REPORT

The 2016 NopSec State of Ransomware Report

The Threat, The Impact, and Mitigation Strategies

NOPSEC

INTRODUCTION

One of the biggest digital security threats that businesses, governments, and consumers all face is Ransomware. What makes Ransomware especially risk-prone is its capacity to inflict extensive damage in an incredibly short space of time, and how difficult to remediate an infection.

The cost of ransomware on businesses – not just in financial terms, but also with respect to lost productivity and potential loss of critical data – is significant. This report will examine the current state of Ransomware. It will explore the strategies employed by different variants to infect machines and extort money, and will shine light on the industries that are most frequently targeted by it.

Finally, it will conclude with strategies for mitigation and damage control. When applied, these can help reduce the impact of a ransomware attack, or prevent it altogether.

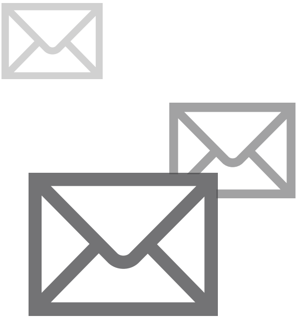
In addition to general information security managers and directors, this report will be of use to anyone in a Chief Information Officer (CIO), Chief Information Security Officer (CISO), or Chief Technology Officer (CTO) role, as well as anyone curious about the current state of ransomware.

OVERVIEW

What Is Ransomware

Ransomware is a type of malware that deliberately interferes with the standard operation of a computer until a ransom is paid.

The earliest examples would simply lock the computer's screen and prevent programs and files from being opened, until a ransom was paid. While these were immensely disruptive, it was possible to recover files by booting the system into an unaffected live CD, and then copying them onto an unaffected storage medium.



In recent years, ransomware has taken a more malevolent turn, with the rise of crypto-ransomware.

This form systematically encrypts files that are stored locally, or are on accessible network file shares, using strong cryptographic algorithms. The ransomware determines what files to encrypt by their file type, with office documents - .docx, .xlsx. pptx and media (photographs and video files) – almost always being targeted.

Once the files have been encrypted, the ransomware will typically upload the private key to a remote server, and then delete the local copy. The victim will then see a demand for payment. This must be paid in order to get the files back.

Often there is a time limit. If the user fails to pay before the clock runs out, the remote server will delete the private key, rendering the files permanently irretrievable.

How ransomware spreads

Ransomware is propagated in a variety of ways. Perhaps the most widely used method is through spam networks.

Ransomware is propagated in a variety of ways. Perhaps the most widely used method is through spam networks.

The Locky variant, for example, is typically spread through emails that contain fake invoices. When opened, the document will ask the user to allow macros. When the user enables them, it will start to encrypt files using strong AES encryption.

There have been multiple examples of ransomware infecting systems by piggybacking off other legitimate applications. The OS X ransomware KeRanger is a well-documented example of this. In March, 2016, an unknown actor managed to surreptitiously include this piece of malware in an update for Transmission - a highly popular bittorrent client..

Paying the Ransom

Payment of a ransom is typically done in one of two ways: Either through a cryptocurrency, like Bitcoin or LiteCoin, or less commonly through a prepaid debit card or gift card.

By far, the most frequent payment method is Bitcoin, which by design includes a number of features that are advantageous to someone working outside the law.

Bitcoin affords the attacker near-total anonymity. Although transactions are permanently recorded on a public ledger called "the blockchain", it is trivial to obfuscate the origins of a payment. Moreover, Bitcoin offers almost instantaneous transfers, and its increasing prominence as a payment method has resulted in the creation of a number of services that make it easy for a non-technical user to purchase and send bitcoins.

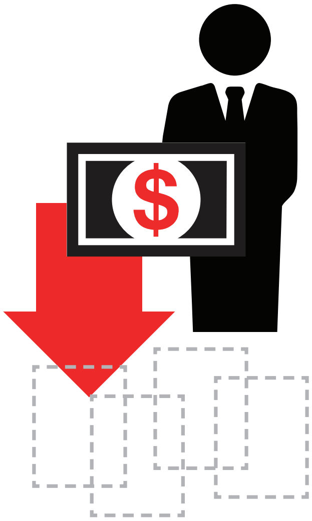
Pre-paid debit cards, like GreenDot's MoneyPak, are also frequently employed by ransomware distributors. One of the most notorious examples of crypto-ransomware, CryptoLocker, accepted payment via this method.

A less common payment method is through gift cards, especially those for Amazon and iTunes. An attacker can exchange these for physical products, music and apps, or resell them to others at a discount.

Interestingly, one ransomware variant identified by Trend Micro in 2011, called TROJ_RANSOM.QOWA, required users to pay a ransom by dialing a premium-rate phone number.

The amount demanded by ransomware differs between variants. CryptoLocker, for example, demanded $300 USD or 300 EUR. Others have demanded significantly more.

It should also be emphasized that payment of a ransom does not necessarily guarantee the safe return of encrypted files.



Payment of a ransom does not necessarily guarantee the safe return of encrypted files.

The business of ransomware

While the payment of ransom may not guarantee the safe return of encrypted files, in most cases, criminals understand that much like a traditional business, reputation is important. In order to maintain credibility in the marketplace and continue to reap rewards, it is in their interest to restore files upon receipt of payment.

In that regard, most ransomware comes with detailed information for victims on how to setup a Bitcoin wallet and make the transfer.

From a business perspective, ransomware is particularly shrewd. The model takes into consideration that stealing data and trying to find a buyer is a risky proposition. It is also time-consuming and has potentially lower returns. By encrypting data, no significant data transfer needs to occur and the victim becomes the buyer.

Some cyber-criminals have gone upstream and provide ransomware tools and services for others to use. For example, the Tox toolkit, was free for hackers to download and distribute. Tox would be provided free of charge and in return would take a 20% cut of all ransom generated.

CURRENT STATISTICS

Given the damage a ransomware infection can potentially cause, the statistics regarding the proliferation of such attacks make a sobering read.

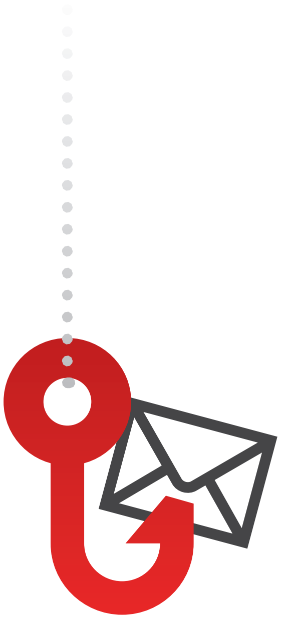
Some of the most startling research comes from the 2015 McAfee Threat Report. This states that during the first quarter of 2015, there were 725,000 ransomware samples collected by their researchers. Contrast that to the previous year, where in the same period only 260,000 malware samples were collected. This represents a year-on-year increase of a staggering 165%.

Individual samples don't necessarily translate into infected computers, however. One company that attempted to gauge the damage inflicted by ransomware was Norton. In its 2015 Ransomware On The Rise report, it identified 68,000 computers that were infected during one calendar month. This equates to an average of 5,700 per day.

It's worth noting that ransomware often intersects with other security threats. According to PhishMe, 93% of all phishing attacks are accompanied with ransomware.

Ransomware represents a significant headache for those tasked with securing essential government computer systems. In a 2015 testimony, the US Department for Homeland Security (DHS) reported that there had been 321 different recorded instances of ransomware-related activity affecting 29 different federal agency networks between June and December 2015.

While this might not sound like a lot, it's worth noting the limited timeframe. It's also worth emphasizing that the statistics only pertain to federal computers, and not those owned and controlled by state or local governments.



93% of all phishing attacks are accompanied with ransomware.

RANSOMWARE VARIANTS

Ransomware isn't homogenous. Amongst crypto-ransomware, there's an incredible diversity of specimens, each differing in how they infect systems, distribute themselves, and the amount they demand in ransom.

Competence isn't always a given. There has also been a spate of homegrown ransomware which has used weak encryption, or in some cases failed to encrypt the files correctly. However, even those seem to have a degree of success in extracting ransoms.

Some of the more sophisticated and notorious examples of ransomware are described below:

CryptoLocker

Perhaps the most widely known crypto-ransomware is CryptoLocker. This emerged at the end of 2013, and in a short amount of time, it managed to infect 500,000 machines. So significant was its impact, CryptoLocker almost became a by-word for ransomware in general, in the way that Google is a byword for online searching.

What's unique about CryptoLocker is how lucrative it was for its operators. By some estimations, it managed to extort $3 million before its command-and-controls were shut down in 2014 by a coalition of police forces based in Europe, North America, South Africa, Australia, and New Zealand.

In 2014, two security firms that were involved in the dismantling of the CryptoLocker network – Fox-IT and FireEye – created a service called Decrypt Cryptolocker, which allowed victims to find the key required to unlock their files

CryptoWall

Following CryptoLocker, the second most notorious ransomware variant is CryptoWall. This threat emerged at the start of 2014. Since then, a number of variants have been released, including : CryptorBit, CryptoDefense, CryptoWall 2.0, CryptoWall 3.0, and more recently CryptoWall 4.0.

The fourth iteration of CryptoWall comes with a number of novel features that make it a potent threat. In addition to improved stealth features, which make it harder to be detected by an antivirus or firewall system, CryptoWall 4.0 also alters file names in order to obfuscate what has been encrypted.

TorrentLocker

At first glances, TorrentLocker is a conventional strain of crypto-ransomware. Infections are almost always initiated by a spam email which contains an infected office document. TorrentLocker then systematically uses AES to encrypt a wide variety of file-types, and then demands a ransom in bitcoin.

But there are a number of key differences that separate TorrentLocker from the other strains of crypto-ransomware.

Firstly, it propagates itself by hijacking the victim's address book and sending out further emails. Furthermore, TorrentLocker expertly uses regionalization in order to more effectively extract ransoms from victims.

The sum demanded will be displayed in the victim's local currency. If that person is in Australia, then it will be displayed in Australian dollars. If the victim is located in the Eurozone, the price will be in euros. It will even list bitcoin exchanges that are located in the victim's country.

Some variants even activated the victim's webcam, in order to create the impression that the victim is under surveillance.

Police Ransomware

Prior to crypto-ransomware becoming the dominant strain, there was police ransomware. This operated under the same principles of crypto-ransomware, where it rendered a computer inoperable until a ransom had been paid.

Dating back to early 2012, the Reveton ransomware is a well-known example of this. Like TorrentLocker, Reveton used localization to increase its efficacy. Once infected, it would present as a message from local law enforcement, and accuse the victim of having been involved in some variety of computer crime.

According to Sophos, Reveton would present itself as being from the FBI, and the police forces of Belgium, Canada, Finland, Greece, Sweden, The UK, and more, depending on where the victim was based.

In order to pressure victims to pay up, Reveton would threaten criminal charges against the user if they did not pay the "fine" within a certain time period – typically 72 hours. It would also display the user's' IP address. Some variants even activated the victim's webcam, in order to create the impression that the victim is under surveillance.

INDUSTRIES AFFECTED

The impact of ransomware can be devastating, however the impact can vary greatly depending upon the industry that it targets.

Healthcare

A sector which has proven to be an enticing target for ransomware operators is healthcare. According to research by Healthcare IT News and HIMSS Analytics, more than half of all hospitals in the United States fell victim to ransomware over a twelve-month period between 2015 and 2016, with another 25 percent saying they were unsure whether an infection had taken place or not.

When ransomware strikes, the costs can be significant. In 2015, the Hollywood Presbyterian Medical Center was hit by a wave of ransomware attacks which caused its President and CEO to declare an "internal emergency."

The ransomware disabled computer systems, including those required to process lab work, pharmacy requests, and CT scans. Departments were paralyzed, and the hospital was forced to call in the support of the Los Angeles Police Department and the FBI.

Ultimately, Hollywood Presbyterian paid a ransom of forty bitcoins, which at the time was roughly equivalent to $17,000.

Not all hospitals appear to be willing to do that. According to the aforementioned survey, only 4.9% of respondents said that they would be prepared to pay a ransom in order to recover patient data. 50.8% of respondents were adamant they would not pay, while 44.3% were unsure.

Perhaps as a consequence of the increasing numbers of hospitals being affected, almost seventy-three percent of hospitals have a business continuity plan that addresses ransomware.

Ransomware presents a risk to organizations using cloud strorage services.

Software as a Service (SaaS)

Cloud storage systems like Google Drive, Office 365 One Drive for Business, and Dropbox have found popularity as a quick and convenient way to share files across an organization. But ransomware also presents a risk to organizations using these services.

If a machine is infected, in addition to impacting any files stored locally, the ransomware will also encrypt any files that are set to synchronize with these services. This means that files which are used across teams and departments will be rendered inaccessible, even to those machines which have not yet been infected.

Financial Services

Ransomware presents a significant risk to financial services organizations. In addition to the cost of resolving an infection, and the lost productivity, there is also a risk of data exfiltration. While, due to the sensitive and competitive nature of financial services, there has not been the same amount of disclosure as in healthcare, ransomware is regarded as a significant risk.

According to Unit 42 – the Palo Alto Networks threat intelligence team – Cryptowall was in the top three threats to the financial services industry in both 2014 and 2015. Palo Alto Networks is also aware of a case from 2014 where a US-based brokerage house fell victim to CryptoWall.

Industry bodies have also sat up and paid attention to the threat presented by ransomware. The Federal Financial Institutions Council (FFIEC) and Financial Services Sector Coordinating Council (FSSCC) have separately issued alerts about cyber-extortion and destructive malware.

Law Enforcement

It's bitterly ironic that one of the sectors that has been most frequently impacted by ransomware is also one that is frequently impersonated by ransomware. There have been a number of incidents where police departments have been infected with ransomware, and having had to pay a ransom.

On February, 2016, Melrose Police Department in Massachusetts fell victim to ransomware which was triggered by a malicious attachment. The attack encrypted a number of vital documents. It also prevented officers from accessing a program called TriTech, which is used for computer-aided dispatch, incident logging, and record management during patrols.

Two days later, the police department paid the ransom of one bitcoin in order to regain access.

In April, 2015, the Tewksbury Police Department, also in Massachusetts, fell victim to a crypto-ransomware. In addition to encrypting local files, the unspecified malware also corrupted the most recent backup. The only remaining backup that hadn't been damaged was eighteen months old.

In order to restore normal function, they had to pay a ransom of $500.

Other law enforcement departments that have fallen victim to ransomware include the Lincoln County Sheriff's department in Maine, who had to pay $318 and the Midlothian Police Department in Illinois, who had to pay $500.

Small Businesses

The indiscriminate nature of ransomware means that small businesses, sole traders, and even consumers aren't safe from the dangers it poses. Smaller businesses often have limited resources to identify or prevent ransomware, and seldom have backups from which they can recover.

Human error is responsible for almost 95% of all security incidents – not just ransomware.

THE HUMAN ELEMENT OF RANSOMWARE

It's easy to focus on the technical aspects of ransomware. There are hundreds of thousands of strains, which each differ in some way. Quite often, these changes are simply cosmetic. As ransomware code is sold from criminal gang to criminal gang, it is tweaked slightly. The ransom letter may be translated or adapted in order to better target a particular demographic.

Sometimes the changes are more significant, include a new approach to propagation, persistence, obfuscation, or infection. With this, it's easy to forget there's a human element to ransomware, which makes it a problem that is hard to solve with technology alone.

According to the IBM Security Services 2014 Cyber Security Intelligence Index, human error is responsible for almost 95% of all security incidents – not just ransomware.

It was reported that the two examples of police departments being felled with ransomware was a consequence of an employee opening an infected email attachment. Spam emails are a common attack vector for ransomware, and many of these emails are crafted to be believable, and to look genuine.

When reporting about TorrentLocker, Sophos remarked that the spam messages used to distribute it showed a "higher degree of grammatical correctness than typical malicious spam campaigns, with few if any spelling mistakes". Sophos suggested that they were most likely written by a native speaker. This is a significant diversion from the language used in other spam emails - especially those of the 419 variant.

Furthermore, the spam messages used to distribute ransomware often adopt the marques and stylings of established and trusted brands, such as Royal Mail, the IRS, and the Australian Tax Office. The aim is to disguise the malicious intent of email until after the user has been infected.

Ransomware developers are aware of the importance of the human element, and use this knowledge to more effectively extract payment.

Others use localization to great effect. In order to create a veneer of believability, the Reveton Police Ransomware presents itself as being from the victim's local law enforcement.

TorrentLocker, on the other hand, converts the ransom demanded into the equivalent in local currency, and lists local bitcoin exchanges based in the user's country.

In the case of TorrentLocker, the operators even refused to push the ransomware executable to machines located in countries that they weren't targeting.

RECOMMENDATIONS

While there is no silver bullet to prevent ransomware infections, there are strategies that can be followed in order to reduce the risk of an infection.

Given the most common attack vector for ransomware is through infected documents sent via email attachments, the most effective strategies will focus on these.

1. **Disable Macros:** The most important step you can take is to disable macros. Thankfully, these do not run by default. This is a security feature that has been present in Microsoft Office for some time.

   However, some ransomware variants are actually able to trick users into enabling macros. Fortunately, in Microsoft Office 2016, there is a policy option that allows an administrator to disallow Word from enabling macros on office files downloaded from the internet. This policy is named: "Block macros from running in Office files from the internet.".

2. **Install Viewers:** If your organization is yet to migrate to Office 2016, it is recommended that Microsoft Office Viewers are installed. These allow a user to view a document without having to enable macros.

3. **User Awareness:** Training efforts should be made in order to educate users on the threats posed to ransomware, and the risks associated with opening email attachments from unrecognized senders.

4. **Least Privilege:** In order to prevent ransomware from infecting a system, it's sensible to set account permissions to the lowest possible setting. Furthermore, as ransomware often takes advantage of security vulnerabilities in Microsoft Office and other applications, it's important to ensure that all systems are regularly patched and updated, and are kept current. In this case, having a well-oiled vulnerability management practice within the organization is vital.

5. **Backup:** Above all, ensure that all files are backed up and versioned. As the Tewksbury Police Department learned, these backups should be kept off-site, and away from the reach of a ransomware infection.

TOOLS TO PREVENT RANSOMWARE

In addition to the above tools and strategies, there are a number of tools which can be deployed in order to prevent, or reduce the impact of a ransomware infection.

Ransomware comes in different guises, operating in different ways. As such, a single point product is rarely sufficient in preventing it. Rather a set of tools are required to combat these threats.

A unified approach

A unified approach is the most efficient and comprehensive way to prevent ransomware from infecting and spreading within your environment. NopSec Unified VRM reduces the risk of an infection occurring as a result of a lapse in procedure in the security team, by automating many of the manual tasks involved with vulnerability risk management.

The Unified VRM Security Configuration tool lets an administrator or security professional assess the security of an operating system by comparing it against industry-standard or compliance checklists. Meanwhile the Unified VRM Network can scan a network to see how well prepared it is to face an external, internet-based threat.

Tying this all together is the NopSec Unified VRM, which comes with a centralized reporting system, and allows management to control all aspects of the incident response process.

Penetration testing will identify the holes that could potentially allow a ransomware infection, allowing IT and security personnel to quickly remediate them

Social Engineering

Social engineering testing is an effective tool to compliment user awareness. Helping expose human flaws in processes that can subsequently be addressed. When considering engaging a social engineering exercise, it is important to bear in mind the objective is not to shame employees. Rather to help identify where processes can be improved.

NopSec recommends and takes a four-phase approach. The first phase is planning, which establishes the scope and aims of the test, as well as any escalation paths. The second phase is an assessment, which is then followed by examining how effectively any vulnerabilities could be exploited, and how easy it is to infiltrate any captured data.

The final phase sees a written report being created, which details what vulnerabilities were found, and any remediation strategies. There is also a cleanup process, which will see any gathered artifacts destroyed.

Penetration testing

In order to see a bigger picture of how secure your organization is, penetration testing can simulate attacks against internet-facing web applications and external networks, as well as internal networks.

When employed, these will identify the holes that could potentially allow a ransomware infection, allowing IT and security personnel to quickly remediate them.

Detection

In the event that prevention controls fail or are bypassed. Detection controls on both the network and host can help quickly identify when ransomware has infected your organisation so that you can take the appropriate remedial steps. A SIEM can be effective in correlating logs from disparate systems and alerting on particular events.

Threat Intelligence

The use of paid, open, vendor-provided, and peer-driven threat intelligence can keep you up to date with the latest ransomware threats and their evolution. Knowing the attack paths, command and control servers, and encryption methods can help you quickly identify and prevent ransomware from spreading through your network.

CONCLUSION

What makes ransomware so effective is that it is simultaneously static and fluid. On one hand, every single piece works from the same general playbook. It's an effective playbook, and has reaped millions for distributors and operators.

On the other hand, ransomware constantly shifts its approach to be more effective in infecting machines. The installation and infection mechanism changes from strain to strain, generation to generation.

Above all, ransomware doesn't discriminate. No matter what industry or vertical, everyone is at risk.

As we have gained a better understanding of how ransomware works, mitigation strategies have emerged. On the human level, this involves training employees to identify potentially malicious emails, and making them aware of the risk of opening suspicious email attachments.

Beyond that, there is the technical aspect of risk. Ensuring that systems are patched and up-to-date; having an assurance strategy, so that you know your systems are secure; ensuring that regular versioned backups are made, and that these are kept off-site, and are isolated from any potential infection.

Above all, to protect against ransomware, enterprises have to ensure they have an ongoing strategy to deal emerging threats.

ABOUT NOPSEC

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.

NOPSEC

For additional information or to schedule a demo, visit www.nopsec.com or email info@nopsec.com.