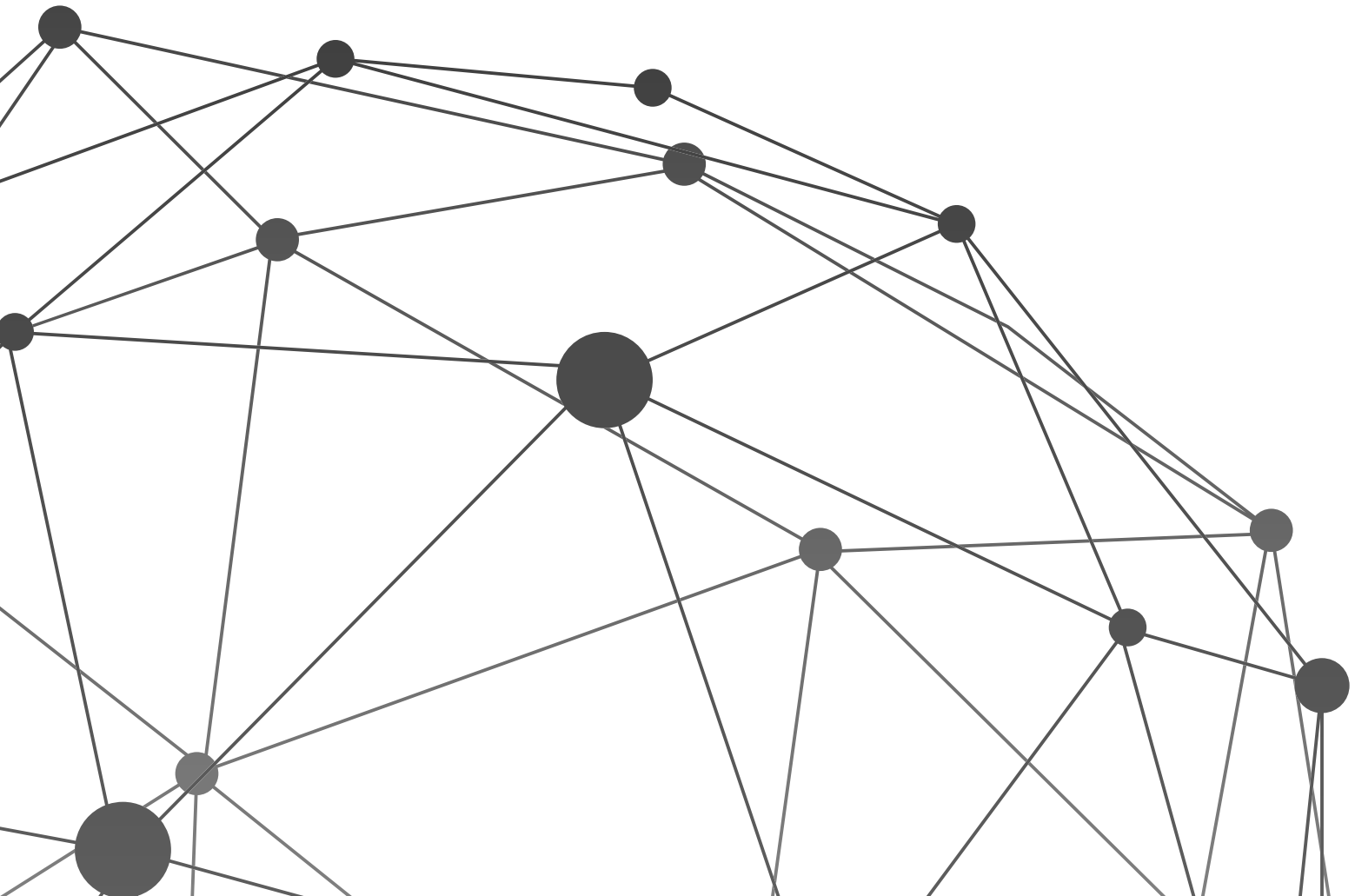
HEAT® software

Avoiding a King's Ransom

Why Ransomware Is More Than a Royal Pain

September 2015



Ransoms are among humanity's oldest means of exploitation. Taking an item of tremendous value – traditionally, a person – and demanding compensation for its return is an effective, if sinister, way for perpetrators to get what they want.

Because the crime is effective, it continues to be committed. But today the item of tremendous value increasingly is personal or corporate data. And the act is achieved through ransomware – an insidious and rapidly emerging threat to individuals and organizations alike.

With ransomware, attackers infiltrate systems – from laptops to servers to data centers – and render their data inaccessible. Often this is achieved through encryption, though less sophisticated means of making data inaccessible can also be used. Unless victims pay a ransom, they'll never see their data again.

Several aspects of this cyber-extortion make it more unsettling than other forms of cyber-crime. One is the seemingly personal nature of the attack. The malware actually communicates with the victim, and the victim must follow its instructions for any hope of data recovery.

Another is the ruthlessness of the attack. Stealing customer information or intellectual property is criminal. But irreversibly encrypting a business's data seems particularly evil.

A third aspect is how helpless digital extortion makes the victim feel. Law enforcement can't stop it. The IT department can't reverse it. Unless you've taken the right steps before ransomware hits, all you can do is pay the ransom and hope for the best.

But with the right proactive measures, you can recover from ransomware after the fact. More important, with the right processes and technologies, you can avoid ransomware exploits and protect your mission-critical data.

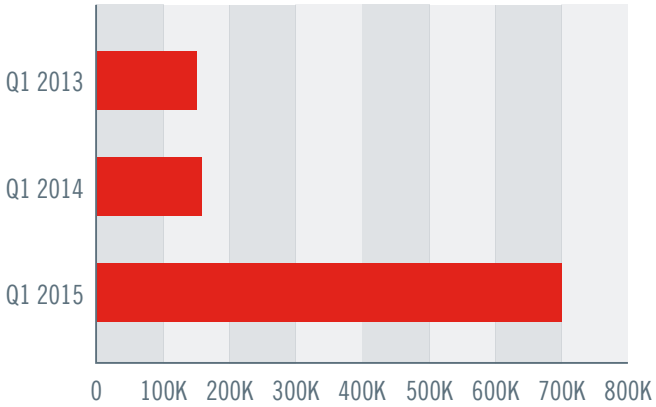
625K

Machines worldwide held hostage by CryptoWall in mid-2014

Ticking Time Bomb

If your organization hasn't been hit with ransomware yet, it's probably only a matter of time. The CryptoWall ransomware variant alone held nearly 625,000 machines hostage and encrypted 5.25 billion files over five months in mid-2014, according to Dell SecureWorks.1 Incidence of ransomware then surged 155 percent in the fourth quarter of 2014 and another 165 percent in the first quarter of 2015, McAfee Labs reports.2 (See Figure 1.)

Figure 1: Ransomware Attacks



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

The primary motivation for online extortion is financial. The CryptoLocker Trojan that was active from September 2013 to May 2014 is believed to have extorted $3 million. Between April 2014 and June 2015, victims reported ransomware-related losses totaling $18 million, the FBI reports.3 Most victims have been in North American and Europe, where they may be more likely to pay ransoms than in other markets. (See Figure 2.)

5.25B

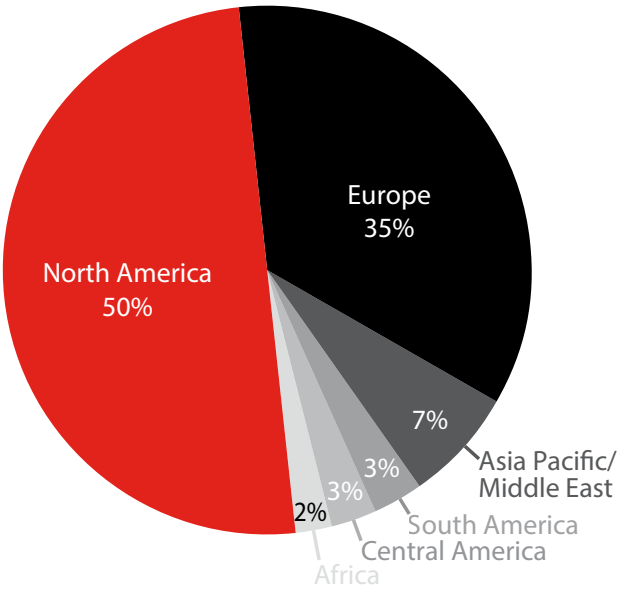
Files Encrypted by CryptoWall in mid-2014

But that probably represents only a small fraction of the ransoms being paid in the face of sophisticated attacks such as CryptoLocker and CryptoWall. While attacks against individuals typically demand about $300, those against businesses and government agencies have reached hundreds of thousands of dollars. And many organizations understandably are reluctant to report ransomware incidents.

$18M

Ransomware losses reported from 2014 to 2015

Figure 2: Ransomware Victims by Geography



Ransomware attackers target wealthy markets where victims are more likely to pay the ransom, such as the United States and Europe.

Ransomware can involve several common tactics and attack vectors:

Ransomware – Any malware that infects a computer or other IT device and restricts user access until the victim pays a ransom can be considered ransomware. Some variants encrypt files. Others merely claim to encrypt files. Some act as screensavers that won't turn off, or continuously launch browser windows to make a machine essentially unusable.

Crypto-ransomware – Crypto-ransomware uses strong cryptography to encrypt files. It then presents victims with an alert that they must pay a ransom to decrypt their data. (See Figure 3.) In fact, the proportion of ransomware that is crypto-ransomware has been steadily on the rise, with a sharp uptick in 2015. (See Figure 4.) Variants have gone by names such as CryptoLocker, CryptoWall and TeslaCrypt. Some variants can jump from machine to machine within a network. They can also look for file shares and attached backups, and extend to web servers or other servers, debilitating business operations.

5 of 6
Proportion of large enterprises targeted with spear-phishing in 2014

Phishing – Ransomware is typically spread through phishing emails that contain malicious attachments. Five out of every six large enterprises were targeted with spear-phishing – malicious emails that appear to be from a trusted source – in 2014, a 40 percent jump over the previous year, Symantec reports.4

Figure 3: Ransomware Alert

Ransomware alerts victims that their files will remain encrypted until they pay the ransom, as shown in this alert from CryptoLocker ransomeware.

Drive-by downloads – Another common ransomware attack vector is unintended downloads from infected websites. Ransomware delivered through a browser must exploit a software vulnerability on the target machine, but that's often quite easy. In fact, 99.9 percent of exploited vulnerabilities were compromised more than a year after they were published in the Department of Homeland Security's Common Vulnerabilities and Exposures list, says Verizon.5

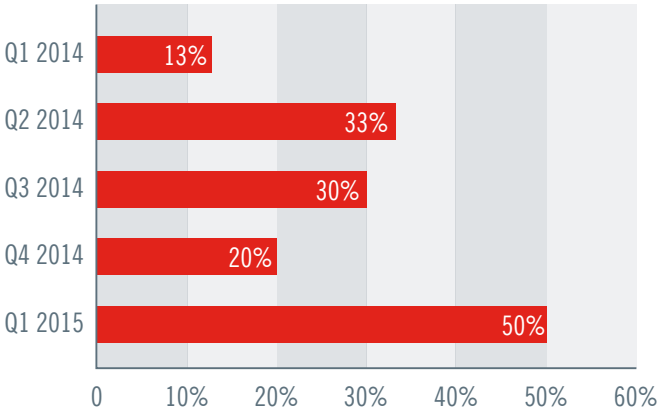
Malvertising – A favorite attack vector of cyber-criminals engaged in online extortion is "malvertising" – the injection of malware-laden ads onto legitimate websites. Popular sites from the New York Times to the Nikkei Stock Exchange have unwittingly carried malvertising. Many variants of crypto-ransomware, including the recent TeslaLocker, are being dropped by malvertising.

99.9%
Percent of exploited vulnerabilities compromised after publication of CVE

USB sticks – Some crypto-ransomware can spread to – and from – attachable devices such as thumb drives. For example, the original CryptoLocker Trojan has been modified into a USB-spreading worm. That means files on removable media are vulnerable to ransomware

attacks. But it also means removable media itself is an attack vector, one that could potentially spread ransomware to corporate servers that hold many more files—and much more mission-critical data—than any thumb drive.

Figure 4: Increase in Crypto Ransomeware



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

To wreak havoc, ransomware simply needs a CPU, storage space and a path of installation. That means it can hit laptops, desktops and servers. It can infect entire data centers. It can target smartphones and tablets; attacks against both Android and iOS devices have already been documented. It can extend to wearables that sync with other devices, such as the Android Wear smartwatch. And in the Internet of Things era, it could potentially hit Internet-connected HVAC or lighting systems.

Early and Often

Once crypto-ransomware encrypts files, there's generally no practical way to decrypt them. So your best measures against ransomware are preventive.

That starts with data backups. If you maintain timely, complete backups, plus the processes to quickly and fully recover backed-up files, you can mitigate a fair amount of the risk of losing data to ransomware. You still incur the potentially considerable time and expense of restoring what could be a very large number of files. But you can avoid paying a conceivably large ransom – as well as the risk the attackers won't actually decrypt your files.

To Pay or Not to Pay?

When ransomware strikes, you need to decide whether to pay the ransom. Law-enforcement authorities and many data-security experts advise against it. But is that the best advice?

The rationale for not paying is that you're encouraging criminal behavior. If enough victims refuse to pay, attackers will lose their financial incentive. Plus, there's no guarantee the attackers will actually decrypt your files after you pay.

But many organizations pony up. Unless they're 100 percent confident they can quickly and fully restore their data from remote backups, many companies might be inclined to pay. Even if they have reliable backups, paying the ransom might the fastest, cheapest way to recover – assuming the perpetrators decrypt the data after they receive payment.

Attackers do have an incentive to decrypt ransomed data, because they have a "reputation" to uphold if they hope to continue doing "business." Some even make available help files on how to pay ransoms using bitcoins.

It's easy for authorities to advise against paying when it's not their data at stake. But when it is their data, even law-enforcement agencies in Illinois, Massachusetts, Tennessee and other jurisdictions have handed over the bitcoins in the face of ransomware.

In short, each organization will have to decide whether to pay based on its own unique situation. The better solution, of course, is implementing the processes and technologies ahead of time to minimize the chances of your data being held for ransom and to maximize your ability to recover quickly.

Note that file-syncing services aren't backups. The encrypted document on your MacBook Air will be just as encrypted in iCloud. Backups on attached drives or network-mapped drives will likewise be encrypted. You need enterprise-class, offsite backups. A good backup rule of thumb is "3 2 1": back up 3 copies of every file, on at least 2 types of media, at least 1 of which is offsite.

With offsite backups, you can restore your files – after the ransomware has finished the encryption process. Once a directory of files has been encrypted, you can restore that directory with your backups. Current ransomware variants have not yet been documented to go back and re-encrypt files.

Bear in mind, however, that your backups may be of already-encrypted files, or a mix of unencrypted and encrypted, if your backup ran while the ransomware process was underway. You may need backups from several days or even several weeks ago, so make sure your backup policy allows for that.

Ransomware and DDoS: Two Bots in a Pod?

Like ransomware exploits, distributed denial-of-service (DDoS) attacks have the power to bring your operations to a standstill. But ransomware and DDoS have more in common than just being pernicious threats.

While DDoS attacks have been prevalent for some time, DDoS extortion has emerged as a new twist. In a DDoS extortion, perpetrators bring your web servers to their knees with a massive volume of data requests. They then demand payment to end the attack.

In May 2015 hackers launched a DDoS attack on Bank of China and Bank of East Asia, two of Honk Kong's largest financial institutions. They demanded payment in bitcoins to avoid another round of attacks.

In fact, in April 2015 alone, more than 100 financial institutions were victims of DDoS extortion, the FBI told MarketWatch.6 Ransoms typically reach tens of thousands of dollars. But DDoS attacks can cost banks more than $100,000 an hour, according to Neustar.7

What's more, DDoS attacks are increasingly used as a smokescreen for ransomware attacks. With IT staff focused on the DDoS event, they don't notice a slowdown in systems as the ransomware encrypts thousands of files. The DDoS distraction gives the ransomware time to move laterally throughout the network to wreak maximum havoc.

Teach Your Users Well

Another way to mitigate against ransomware is through education. Despite years of warnings about suspicious emails and websites, users still fall prey. Nearly one-quarter of email recipients open phishing messages, and 11 percent click on phishing attachments, according to Verizon. Put another way, a campaign of just 10 emails has a greater than 90 percent chance of creating a victim.8

23%
Percent of email recipients
who open phishing messages

11%
Percent of email recipients
who click on phishing attachments

So, redouble your efforts to ensure that users understand the risks, as well as their responsibilities in helping to protect corporate information. Ensure that new employees are trained during onboarding, but also make sure existing workers are re-trained on an ongoing basis. Work with your HR and internal communications departments to help engrain data security into your organization's DNA.

Be specific in your guidelines on avoiding ransomware schemes. Many phishing emails include subject lines about package deliveries, payroll or payments – topics that are enticing and may seem legitimate. Tell users what to look for. Advise them not to open PDF attachments or install screensavers, for example, until they've been scanned by your antivirus (AV) software. Let them know that if they click on a file icon and it appears to do nothing or it disappears, they should immediately report the event to IT.

Similarly, make sure your IT staff is familiar with ransomware: how to spot suspect files or URLs, what to do when they see unexplained system slowdowns, how to advise users who report ransomware on their devices. Codify processes that specify how systems are monitored, how suspected phishing attempts are reported, who the report is shared with, what steps to take following a ransomware infection, and so on. Fast action, such as immediately taking an affected machine offline, can prevent a ransomware attack from moving laterally through your network and affecting other systems.

White-Knight Whitelisting

But your most effective defense against ransomware is application control in the form of intelligent whitelisting. Why? Because effective whitelisting software prevents any executable from running on your network unless it's explicitly on the whitelist. That means even if ransomware ends up on one of your machines, it simply won't run – no encrypted files, no inaccessible data, no worries.

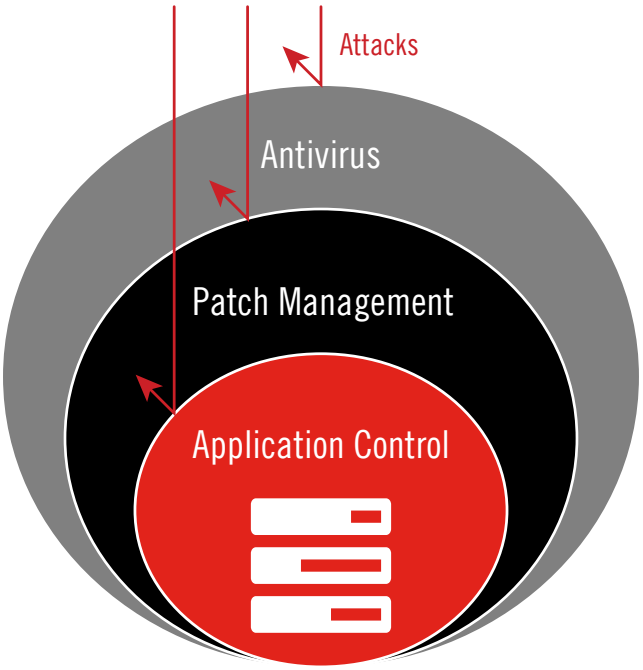
Intelligent whitelisting is an approach to application control that lets you prevent malware and unapproved software from running on your machines, while giving you the flexibility to adapt to changing business needs. It starts with a local whitelist and a trust engine that lets you define criteria for trusted applications. You can specify trusted publishers, updaters, paths or locations. You can also specify trusted authorizers, so certain users can maintain productivity by using software that would otherwise be blocked – a risk, yes, but at least you can prevent any contagion from spreading.

An intelligent whitelisting solution also lets you maintain a blacklist of denied applications. The blacklist can override the whitelist to block specific applications, even if they aren't malware per se, for security, productivity, bandwidth usage or other business reasons.

Protected to the Hilt

Intelligent whitelisting is a key element in a layered, defense-in-depth approach to data security. (See Figure 5.) In addition to application control, such a comprehensive strategy should include AV, device control, patch management and configuration management:

Figure 5: Intelligent Whitelisting Layered Defense



Application control in the form of intelligent whitelisting can protect against ransomware attacks that would otherwise be missed.

AV – Effective AV quickly and accurately identifies all known viruses, worms, Trojan horses, rootkits, keyloggers, spyware, adware and yes, ransomware. It also employs multiple detection techniques to identify and block zero-day exploits.

AV should combine traditional signature-matching capabilities with newer heuristic-based approaches such as partial pattern matching, behavioral analysis and general exploit detection to provide the most proactive protection. It should also enable granular policy management, with the ability to schedule multiple AV scans per endpoint with various scan settings and times.

Device control – Ransomware can spread to attachable devices such as thumb drives. Protection against such crypto-ransomware calls for effective device control.

Device control lets you set rules about what kinds of devices can be loaded on an endpoint. Those rules can be granular, addressing type, brand and even individual USB drive. Effective device control centrally automates the discovery and management of removable devices. It defines and enforces device use policies by group and by user, with flexible exception management. It should also capture detailed forensic information to track data events.

Patch management – Patch management remains one of the most effective means of thwarting attacks, including ransomware. The premise is simple: Reduce the known vulnerabilities in your environment to minimize the exploitable surface area. To protect against ransomware in particular, be sure to patch your operating systems, Microsoft Office, .NET, Adobe applications, your browsers and browser plug-ins.

To that end, centralized patch management is key. Without a centralized solution, you need to rely on multiple individual updates from every software vendor. That becomes impossible to manage, it can degrade endpoint and network performance, and it assumes users aren't turning off auto-updates and exposing you to risk.

Configuration management – To ward off ransomware, set browser security to the highest possible to reduce the chances that malicious content can be downloaded from a website, and that a malicious script can run. Also use the browser's Do Not Track feature to reduce the number ads users see and their chance of encountering malvertising.

In addition, monitor outgoing traffic. Ransomware binaries sometimes include hardcoded URLs to connect to a command-and-control server to allow encryption to happen. Block known malicious URLs and watch for "nonsense" URLs that look suspicious. When in doubt, block first and ask questions later.

You **Can** Prevent Ransomware

Make no mistake: Ransomware is the next big scourge to strike IT departments and the mission-critical data they protect. It's not a trivial threat, and it's one your organization is almost certain to encounter. But by taking preventive measures now—including rigorous data backups, thorough user training, and defense-in-depth data security led by intelligent whitelisting – you can mitigate the risk of ransomware and other malicious attacks, without ransoming your organization's success.

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