CYBER SECURITY GUIDE TO RANSOMWARE:

PROACTIVE PROTECTION, MITIGATION, & SAFETY

//PROACTIVE PROTECTION, MITIGATION, & SAFETY

//PROVEN CYBER SECURITY GUIDE TO RANSOMWARE:

V3.0.1

Table of Contents

Introduction

We would first of all like to thank you for entrusting us with the handling of your critical data during a difficult time. We hope that your data recovery experience was efficient and that all your files were successfully recovered in a timely manner. This document is a comprehensive guide to raise awareness and protect you from ransomware moving forward. Our goal is for you to be as fully prepared as possible to prevent an attack in the future.

Cyber threats are continuing to evolve through the use of ransomware virus invasions. The sophistication of these intrusions can leave an entire network crippled by encrypting every useful file extension. Taking a few preventative and proactive steps will help to secure your vital data.

Growing Threats

The Department of Justice recently announced that the Internet Crime Complaint Center (IC3) had received approximately 7,750 public complaints regarding ransomware since 2005. According to the Cyber Threat Alliance, CryptoWall ransomware alone accounts for $325 million in losses.[1] Also, Forbes reports that Locky ransomware variants are infecting over 90,000 machines daily.[2] Cybersecurity firm Kaspersky Lab recently released a publication stating that ransomware infections have reached pandemic rates and that they will not be decreasing any time soon.[3] In the past year alone, they estimate that ransomware attacks have grown by over 500%.[4]

Ransomware costs include ransoms paid in addition to the associated cost of lost data. Many victims also incur additional costs associated with network mitigation, network countermeasures, loss of productivity, legal fees, IT services, and the purchase of credit monitoring services for employees or customers.[5]

How Did My Files Become Encrypted?

There are numerous ways ransomware developers are spreading their malicious virus encryptions. In this section, we will outline the most common methods of infiltration and warning signals.

Remote Desktop Protocol (RDP) Exposure

Many ransomware variants such as Dharma/Crysis, AES-Matrix, Samas/Samasam, and other varients are spread via remote desktop protocol (RDP). Remote desktop protocol allows users to initiate a session with a remote computer. Once connected via remote desktop protocol the attacker will have access to the computer just as if he was sitting at the keyboard. Once in the network, Proven Data's forensics team has observed attackers uninstall anti-virus, steal passwords, leave backdoors, steal files and encrypt entire networks with ransomware!

While allowing RDP sessions from computers already within your network may be an important part of day to day business operations, systems should never have remote desktop exposed directly to the internet. Doing so allows hackers to use different types of exploits to attack the system and gain entry to your network. If remote access is required for business Proven Data strongly recommends deploying a VPN solution utilizing multi-factor authentication. As this may be an expense too large for smaller customers, a commercial login tool such as LogMeIn or TeamViewer may be substituted for the VPN, again using multi-factor authentication for logging in. If RDP is not needed, Proven Data recommends disabling this feature at the firewall.

Email Attachments

The most common method of infiltration seems to be emails disguised as being sent by legitimate organizations, trying to convince you to open an attachment. They will even attempt to build your trust by spoofing an email address to make the message and attachment seem like they are from a legitimate source. It is critical to know what to look for in email attachments and what to avoid opening. The links embedded inside of these spam emails could also potentially be malicious. These emails will very often pass through spam filters in your anti-virus software. Examples:

- Fake FedEx/UPS invoices
- Fake FedEx/UPS shipping labels
- Correspondence from someone in the form of an attachment
- Outstanding debt or fine to an organization (e.g. the IRS, police, government)
- A faxed attachment

Raising the awareness of all employees and talking about these warning signs are the best ways to prevent ransomware. Ransomware is constantly evolving, so it is important to keep up-to-date with the latest trends.

Vulnerabilities in Out-of-Date Software

Certain types of software have been exploited in the past, so it is critical to install updates when prompted. Be extremely careful that the update you are installing is legitimate, as some ransomware is even spread through notifications of false updates (in particular, through fake Flash updates). Some ransomware can also be spread through the Angler exploit kit which targets Windows updates, Adobe Flash, JavaScript, and Microsoft Silverlight.[6] For more information on Angler exploit, click here for an article which explains it well.

Weak Passwords

If you were hit with one of the targeted ransomware attack variants which include Troldesh (xtbl), DMA Locker, Dharma, .Wallet, Samas, or any variant in which there is an email address to contact, it is more than likely that an RDP (remote desktop protocol) password was exploited. Hackers can brute force your password if it is weak, or use a password dictionary such as **rockyou.txt**. Passwords may also be available for purchase on the dark web from other hackers.[7] It is also recommended that you change your default passwords for new devices that you bring into your network. Even with the strongest passwords, there is a chance that a hacker can exploit RDP through a vulnerability. We strongly recommend disabling RDP to the internet and use alternatives such as a VPN tunnel.

Torrents

Downloading music, videos, games, or anything through a torrent may give you ransomware unknowingly. It is very easy to disguise a file as something which may appear legitimate but is not.

Fake Advertisements (Malvertising)

Ads on websites are becoming another popular method of spreading ransomware. Crypto-ransomware has been found lurking in ads served on popular websites, including the BBC, the New York Times, MSN and AOL. Malvertising typically occurs when cyber criminals create ads that are perceived as legitimate but spread malware by hiding a small piece of code deep within them which connects a victim's computer to criminal servers. Ben Harknett, vice-president for Europe at cybersecurity firm RiskIQ stated that "Recent research we carried out at RiskIQ revealed that malvertising jumped up over 300% year on year between 2014 and 2015 following a string of major publishing sites, such as Forbes.com, Huffington Post and the Daily Mail, being exploited by malvertising campaigns."[6]

Prevention

Anti-Virus, Anti-Malware, Anti-Ransomware

Today's ransomware protection goes beyond the standard firewall and requires a full security suite, including anti-malware and virus protection software. Cyber hackers are continually evolving their software, searching for methods to enter your system undetected. Each layer of a security suite will attempt to catch the attack. If a new variation gets past the anti-malware, the additional protection level within a robust firewall can thwart the connection with the Command and Control (C&C) server confirming the encryption file instructions. We recommend the following ransomware protection below.

For Business**:**

- Sophos Endpoint Protection
- Malwarebytes Business

For Personal**:**

- Malwarebytes Home

There is an anti-ransomware product now available from Malwarebytes, however, be aware that it is a beta version so it may have some bugs. We have tested it on several variants, and it has worked effectively. It recognizes when files become encrypted and will lock down your system to prevent the encryption of further files. It is one of the first tools available of its kind and can be downloaded here: Malwarebytes Anti-Ransomware

Software Updates

Cyber hackers depend on the fact that many people allow their systems to function without timely updates, making them vulnerable to exploitation. IT security consultants advise businesses and consumers to keep their applications and systems up-to-date with the latest security patches.

Many organizations rely on WSUS to perform Windows OS updates. This does not cover third-party updates. Having a vulnerability management program helps identify all vulnerabilities due to configuration and third-party.

The easiest way to ensure software updates/patches are promptly installed is to enable automatic updates. Hackers use vulnerabilities in **Windows, Microsoft Silverlight, Oracle Java, and Flash** to infect your system with malware, so frequent updates are critical.

Security Awareness Training

One of the most common methods of obtaining access to a company is through social engineering. It is critical to train your users on different areas such as vishing, spam, whaling, impersonation, and USB devices. A penetrator could convince an employee to give access to the company. From there, the penetrator could install instal ransomware on the system. Organizations such as offer Security Awareness training that will help in preventing these types of attacks.

As the old saying goes, you are only as secure as your user base. This saying will withstand the test of time. There are several offerings that Proven Data recommends for security awareness training. Phishme, Wambat, and KnowB4 Security are both excellent resources. If you would like us to perform a phishing campaign test, you may contact us through the case management system or call us directly.

It is important to know potentially malicious warning signals. You should never open an email or a link from an untrusted source or anything that seems out of the ordinary. If a website seems questionable, avoid it altogether. Also, be wary of fake advertisements.

Data Backup

When virus protections fail due to zero-day exploits, backing up your data outside of your computer or network is the single best method to combat ransomware. In the case of a ransomware attack, you will be able to restore your system to the time before it was encrypted. It is critical to note that any mapped network drives or external hard drives/flash drives which are connected are also vulnerable to a ransomware attack. If you choose to use an external hard drive as a backup measure, unplug it as soon as the backup is complete to avoid infection should you encounter ransomware. A scheduled daily backup is recommended in many cases to avoid large lapses in data capture periods.

Testing data restores is as important as performing the back-up. These restore procedures should be tested probably quarterly as a minimum.

To assist both individuals and companies in backup efforts, we have partnered with Carbonite, one of the most reputable cloud-based backup solution providers. Together we have established a method to help configure the backup process so that little technology knowledge is needed. We help all our clients with the consultation and implementation of this process at no cost to you.

**Additionally, by signing up using the “try now link” within the link below, we will see your account in our dashboard. This grants us the ability to monitor your backups to ensure they are running as scheduled. If there are ever any issues, we get notified real time and take the appropriate actions to ensure issues have been addressed. We offer this as a courtesy to all clients who have used our services.

Please note we do not markup Carbonite’s subscription fees, and we do not have access to your data!

Click here for the Carbonite information.

Cyber Security & Insurance Policy

Although cyber insurance won't ultimately protect your business from ransomware, it will keep you prepared financially should a ransomware intrusion occur. Organizations should have cyber security insurance which is part of a risk management plan. A cyber insurance policy, also referred to as cyber risk insurance or cyber liability insurance coverage (CLIC), is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event. [10] What exactly will a cyber security insurance policy cover? Outlined below in are some of the most common coverages.

- Forensics investigation – Forensics would be required to determine if and when an intrusion has occurred and provide preventative solutions from the same breach occurring again. HIPAA has made it mandatory for medical institutions to report ransomware attacks (Proven Data also provides forensic investigations for ransomware attacks). Here is the link to the article from HHS.gov. In this document, it also states that organizations are supposed to incorporate lessons learned and or have a risk analysis and implement security measures to mitigate or remediate the risk.
- Business loss liability – Many cyber insurance policies cover monetary loss from network/user downtime, business interruption, data loss recovery and costs involved in managing a crisis, which may involve repairing reputation damage.[10]
- Privacy and notification – This includes required data breach notifications to the customer and other affected parties, which are mandated by law in many jurisdictions, and credit monitoring for customers whose information was or may have been breached. [10]
- Lawsuits and extortion: This includes legal expenses associated with the release of confidential information and intellectual property, legal settlements and regulatory fines. This may also include the costs of cyber extortion, such as from ransomware. [10]

From the same resource, we also will reference in quotes below what to look for when comparing different cyber insurance policies.

"

- Does the insurance company offer one or more types of cyber insurance policies or is the coverage simply an extension of an existing policy? In most cases, a stand-alone policy is best and more comprehensive. Also find out if the policy is customizable to an organization.

- What are the deductibles? Be sure to compare deductibles closely among insurers, just like you do with health, vehicle and facility policies.
- How does coverage and limits apply to both first and third parties? For example, does the policy cover third-party service providers? On that note, find out if your service providers have cyber insurance and how it affects your agreement.
- Does the policy cover any attack to which an organization falls victim or only targeted attacks against that organization in particular?
- Does the policy cover non-malicious actions taken by an employee? This is part of the E&O coverage that applies to cyber insurance as well.
- Does the policy cover social engineering as well as network attacks? Social engineering plays a role in all kinds of attacks, including phishing, spear phishing and advanced persistent threats (APTs)
- Because APTs take place over time, which can be months to years, does the policy include time frames within which coverage applies? "[10]

It is important to be prepared in the event an unfortunate intrusion occurs. The chances of an attack on business have significantly increased over the past decade and losses are tremendous.

Enable Hidden File Extensions

Ransomware has been successful due to its sneaky ability to hide damaging .exe files within seemingly harmless files such as .pdf or Word documents. This ability is a loophole within the Windows environment, as it hides known file extensions. Check your Windows version for the instructions to see/view the ‘full file extensions,' and therefore be prepared when a malicious attachment is sent.

Disable/Deny Emails with these specific file extensions

A majority of gateway mail scanners already include the function of denying email with .exe (executable) extensions, .js, bat, chm, hlp, cmd, com, cpl, crt, exe, hlp, hta, inf, ins, isp, jse, lnk, mdb, pcd, pif, reg, scr, sct, shs, vbs, ps1, ps2, zip, gz, tgz, 7z. The executable file is the method used to gain access and encrypt your computer and network. You should also have the ability to deny file extensions, including any embedded malicious file attachments. Be aware also that zip file attachments (.zip files) can contain a multitude of file types. Cloud services should provide options for you to deny .zip files via a password protection ability.

Deny or Disable AppData/LocalAppData Folder Files

Ransomware makes use of the AppData/LocalAppData folders to run their executable virus software. You have the option of creating rules within Windows or through intrusion prevention software to disable anything that tries to make use of these folders and run malicious code. If you have legitimate programs that take advantage of these folders, you can exclude them from the deny/disable rules.

Disable Remote Desktop Protocol (RDP)

RDP is used to allow remote access to your computer or network. Typically, this is for technical support or viewing/sharing desktop information. It is also used in some of the more standard conference software available. Many firewalls have a denial ability already built in. RDP should not be enabled to the internet.

If an organization has a requirement for remote access, this should be enabled through a remote access VPN. This can be accomplished via a Pulse Gateway, or a Cisco ASA with Any Connect to name a couple.

Many of our clients require RDP for their software to function. Turning it off may not be an option. For those, we would recommend a 2 factor VPN. We can help provide suggestions on what to buy. We can also help clients configure and setup their VPN.

** If you have a server and you were hit with Samas, Troldesh (.xtbl), DMA Locker, or any variant in which an email address is attached to your files, it is critical to take the steps advised in this section.

** Instructions for various Windows versions to disable RDP:

Windows XP RDP disable

Windows 7 RDP disable

Windows 8 RDP disable

Windows 10 RDP disable

Use a Ransomware Prevention Kit Option

This is a type of new technology that takes care of some of the most technical requirements, such as disabling files running from the App Data and Local App Data folders, and disallowing any .exe and .zip files. Once installed, you will need to check the provider's site for updates continually. The **Cryptolocker Prevention Kit** is an example. If you have the need to create 'exemptions' from their Group Policy rules, they provide an instruction document to help.

Create Strong Passwords

Proven Data has encountered a surprisingly large number of ransomware recovery cases as a result of weak username and password combinations. Hackers have tools to scan and brute force weak passwords quite easily. We cannot stress the importance of creating strong passwords to avoid this enough. We recommend using a strong password generator, such as the one found here: http://passwordsgenerator.net/

Other Tips

- Verify Transport Layer Security (TLS) 1.2 is enabled for the RDP service.
- Change the internal RDP port from default 3389 to something else. Do not enable RDP to the internet.
- Whitelist (approve) IP's that are allowed access over the RDP port that is forwarded.
- Set up a virtual private network (VPN) tunnel, allowing only local traffic to remotely access the server
- If you require access to a server outside your network, we suggest using a service like TeamViewer and enabling two-factor authentication
- Review the windows share permissions to ensure that common users do not have "write access" to shares. If a user does not have access to write files then the ransomware cannot encrypt the file.
- Configure AV to prevent the changing of file to those that have ransomware extensions. (eg, .locky). Here is a link to a McAfee document illustrating the concept.
- Removing admin access from all users. This will prevent attaching to ADMIN$, IPC$, etc.
- Enable Tamper Protection on your antivirus
- Separate the backup systems from the user workstations by a firewall and only allow the correct ports to accomplish the backup.

- Web filtering will also assist in preventing ransomware. This can be accomplished through AV or a product like OpenDNS.
- Performing GEO-IP blocking can also disrupt a ransomware attack. If the adversary infrastructure is hosted in a different country other than the US and Geo blocking is preventing connections from anywhere other than the US then the attack chain will be broken. (We have personally seen this multiple times where the compromised web server (in the US) redirected to the site hosting the exploit kit (RIG/Angler/etc). The exploit kit site was in a different nation and the EK was blocked from being delivered.
- There is also an open source ransomware tracker list that can be used as a blacklist for either proactive blocking or alerting.
- System security baselines should also be implemented. The Center for Internet Security (CIS) has free benchmarks to ensure the systems have been hardened. These can also be used by Nessus to scan a system to ensure that the system is compliant with the benchmarks.
- Block internet access to non-work related email websites, such as Gmail, Yahoo, Juno, etc
- Use an ad-blocker.

What to Do if You are Hit with Ransomware

If you find that you have potentially had a ransomware attack and have not accomplished the suggested security protocols, you have some limited options. Ransomware recovery and removal can be accomplished with a few actions on your part to help limit the damage. If you are not comfortable taking these steps, it is recommended you seek assistance from an experienced ransomware remediation company like Proven Data to ensure proper handling of the situation.

- **Immediately Disconnect the Network as well as Wi-Fi**

  If you suspect a ransomware attack but have not seen the familiar 'ransom screen' displayed, you have a small amount of time to take action to cease the communication with the C&C server before it completes the encryption of your files. Time is of the essence, as the encryption process needs time to complete the encryption process. Disconnect all Wi-Fi devices as well as any connections to all network servers. This is not a guarantee against encryption, but it may be able to limit the damage.

- **Run Anti-Malware Software**

You will need to remove the executable file spreading the encryption through your system as soon as possible to minimize the number of files which become encrypted.

- **Use Your System-Restore/Shadow Copies to Return to a Previous Safe/Clean Condition**

  If you are using Windows, you may be able to make use of 'System Restore' to return to a previous or 'clean' state. Be aware that many of the malware programs have the ability to 'shadow' the files from System Restore, which means those critical files will not be available during the restore process. Some of the newer malware will also make attempts to disable System Restore and may delete files if you institute an executable file, which may be necessary during the restore or as a part of the standard Windows process. This is not a failsafe method, but if you act quickly, you may be able to outsmart the malware.

  - If the organization is using virtualization, the organization could use system snapshots as a quick b/u restore procedure. If the company requires forensics, clients are required to separate the infected machine from the network and let Proven Data or another forensic company perform a digital forensic analysis.

- **Identify Reporting Requirements**

Depending on the type of data impacted by the ransomware, you may have legal obligations for investigation. If the impacted data contains PHI, PII, or other regulated data, please contact Proven Data for assistance. Do not take steps to wipe, re-image, or restore the system from backups as may result in a loss of valuable evidence which may be beneficial to a digital forensic investigation.

- **Report The Crime to Authorities**

US-based: https://www.ic3.gov/complaint/

Europe: https://www.europol.europa.eu/content/report-cybercrime

Additional Ransomware Recovery Information

If you are a Proven Data customer and are concerned about ransomware protection or think ransomware has targeted you, call 877-364-5161 for immediate assistance.

DISCLAIMER

PROVEN DATA RECOMMENDS ALL OF THE TIPS IN THIS ARTICLE BUT DOES NOT GUARANTEE YOU WILL BE PROTECTED AGAINST 100% OF RANSOMWARE ATTACKS AND ASSUMES NO LIABILITY FOR ANY SUBSEQUENT INTRUSIONS.

References:

(1) https://www.cyberthreatalliance.org/wp-content/uploads/2018/02/cryptowall-report.pdf

(2) http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#7554fccb75b0

(3) https://blog.kaspersky.com/ransomware-blocker-to-cryptor/12435/

(4) http://www.ciodive.com/news/kaspersky-lab-ransomware-attacks-spike-500-in-last-12-months/421584/

(5) https://www.ic3.gov/media/2015/150623.aspx

(6) http://www.computerweekly.com/news/4500278672/Crypto-ransomware-lurks-in-ads-on-popular-websites

(7) http://www.scmagazine.com/ransomware-using-remote-desktop-to-spread-itself/article/448398/

(8) http://www.scmagazine.com/ic3-warns-of-attack-using-ransomware-to-drop-trojans-and-keyloggers/article/394762/

(9) https://en.wikipedia.org/wiki/Keystroke_logging

10) http://www.csoonline.com/article/3065474/cyber-attacks-espionage/what-is-cyber-insurance-and-why-you-need-it.html