US SIGNAL®

A Q&A on Ransomware with US Signal

With the rising number of successful ransomware attacks — and the increasing ransom amounts being demanded by cybercriminals — it's not surprising that people from the server room to the board room have questions about ransomware. In this document, Trevor Bidle (TB), *Information Security and Compliance Officer, and* Jorel Van Os (JV), *Information Security Analyst, address some of the most frequently asked questions US Signal receives about this notorious form of malware.*

What makes ransomware attacks different from other types of cyber-attacks?

TB: Most cyber-attacks involve malware in the form of a computer virus, a worm, or both. A virus piggybacks on something like an attachment in an e-mail. A worm starts on a networked computer system and attempts to subvert one or more computers on the network. When both are used, it's easy for the malware to remain hidden and self-propagate among files on the host computer and then to other computers. These types of cyber-attacks tend to be specific to a platform like Windows or an application. This allows the malware to target specific security vulnerabilities or improperly configured systems.

Ransomware is a type of malware, but it differs in its approach after a successful attack. A lot of malware is simply annoying or slightly malicious, deleting files or changing the system configuration. The more malicious kind might reformat a disk or corrupt files on the system. Or, it might hide and communicate with a control system so it can be part of a distributed denial of service (DDOS) attack. Some types of malware may also try to capture information from passwords and keystrokes to documents, and then forward this information to a control system.

In the case of ransomware, it encrypts a system's disk or files as part of its attack. It then notifies the system's user that it has been attacked and demands some sort of payment to restore the files or disk to their prior state. However, paying a ransom does not necessarily guarantee the files or disk will be released.

Why are ransomware attacks so successful?

TB: Attackers in a well-executed campaign can make significant money for minimal investment, so they are highly motivated. However, one of the key drivers behind the success of ransomware is human behavior. Consider two of the primary means by which ransomware was spread in 2017.

There are phishing emails that entice users to click a link or open an attachment, which then releases the ransomware. People are curious by nature and want to know what was sent to them. They often don't stop to think that the email is a ploy. Frequent security training is essential in impressing upon users the importance of not clicking on suspicious links or attachments. Prohibiting the sending or receiving of emails that contain executable files as attachments or stripping those attachments before the email can be delivered to its intended recipient is also an option.

Human behavior is also behind unpatched software vulnerabilities that can easily be exploited. With all the multiple competing responsibilities they have, IT personnel in charge of patch management may not make applying the latest patches a priority. Or, they haven't implemented a comprehensive patch scheduling program that provides guidance in terms of vetting security and patch updates, installing them, testing them, auditing, and assessing them. Correcting the situation isn't a matter of changing behavior. What will help is allocating more resources to IT to ensure adequate staffing and in-house expertise is available to implement a strong patch management program. An alternative is to outsource patch management to a managed services provider.

Recommendations from US Signal:

Before an Attack:

- Conduct frequent security training with employees at all levels of your organization.
- Perform periodic port and vulnerability scans
- Centralize security logging
- Enforce strong authentication
- Disable unnecessary, vulnerable services
- Practice strong, timely patch management
- Deploy domain name system (DNS) layer protection
- Automatically enable endpoint protection
- Enable email gateway security
- Restrict lateral attack movement
- Enforce the principle of least privilege
- Perform regular backups of critical systems and data and store offsite

During an Attack:

- Isolate infected machines if possible
- Activate incident response plan
- Communicate timely, accurate information

After an Attack:

- Collect and preserve evidence
- Analyze forensic data
- Perform root cause analysis

What's the most costly or damaging aspect of a ransomware attack?

JV: The cost of a ransomware attack to an organization depends on the organization and the specifics of the attack. After the widely reported ransomware attack on Hollywood Presbyterian Medical Center, that institution decided to pay the ransom of $17,000. It's likely that the ransom was the least expensive part of the attack. The bad press, loss of customer confidence, potential compliance violations, and system/business downtime all likely cost many times more.

According to IBM's 11th Annual Cost of Data Breach Study, the average consolidated total cost of a data breach grew from $3.8 million to $4 million, and the average cost incurred for each lost or stolen record containing confidential information increased from $154 to $158.

There are also costs associated with noncompliance stemming from ransomware attacks assessed by state and federal regulators such as the Office of Civil Rights for HIPAA violations, as well as by other organizations. For example, if a merchant experiences a security breach and is found to be non-compliant with PCI, it may be subject to fines from their acquiring banks.

Depending on the circumstances of the attack, the merchant may be required to pay up to $100,000 each month it is not compliant with the PCI standards. Damage to the company's brand will also occur between negative publicity and the company being placed on the OCR Breach List.

Are there ways to decrypt data without paying a ransom for a decryption key?

JV: In some cases, it is possible to decrypt data and not pay a ransom. The No More Ransomware project has a list of free decryption tools. If the ransomware author made an implementation mistake, it is sometimes possible to break or reverse engineer the encryption. Sometimes, the ransomware authors leak their own keys. Or, law enforcement seizes the server with the keys on them and releases them publicly. In other cases, the encryption cannot be defeated, and it's necessary to restore from backups or pay the ransom and hope it works.

In the case of the NotPetya ransomware, once encrypted, the data is lost as no keys were created by the attacker that will decrypt the data. It is also important to note that once the data is decrypted and the ransom paid, twice the current storage will be needed to allow for the unencrypted copies to be created. This has been a challenge for many of the companies that have paid the ransom since they have nowhere for the data to go.

Will ransomware attacks continue to evolve? If yes, why and how?

JV: Ransomware attacks will absolutely continue to increase and evolve. The reason why is because they are so profitable. Estimates vary based on the ransomware variant and the country or region of the world impact, around the globe, but up to 50% or more of ransomware victims end up paying the ransom. That can run anywhere between $300 and $1,000+ per infected machine. Ransoms are usually paid in Bitcoin, which makes them very difficult or impossible to trace.

My prediction is that we will see an increase in ransomware-as-a-service. Advanced cybercriminals author the malicious code in the ransomware, and then make it available for others to download and use. The authors may provide it for free or charge a small fee up front, and then take a cut of each ransom. This incentivizes a higher volume of attacks and higher ransom requests.

I also believe we will see an increase in state-sponsored ransomware or malware that is made to look like ransomware for its press value. We will also see more ransomware based off both zero-day exploits and existing exploits that were found in leaks, like EternalBlue. Leaked government exploits will continue to be sought after and used for both their overall effectiveness and political value.

What is IT resilience and why is it important in combating ransomware attacks?

TB: IT resilience is having the people, plans, hardware, software, and backups in place to continue operating in the event of a fault or incident occurring. Utilizing modern firewalls and endpoint protection, along with email protection, provides initial defenses. Ensuring that patching and vulnerability management are occurring provides another layer of defense. Ultimately, having offsite backups that are secured separate from normal operations and having the hardware or third-party providers available with hardware to enable quick restoration is key to being able to efficiently restore and maintain services. It is important to remember that, in the case of ransomware, replication is not part of the resilience strategy as it will replicate the ransomware.

What steps should companies take to enhance their IT resilience?

TB: Establish business continuity/disaster recovery (BC/DR) and incident response plans that are regularly updated. Know which machines exist. Establish criticality lists for machines, and ensure those machines are backed up to an offsite secure location or third-party provider that is separate from the enterprise network. Have a resource plan in place incase an event occurs so that you have access to the necessary internal resources. Or have those from a third-party provider establish an environment to operate in should an attack occur.

Ensure a well-established patch management program is in place, utilize endpoint protection, and have modern firewall technology with advanced threat protection. Establish a backup routine with a disconnected backup platform that the ransomware cannot spread to. An enterprise backup solution that is off site at a third party, separate from the enterprise network, is a good line of defense to help mitigate the impact of a ransomware attack.

Free Resources Available

US Signal offers a variety of free resources to help you understand and combat IT security issues such as ransomware. You can also take advantage of a free consultation with a US Signal solution architect to assess your current IT service portfolio and determine how it can be made more resilient.

Available Resources

Whitepaper — Ransomware: The Enemy at the Gate: A Guide to Keeping It Out

eBook — 10 Tips for Combatting Ransomware

eBook — Data Protection 101

Whitepaper — A Guide to DR Planning

Webinar — Creating IT Resiliency in your DR Plan

Webinar — Controlling Creep: Streamlining Data Security and Compliance

Schedule a Free Consultation

Call 866.2. SIGNAL or email info@ussignal.com