Responding to a Ransomware Attack: What You Need to Know

Credit Union Times

http://www.cutimes.com/2017/04/04/responding-to-a-ransomware-attack-what-you-need-to

By Rishi Bhargava April 04, 2017 • Reprints

Between 2005 and 2016, ransomware infections were more common than data breaches, making them the most pervasive cyberthreat of the last 11 years. Ransomware attacks may encrypt folders and files or even the entire hard drive, or they may just lock the devices so that users cannot access them. In recent years, attacks have become increasing sophisticated; crypters can make reverse-engineering extremely difficult, and offline encryption methods can eliminate the need for command and control communications by taking advantage of legitimate features.

Growth of Ransomware Attacks

Ransomware attacks have become increasingly common during the past three years. A report from Kaspersky Lab revealed that its solutions found ransomware on more than 50,000 computers connected to corporate networks in 2015, which was twice the number detected the year before. In 2016, almost $210 million was paid to ransomware cybercriminals during the first quarter alone and the FBI estimated that without paying losses for the year would have exceeded $1 billion.

Ransomware is not actually a new method of attack. The first known instance was PC Cyborg, a Trojan distributed by Dr. Joseph Popp in 1989. The malware would encrypt all files and hide all folders on the computer's hard drive. A script demanded $189 in ransom, and the computer would not function until payment was received and the actions reversed. It did not take long for recovery tools to reverse the effects, but newer attacks have featured stronger encryption to foil decryption tools, making it almost impossible for victims to unlock their own computers.

Approximately 17 years after the introduction of PC Cyborg, a new strain called Archievus was released. Archievus was the first ransomware attack to use RSA encryption as well as the first known ransomware to use asymmetric encryption. It encrypted every file in the “My Documents” directory, and it was very difficult to remove unless victims purchased the password necessary to decrypt the documents.

Individuals were the primary targets of "scareware" schemes that warned users their computers had been infected with malware that could be removed only by purchasing an antivirus software. The antivirus software was actually fake, and the only true threat was the warning message that repeatedly appeared, leading many people to pay the ransom just so the message would go away.

By 2011, anonymous payment methods made it easier for hackers to collect ransoms. Most payment demands require victims to remit payment in bitcoins, but various anonymous cash cards are also popular payment methods. However, hackers can also make other ransom demands. For example, “hacktivists” might demand that a company reduce its carbon footprint or that an individual spread the malware to a set number of contacts to unlock his own computer.

Attacks Focusing More on Organizations

For many years, ransomware attacks targeted home computers or small businesses. These were considered low-hanging fruit as these users were often less sophisticated and had fewer protections. The typical ransom demand for a home computer was between $200 and $500. However, as hackers refined their skills, they began to focus on larger organizations with the budgets to pay substantial ransoms for the files and systems needed to conduct daily operations.

In the past few years, there have been several well-publicized ransomware attacks on major organizations.

- In 2016, Hollywood Presbyterian Medical Center suffered a ransomware attack that shut down its computer network for more than a week, resulting in mass chaos. The hospital was forced to transfer some patients to other facilities to ensure that they received the necessary care. Only after the ransom – 40 bitcoins or the equivalent of $17,000 – was paid could HPMC regain the use of its malware-encrypted files.
- In 2015, the Swedesboro-Woolwich School District in New Jersey was the victim of a ransomware attack. The encrypted files were primarily staff-generated Excel spreadsheets and Word documents. The attack forced the district to delay its assessment tests, but the decision was made to not pay the ransom; the district had adequate backups to restore the servers.
- A sheriff’s office in Tennessee paid a ransom of $500 after suffering a ransomware attack, but when Detroit city government was attacked, the demanded ransom of approximately $800,000 in bitcoins was not paid.

The Phases of an Attack

Whether the ransomware attack is a targeted attack or a mass distribution, the attack will follow five distinct phases. Understanding the phases can help increase the chance of a successful defense.

1. Infection: The attack cannot succeed unless the malware can be placed on a computer. Many ransomware attacks result from a phishing campaign, often through emails with infected attachments or compromised links. However, exploit kits that exploit vulnerabilities in software applications such as Internet Explorer and Adobe Flash are the preferred method for some malware attacks, including CryptoLocker.

2. Execution: An executable file will be placed on the target's computer, usually beneath the user's profile in the "TEMP" or "APPDATA" folder.

3. Backup Removal: Within seconds of the execution, the ransomware finds and removes backup folders and files that exist on the system. On systems running Windows, the vssadmin tool is often used to delete volume shadow copies; this will create event log entries that can make detection easier.

4. Encryption: After removing backups, a secure key exchange may be performed with the C2 server. However, some ransomware types, including the SamSam malware, do not need to communicate with the C2 server; the encryption can be performed locally.

5. Cleanup: The final phase is to present the demand instructions and remove the evidence of the malware code. The presentation of the payment demand can help identify the strain of ransomware. For example, Locky changes the wallpaper to include instructions, while CryptoWall V3 stores the instructions in a HELP_DECRYPT file.

Preparing and Responding to a Ransomware Attack

When it comes to handling a ransomware attack, protection and prevention are the best and most effective defenses. There are five critical steps in defending against a ransomware attack.

Prepare for an attack:

- Be proactive about patching to eliminate vulnerabilities.
- Be proactive about backing up your system and store backup files offsite or at least in a location other than your server.
- Have a well-defined incident response plan that includes an explicit plan for a ransomware attack. Fast action is critical for a ransomware defense. You will also need to develop a specific recovery plan for these types of attacks.
- Adopt the practice of assigning the least privileges, especially for file shares. Limiting exposure can also limit the damage that a ransomware infection can cause.
- Deploy endpoint protection tools that can detect early attacks and respond to them quickly and automatically.
- Educate your end users. People are the weakest link in most organizations, so make sure that they know what to look for and how to avoid phishing schemes. Educate them about malvertising and warn them against plugging in any portable storage devices of unknown origin.

Detect attacks early:

- Get signatures into your network devices. Numerous signatures are available for attacks such as Locky and CrytoWall. However, these are normally version-dependent, so you will need to be proactive about updating them.
- Screen email. Use automated tools that can detect executable or malicious attachments.
- Look for files in commonly exploited areas. For example, look for executions from the APPDATA or TEMP folders, the key exchange procedure or the vssadmin command execution.

Contain the damage:

- Security automation and orchestration tools can help contain the damage significantly. The time between detection and containment is critical to minimize lateral damage and spreading of infection.
- Disable the connection or try to shut down the system quickly to minimize damage. These steps can be also automated to respond quickly and consistently.

Eradicate the ransomware:

- Replacing the machines is the best option. With all types of malware, including ransomware, it is almost impossible to know whether there are hidden files remaining on the system that could launch another infection.
- Network locations such as file shares or mailboxes may require cleaning. Remove the ransomware instructions or malicious email message.
- After cleaning, be proactive about continuing to monitor signatures to detect signs that the attack is emerging once more.

Follow your recovery plan to get operations back to normal:

- If you have verified, clean backups, restoring affected files can be accomplished in relatively little time without the need to pay the ransom.
- Investigate the vector so that you can shore up your defenses. The infection vector could be a phishing email, an internet-based attack kit or another exploitation. Knowing how the attacker penetrated your defenses can help prevent future attacks.
- Report the incident. Victims are encouraged to report ransomware attacks to the FBI's Internet Crime Complaint Center.

Conclusion

An increasing number of organizations are suffering ransomware attacks, and experts predict that the numbers are only going to climb. Attackers have the potential to make large sums of money, which means that they are sure to ramp up even more.

Regardless of its size, virtually every organization is vulnerable to an attack, and the consequences of a successful ransomware attack can go far beyond the payment of the ransom. Lost business, customer inconvenience, lost productivity and negative publicity can result as well.

Rishi Bhargava is Co-founder and Vice President of Marketing for Demisto. He can be reached at 408-905-8344 or rishi@demisto.com.