WHITEPAPER

RANSOMWARE

ENEMY AT THE GATE

201 Ionia Ave, Grand Rapids, MI 49503 | 866.2.SIGNAL | ussignal.com

Introduction

They are out there waiting. “They” are the notorious, largely unknown cyber-criminals, ready to wreak havoc by taking advantage of information technology vulnerabilities. Their weapons of choice are an ever-growing array of sophisticated viruses, phishing scams, and a tool that’s proven to have devastating repercussions — ransomware.

Ransomware is a type of malware that secretly enters a user’s system, usually because a computer user opened an email and clicked on a malicious link or attachment. Once in, the ransomware silently encrypts the user’s data. A “ransom” message is then displayed, demanding a payment for the key to decrypt the data.

Ransomware has become big business in the world of cyber-criminals. According to the Internet Security Threat Report released in April 2017, there were 1,271 ransomware attacks detected a day in 2016, up 36% from 2015[1] . Global ransomware damage costs could exceed $5 billion in 2017[2].

A ransomware attack could be happening right now, as unaware or negligent employees at any number of companies around the world click links in spam emails or activate macros in malicious documents. Their companies’ data will quickly be encrypted, and a ransom of hundreds, thousands or even millions of dollars will be demanded for the data to be unlocked.

There is no single, guaranteed strategy for preventing a ransomware attack, or for recovering quickly if one does occur. However, there are protocols, practices, and processes to help mitigate attacks and minimize their damage. This whitepaper looks at some of them, as well as provides an overview of what ransomware is, how it works, and how to deal with an attack should one occur.

[1] Symentac, Internet Security Report 2017. ISTR 22: Extraordinary Attacks, High-Dollar Heists, Electoral Disruption. April 2017. https://resource.elq.symantec.com/LP=3980?cid=70138000001B-jppAAC&mc=202671&ot=wp&tt=sw&inid=symc_threat-report_regular_to_leadgen_form_LP-3980_ISTR22-report-main

[2] CyberSecurity Ventures. Ransomware Damage Report, 2017 Edition. May 18, 2017. http://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/

Ransomware: In the Beginning

To combat ransomware and its ill effects, it's important to understand how it originated and why it's become so pervasive. While its origins are open to debate, many cite the AIDS trojan as the first documented case of ransomware.

Also known as the PC Cyborg virus, the AIDS trojan was released via floppy disk in 1989 by an eccentric biologist named Joseph Popp. He distributed 20,000 disks labeled "AIDS Information - Introductory Diskettes" to attendees of the World Health Organization's AIDS conference.

While the disks did include a program that measured a person's risk of contracting AIDS based on responses to an interactive survey, they also contained a virus that encrypted victims' files after they had rebooted their computer 90 times. To regain access, users were ordered to send $189 to a designated PO box.

Despite all the resources devoted to fighting ransomware, cyber-criminals keep finding ways to use it to their advantage. Even the biggest name companies aren't safe.

Fortunately, an easily reversible form of cryptography had been used to hijack victims' hard drives. Decryption tools were quickly released, limiting the damage and costs. Nonetheless, the AIDS trojan exposed how easy it was to gain access to users' systems and coerce those users into paying.

Various forms of ransomware appeared in the following years but it wasn't until the mid-2000s that they started employing difficult-to-crack encryption algorithms such as RSA — a public-key cryptosystem used for secure data transmission. In 2011, combating cyber-criminals got tougher. Ransomware appeared as what looked like a Windows Product Activation notice, making it difficult for users to distinguish between real notifications and malware.

Then in 2012, the ransomware game became even more deceptive with the introduction of the Reveton worm. Also known as the "Police Trojan," it would display a warning supposedly from a law enforcement agency claiming that the computer has been used for illegal purposes. It would then restrict access to the computer and files. Users were literally locked out of their computers unless they paid a "fine" through a service such as Ukash.

Cyber-criminals upped their game again in 2013 with the release of CryptoLocker. The ransomware encrypted files and then demanded a ransom in return for a key to decrypt them. It infected more than 250,000 systems between September and December 2013[3]. Its creators earned more than $3 million before the Gameover ZeuS botnet used to carry out the attacks was taken out[4] . Nonetheless, CryptoLocker became the template for most of the ransomware that has attacked since.

Despite all the resources devoted to fighting ransomware, cyber-criminals keep finding ways to use it to their advantage. Even the biggest name companies aren't safe.

[3] Keith Jarvis, SecureWorks Counter Threat Unit™ Threat Intelligence "CryptoLocker Ransomware." December 18, 2013 https://www.secureworks.com/research/cryptolocker-ransomware

[4] Evan Perez, CNN Money. "U.S. takes out computer malware that stole millions." June 3, 2014: 7:52 AM ET. http://money.cnn.com/2014/06/02/technology/security/gameover-zeus-botnet/index.html

On May 12, 2017 the largest cyber-attack, as of that date, ravaged businesses around the world. A ransomware worm dubbed “WannaCry” leveraged a vulnerability in the Microsoft Windows operating system. While it primarily struck Windows 7 users, Windows XP users were hit as well. In just a few hours it infected more than 300,000 machines in over 150 countries, encrypting data and demanding ransom payments in bitcoins. The list of victims reads like a list of ‘who’s who.” Among them: FedEx, Hitachi, Honda, LATAM Airlines Group, the Ministry of Internal Affairs of the Russian Federation, Nissan Motor Manufacturing UK, Portugal Telecom, Shandong University, and the State Governments of India.

Ransomware Pays

Ransomware continues to grow in popularity among cyber-thieves because it has proven to be lucrative. According to the FBI, ransomware payments in 2016 were expected to hit approximately a billion dollars, compared to $24 million in 2015[5] . Many companies find it easier to pay a ransom and get the decryption keys to unlock their data rather than spend time and money attempting to get their systems back online internally.

Of course, cyber-criminals aren’t content with the status quo. They are getting increasingly creative in how they monetize their activities as exemplified by Cerber ransomware. In 2016, its authors offered their software “as a service” in return for a 40% cut of the profits from the ransoms that were paid. Cerber infected 150,000 victims in July 2016 alone. Of the estimated $195,000 paid in ransoms, $78,000 went to the ransomware’s authors.[6]

> *According to the FBI, ransomware payments in 2016 were expected to hit approximately a billion dollars, compared to $24 million in 2015.*

Not surprising, the profit potential of ransomware is heating up the competition between cyber-criminals. Petya, one of the first types of ransomware to offer ransomware as a service, fell victim to the creators of another ransomware called PetrWrap. Those cybercriminals cracked the Petya code and used it to perform their own ransomware attacks. And, they did so without paying the authors of Petya.[7]

Not Your Ordinary Malware

As already noted, ransomware has distinctive features that distinguish it from other types of malicious software — and that make it far more sinister. For example, it can encrypt all kinds of files, including documents, pictures, videos, audio files, and just about anything else that might reside on a computer. It can also scramble file names, so a user won’t even know which data has been affected.

By using unbreakable encryption, ransomware prevents most users from being able to decrypt their files on their own. However, ransomware isn’t always just about encrypting files. Some forms may have data exfiltration capabilities. That means they can extract data from an infected computer, such as usernames and passwords, and send that information to a server controlled by cyber-criminals.

[5] *Herb Weisbaum. NBC News. “Ransomware: Now a Billion Dollar a Year Crime and Growing.” January 9, 2017. http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646*

[6] *Check Point Threat Intelligence Research Team. “CerberRing: An In-Depth Exposé on Cerber Ransomware-as-a-Service.” August 16, 2016. https://blog.checkpoint.com/2016/08/16/cerberring/*

[7] *Anton Ivanov, Fedor Sinitsyn, SecureList. “PetrWrap: the new Petya-based ransomware used in targeted attacks.” March 14, 2017. 8:59 am. https://securelist.com/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/77762/*

Ransomware can also spread to other computers connected to a local network, creating further damage. It often recruits the infected computers into botnets, so cyber-criminals can expand their infrastructure and launch more attacks. What makes ransomware exceptionally difficult to stop is the fact that it uses a complex set of evasion techniques to go undetected by traditional antivirus products, cybersecurity experts, and law enforcement agencies.

Many incorporate built-in traffic anonymizers to avoid tracking by security experts and law enforcement and to receive ransom payments. Others use domain shadowing to hide their activities as well as the communication between the downloader and the servers they control. Then there are those that use encrypted payloads, making it more difficult for antivirus to detect the ransomware. Ransomware also tends to be polymorphic. It can mutate and create new variations without altering its function. It should also be noted that ransomware can remain inactive on the system until the computer is in its most vulnerable state and then strike fast.

Know Your Ransomware

There are several types of ransomware, and new variations are coming out at an ever-increasing pace. Some use encryption, while others ship as virus loads. Still, others are based on PowerShell. However, most ransomware can be classified in one of two categories: encrypting ransomware and locker ransomware.

Encrypting ransomware is designed to block system files by encrypting the data. Payment is then demanded in exchange for a key to decrypt the blocked content. Among the most notorious among this type of ransomware are CryptoLocker and Locky.

Locker ransomware is designed to lock a victim out of the operating system, making it impossible to access the desktop and any apps or files. The files are not encrypted, but a ransom is still demanded for the infected computer to be unlocked. Some locker ransomware will infect the master boot record, the section of a PC’s hard drive which enables the operating system to boot up. When that happens, the boot process can’t complete, and prompts a ransom note to be displayed on the screen. Examples include the Satana and Petya.

The Typical Ransomware Attack

A ransom attack usually begins with what appears to be a normal email. What’s not normal about it is that it may contain a malware attachment or a click-through link to an infected website. A fake pop-up ad sometimes appears on a user’s screen, claiming the user’s system has been infected and instructing the user to click on a link for help. In some cases, it may create a new master boot record for the drive. A message then appears demanding payment for a key to decrypt the user’s data.

Payment is often requested in bitcoins, digital currency that works like a credit card but with no personal identifying information, which makes it difficult to track down the recipients of it. Ransomware also sometimes employs geographical targeting, meaning the ransom demand is translated into the target’s native language, to increase the chances for the ransom to be paid.

Typically, there's a deadline for paying the ransom. If the deadline isn't met, the ransom increases. Or, the ransomware may flood the user's screen with pornographic images or use other mechanisms to force the user to pay up. Some forms also infect their hosts with more malware to steal users' login credentials for online banking and retail transactions. Others may search for additional computers to infect on the same network.

To Pay or Not to Pay

Most law enforcement agencies and security experts advise against paying digital ransoms, and for good reason. Paying the ransom may not yield a happy ending. There's the possibility that the attackers may not actually have the keys to decrypt the hijacked data, or they may simply refuse to supply them. Plus, you open yourself and your organization up to future extortion attempts.

Nonetheless, many companies choose to pay the ransoms. They fear not doing so could be catastrophic due to the costs of downtime and the interruption to their business. There's also reputational damage to consider. Cyber-criminals not only can keep data held hostage, but can also expose the data if payment is not made. This could severely damage an organization's reputation and brand value, particularly if customer information is involved.

70% of businesses infected with ransomware paid ransom to regain access to business data and systems.

In a study conducted by IBM Security[8] , 70% of businesses infected with ransomware paid ransom to regain access to business data and systems. Half of those paid over $10,000 and 20% paid over $40,000. Nearly 60 percent of all business executives said they would be willing to pay ransom to recover data, including financial records, customer records, intellectual property and business plans. Overall, 25 percent of business executives said, depending upon the data type, they would be willing to pay between $20,000 and $50,000 to get access back to data.

Top Ransomware Targets

Cybercriminals are indiscriminate when it comes to their ransomware targets. They'll steal from individual users as well as global corporations. When they do go after individuals, it's largely because they are relatively easy marks. Despite all the advice and warnings, individual users often don't back up their data or keep their software up-to-date. Many are also inclined to click on almost anything. Most home users still rely entirely on antivirus to protect them from threats. Unfortunately, most antivirus programs are not effective in identifying and protecting against ransomware.

However, it's the larger institutions such as corporations, schools, hospitals, and even government organizations that cyber-criminals prefer; that's where the money is. They know that a successful infection can cause major business disruptions, which will increase their chances of getting paid. They also know that many businesses would rather not report an infection for fear or legal consequences and brand damage.

[8] *Limor Kessem, SecurityIntelligence. "Ransomware: How Consumers and Businesses Value Their Data." December 14, 2016 https://securityintelligence.com/media/ransomware-report/*

Many of these organizations manage huge databases of personal and confidential information that cyber-criminals can sell on the black market. One study reported that the per record value of financial account data ranged from $14.00 to $25.00. Medical account data earned from $0.03 to $2.42. Credit and debit cards averaged between $4.00 to $5.00.[9]

Big company computer systems also tend to be complex, making them prone to vulnerabilities that can easily be exploited. Because ransomware can also affect servers and cloud-based file-sharing systems, there's even greater potential for data hijacking.

There's also the human factor. Employees can be negligent, unsuspecting, or uneducated about security protocols and inadvertently click on a link that introduces ransomware into their company's system. Weak BYOD (bring your own device) policies don't help.

Attack Prevention Best Practices

Ideally, you should never have to use decryption tools because you've been able to stave off ransomware attacks. Among the best ways to accomplish this is to employ a multi-layered approach that prevents ransomware from reaching your networks and systems.

The following are some of the best practices to incorporate into your data protection strategy:

- Regularly back up data and store the backups on a separate system that can't be accessed from a network. Verify the data backup process is capturing all necessary data and that the restore process works in your environment.
- Keep software up to date, including all security patches.
- Conduct frequent security training to help employees understand and avoid common security pitfalls such as clicking on links in spam email or opening attachments from unknown sources.
- Get rid of default system administrator accounts to prevent ransomware from using them to perform their operations.
- Eliminate local administrative rights to prevent ransomware from running on a local system to block access to critical system resources and files
- Employ robust filtering to reduce spam or potential malicious attacks in employee's inboxes.
- Use an email security appliance to block attachments, and limit the types of file extensions that can be delivered via email.
- Use anti-malware products that detect and block ransomware at both the file level and process level.
- Limit the write permission to a small number of directories to help prevent ransomware variants from carrying out their actions.
- Require a login at access points such as local and mapped drives.
- Use firewalls that implement whitelisting or robust blacklisting to reduce web-based malware downloads and to deter ransomware from connecting to command-and-control servers.
- Make sure firewalls limit or block remote desktop protocol (RDP) and other remote management services at the network level.
- Employ third-party, carefully vetted cloud services for your applications and data from companies with infrastructure that meet HIPAA, PCI, and other regulatory requirements and/or have private network connections.

[9] *Christiaan Beek, Charles McFarland, and Raj Samani, Advanced Programs Group, Intel Security. "Health Warning - Cyberattacks are targeting the health care industry." October 2016. https://www.mcafee.com/us/resources/reports/rp-health-warning.pdf*

Ransomware Attack Survival

While the practices described will help prevent a ransomware attack, there's no guarantee that one won't happen. If it does, your organization must be prepared to minimize downtime and damages. If you suspect a ransomware attack, do the following:

- Capture a snapshot of the system memory if you can to help locate the ransomware's attack vector and any cryptographic material that can assist in decrypting data.
- Shut down the system believed to be infected to prevent the further spread of the ransomware. This includes Wi-Fi and Bluetooth connections.
- Disable automated backups to local or external storage.
- Recall all emails suspected of carrying the ransomware attack to prevent further spread of the attack.
- Block network access to any identified command-and-control servers used by ransomware.

Integrate the above steps into your disaster recovery plan. Your plan should also detail how to deal with ransom demands. Some organizations choose to inform authorities so they can help with the investigation. Others prefer not to risk downtime and data loss by going ahead with a ransom payment. There is no right or wrong option. It will depend largely on your organization's risk profile and how much potential downtime it can tolerate.

The Challenge Continues

Ransomware is a highly successful enterprise for cyber-criminals and will continue growing in sophistication and attack frequency. The Internet of Things (IoT) may make things even more lucrative for cyber-criminals as the introduction of sensor-embedded devices provide billions of new attack vectors. It's not a stretch to think that someday ransomware could be used to try to disable the entire infrastructure of a business or even the government until the ransom is paid.

Law enforcement agencies, government entities, and security experts are working diligently to tackle the problem. However, it's incumbent on potential targets of ransomware to do their part to keep the enemy at bay as well. That includes employing security best practices, and having a comprehensive, frequently updated data protection strategy in place, and always being vigilant.

Learn More

For more information on combating ransomware and other cyber security threats, talk to a US Signal expert. Call 866.274.4625or email info@ussignal.com

You can also take advantage of this free resource from US Signal: Data Protection 101.