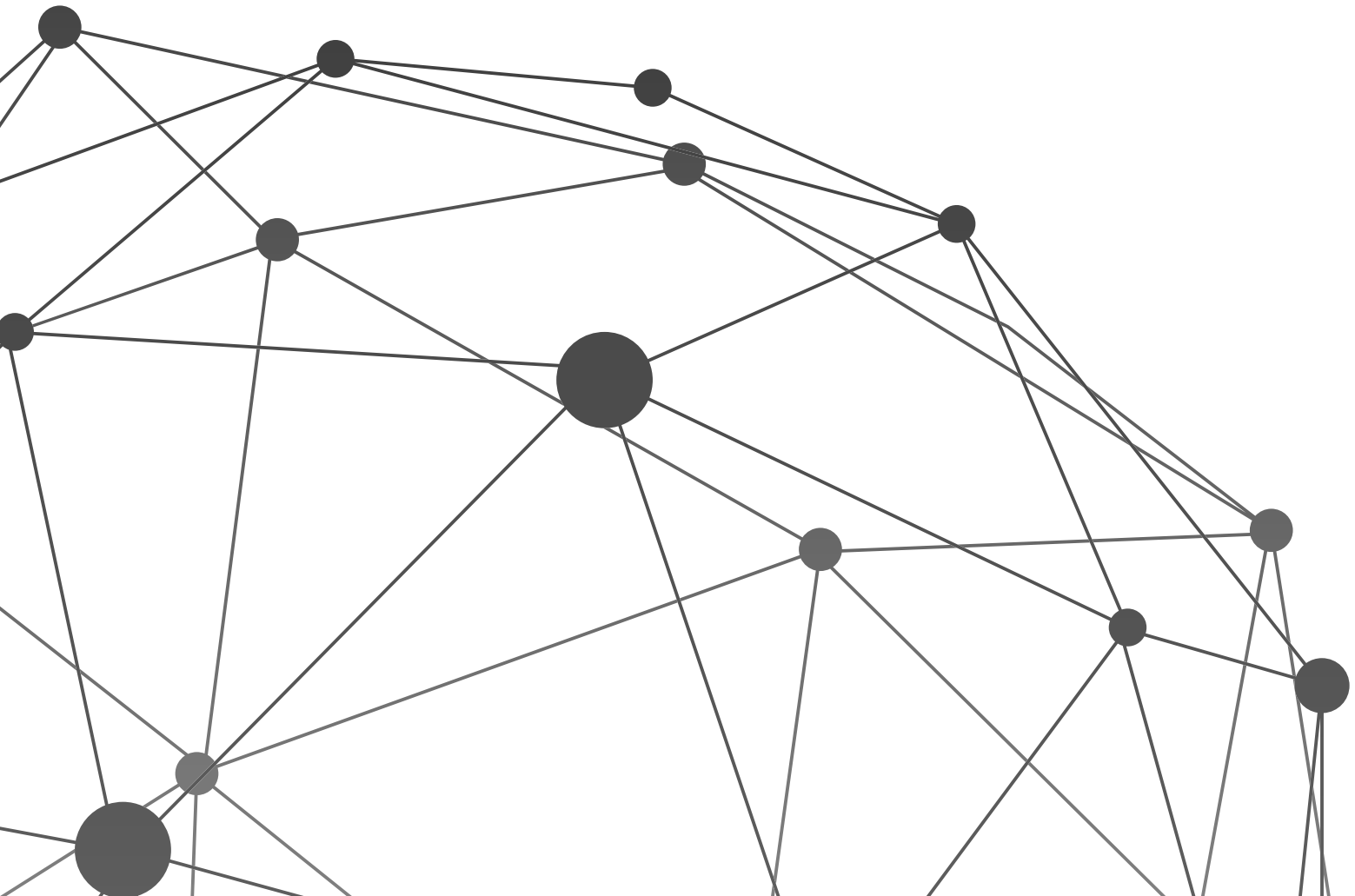
HEAT® software

Ransomware:

The New Normal in Malware

September 2015



What Is Ransomware?

Ransomware is the fastest growing threat in the world of malware. And unlike most malware in the past, you can't simply use anti-malware tools to recover from this category of attack. Ransomware is malware specifically designed to restrict access to a computer system and then demand that a ransom be paid in order to restore access to the system.

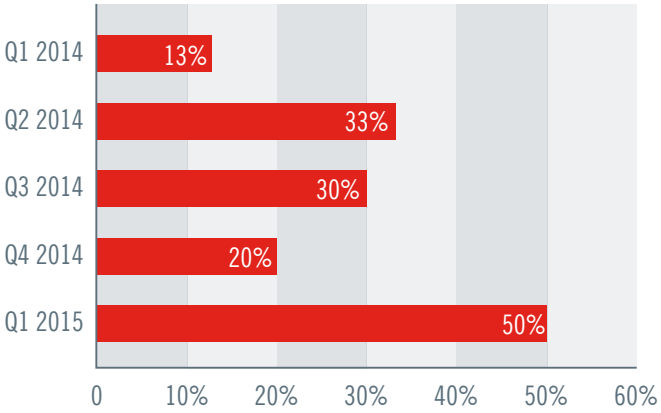
Malware, Not Virus

Ransomware is malware – it is malicious software. It's usually not a virus though, meaning it doesn't replicate itself across multiple computers on a network. Of course, there are always exceptions to the rule. But for the most part ransomware does not spread from one computer to another across internal networks. It does leverage the network for communicating with command and control (C&C) servers, and to access attached and mapped drives. Finding ransomware on one machine does not automatically mean it has spread to other machines on the network.

Restricts Access, Or Encrypts

Not all ransomware encrypts the files on your PC. The general goal of ransomware is restrict access to the useful files on the device, or prevent you from using the device at all, until the ransom is paid. Encrypting files is one method of accomplishing that goal – but encryption is complex to code. Other effective methods ransomware uses are to prevent you from closing browser windows, imitating the OS registration process, opening full screen modal windows[1] which can't be closed, and other similar tactics. That said, since 2013 a growing percentage of these attacks have used file encryption, called crypto-ransomware – and this has become the most common tactic.

Figure 1: Increase in Crypto-Ransomeware



Fully one-half of all ransomware is now crypto-ransomware, the type that encrypts files. Source: Trend Micro

Another common tactic is intimidation. This approach, called "scareware" or "copware," purports to be a law enforcement agency in your country, automatically detecting your location by your IP address. It claims you have been involved in illegal activity online, typically involving copyright infringement or other illegal content. The text of the threat indicates that you must pay a fine to avoid prosecution and regain access to your device. A newer variant looks through your browser history to see if there are any sites it can cite in the UI which will serve as apparent proof of illegal content, since you will recognize them as visited sites. It then says all your activities are now being recorded and evidence on your machine is being preserved. Sometimes there's even a webcam photo of you as proof of having control over your device. This type of scareware ransomware has gained popularity and is prominent on mobile devices where file encryption is more complex, if it's possible at all.

Fake Antivrus

The idea behind ransomware may have its roots in fake antivirus scams which were popular through 2011. Fake antivirus convinces the victim there is a problem they must pay to remove. Cryptographic ransomware makes the problem real.

Scareware Works

A 21-year-old Virginia resident who was the target of a scareware attack felt such guilt he turned himself into authorities and was subsequently charged with accessing and possessing illegal content. More seriously, a 38-year-old Romanian man killed his 4-year-old son and then committed suicide after receiving a fake police notice popup, believing it was real.

Your Phone is a Computer System

Computers aren't the only devices subject to ransomware. All that's needed to create a ransomware-friendly environment is a CPU, storage space, a method to install software, ideally some RAM, and a vulnerability to exploit. By this definition thermostats, microwaves, televisions, and even cars are potential targets for ransomware.

Ransomware has already been seen on Android and on iOS devices. In these cases, the victim installs an app masquerading as a game or as having some other seemingly benign purpose. The app then takes control of the device and the victim must pay to disable or uninstall it.

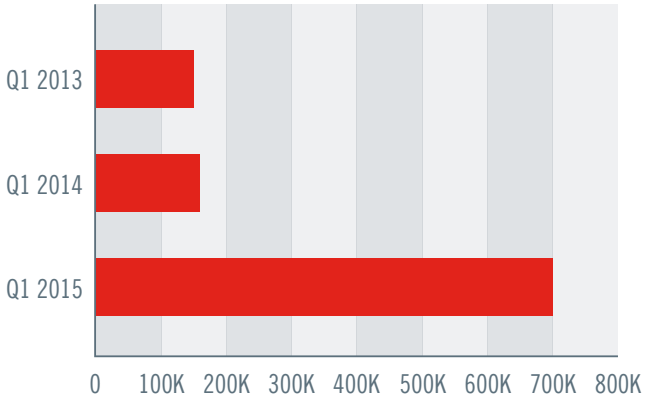
Explosive Growth in Ransomware

Ransomware has existed almost as long as the IBM PC, and has seen huge growth starting in 2013. The first widely-reported ransomware attack was in 1989.[2] Social engineering deception convinced victims to install the software from 5.25" diskettes. Buried in the EULA was the disclosure that the user would have to pay to use the software, and that the functionality of their PC would be adversely impacted if they didn't. The ransom was to be mailed to a Post Office box in Panama. Thousands of diskettes were made and distributed. It's unknown how many machines were actually infected, but the author eventually faced only 11 counts of blackmail.[3]

As the internet, World Wide Web, and email became pervasive, ransomware also.

Fast-forward to Q2-2012, and ransomware incidents have tripled from the same quarter the previous year.[4] In June of 2015 the U.S. Federal Bureau of Investigation reported that in the preceding 90 days they received 992 complaints regarding one variant of ransomware, CryptoWall, alone.[5] This represents a small portion of incidents, those reported to FBI. Intel researchers confirm this with their own data. They report a 155% increase in attacks in Q4-2014, and another 165% increase in Q1-2015.[6]

Figure 1: Ransomware Attacks



The incidence of ransomeware attacks has increased dramatically. Source: McAfee Labs

Cryptographic ransomware is rapidly becoming the most popular form of ransomware. Crypto-ransomware encrypts the files on the victim machine using strong encryption techniques. Encryption is not the only technique that cybercriminals use, and ransoms aren't always monetary. In some targeted cases, databases are stolen and the owner is threatened with public release of the information if certain conditions aren't met, such as changes in organizational policy.

Ransomware Prevention

This paper focuses primarily on crypto-ransomware, but the preventative measures described will also help protect against non-encrypting ransomware and malware in general.

Who Does Ransomware Affect?

Unlike Advanced Persistent Threats (APTs) or other malware with espionage-related goals, ransomware is generally not targeted at any specific individual or organization. Targets are opportunistic. Ransomware is typically delivered via phishing emails, drive-by downloads, or malvertising. Anyone with an email address or a web browser is a potential victim.

Malvertising on the Rise

Malvertising is the use of online banner adver-tising networks to distribute malicious content. Appearing on reputable sites and indistinguish-able from legitimate advertisements, users click them and the malware exploits a browser or plugin vulnerability. Malvertising is affecting more users than ever, and continuing to grow.[7]

Grandmothers, small business owners, individual staff of large organizations, and even government agencies have reported being victims of ransomware.

- A reporter from the New York Times wrote about her mother's experience with ransomware.[8] Her mother tried everything she could to recover her files without paying the ransom. She ultimately paid the ransom in order to get her personal files back.
- A small Santa Monica, California based commercial real estate firm was a victim of ransomware. They were able to recover from backups. Even though they didn't pay the $500 ransom, they were offline for two days and spent 10+ hours restoring their data from backups.[9]
- In Dickson County Tennessee, the Sheriff's office became a victim of ransomware when an employee clicked on a banner ad which delivered the malware. After engaging the FBI and even the military, they decided to pay the ransom to regain access to all 72,000 of their files containing autopsy reports, witness statements, crime scene photographs, and more.[10]

Targets are not geographically chosen either. Australia, Europe, and the United States are commonly victimized. South America and Asia see the lowest rates of infection.[11] Some variants of ransomware do exclude certain countries from victimization. Since most ransomware seems to originate in Russia, excluded countries typically include Russia and its neighboring politically-friendly countries.

Is Ransomware Here to Stay?

Ransomware's growth in popularity is not random. There are several factors which are enabling this growth and will continue to do so.

Profit

The prime factor is that, for the cybercriminal, the path to profit is clear and direct. Other malware targets such as stolen identities or credit cards require another transaction to sell them. Much of the value is lost when selling stolen information. Cybercriminals have to steal a large volume of information, and can only sell so much of it before it becomes worthless. With ransomware, the ransom is pure profit. The attacker has some up-front costs in buying a malware kit and mailing list or web server, but those are quickly recovered in a small number of victims. Ransomware is easy money by comparison.

Technology

In recent years sophisticated encryption technology has become more prevalent and more accessible. Operating systems now have built-in encryption capabilities to leverage. Weaknesses in encryption schemes have been exposed, and encryption as a whole has improved. Key lengths increase with computing power, and encryption algorithms become more efficient. This not only makes legitimate encryption easier, but it makes a ransomware author's job easier as well.

Anonymity

Another contributing factor is easier anonymity. Cybercriminals have to go to great lengths to hide their identity and location. Anonymous networks such as Tor has made it far easier to obscure the path from the victim machine back to the C&C server and ultimately the perpetrator. Anonymous currency has also contributed to the rise of ransomware. The risk of payments being traced to the payee is very low. Bitcoin has become the currency of choice. Not regulated by any government, and with Bitcoin laundries readily available, cybercriminals can essentially take payments directly from their victims and escape identification.

There is no evidence to suggest that any of these contributing factors will reverse course. The environment is becoming more ransomware-friendly, and is apt to stay that way. For the foreseeable future, ransomware is here to stay.

Ransoms Before Bitcoin

Before anonymous currencies were available, ransom payment methods included snail-mailing a check to a P.O. Box, SMS with high charges, and telephone long distance calling fees.

How Does Ransomware Work?

Understanding how ransomware works will provide insight into what protections can be put into place to prevent it or recover from it. Here is the typical process crypto-ransomware follows to infect your systems, and how you can defend against it.

Step 1: Delivery Mechanism

Attack	Defend
The first step, as with any malware, is to get the ransomware onto the victim machine. One common technique is phishing email campaigns with malicious attachments. The victim clicks on the attachment and unknowingly installs the ransomware on their machine. Another common delivery method is drive-by downloads triggered by web browsing. Other techniques include malvertising and leveraging dormant machines on existing botnets.	As these techniques are common for all classes of virus and malware delivery, the defenses are common as well. User education is a front-line defense against phishing campaigns. Informing your user base that there are active phishing campaigns will increase their alertness to unexpected emails and attachments. Sharing specific Subject lines or body content of known phishing emails increases the effectiveness of the user education effort. Drive-by downloads are best defended against by keeping all browser patches current, and by keeping add-ons and plug-ins updated. Also, uninstall any unused plug-ins, add-ons, and browsers. Finally, enforce secure browser settings. Disable third-party content wherever possible, use the do-not-track feature of the browser, and limit the flexibility of scripts on webpages to a reasonable extent.

Step 2: Exploit a Vulnerability

Attack	Defend
Once the ransomware is on the victim machine, it must exploit some vulnerability to install itself and gain the system access it needs to complete its tasks. The ransomware may exploit vulnerabilities in the operating system, third-party applications, or web browsers. It may attempt multiple exploits until one succeeds.	Defense at this step is also universal. Keeping patch levels current on the operating system and third-party applications, and uninstalling unused software reduces the number of vulnerabilities the ransomware will be able to exploit.

Step 3: Weaken the Security Posture

Attack	Defend
The ransomware will disguise itself as legitimate process such as `explorer.exe` and `svchost.exe`. It often does this using techniques such as memory injection. Most modern ransomware variants implement several anti-detection techniques to avoid exposure by any existing anti-virus and intrusion detection tools. Depending on the variant of ransomware, it will then disable non-SSL connection warnings to the user, replace the proxy settings, disable recovery or repair attempts by the operating system, disable a variety of anti-malware processes, and configure itself to load on boot even in Safe Mode. Some ransomware also securely and silently deletes volume shadow files using the Volume Shadow Copy Service to prevent files from being restored after encryption.	Once the ransomware has exploited a vulnerability and is running, more sophisticated defenses are required. Application Control creates a whitelisted environment wherein an unauthorized application, such as ransomware, is not able to execute. Memory injection protection prevents malware from injecting itself inside a legitimate process as a cloaking technique. Monitoring and enforcing secure configurations on machines can also help defend against this step in the ransomware process.

Step 4: Establish Communications

Attack	Defend
After installation, the ransomware will contact a command and control (C&C) server. It may need to download additional code. It also creates and sends unique identifiers for the victim machine to the C&C server. The C&C server responds with instructional text for paying the ransom which will eventually be displayed to the user in the appropriate language. C&C servers are sometimes located on the open web, having unintelligible URLs. Increasingly they are hidden in Tor or I2P networks[12] for anonymity purposes. The URLs for the C&C servers are often hardcoded into the ransomware. But more sophisticated ransomware employ Fast Flux or Domain Generation Algorithm (DGA) approaches to create a group of URLs. The operator of the ransomware uses the identical algorithm with an identical seed to generate the same list of URLs, then registers a few of them. The infected machine then checks each URL in the list until it successfully contacts a C&C server. In this way, URLs exist mere hours before being used, making URL blacklisting almost impossible. CryptoWall's C&C server will also check the country of the victim machine against a list of countries in which the author does not want to operate, and also checks to be sure it is the only instance of CryptoWall on the machine. Warning: CTB-Locker is an exception to this order of operations. As a feature, CTB-Locker will not contact its C&C server until after encryption is complete. This helps the ransomware avoid early detection through network monitoring.	Preventing the ransomware from establishing communications is not straightforward. The best opportunity for blocking C&C server communications is with the organizational firewall. The firewall on the victim machine will have been compromised in the previous step. For ransomware which has its C&C URLs hard-coded, you may be able to read these URLs directly from the file in a hex file viewer, and then set firewall rules to block those URLs. You can also set firewall rules to block patterns such as "*.onion" to block Tor traffic altogether.[13] For other cases, you may find unintelligible URLs in your log files, and can then block traffic to those URLs to prevent any further victim machines from accessing them. Data from your threat intelligence feed can also help filter out known bad URLs.

Step 5: Encryption of Files

Attack	Defend
Modern ransomware uses strong encryption. Some have claimed key lengths up to 3072 bits, although 2048-bit key lengths are more common. Hardcoded into the ransomware is a list of file extensions it will encrypt. Early ransomware used a list of about 44 extensions; modern ransomware uses lists of over 200 different file extensions. The list does not include executable files, configuration files, or other files the operating system may need to continue to function. All drives with drive letters are processed, regardless of whether they are internal, removable, or network drives. The ransomware proceeds through each folder on each drive, encrypting files which match a file extension in its list. The original file is overwritten by the encrypted file to make recovery more difficult or impossible.	At this point in the process, there are few defenses. The ransomware has compromised the machine and the environment, and is in control. Application Control continues to be an option at this step, since it will prevent the encryption process from running. Active file integrity monitoring will also flag up alerts of changing file sizes and potentially dates. Encryption is a computationally intensive process. If a user on an infected machine notices extensive CPU usage or hard drive activity, ransomware may be at work. In this case, catching ransomware in the act, it is advisable to disconnect the network cable and turn off any wireless network adapters immediately. If the process can be stopped before any mapped network drives which the entire organization utilizes, a great savings can be realized. Also, any removable storage such as removable hard drives should be disconnected – especially if those drives are used for backup purposes.

Step 6: Demanding the Ransom

Once the encryption process is complete, the user is notified that their important files have been encrypted. A screen is presented to the user which displays either HTML or an image file which it received from the C&C server. Additional notification methods include changing the Desktop wallpaper to this image, placing a text file with instructions on the Desktop, or placing a text file in each folder where files were encrypted.

The notification includes information critical to recovering the files. It will let the user know how much money is being demanded, and whether that amount will increase after a given number of days, usually 3 to 7.

It will explain which payment methods are accepted. Payment to a predetermined Bitcoin wallet is quickly becoming the standard. Other options include untraceable cash transfer methods such as Ukash, paysafecard, and MoneyPak.

Users are typically unfamiliar with Bitcoins, and must learn how to buy them. Ransomers include instructions for this. They also include instructions for downloading and installing Tor if it's required to make the payment.

Step 7: Decrypting Files

After the ransom is paid, the user typically receives a decryption key. The key is unique to the affected machine. They must type the key into the interface to start the decryption process. The ransomware then starts decrypting the files until it has restored each encrypted file. There is often a list of encrypted files placed in the registry so it can keep track. Any network or removable drives with encrypted files should be connected during the decryption process.

Step 8: Configuration Restoration

After decryption of the files is complete, there's still work to do. The ransomware may still reside on the victim machine. Antivirus and antimalware tools can be used to identify and remove any files belonging to the ransomware. Also, remember that the ransomware weakened the security posture of the machine in its early stages so that it could operate undetected. Those settings need to be restored.

Many organizations take more broad action after a ransomware attack. Equipment and software upgrades are commonly made. New protection software is purchased and installed. Outside security consultants are usually hired to evaluate the environment and make recommendations for improvements.

Protecting Systems from Ransomware

The most effective defense against ransomware is **Application Control**. In a whitelisted environment, only authorized applications are allowed to execute. Regardless of how ransomware finds its way onto a computer, it will not be able to execute unless it is specifically authorized. The malware can then be identified by anti-virus as signatures are updated, or from Application Control logs which will show that its execution attempt was blocked.

With Application Control from Lumension, a HEAT Software company, IT administrators can quickly identify all applications running in their environment and enforce a comprehensive whitelist policy that prevents unauthorized applications, malware and un-trusted change.

Application Control also includes **Memory Injection Protection**, which protects against advanced in-memory exploits, including DLL Injection and Reflective Memory Injection attacks, which can evade standard endpoint security products. This additional layer of protection will prevent the ransomware from injecting itself into an `svchost.exe` or `explorer.exe` process. This is important in instances where the ransomware is delivered through a drive-by download and tries to exploit a vulnerability in the browser or a browser plug-in such as Flash or Java.

The next most effective defense against ransomware is to keep systems' patch levels current. All ransomware needs some to exploit some vulnerability. Most exploits are of vulnerabilities for which a patch has been issued by the vendor. **Patch and Remediation** is the world's leading patch management solution, and is available as a modular offering on the Endpoint Management and Security Suite. With Patch and Remediation, you can automatically identify and patch heterogeneous operating systems, Microsoft security and non-security vulnerabilities, 3rd party applications, and endpoint configurations – all of which is seamlessly managed through a single console.

Patching Will Stop Ransomware

Researchers intentionally trying to infect test machines with CryptoWall were unable to do so. They learned the Java version on the test machine had a fix for the vulnerability the ransomware was trying to exploit, rendering the ransomware ineffective. Patching is a good defense.

User Education is another valuable tool in preventing ransomware attacks. Commonly ransomware is delivered as a PDF, ZIP, or DOC file attached to a phishing email. The believability of phishing emails has increased, and busy users are likely to click on the attachments without a second thought. Educating users about which phishing emails are being currently circulated, going directly to websites rather than clicking links, and not opening attachments is a good start in reducing the number of successful infections. Providing users with a mechanism in your ITSM system to report, and receive feedback on, suspect email or attachments will also be useful.

Enforcing **Secure Browser Configurations** will also contribute to your defenses against ransomware. Any settings related to third-party websites should be restrictive, as well as any tracking settings. Consider prompting for some plug-ins rather than allowing them to execute automatically.

Implementing a solid **Data Backup Plan** is also crucial. Having current backups means not having to pay ransoms. The ransomware can be removed and the unencrypted files restored. Backup best practice is the 3-2-1 rule. Have 3 copies of every file – the original and two backups – on 2 different media, and at least 1 of those copies physically located offsite. Having current backups when infected with ransomware can mean the difference between major business interruptions and a non-event.

[1] A modal window is one which prevents you from accessing other windows until it's closed. Non-modal windows can be resized, minimized, closed, switched in and out of, etc.

[2] http://www.securityfocus.com/advisories/700

[3] http://www.securityfocus.com/columnists/102

[4] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2012.pdf

[5] http://www.ic3.gov/media/2015/150623.aspx

[6] http://www.mcafee.com/ca/about/news/2015/q2/20150609-01.aspx

[7] http://www.csoonline.com/article/2947681/vulnerabilities/malvertising-reaches-record-levels-in-june.html

[8] http://www.nytimes.com/2015/01/04/opinion/sunday/how-my-mom-got-hacked.html

[9] http://www.wsj.com/articles/ransomware-a-growing-threat-to-small-businesses-1429127403

[10] http://www.scrippsmedia.com/newschannel5/news/Sheriffs-Office-Forced-To-Pay-Ransom-For-Their-Own-Case-Files-282493831.html

[11] http://blog.trendmicro.com/trendlabs-security-intelligence/cryptowall-3-0-ransomware-partners-with-fareit-spyware/

[12] Tor (The Onion Router) and I2P (Invisible Internet Project) networks are designed to provide strong privacy capabilities, and aside from perfectly legitimate reasons is often used to access the so-called darknet for illegal purposes.

[13] In fact, in their Q3-2015 Threat Intelligence Quarterly report, IBM recommends this step as a general rule for security-minded organizations.

Ransomware Preparedness Checklist

Use this handy worksheet as you assess your ransomware defenses.

☐ User Education

It all starts with users. Make them aware of the prevalence of ransomware. Share information about suspect emails, safe browsing practices, and malvertising.

☐ Security Reporting System

Leverage your ITSM system to create a way for your users to report, and learn about, phishing attempts that might lead to a ransomware attack.

☐ Incident Response Plan

Update your IR plan to cover a ransomware attack, and practice it from detection to recovery to ensure all components of the procedure work.

☐ Data Backup Plan

Implement a 3-2-1 Data Backup Plan. 3 copies of every file – the original and 2 backups. Backups should be on 2 different media, and 1 copy must be kept offsite.

☐ Application Control

In a whitelisted environment, unapproved and untrusted programs such as ransomware are not able execute from a file on disk.

☐ Memory Injection Protection

Some ransomware variants inject themselves into legitimate processes without using a file on disk. Memory Injection Protection monitors legitimate processes for such suspicious activity, and terminates the process when it has been compromised

☐ Centralized Patch Management

Operating systems, native and third-party applications, plug-ins and add-ons all need to be patched to current levels. Ransomware needs a vulnerability to exploit. The fewer vulnerabilities which exist in your environment, the more secure it is.

☐ Secure Browser Settings

Enforce a restrictive but reasonable browser configuration for Internet Explorer, Chrome, Firefox, Safari, and any other browsers in your environment.

HEAT Software USA Inc.
490 N. McCarthy Blvd. Milpitas, CA 95035 USA
P. +1 800.776.7889 or +1 408.601.2800