take to prepare for a ransomware attack, see Ransomware: What to Do When Your Files Are Held Hostage, developed by analysts at LBMC Information Security.

With ransomware attacks on the rise, businesses must be vigilant and guard against this latest cybersecurity threat, and they must have a plan in place in the event they are a victim. Baker Donelson develops tailored incident response plans for its clients on a daily basis. We advise clients to play offense long before they are called upon to play defense. Having a detailed incident response plan and a pre-negotiated vendor response contract are key to any solid response plan. If the U.S. were to have several major attacks at once, forensic and technical analysts would be in short supply. It is important to build contractual and professional relationships with these vendors long before an attack hits. A vendor that knows your systems, policies and procedures will be able to respond to stop an attack and analyze an attack much more efficiently.

The Firm's Data Protection, Privacy and Cybersecurity Team is here to help your company prepare for cyber-attacks, respond to them and in the event of one, repair your company and go after those responsible. For more information, please contact Samuel L. Felker, Eric Setterlund, Gina Greenwood or another member of our Data Protection, Privacy and Cybersecurity Team.

Also, stay tuned for our next installment which will discuss how to accomplish your New Year's Resolution of promptly and properly purging your business of all unnecessary data.

About the Authors

Samuel L. Felker
Nashville
615.726.5558
samfelker@bakerdonelson.com

Eric Setterlund
Chattanooga
423.209.4221
esetterlund@bakerdonelson.com

Gina Greenwood
Atlanta
478.765.1804
ggreenwood@bakerdonelson.com

www.bakerdonelson.com