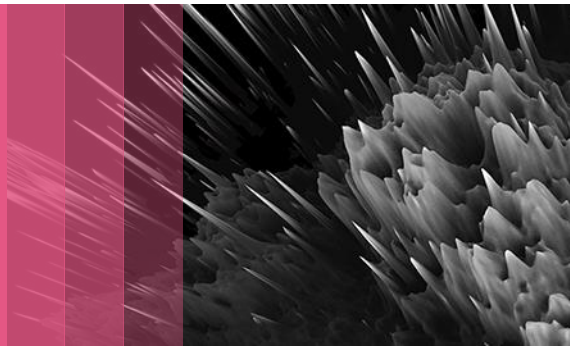
RANSOMWARE:
ATTACK TRENDS, PREVENTION, AND RESPONSE



EXECUTIVE SUMMARY

For the past decade, hackers motivated by financial gain – as opposed to those focused on stealing specific intellectual property or acting for political reasons – turned to banker Trojans as their primary approach. But, the tide has shifted. Banker Trojans have been eclipsed by ransomware as the preferred weapon of hackers everywhere, and in recent months, security incidents attributable to ransomware have been seen at an alarming rate in businesses and government organizations.

The rise of ransomware has become a global epidemic. It continues to accumulate victims worldwide, forcing companies to decide between attempting to recover data from backups (and potentially losing vital data since the last backup) and paying significant sums of ransom to hackers. Ransomware has made recent headlines by accumulating high profile casualties, including a Los Angeles hospital, an Oregon church and two German hospitals. The last several years, have resulted in an increasing volume of new ransomware attacks and variants. From CryptoLocker, Locky, and Kovter, to recent attacks leveraging CryptXXX, and Petya, it seems we hear about a ransomware attack every day, with new variants appearing almost on a weekly basis.

While ransomware has been around for some time, it has really been in the last two years that it has moved to the top of the attacker's toolbox. Ransomware has taken thousands of individuals and entire corporations hostage, destroyed valuable data, and accumulated 100's of millions of dollars in gains for skilled hackers. As security vendors continue to develop defenses to detect and block traditional attacks, ransomware has evolved; becoming more adept at hiding inside documents, leveraging websites that appear innocuous to the user, and avoiding detection by traditional antivirus and signature based solutions. Hackers easily swoop in, quickly encrypt files, and receive a significant payout in return for a decryption key that may or may not work, and then disappear without a trace.

As the frequency of these attacks increases, organizations are becoming acutely aware of the risks posed by ransomware. Yet most are unprepared to defend against the latest evolution of ransomware techniques. Deepen your understanding of the threat of ransomware. Learn how to better protect your business assets by reading this white paper highlighting the challenges enterprises face, and best practices to prevent ransomware attacks and limit their impact on organizations.

> "KNOWING IS NOT UNDERSTANDING. THERE IS A GREAT DIFFERENCE BETWEEN KNOWING AND UNDERSTANDING: YOU CAN KNOW A LOT ABOUT SOMETHING AND NOT REALLY UNDERSTAND IT."
>
> CHARLES KETTERING

July 2016

THE RISE OF RANSOMWARE

In the last several years, ransomware has become attractive to hackers seeking an alternative to the banker Trojan as it offers many advantages to developers. It is easier to implement, requires little customization, provides easier access to funds, and does not require a live channel or constant communication with the C&C server to successfully execute. For the attacker, this makes it easier and more cost efficient to extort more money.

Hacking for Financial Gain – The Shift from Banker Trojans to Ransomware

For more than a decade, banker Trojans were one of the most prominent threats in the cyber world. Banker malware was exceedingly profitable for attackers, but it had its limitations. It was once simple for a hacker to create a mirror of the bank's website, capture user credentials, and transfer funds. As fraud detection improved, and 2-factor authentication became the norm, today an attacker typically needs more than just credentials to succeed. They must also leverage the attack from a device previously authenticated by the user. To be effective, banker Trojans, like the one used in the Zeus campaigns, need to be targeted at specific audiences, must be customized for each banking site, and must be localized to address different languages. This type of attack requires much more effort, and a blanket campaign is no longer possible.

Making matters even more complex are the logistics of actually obtaining the funds from the victim. Funds must be transferred from the target account to a mule account. This requires the banking malware to keep a live channel during the attack. If the Command & Control (C&C) server is shutdown during the process, the attacker will not be successful. Even if they can address these challenges, the attacker still runs the risk that the transfer will be blocked by the bank (in the case of fraud detection technology for example), or that the transaction triggers a silent alert to catch the attacker when they withdraw the funds in person. The ability to trace physical retrieval or electronic movement of funds creates a real risk for the attacker. These challenges impact the associated costs, time required, and relative success rates of banker Trojans, which has driven attackers to adopt alternative methodologies instead.

Ransomware Attack Vectors

In its simplest form, ransomware is malware that encrypts the victim's files and then demands a ransom be paid in order to decrypt the files. The most common infection method used in ransomware campaigns is spam or phishing emails. The email contains an attached Word document (or other document) that contains a malicious macro. The user opens the file, enabling the macro. The malicious macro runs a script that downloads the malware's executable file, installs it on the victim's computer, scans for files on the system and encrypts them. Additional vectors include drive-by malware or the promotion of infected content downloads at "watering holes" – sites that have been socially engineered to attract visitors from the target company or industry.

Executing the Attack – Simple and Straightforward

Once the files are encrypted, the victim is shown a ransom note, asking for payment in return for a decryption key to regain access to their files. Unlike a banker Trojan, ransomware requires little customization. To localize a ransomware campaign, developers need only to translate the ransom note into the local language. Developers can even skip that step by referring users to Google Translate. The ransom note provides payment directions to victims and a window of time to pay up or lose their files permanently.

> "THE MOST COMMON INFECTION METHOD USED IN RANSOMWARE CAMPAIGNS IS SPAM OR PHISHING EMAILS"

Ransomware Payment Models Are More Reliable

Attackers have found ways to get around the funds transfer challenges faced by banker Trojans. Most current ransomware uses Bitcoin currency for payment, rather than government-backed currency. This offers several distinct advantages. Unlike the use of credit cards or account-to-account transactions, it enables funds to be transferred without an option to dispute or cancel the transaction at a later date. Bitcoin wallet shuffling allows the attacker to remain anonymous and the transaction to remain untraceable by the authorities. And changing Bitcoins into the currency of choice is as easy as using an ATM.

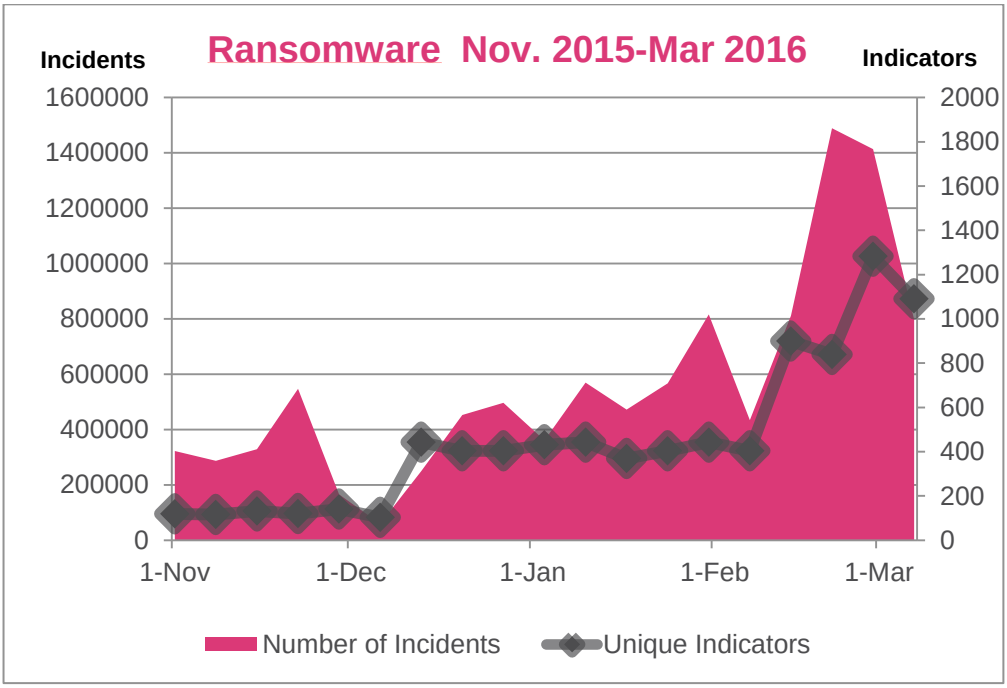
No Communication – No Problem

The final factor driving the shift to ransomware is one of communications. Ransomware does not require an open line of communication after the infection. After the files are encrypted, it becomes the victim's responsibility to follow the directions in the ransom note to find the attacker in the TOR anonymized underground, and complete the transaction. There is no additional action required by the attacker, and the motivation to complete the payment is entirely on the victim if they wish to retrieve their files. Recent variants of ransomware do not even require communication to obtain the encryption key used to lock the user files. Instead, they come packaged with a pre-determined public key, making it unnecessary to even establish a live connection to a C&C server to successfully generate revenues.

> PAYING RANSOM BY BITCOIN ENABLES FUNDS TO BE TRANSFERRED WITHOUT AN OPTION TO DISPUTE OR CANCEL THE TRANSACTION AT A LATER DATE

These advantages, and the resulting revenues, have driven the popularity of ransomware in recent months as can be seen in the chart below based upon Check Point research data.

Figure 1. Growth of Ransomware Attacks, November 2015 – March 2016



EVOLVING TARGETS: FROM CONSUMER TO ENTERPRISE

Individuals

On the surface, attacking individual users may not appear to be lucrative, especially if you are only looking at a single instance. Attackers targeting individuals tend to keep their ransom relatively low, hoping to entice victims to pay up quickly, rather than trying to thwart the attack. The payout for a single attack may range from a hundred to one thousand dollars (although in practice, payment is now typically in Bitcoin). But for the attacker, this is a game of numbers, with most attacks broadcast to multiple prospective victims, and with each win encouraging them to play on. Rather than catching a single victim, an attacker can easily cast a broad net to lure dozens of targets using the same phishing scams or malicious web content. Even if only a few take the bait, the return vs. effort remains fairly low.

In addition, individual computer users remain a fairly compliant target. Few individuals have IT resources at their disposal to combat a ransomware attack. They are less likely to have up-to-date protections, and often will not have recent backups to restore from. When attacked, rather than risking losing family photographs, entire music libraries, and other valuable personal documents, individuals are likely to pay the ransom as long as it is set at a reasonable level.

Business Targets

Ransomware has predominantly targeted private users in the past.[1] Recently, several factors have driven attackers to shift their focus, targeting larger organizations across a broader range of business sectors. Victims include Police departments, nonprofit organizations, schools, universities and hospitals. Businesses have proven to be a lucrative target for extorters for several reasons. First, they are more dependent than individuals upon data to operate. This provides greater incentive for them to pay ransom. Second, corporations typically have deeper pockets than individuals. Attackers can target fewer victims and extort larger sums of money.

> “BUSINESSES HAVE PROVEN TO BE A LUCRATIVE TARGET FOR EXTORTERS, AS THEY HAVE A GREATER INCENTIVE TO PAY RANSOM DEMANDS.”

Organizations that are highly distributed, highly mobile, or have remote employees are especially vulnerable to ransomware attacks. Organizations with multiple locations will find it difficult to maintain consistent training, policy, and procedures across their different locations. Remote sites and smaller sites may not have local IT or security resources to assist users with recovery. As the number of employees, quantity of facilities, and diversity of locations grow, the challenge multiplies.

IMPACT OF SOCIAL ENGINEERING

Social engineering represents an increasingly popular path into the organization, improving the likelihood an attack will be successful. It is relatively easy for an attacker to conduct basic research into a target company, and then deceive an employee using a phishing email that spoofs an entity known to the victim. Perhaps the victim receives an email that looks to be an order from a customer, or an invoice from a supplier. The recipient innocently clicks, and unwittingly opens a file containing the payload that installs and activates the ransomware. Combining social engineering with malware embedded in seemingly safe document formats, attackers have been able to convince even sophisticated security professionals to open malicious attachments.

[1] http://blog.checkpoint.com/2015/06/01/troldesh-new-ransomware-from-russia/

AN ELUSIVE THREAT

One of the reasons ransomware is getting past the defenses of many organizations is that attackers have upgraded different aspects of ransomware to make it much more evasive. Traditional security products, such as antivirus and other signature-based protections, are fundamentally backwards-looking – they detect either previously seen malware or specific behaviors seen in previous attacks. Ransomware has found various methods to avoid detection and successfully infect computers.

One of these methods is to embed ransomware inside slightly different versions of common documents, such as Word, Excel, PDF — but by changing the content it is packaged with the attachment no longer matches known hashes. A recent example using this technique is the Locky ransomware.[2] By packaging unique documents with ransomware in macro commands, each email attachment is slightly different, and therefore is not detected by traditional signature-based protections. To convince users to enable the macro commands, ransomware applies social engineering techniques. These ploys can be extremely deceiving, fooling even the most cautious users. Social engineering is a low tech attack vector with an alarmingly high success rate in bypassing traditional AV defenses.[3] Once the macro command is enabled, it fetches the malware executable from the hacker's drop-zone and launches it.[4] The ransomware is activated and encrypts as many files it can reach.

Modern ransomware is capable of reaching beyond an individual user's system, damaging large portions of an organization's data through a single infection. Malware can achieve broader impact by encrypting content available to a given system throughout the network. The infamous CryptoLocker ransomware, for example, tries to access all of the network drives it can find and encrypt them.[5] In addition, certain types of ransomware, such as the CTB Locker, specifically target websites. Since businesses are more likely to have a web presence, this method of operation puts mostly businesses and not private users at risk.[6]

STRATEGIES TO FIGHT RANSOMWARE

Preventative Measures

In the war against ransomware, there are a number of things you can do to prevent becoming a victim. Following these best practices can be a critical component in avoiding ransomware attacks and can help minimize the damage caused by a successful ransomware campaign against your organization.

Consistently back up your important files, preferably using air-gapped storage.[7] If possible, enable automatic backups for your employees so you are not relying on users to remember to follow through with their backups. In the event of a ransomware attack, it may be possible to use these backups in lieu of paying ransom, or at least allow you to decide for yourself whether the cost of restoring from backups is more or less than the requested ransom.

Employee education has been a key element in avoiding malware infections, and also applies to ransomware. The basics of considering where files came from, and whether or not they can trust the sender continue to be worthy of reminding users.[8]

In addition, ensuring that users only have access to the information and resources required to execute their jobs significantly reduces the possibility of lateral movement of a ransomware attack, and will minimize the potential impact of a successful attack on your organization. While addressing a ransomware attack on one user host may be a hassle, the potential implications of a network-wide attack can be dramatically greater.

FIGHTING RANSOMWARE
Preventative Measures

- ✓ *Back up your data and enable automatic backups*
- ✓ *Educate employees to recognize potential threats*
- ✓ *Limit Access to Prevent Lateral Movement*
- ✓ *Keep AV and other signature-based protections up-to-date*
- ✓ *Implement advanced threat extraction and sandboxing technologies*

---

[2] http://blog.checkpoint.com/2016/03/02/locky-ransomware/, http://arstechnica.com/security/2016/02/locky-crypto-ransomware-rides-in-on-malicious-word-document-macro/
[3] https://medium.com/@networksecurity/it-s-time-to-secure-microsoft-office-be50ec2797e3#.9y7xkrheq
[4] http://thehackernews.com/2016/02/locky-ransomware-decrypt.html
[5] http://krebsonsecurity.com/2013/11/how-to-avoid-cryptolocker-ransomware/
[6] http://www.pcworld.com/article/3038207/security/ctb-locker-ransomware-hits-over-100-websites.html
[7] http://blog.checkpoint.com/2015/08/17/what-you-can-and-cant-do-against-ransomware/
[8] http://blog.checkpoint.com/2015/08/17/what-you-can-and-cant-do-against-ransomware/

Moving to the role of Information Security in preventing attacks, it is certainly beneficial to keep antivirus and other signature-based protections are in place and kept up-to-date. But keep in mind that signature-based protections alone are not sufficient to detect and prevent sophisticated ransomware attacks designed to evade traditional protections. A multi-layered approach provides the best opportunity to fend off ransomware and the damage it could cause. Two key components in a multi-layered approach are threat extraction (file sanitization) and advanced sandboxing. Each element provides distinct protection, that when used together, offer a comprehensive solution for protection at the network level, and directly on endpoint devices.

Documents containing embedded macros or exploits serve as an effective means of triggering initial infection. The best way to prevent infection in this manner is to filter malicious content out of documents using Threat Extraction. By stripping them of all active elements, organizations can neutralize attacks by promptly delivering a clean, sanitized document that minimizes risk to users. And, unlike humans, Threat Extraction is completely immune to social engineering.

Advanced sandboxing (threat emulation) provides a second element in a multi-layered security approach. It works in parallel with threat extraction to protect against unknown malware and zero-day attacks. Unlike antivirus and other solutions, it is not signature based. The Advanced sandboxing in Check Point SandBlast analyzes a file's behavior using several indicators, including dynamic analysis. In addition it uses unique evasion resistant CPU-level detection, to detect and block the most complex malware in the exploit phase before it even has a chance to deploy.

In addition to providing strong network protection, endpoint devices must be protected against attacks outside the perimeter of network defenses. Users working remotely, outside the protection of the corporate gateways, contractors connecting external devices to the corporate network, and removable storage devices containing malware unbeknownst to the owner, all represent leverage points for an adept attacker. SandBlast Agent extends advanced zero-day protection to endpoint devices to protect against unknown malware and advanced threats.

Response after Infection

While preventing ransomware is the ideal scenario, knowing what to do in the event of a ransomware attack, and implementing tools capable of identifying an incident and containing ransomware infections can mean the difference between losing one computer and a more extensive infection.

If you are prepared for attacks through unprotected channels, detecting the ransomware within your network and blocking any communication between the ransomware and its command & control server using Anti-Bot technology will limit, and possibly block, its ability to operate. Many (but not all) types of ransomware cannot encrypt files without first retrieving an encryption key from a control server.[9] Quarantining malicious processes and communications rapidly and effectively can contain and possibly remediate the threat.

Even if the ransomware manages to encrypt files on the infected device, Anti-Bot technology can automatically lock down the infected device preventing spread to network storage or other systems. This can dramatically reduce the damage caused by the ransomware and limit the subsequent business impact.

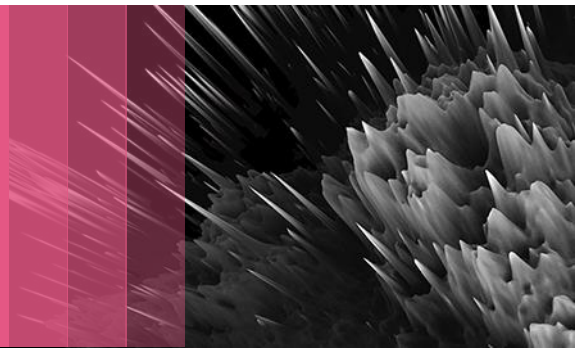
FIGHTING RANSOMWARE
Post-Infection Measures

- ✓ *Prevent ransomware communication with bot detection and blocking*
- ✓ *Quickly contain ransomware infections to minimize business impact*
- ✓ *Utilize forensics data to fully disinfect the attack and avoid further damage*

[9] http://blog.checkpoint.com/2013/11/14/defeating-cryptolocker-with-threatcloud-and-gateway-threat-prevention/

Once you have managed to contain the ransomware, it is important to treat the whole infection and remediate the attack. Attacks must be dealt with as a whole, and protections must be implemented to keep it from reoccurring elsewhere. To succeed, the incident response team (IRT) needs to analyze all aspects of the attack, from point of entry and path of travel, to scope of damage. Implementing and using automated forensic analysis tools greatly improves the ability of the IRT to understand how attacks infiltrated their networks in the first place. Automatic forensic analysis provides a comprehensive attack view, and provides guidance for remediation. These tools dramatically reduce the time for event analysis, taking what was previously an endeavor that took hours or days, and reducing it to minutes, enabling the information security staff to understand and respond to an attack much more efficiently and effectively.

THE BOTTOM LINE



IT'S NO LONGER AN OPTION

Ransomware is on the rise. While many organizations have protected their files, data, and systems by implementing antivirus software and other signature-based solutions, these methods, while essential, are defenseless against advanced ransomware attacks designed to evade detection by traditional methods. Organizations need to implement a multi-layered approach to security to address the challenges of modern ransomware and effectively protect their network and endpoint devices.

This approach must be comprehensive, including both preventative measures and efficient response and remediation tools. The advanced sandboxing capabilities in SandBlast Zero-Day Protection combine both traditional OS-level and CPU-level detection to proactively protect your valuable assets from zero-day and advanced persistent threats. At the same time, SandBlast Threat Extraction capabilities filter potentially malicious elements out of documents, promptly delivering sanitized content that minimizes risk to users. These tools, coupled with traditional signature-based prevention, are critical elements in defending organizations against ransomware attacks.

Protection cannot be limited to the network. Providing an equivalent level of protection to endpoint devices is a critical component to ensuing comprehensive security coverage. SandBlast Agent extends the defenses of SandBlast Zero-Day protection to defend endpoint devices against unknown malware, and advanced zero-day threats.

While prevention is critical, organizations must also implement tools that enable them to understand, respond to, and limit the scope of an attack. Anti-Bot, both at the network level and on endpoints themselves to protect while roaming, enables organizations to rapidly detect ransomware within your network and block any communication between the ransomware and its command & control server before it can cause additional damage. This can be leveraged to quarantine malicious process and communications, and lock down infected devices to limit the potential impact of the ransomware attack. After the attack, IT teams need to utilize the most advanced automated forensic analysis tools to understand the full attack plane and remediate appropriately, quickly and effectively.

To learn more about threat prevention and how SandBlast Zero-Day Protection and SandBlast Agent can help protect your company against ransomware, please visit our website at www.checkpoint.com/sandblast.

> "ANTIVIRUS AND OTHER SIGNATURE-BASED SOLUTIONS, WHILE ESSENTIAL ARE DEFENSLESS AGAINST ADVANCED RANSOMWARE"

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

July 2016