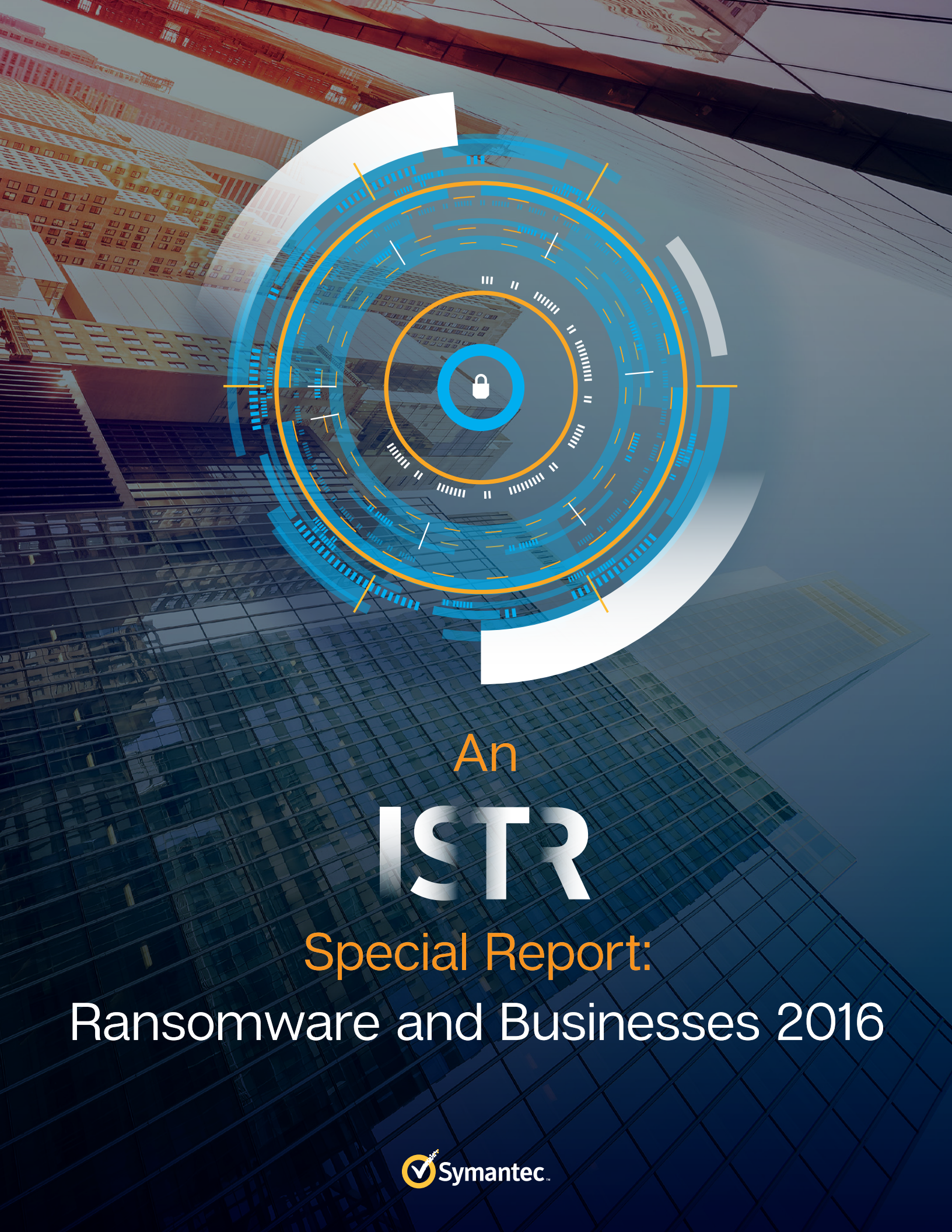


An

ISTR

Special Report:

Ransomware and Businesses 2016

Symantec

CONTENTS

CHARTS & TABLES

EXECUTIVE SUMMARY

Ransomware has quickly emerged as one of the most dangerous cyberthreats facing both organizations and consumers, with global losses now likely running to hundreds of millions of dollars.

The past 12 months have seen ransomware reach a new level of maturity and menace. Major ransomware gangs are capable of pushing their malware to millions of computers. Users who are hit with ransomware find their valuable data locked with strong, often unbreakable encryption.

The perfection of the ransomware business model has created a gold-rush mentality among attackers, as growing numbers seek to cash in. Infection numbers are trending upwards, with the number of new ransomware families discovered annually reaching an all-time high of 100 in 2015. Today, the average ransom demanded by attackers has jumped to US$679.

Attacks against organizations are slowly increasing. While wide-scale, indiscriminate ransomware campaigns remain the most prevalent form of threat, new and more advanced attacks are emerging. A growing number of gangs are beginning to focus on targeted attacks against large organizations. As demonstrated by the two case studies in this report, these attacks involve a high level of technical expertise, using techniques more commonly seen in cyberespionage campaigns to break into and traverse the target's network.

Although more complex and time-consuming to perform, a successful targeted attack on an organization can potentially infect thousands of computers, causing massive operational disruption and serious damage to revenues and reputation. Once cybercrime gangs see some businesses succumb to these attacks and pay the ransom, more attackers will follow suit in a bid to grab their share of the potential profits.

Organizations need to be fully aware of the threat posed by ransomware and make building their defenses an ongoing priority. While a multilayered approach to security minimizes the chance of infection, it's also vital to educate end users about ransomware and encourage them to adopt best practices. As ransomware gangs continue to refine their tactics, organizations cannot become complacent. Businesses should continue to review and improve their security in the face of this rapidly evolving threat.

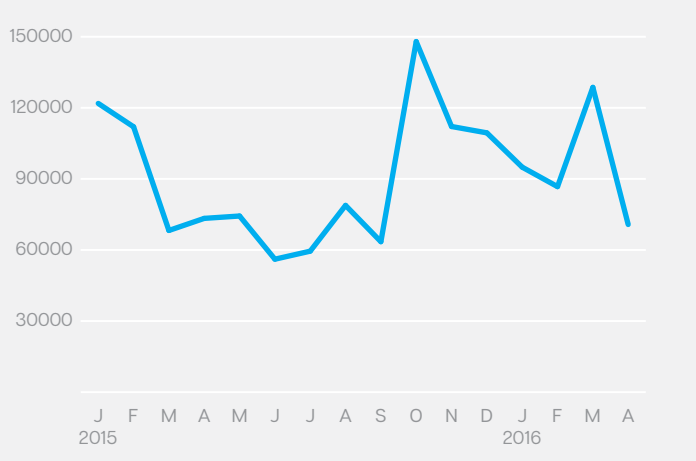
KEY FINDINGS

- While ransomware attacks to date have been largely indiscriminate, there is evidence that attackers have a growing interest in hitting businesses with targeted attacks.
- A number of ransomware groups have begun using advanced attack techniques, displaying a level of expertise similar to that seen in many cyberespionage attacks.
- The Services sector, with 38 percent of organizational infections, was by far the most affected business sector. Manufacturing, with 17 percent of infections, along with Finance, Insurance and Real Estate, and Public Administration (both on 10 percent) also figured highly.
- The average ransom demand has more than doubled and is now $679, up from $294 at the end of 2015.
- The number of new ransomware families discovered has been steadily increasing since 2011. Last year was a record high, with 100 new families discovered.
- The advent of ransomware-as-a-service (RaaS) means a larger number of cybercriminals can acquire their own ransomware, including those with relatively low levels of expertise.
- The shift towards crypto-ransomware has continued. All bar one of the new variants discovered so far in 2016 are crypto-ransomware, compared to around 80 percent last year.
- Between January 2015 and April 2016, the US was the region most affected by ransomware, with 28 percent of global infections. Canada, Australia, India, Japan, Italy, the UK, Germany, the Netherlands, and Malaysia round out the top 10. Around 43 percent of ransomware victims were employees in organizations.

RANSOMWARE OVERVIEW

After dipping in the first quarter of 2015, overall ransomware infection numbers began to climb in the fourth quater, spiking in October and November 2015, and again in March 2016. The Infection spike in March 2016 coincided with the arrival of the virulent Locky ransomware (Trojan.Cryptolocker.AF).

Figure 1. Overall Ransomware Infections by Month from January 2015 to April 2016



The Rise of Crypto-Ransomware

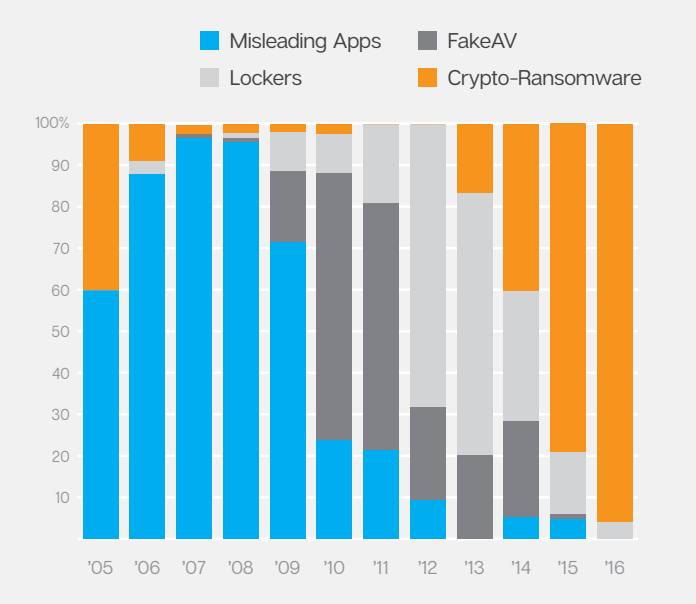
A pronounced trend in recent years has been the shift towards crypto-ransomware. In our last ransomware whitepaper, we noted that the proportion of new variants classified as crypto-ransomware was growing year-on-year. That trend has continued into 2016 and, so far this year, all bar one of the new ransomware families documented by Symantec are crypto-ransomware.

Seven to ten years ago, the market was dominated with misleading applications, many of which were designed to pose as antivirus software. These risks informed users that something was wrong with their computer, such as a malware infection or software fault. The attackers then requested payment to "fix" the problem.

Locker-type threats later eclipsed fake antivirus apps. Lockers block access to an infected device but don't encrypt or delete any files. If the malware is removed, full access to the device is usually restored. After enjoying a brief heyday in 2012 and 2013, lockers have steadily declined, with crypto-ransomware taking over.

The shift towards crypto-ransomware can be explained by the fact that it is usually the most effective form of ransomware. If implemented correctly, crypto-ransomware will use unbreakable encryption on the user's files. Removing the malware will not solve the problem; the user will still be left with inaccessible files. If the victim has no backups of these files, then paying the ransom may be the only way to recover them. The crypto-ransomware business model has been perfected over the past two years and it's hardly surprising that it is now dominating the scene.

Figure 2. Percentage of New Families of Misleading Apps, Fake AV, Locker Ransomware, and Crypto-Ransomware Identified Between 2005 and June 2016

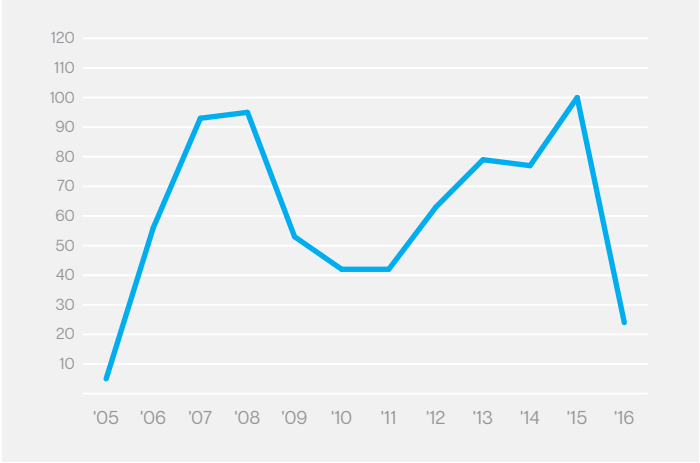


Record Number of New Ransomware Families

The success of crypto-ransomware in recent years has prompted a surge in the number of new ransomware families being created. 2015 was a record year for ransomware, with Symantec logging 100 new ransomware families, the highest to date.

A growing number of cybercrime groups appear to be attempting to capitalize on ransomware. It is now also easier than ever to create your own ransomware with ransomware creation kits, or ransomware-as-a-service (RaaS), now emerging on the cybercrime underground.

Figure 3. New Ransomware Families Discovered by Year (2016 Figure Records New Families Discovered up to End of April)

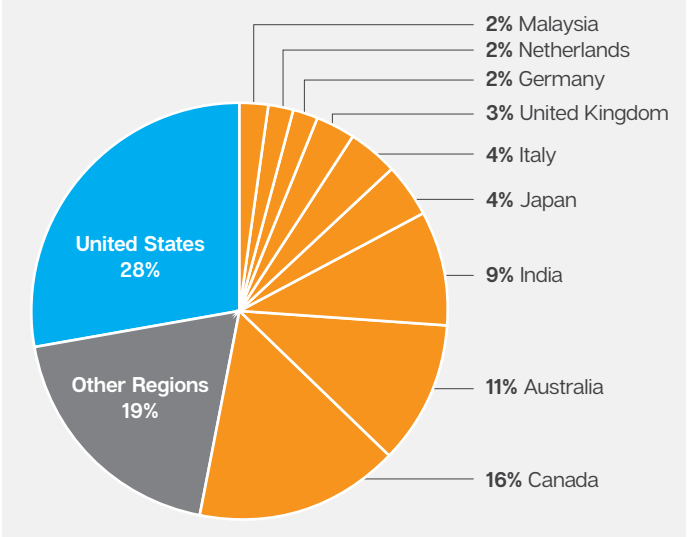


US Continues to Be Most Affected by Ransomware

With over a quarter of all infections logged between January 2015 and April 2016, the US continues to be the region most affected by ransomware. Canada (16 percent), Australia (11 percent), and India (nine percent) are also heavily affected. Western European nations such as Italy (four percent), the UK (three percent), Germany (two percent), and the Netherlands (two percent) figure highly in infection statistics. Other countries that feature in the top ten are Japan (four percent) and Malaysia (two percent).

The statistics indicate that attackers are largely concentrating on developed, affluent nations as the focus of their campaigns.

Figure 4. Ransomware Infections by Region, January 2015 – April 2016



New Techniques

Over the past year, ransomware attackers have added a number of new techniques to their arsenal. Several new ransomware families have been coded in different programming languages, such as JavaScript, PHP, PowerShell, or Python. Attackers used these languages in an effort to evade detection by security products.

A number of high-profile ransomware families have also begun to add features beyond the core functionality of locking devices or encrypting files. For example, CryptXXX (Trojan.Cryptolocker.AN) contains an additional feature that allows it to gather Bitcoin wallet data and send it to the attackers. Cerber (Trojan.Cryptolocker.AH) is reportedly capable of adding the infected computer to a botnet which can be used to carry out distributed denial of service (DDoS) attacks.

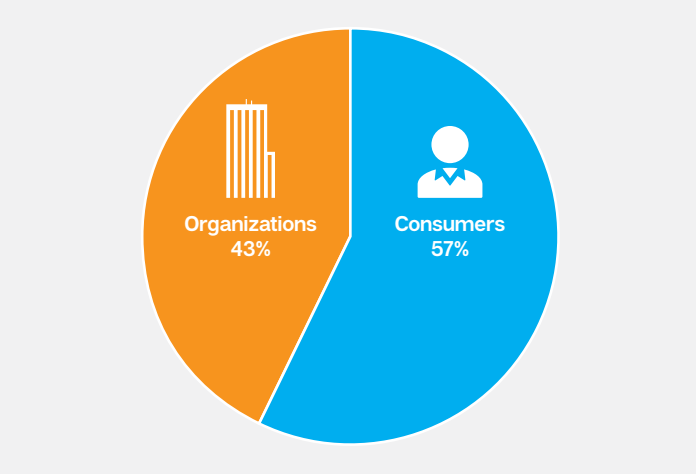
Chimera (Trojan.Ransomcrypt.V) makes an additional threat in its ransom message. In addition to encrypting files, the malware threatens to post the victims files, including pictures and videos, on the internet.

The adoption of these new techniques demonstrates how ransomware is continuously evolving to maintain its foothold and remain profitable.

Who Are the Victims?

Consumers are the most likely victims of ransomware, accounting for 57 percent of all infections between January 2015 and April 2016. While most major ransomware groups tend to be indiscriminate in their attacks, consumers are often less likely to have robust security in place, increasing the possibility they could fall victim to ransomware.

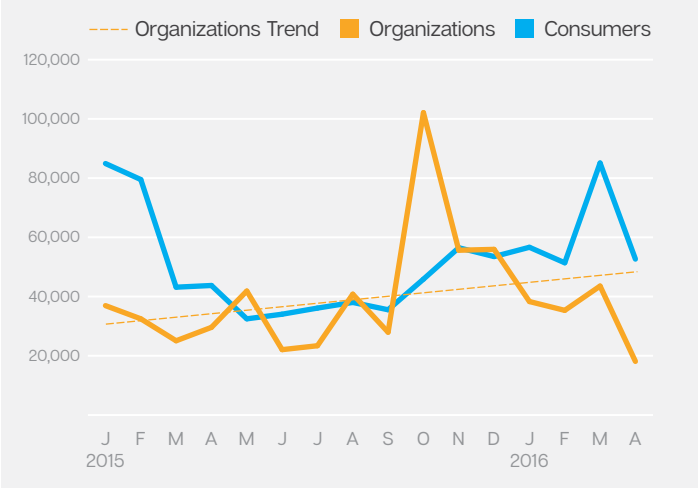
Figure 5. Consumer vs. Organization Ransomware Infections, January 2015 – April 2016



At the beginning of 2015, the proportion of consumer infections was more than double that of organization infections. Consumer infections dropped during the first quarter of 2015, with the breakdown between the two categories of targets remaining roughly equal for much of the year. October 2015 proved to be an exception to this trend, as there was a spike in organization infections. Looking at the month-to-month statistics, the long term trend has been a slow but steady increase in ransomware attacks on organizations.

Despite this trend, the first quarter of 2016 has seen consumer infections once again beginning to move ahead of organizations. With no evidence to suggest that attackers are focusing more on consumers, one explanation for this divergence in recent months is that there is a growing awareness among businesses of the danger posed by ransomware. Threats such as TeslaCrypt (Trojan.Cryptolocker.N) and Locky were spread widely in massive spam campaigns in late 2015 and early 2016, and many businesses were hit in this onslaught of spam. An increased focus on security may mean that fewer ransomware payloads are making it on to computers in organizations.

Figure 6. Consumer vs. Organization Ransomware Infections by Month, January 2015 – April 2016



What Kinds of Organizations Are Most Likely to Be Infected?

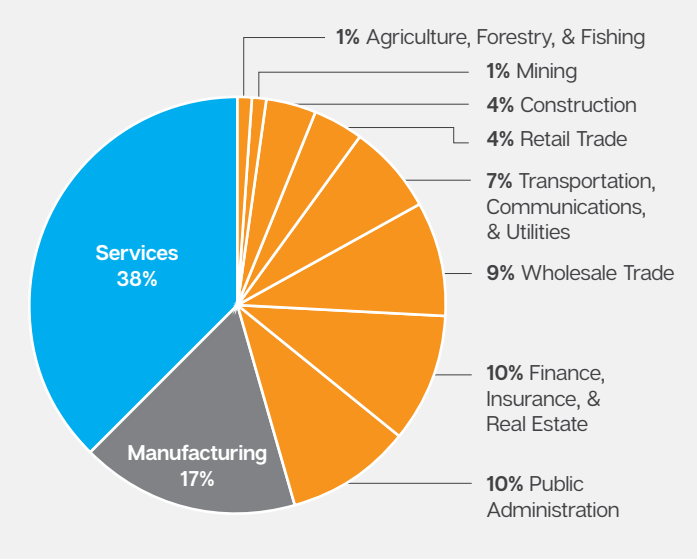
Almost every sector has been affected by ransomware in recent years, but some types of organizations appear to be harder hit than others. Analysis of infections in known sectors has found that between January 2015 and April 2016, the Services sector, with 38 percent of infected computers, was by far most affected by ransomware.

Manufacturing, with 17 percent of infections, along with Finance, Insurance, and Real Estate, and Public Administration (both on 10 percent) also figured highly. Rounding out the top 10 were Wholesale Trade (nine percent), Transportation, Communications, and Utilities (seven percent), Retail Trade (four percent), Construction (four percent), Mining (one percent), and Agriculture, Forestry and Fishing (one percent).

As yet, it is unclear why some sectors are more affected than others. One possible explanation is that organizations with a higher level of integration with different internet services tend to have a higher exposure to infection risks, hence the large number of Services sector infections.

While attacks against the Healthcare sector have been widely reported in recent months, it does not appear among the most frequently infected sectors. This is because most of the latest high-profile Healthcare infections were targeted attacks. Although highly damaging to the affected organizations, these kinds of attacks are still relatively low in frequency and overall infection statistics are dominated by ransomware variants used in wide-scale, indiscriminate attacks. To learn more about targeted attacks, see the section: Businesses: The Next Big Target.

Figure 7. Ransomware Infections by Organization Sector, January 2015 – April 2016



FACTORS DRIVING GROWTH AND PERSISTENCE

The crypto-ransomware market has approached a state of maturity in the past two years. This perfection of the ransomware business model has been driven by a number of key factors.

Encryption

One of the main drivers of growth has been the easy availability of strong encryption implementations, which has helped malicious actors create potent threats. Effective deployment of encryption was one of the main obstacles attackers have had to overcome, and they have made significant strides in recent years.

Early variants of crypto-ransomware often had obvious design flaws. The errors included leaving the encryption key on the infected computer or using the same encryption key for all infections, which meant anyone who obtained the key could share it with other victims. While such mistakes still occur, they are now far less common. The latest ransomware families generate new unique keys for each infection.

Many of the recent generations of ransomware use a combination of symmetric and asymmetric encryption. Symmetric encryption uses the same private key for encrypting and decrypting files. The advantage symmetric encryption provides is that it can quickly encrypt files. This is important for attackers since they wish to complete encryption before the infection is discovered. The downside of symmetric encryption for the attackers is that if the key is discovered during encryption, the victim can use it to decrypt all the data.

Asymmetric encryption uses two encryption keys: public and private. The public key is stored on the victim's computer and is used to encrypt files. The private key is needed to decrypt files and is stored remotely. It is more secure, but the encryption process is much slower.

Combining the two methods allows attackers to leverage the strengths of both and is common practice for all developers. Attackers can encrypt the victim's files rapidly using symmetric encryption and then employ asymmetric encryption to encrypt the symmetric encryption key. As a result, the more secure but slower asymmetric method is needed to encrypt only one file.

Advent of Cryptocurrencies

Ransom payment has always proved a challenge for cybercriminals, who need a method that is easily accessible to victim and easily convertible to cash but also untraceable. Previously attackers relied largely on payment vouchers.

The rise of Bitcoin and other cryptocurrencies provided an alternative that operates outside the traditional financial system. Although not wholly anonymous, Bitcoin movements can be obfuscated by moving through chains of wallets and tumbler services. Bitcoin wallets are free and disposable, meaning attackers can generate a new, unique wallet for each infection, making it more difficult for law enforcement to follow all earnings.

Widespread public awareness of Bitcoin also means that victims may be less suspicious of the cryptocurrency, so are more likely to buy bitcoins and pay the ransom. Some ransomware families have experimented with voucher cards for online shops as payment, such as iTunes gift cards, but with not as much success, as they are easier to trace and harder to cash out.

Effective Infection Vectors

Developing an effective form of ransomware is only half the battle for attackers. They also need to ensure that their ransomware spreads to as many users as possible. The past year has seen some ransomware groups, such as TeslaCrypt and Locky, mount major spam campaigns. This resulted in millions of users being hit on an almost daily basis. Even if only a small fraction became infected, the attackers behind these compromises would be likely to profit significantly.

In addition to this, several major exploit kits have been observed distributing ransomware. For example, in recent months, the Angler exploit kit was one of the main delivery channels for CryptXXX. The Neutrino exploit kit has been spotted pushing a number of ransomware variants including Locky, Cerber, and CryptoWall (Trojan.Cryptowall).

Advanced Attack Techniques

A number of ransomware groups have begun using advanced attack techniques to mount targeted attacks against organizations. The level of expertise employed in these attacks is similar to that seen in many cyberespionage attacks. Attackers have managed to gain a foothold on networks by exploiting vulnerabilities in public-facing web servers and then traversing the network using legitimate tools, before identifying and infecting hundreds of computers. The time and skill required to mount such attacks is far in excess of that required for standard ransomware campaigns, but the rewards are potentially much greater.

Ransomware-as-a-Service

The emergence of RaaS has made entry into the ransomware arena possible for many who would otherwise be excluded. It is now possible for someone with relatively little skill to pay for a ransomware executable and access to a user interface to track their victims. The RaaS creators then sit back and wait for their customers to distribute the malware, earning a percentage of the profits.

INFECTION VECTORS

There are multiple ways ransomware can infect a computer, some of which are more prevalent than others.

Malicious Email

One of the most common methods to spread ransomware, and malware in general, is through malicious spam email. This spam is distributed using botnets—networks of compromised computers, ranging from hundreds to millions of infected computers. The botnet sends out large numbers of spam emails that use social-engineering tactics to trick recipients into compromising their computers. Infection may occur if the user performs any of the following actions:

- Opens a malicious attachment that directly installs the ransomware
- Opens a malicious attachment that initiates a second-stage delivery through a downloader (usually a macro), which subsequently downloads and installs the ransomware
- Clicks a link that points to an exploit kit which will ultimately lead to the malware being installed on the computer

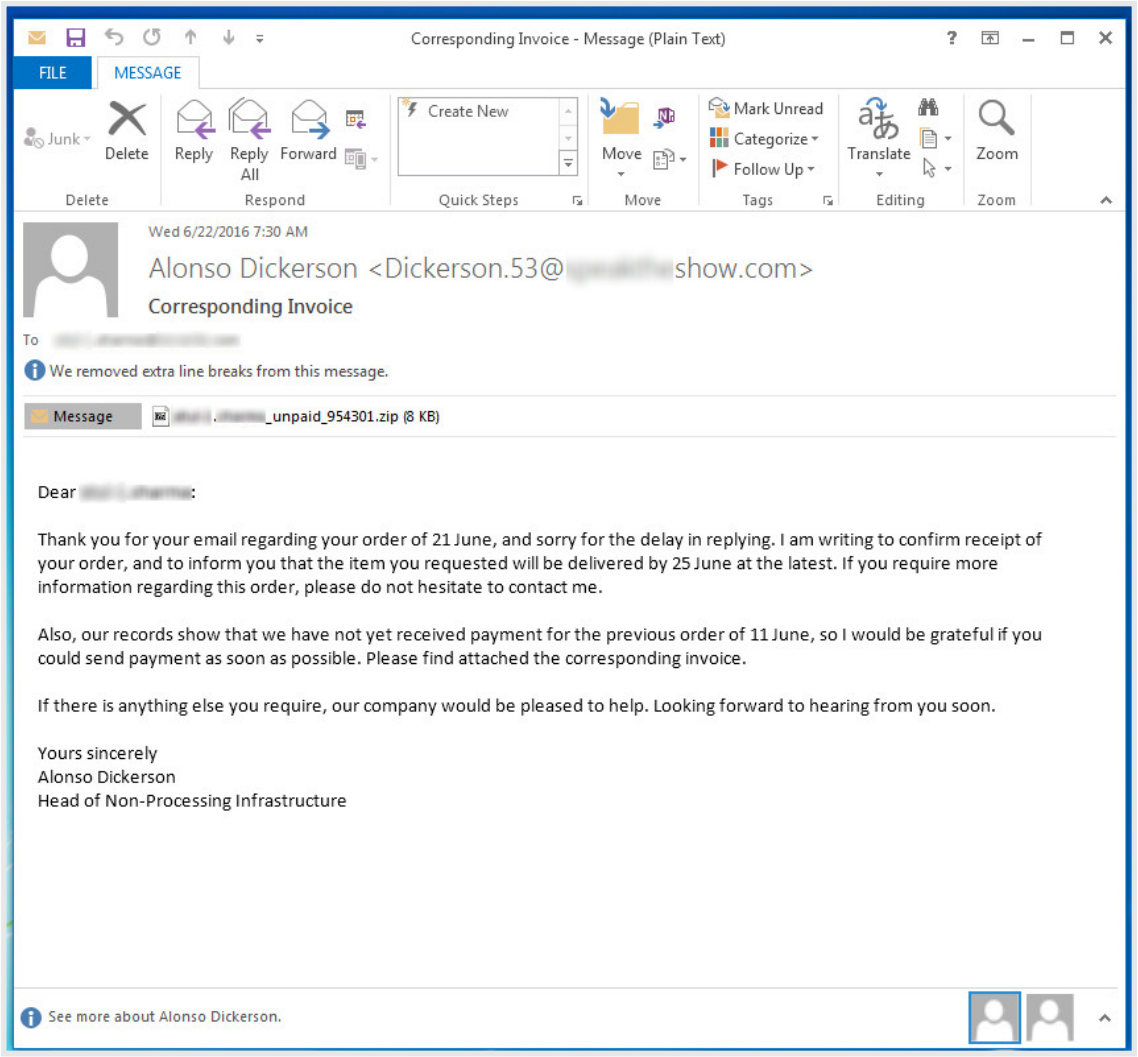
The spam used to distribute ransomware often poses as an important email from a well-known organization, such as the following:

- A notification from the post office or another shipment company, informing the recipient of a delivery
- A message from a utility provider about an overdue bill
- An alert about the recipient's tax return
- Invoices for goods and services
- Fake credit card reward schemes

Each spam variation relies on users' inherent instinct to act on messages that appear to be urgent.

Figure 8 shows a typical invoice spam example. In this spam run, Symantec blocked over 500,000 malicious emails distributing Locky. Although this amount is typical for a ransomware spam campaign, the number of blocked emails can sometimes reach into the millions.

Figure 8. Example of Spam Email Distributing Locky



Attackers employ various tactics to help them effectively spread ransomware through spam email. For example, earlier this year, some attackers used Windows Script Files (WSF) to bypass email filtering. Files with the .wsf extension can be launched like an executable file. Once the email attachment—a zipped folder appearing to contain a .doc file—is opened, the .wsf file is executed and CryptoWall is installed on the victim's computer.

We also saw ransomware composed entirely of JavaScript, which was being spread through spam attachments posing as .doc files. Once the malicious attachment was opened, JS.Racryptor, also known as RAA, immediately began encrypting files. This wasn't the first time JavaScript was used in a ransomware campaign. Ransom32 (Trojan.Ransomcrypt.Y) used NW.js, a framework for developing desktop applications for Windows, Linux, and Mac OS X using JavaScript. However, while Ransomware32 was packaged into an executable file, RAA was delivered solely by a JavaScript file.

Spam remains one of the most prevalent methods to spread ransomware because it is easy to carry out, as it relies on social engineering rather than more advanced techniques. By sending vast amounts of spam email, attackers can reach a large number of victims in a short period of time. New tactics, such as the use of .wsf files and even the return of old tricks such as malicious macros, mean that users and organizations need to exercise caution when dealing with email, no matter how innocuous the message may seem.

Protection from malicious emails requires a multilayered approach including the use of email-scanning services as well as educating users on email best practices. Symantec Email Security.cloud and Symantec Messaging Gateway can block email-based threats, including malware, malicious URLs, and phishing attempts before they reach users. The products also use code analysis and emulation to discover and block malicious JavaScript within emails.

Exploit Kits

Exploit kits (EKs) are another prevalent infection vector for ransomware. These toolkits exploit vulnerabilities in software in order to install malware. Exploit kit attackers compromise third-party web servers and inject iframes into the web pages hosted on them. The iframes direct browsers to the exploit kit servers.

Attackers can redirect users to EKs in the following ways:

- Malicious links in spam email or social media posts
- Malvertisements
- Redirected web traffic from traffic distribution services

The criminals behind these kits rely on users running outdated or unpatched software on their computers and, unfortunately, have an overabundance of potential targets. Symantec blocks as many as 1.2 million attacks per day from all EKs.

The operators of EKs favor zero-day vulnerabilities, as these unpatched flaws will provide the highest return on investment. The kit operators are in a constant race with software developers to integrate new exploits before the vulnerabilities are patched. Until it abruptly disappeared in June 2016, the Angler EK was leading the pack. In 2015, Symantec blocked 19.5 million attacks from Angler alone. Angler mostly attempted to exploit vulnerabilities in Adobe Flash, with 64 percent of attacks targeting Windows 7 computers.

Cybercriminals may pay EK operators to distribute ransomware. As a result, the threats that each kit serves can change over time. Our data shows that in May 2016, the Angler and Neutrino EKs were mostly distributing the CryptXXX ransomware. Neutrino and Magnitude were delivering Cerber. Rig was distributing both Cerber and Locky.

However, circumstances can change fast in the world of cybercrime, as seen in June 2016 with the sudden drop in activity from several notable cybercrime groups behind threats such as Locky, Dridex, Angler, and Necurs (Backdoor.Necurs). Symantec telemetry saw all these threats either greatly reduce their activity or practically cease operating during this time (although Locky has now resurfaced and the others, apart from Angler, are also beginning to resume activity).

The cause of this reduction of activity remains a mystery, though it did occur around the same time as the arrest of a number of suspected banking fraud cybercriminals in Russia. While there are no known links between the alleged cybercriminals and the affected threats, the Locky, Dridex, Angler, and Necurs groups may have used the infrastructure that was shut down or seized during the law enforcement operation. Events like this show how quickly the threat landscape can change and the importance of reliable intelligence to stay one step ahead.

Symantec recently found what appeared to be tech support scammers redirecting their victims to an EK to spread ransomware. The scammers performed the usual tech support fraud by trying to fool the victim into paying to fix nonexistent computer problems. However, the scammers simultaneously redirected the user to the Nuclear EK which served CryptoWall.

While we've seen tech support scams use ransomware techniques in the past, this is the first time we've seen them use actual ransomware. The tech support scammers may have been attempting to increase their chances of earning money from their victims. Alternatively, the scammers themselves may have been the victim of a separate attack. Exploit kit operators could have compromised the scammers' servers during this campaign to deliver their own ransomware.

Other Infection Vectors

While email and exploit kits are the two predominant methods used to spread ransomware, the following techniques are also deployed:

Malvertising: Malicious ads are placed through ad networks whose ads are distributed through trusted websites with a high volume of visitors. The visitor doesn't even have to click on the ad in some cases, as simply loading the web page hosting the malvertisement will lead to infection, often through redirection to an exploit kit. The malicious components of the ads are only present for a short period of time and, once removed, all traces of its presence disappear. Ransomware criminals avail of malvertising because they can purchase ad space through real-time ad-bidding networks, making it easy to target people located in economically strong locations.

Other malware: Ransomware may also arrive on a compromised computer through other malware. One such case involved the infamous Dridex botnet, known for harvesting banking credentials. Following a takedown operation which saw one of the Dridex botmasters arrested, the botnet was disrupted to some extent but quickly recovered. The Dridex botnet is segregated into several subnets, likely operated by different individuals. Shortly after the takedown, one of the subnets switched from sending out spam containing Dridex to distributing spam containing a downloader which retrieved Locky. Bots may also be made to install ransomware as a last ditch attempt to monetize infected computers.

Brute-forcing passwords: An emerging tactic for spreading ransomware is by way of brute-forcing login credentials for software used on servers. The criminals behind the Bucbi ransomware (Trojan.Ransomcrypt.AO) use this method to gain a foothold on remote desktop protocol (RDP) servers. The threat then encrypts files on computers and other servers that the RDP server has access to.

Exploiting server vulnerabilities: Attackers have been recently seen targeting vulnerable software running on servers to gain access to an organization's network. The gang behind the SamSam ransomware (Trojan.Ransomcrypt.AE) use freely

available tools to find and exploit vulnerabilities to spread their malware throughout the network.

The past year also saw the arrival of the Linux.Encoder (Unix.Ransomcrypt) ransomware family and a new variant of CTB-Locker (Trojan.Cryptolocker.G). Linux.Encoder focuses on the Linux operating system, with its main target being computers with web servers deployed on them. The attackers exploit vulnerabilities in site plugins or third-party software to infect victims. Linux.Encoder then encrypts directories associated with website files, rendering any site hosted on the affected computer unusable.

Self-propagation: While we have seen Android ransomware display worm-like behavior by spreading to all contacts on a device's address book using SMS messages, ZCryptor (W32.Cryptolocker.AQ) is possibly the first to display this self-propagation behavior on the Windows platform. ZCryptor infects all removable drives with a copy of itself before it begins encrypting, increasing its chances of spreading to other computers.

SMS messages and third-party app stores: As previously mentioned, Android ransomware threats can be spread through SMS messages; however, they can also make it onto a device by way of untrusted third-party app stores. An example of this can be seen with Android.Lockdroid.E, which poses as a pornographic video player on third-party app stores. Instead of playing adult videos, however, the app snaps a picture of the victim using the device's camera and includes the image as part of the ransom note.

PLATFORMS AFFECTED BY RANSOMWARE

While attacks against Windows users continue to dominate the ransomware landscape, there has been a growing number of ransomware campaigns against other platforms. This trend is likely to continue as groups compete to find unexploited target groups.

Windows Users

Indiscriminate campaigns affecting both businesses and consumers are by far the most predominant forms of ransomware attack. Most attack groups simply attempt to infect as many computers as possible to maximize their returns. As a result, the majority of ransomware variants are designed to attack Windows computers.

Windows home users continue to be one of the biggest victim groups. In comparison to businesses, home users are less likely to use security software or keep up-to-date backups of valuable data, making their computers more vulnerable to attack. While home users may not have the means to pay large ransoms, the sheer volume of potential victims means that they can still be a highly lucrative target.

Businesses are also affected by the same ransomware attacks hitting home users. If the organization isn't protected, the consequences could be devastating. While the home user may be faced with a $500 ransom demand for one infected computer, the ransom demand for multiple infections at an organization could quickly rack up to tens of thousands of dollars.

In addition to these wide-scale attacks, ransomware groups are now showing a growing interest in specifically targeting organizations with customized attacks (see the section: Businesses: The Next Big Target).

Mobile Users

Given the popularity of smartphones, it is not surprising that ransomware attackers are increasingly looking to compromise these devices. A number of Android threats have emerged in recent years, the majority of which are locker-type threats. However, crypto-ransomware for Android devices has also emerged in the form of the Russian-language Simplocker (Android.Simplocker) and its English-language variant (Android.Simplocker.B).

At present, there have been no documented cases of iOS-specific ransomware, but web-based variants do affect iOS devices.

Mac OS X Users

Until recently, ransomware groups mostly ignored Mac OS X users. In March 2016, a threat known as KeRanger (OSX.Keranger) became the first widespread ransomware to target the Mac OS X operating system. KeRanger was briefly distributed in a compromised version of the installer for the Transmission BitTorrent client.

KeRanger behaved similarly to modern Windows ransomware, searching for and encrypting approximately 300 different file types before demanding a ransom of one bitcoin (US$678 at the time of writing).

The malware was signed with a valid Mac Developer ID. This meant that KeRanger could bypass Mac OS X's Gatekeeper feature, which is designed to block software from untrusted sources. Apple quickly revoked the Developer ID that KeRanger used.

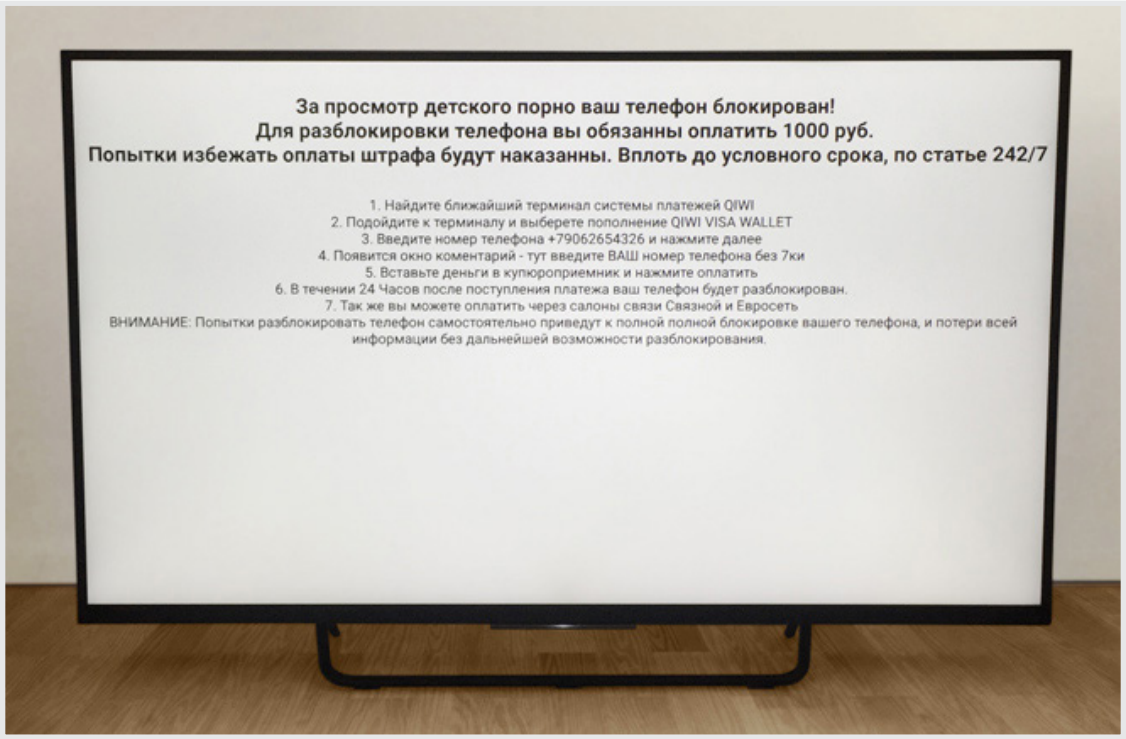
Prior to this, in November 2015, a Brazilian cybersecurity researcher Rafael Salema Marques developed a proof-of-concept (PoC) ransomware known as Mabouia (OSX.Ransomcrypt). Marques did this to highlight the fact that Mac OS X computers may not be immune to ransomware.

Future Targets

The growth of the Internet of Things (IoT) has multiplied the range of devices that could potentially be infected with ransomware. With a growing awareness of ransomware affecting traditional computers, attackers may turn to IoT to find new, softer targets.

For example, Android ransomware Flocker (Android.Lockdroid.E) is capable of locking Android smart TVs. Flocker's latest version asks victims to pay $200 in iTunes gift cards as a ransom. This kind of attack is something that was predicted last year by Symantec researcher Candid Wueest, who demonstrated a successful ransomware attack against a smart TV.

Figure 9. A Smart TV Infected with Ransomware



Smart watches are also another potential avenue of attack. Last year, Symantec demonstrated a successful proof-of-concept ransomware attack against an Android Moto 360 smartwatch.

One worrying potential target is industrial control systems (ICS). There have already been examples of malware attacks against ICS devices, the most famous of which was Stuxnet. Given the recent emergence of targeted ransomware attacks and the potential for disruption that an ICS attack could cause, it may only be a matter of time before attackers shift their attention to this arena. If attackers use extortion attacks to disrupt the manufacturing process, then the impact could be devastating.

MAJOR RANSOMWARE FAMILIES

The ransomware landscape is constantly shifting, with new families appearing every month. In tandem with the rise of new threats, older ransomware families can disappear as quickly as they emerged. One notable example is TeslaCrypt, which was one of the most widespread ransomware variants in late 2015 and early 2016. In May 2016, the group suddenly ceased operations and released a universal decryption key. The attackers made the announcement on their Tor website with a terse note stating the project was "closed," signing off with "we are sorry."

The following are three of the mostly widely circulated crypto-ransomware threats at the time of writing:

Cerber

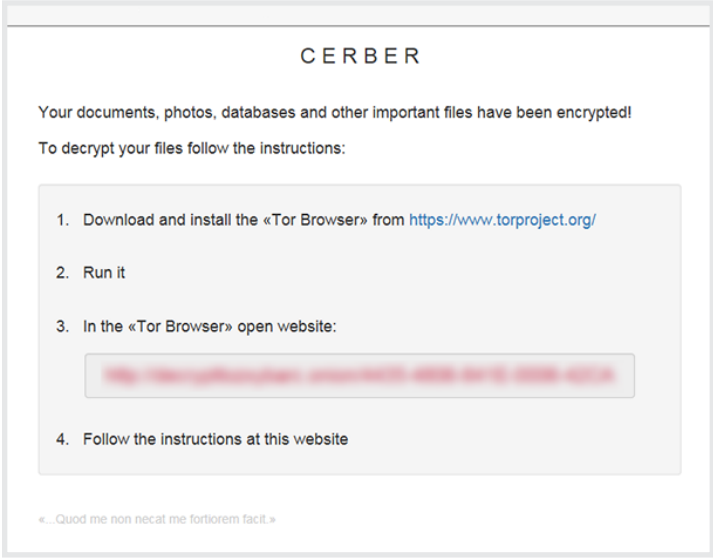
Detection name: Trojan.Cryptolocker.AH

Ransom amount: 1.24 to 2.48 BTC ($513 to $1,026 on March 2016 rates)

Discovery: March 2016

Known infection vectors: Spam campaigns, Neutrino exploit kit, Magnitude exploit kit

Figure 10. Cerber Ransom Note, Informing the User That Their Files Have Been Encrypted and Providing Users with Instructions on How to Decrypt Them



Cerber is one of the newest arrivals on the ransomware scene, but has managed to make a significant impact quickly since it emerged in March. Like Locky, Cerber appears to have access to the Dridex spam network, meaning it can be pushed out quickly in large spam campaigns. Cerber has also been spread by some of the major exploit kits. One of Cerber's novel features lets the threat read the ransom note aloud to the victim, using a text-to-speech (TTS) module.

CryptXXX

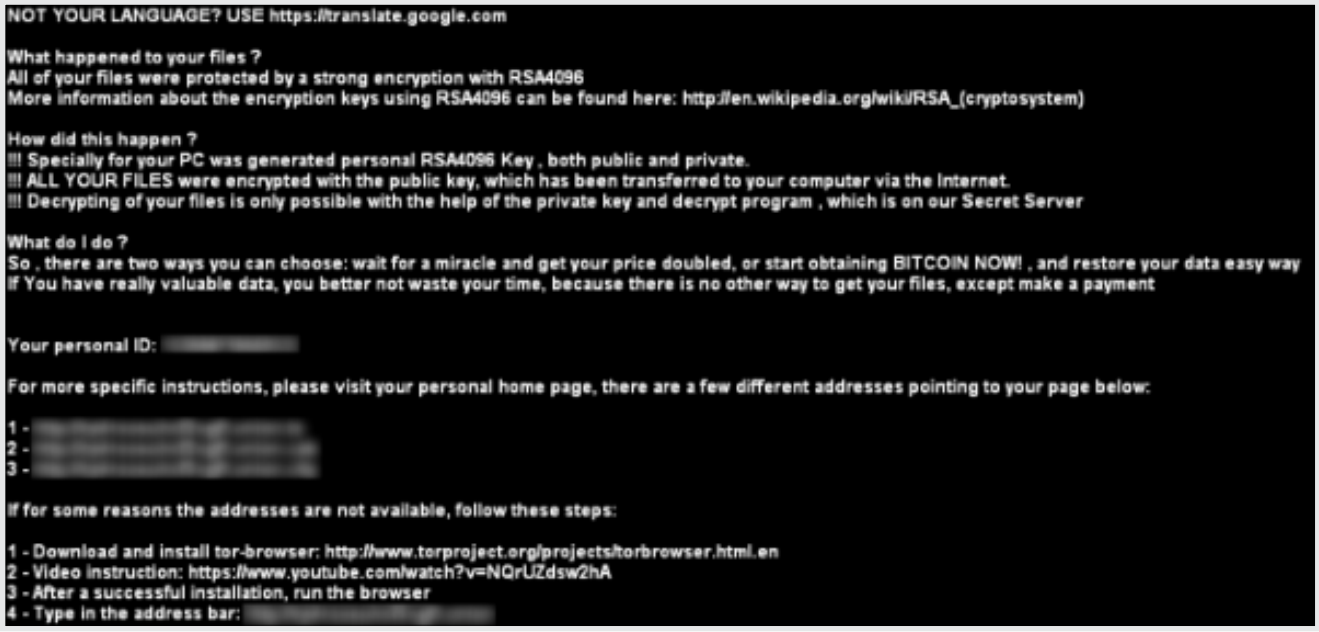
Detection name: Trojan.Cryptolocker.AN

Ransom amount: $500 in bitcoin

Discovery: April 2016

Known infection vectors: Angler exploit kit, Neutrino exploit kit

Figure 11. CryptXXX Ransom Note, Saying That the User's Files Have Been Encrypted and Demanding Payment to Decrypt Them



Reportedly developed by the same attackers behind Reveton (Trojan.Ransomlock.G), CryptXXX first appeared in April 2016 and was circulated widely in the weeks that followed. Until recently, CryptXX was primarily spread by websites compromised to redirect users to the Angler exploit kit. These attacks involved Angler first dropping Trojan.Bedep on the affected computer. Trojan.Bedep then infected the computer with CryptXXX.

The disappearance of the Angler exploit kit in early June prompted a fall-off in CryptXXX activity. The threat has since remerged and is now being spread by the Neutrino exploit kit.

Initial variants of CryptXXX used weak encryption, allowing security researchers to create a decryption tool for compromised computers. However, the attackers responded quickly and newer variants of the malware employ better encryption, making the tool ineffective.

CryptXXX contains a feature allowing it to gather Bitcoin wallet data and send it to the attackers.

Locky

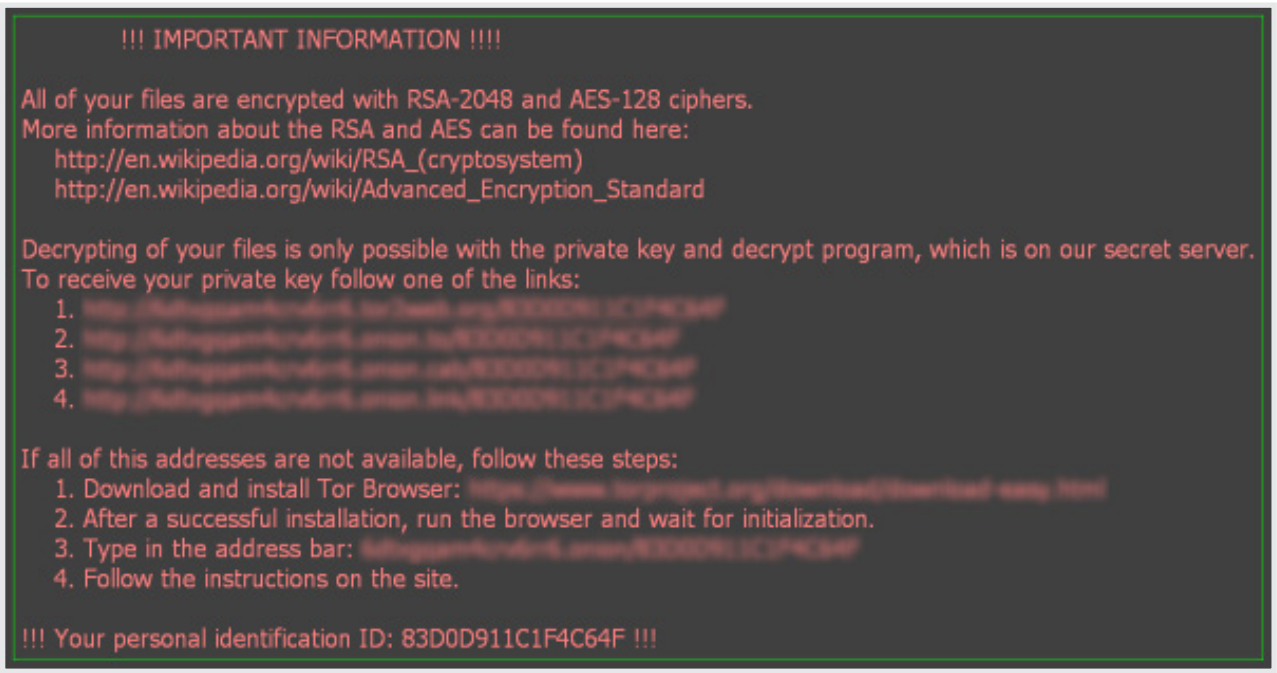
Detection name: Trojan.Cryptolocker.AF

Ransom amount: 0.5 to 1 bitcoin ($200 to $400 on February 2016 rates)

Discovery: February 2016

Known infection vectors: Spam campaigns, Neutrino exploit kit, Nuclear exploit kit

Figure 12. Locky Ransom Note, Saying That the User's Files Have Been Encrypted and Offering Instructions on How to Obtain the Decryption Program



Since its emergence in early 2016, Locky has been one of the most prolific ransomware variants created to date. The attackers behind Locky spread the threat through the same spam network used by the Dridex financial Trojan. This allows the attackers to send out massive waves of spam containing the ransomware. Locky has also been distributed through a number of exploit kits.

The Locky group has recently begun using a new downloader, known as Rockloader (Downloader.Zirchap), in its spam campaigns. Victims are first infected with Rockloader, which then downloads Locky onto the computer.

Locky experienced a sudden drop in activity in early June, prompting speculation that it had disappeared for good. However, after a quiet period of approximately three weeks, spam campaigns spreading Locky resumed again.

BUSINESSES: THE NEXT BIG TARGET

Realizing the potential for higher profits, cybercriminals are increasingly targeting the business space. We have seen this trend emerge in other attack campaigns, such as:

- Business email compromise (BEC) scams, which attempt to trick C-level executives into making large wire transfer payments
- Bug-poaching attacks, which involve attackers compromising corporate servers, stealing data (as proof of compromise), and requesting a fee for information on how the attack was carried out
- The Carbanak gang, which target banks directly rather than bank customers

Ransomware gangs have become the latest to follow the trend. Holding businesses to ransom can significantly raise attackers' return on investment. Symantec has seen a steady increase in the number of organizations targeted with ransomware in recent times. Most of these new victims are hit in indiscriminate campaigns, where employees have opened a malicious spam email or visited a malicious website. However, a growing number are victims of far more dangerous, targeted campaigns.

Many of these targeted ransomware attacks use similar tactics to advanced persistent threats (APT) such as:

- Using freely available, dual-use tools to help gain a foothold and move through a network
- Obtaining administrator credentials and using them for lateral movement
- Conducting reconnaissance to gain information that could help criminals extort money from the target organization

In a previous ransomware paper, Symantec noted some early signs of this emerging trend. Some cases dated back as far as 2012 when several Australian businesses were infected with crypto-ransomware demanding up to AU$5,000 (US$3,700) to decrypt files. One of these Australian businesses was a medical center, perhaps an early sign of things to come, as several healthcare entities around the world were recently infected with ransomware.

The past year has seen many news outlets reporting that ransomware infected multiple hospital and medical center networks, encrypted files, and held the data to ransom. Some of these cases were likely the result of large-scale, indiscriminate campaigns but others were undeniably targeted. The rise of these types of attacks has prompted the FBI as well as the US and Canadian governments to issue alerts to businesses about ransomware.

CASE STUDY: ANATOMY OF AN ADVANCED RANSOMWARE ATTACK

Symantec Incident Response recently assisted in the response to a ransomware outbreak at a large organization. The ransomware had spread to hundreds of computers, encrypted client data, and caused critical systems to go offline. The investigation revealed a ransomware attack which shared more commonalities with an APT-style attack than regular cybercrime activity.

The Culprit

As the first step, Symantec investigators identified the ransomware used in the attack as a strain of SamSam, which is known to be targeted at organizations. A full scan of the customer's network using Symantec Endpoint Protection (SEP) revealed the extent of the infection and identified all compromised computers.

Infiltration

By plotting the infected computers, Symantec investigators developed a number of investigative leads and built up a profile of the attack. The team discovered that the attackers' initial point of entry was a public-facing web server. The attackers used an exploit for an unpatched vulnerability to compromise this web server. This provided the attackers with a foothold on the victim's network.

Lateral Movement

Once in, the attackers used a number of publicly available tools, such as Microsoft Sysinternals utilities, to traverse the victim's network. By using legitimate tools to perform these tasks, the attackers limited their risk of detection before the attack was complete. This is a common technique used in advanced attacks. These tools allowed the attackers to map every accessible computer on the organization's network to help identify the most valuable assets to target.

Payload and Ransom

Once the targeted computers were identified, the attackers used a batch script called f.bat to deploy SamSam and a public encryption key on each computer. The script also deleted volume shadow copies from the computers, which prevented any files from being restored from them following infection. The attackers then distributed a tool called sqlsrvtmg1.exe. This executable searched for any running backup processes and stopped them. It also deleted any backup-related files it found.

The final step of the infection process was the distribution of another batch script called reg.bat. This initiated the encryption process on each infected computer. SamSam is configured to encrypt hundreds of different file types. Once the encryption process was completed, the ransomware deleted itself, leaving the encrypted files and a ransom note on the desktop. The note instructed the victim to visit a website and pay a ransom of 1.5 Bitcoin (US$989 at the time of writing) for each infected computer.

Remediation and Restoration

Using SEP behavioral and file-based signatures, Symantec Incident Response was able to contain and eradicate the outbreak. The remediation operation began with the identification and deletion of all encrypted files. The customer then moved onto the lengthy process of restoring unencrypted versions of the files from backups. In some instances, files were permanently lost because users had stored files locally rather than on mandated file servers, meaning they were not backed up. The servers that were identified as the initial point of compromise were rebuilt by the vendor that supplied their software.

Lessons Learned

This investigation revealed how ransomware infections are no longer just opportunistic mass attacks. Cybercriminals are now adopting techniques traditionally seen in advanced espionage attacks and are using them for targeted ransomware infections. This demonstrates a further maturing of cybercrime and shows how organizations are firmly in the sights of cybercriminals.

During the investigation, Symantec Incident Response identified some key issues for the customer:

1. An unpatched vulnerability on a public-facing server provided the attackers with a means of getting into its network. Immediate patching of all key software packages reduces the risk of compromise in this way.
2. End users who failed to follow company policy (by saving their files locally rather than on a file server) were a factor in the permanent loss of data. As a result, there were no backup copies of these files so they couldn't be restored.
3. While SEP was installed on all workstations and servers, SEP's Application and Device Control feature had not been deployed on the organization's servers, meaning the customer didn't benefit from a vital and effective tool that could have helped block the spread of infection.

By calling in Symantec Incident Response, the customer was able to quickly identify every infected computer and prevent the attackers from doing any further damage. By identifying the source of the initial attack and mapping how the attackers traversed the victim's network, Incident Response was able to provide the customer with specific action items to bolster defenses and prevent further attacks.

Organization-Specific Payloads

Ransomware aimed at individual end users adopts a scattershot approach. In these campaigns, the attackers effectively cast the net as wide as possible, hoping to catch as many victims as they can. With targeted ransomware, the attackers tailor their efforts to a specific target with a much more hands-on approach.

For example, SamSam targets servers running unpatched versions of Red Hat's JBoss (also known as WildFly), instead of targeting individual users though spam or drive-by download attacks. The SamSam attackers use freely available tools, such as the open-source testing tool JexBoss, to identify vulnerable servers. Once in, the attackers may steal credentials and conduct further reconnaissance before encrypting any files. The use of open-source and well-known tools can help threats stay under the radar, as many of the tools, such as Microsoft's Sysinternals, which was used by SamSam, are commonplace on enterprise networks.

Another example of a targeted ransomware attack was how the criminals behind the Bucbi ransomware compromise RDP servers. Once inside the network, the attackers use the RDP server for lateral movement and may spend some time on reconnaissance, learning about the organization's backup policies, for example. When the attackers have the information they need, they activate the ransomware, encrypting files found on computers or other servers connected to the RDP server. The ransom demand is not made in the typical way and is instead done using email, allowing the criminals to negotiate a higher amount by leveraging the information they obtained during their reconnaissance.

Another difference between targeted attacks and conventional ransomware can be the methods used to set up the encryption. Normally, ransomware contacts its command and control (C&C) server, which generates an RSA key pair and sends the public key back for the malware to use in the encryption stage. However, the SamSam attackers, for instance, generate the RSA key pair themselves and upload the public key with the ransomware while infecting the targeted server.

There is also ransomware that compromises servers and waits for several months before it demands payment. In the case of PHP.Ransomcrypt.A, the threat silently encrypts data written to the infected web server and decrypts it as it is read. Once enough time has passed, the attackers remove the private encryption key from the server and send a ransom note to the website owner. This waiting period is to ensure all incremental backups are also encrypted before the ransom demand is made.

Attackers focusing on organizations need to gain a foothold on the network before they can spread their ransomware. As discussed, servers are an ideal way to do this by targeting them in the following ways:

- Brute-forcing credentials for RDP servers, as in the case of Bucbi
- Targeting vulnerabilities in web plugins to gain access to web servers, as in the case of Linux.Encoder
- Exploiting flaws in JBoss servers, as in the case of SamSam

Once a server has been compromised, the attackers can move laterally within the network and infect connected computers.

Some key points that mark targeted ransomware attacks apart from traditional ransomware campaigns include:

- Using sophisticated techniques to infiltrate networks, such as exploiting vulnerabilities
- Moving laterally across the network to infect numerous computers or find valuable targets such as databases to amplify the impact of an attack. This also provides the attackers with ample opportunity to perform reconnaissance on the target.
- Using legitimate tools to keep a low profile
- Deleting backup files to prevent victims from recovering affected data, encouraging them to pay the ransom

Consumer ransomware campaigns are automated, but targeted attacks require a lot of work on the part of the attackers. However, this drawback is balanced by a potential for higher profits, since businesses are likely to have critical data assets of greater value and deeper pockets than consumers.

CASE STUDY: RANSOMWARE AS A DECOY

Symantec Incident Response recently assisted in an investigation on what appeared to be a mass ransomware infection at a large company. On the surface, it looked as though hundreds of the firm's computers had been infected with a variant of CryptoWall.

Fake Ransomware

After collecting samples of the malware and tools used by the attackers, Symantec began its analysis. Shortly after the investigation began, it became clear that there was something interesting going on with this "ransomware" attack. When our investigators looked into the ransomware sample, they found that the malware hadn't actually encrypted any files and had just overwritten them with junk data.

The malware, dubbed Trojan.Phonywall, displayed a ransom note identical to the real CryptoWall message, the only difference being the payment URL. CryptoWall payment URLs are usually unique to each infection but Phonywall's was hardcoded and merely copied from a CryptoWall ransom note posted online.

APT Attack Similarities

The decoy's discovery was the first step in uncovering what turned out to be a well-crafted and targeted attack that used fake ransomware to divert attention away from the attackers' true goal: data theft.

The compromise shared many similarities to APT attacks. Symantec found that the attackers had compromised the company five months prior to the deployment of the decoy ransomware. To gain entry during the first stage of the attack, the cybercriminals used both watering hole attacks and spear-phishing emails with malicious attachments. The attackers then used back door malware and freely available penetration testing tools to consolidate their position within the network and proceeded to compromise administrator account credentials. They then used the credentials to compromise file, application, and email servers within the company, as well as multiple workstations.

Covering Their Tracks

Over a period of approximately five months, the attackers managed to steal thousands of files from the targeted company before attempting to cover their tracks using the Phonywall decoy. The attackers used the stolen admin credentials to deploy Phonywall to 33 percent of the company's workstations. In total, the fake ransomware threat had overwritten data on 723 computers.

There has been instances in the past where attackers have employed DDoS attacks to cover up intrusions. However, the use of ransomware-like activity as a decoy is an interesting addition to the attackers' repertoire.

Lessons Learned

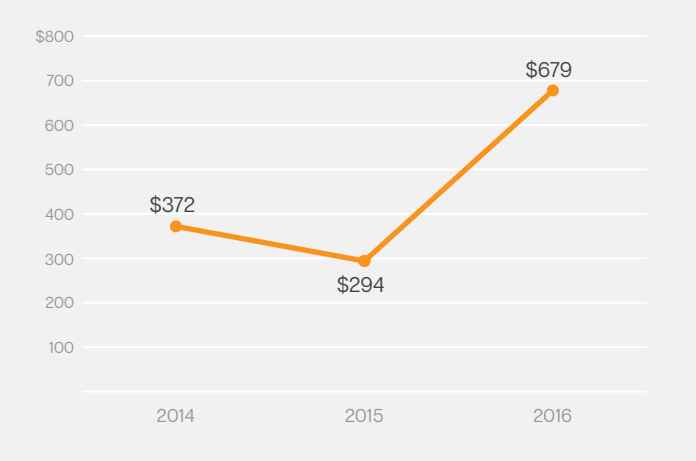
1. Ransomware has become an everyday part of the threat landscape. Businesses that think they have been infected with ransomware may decide to merely accept the situation and not investigate any further. All the while, it is possible that the apparent ransomware attack was only meant as a distraction while the real malicious act was data theft.
2. Cybercriminals now know that the majority of people have some understanding of ransomware and what it can do. The attackers may use this knowledge to cover up more advanced attacks.
3. The attackers used spear-phishing emails in the first stage of their attack. Employee training may have reduced the risk of malicious emails being opened in the first place.
4. By involving Symantec Incident Response, the customer was able to uncover the true goals of the attackers and deal with the theft of company data instead of potentially paying a ransom which would not have recovered any files.

IMPACT OF RANSOMWARE

The average ransom demanded by attackers has once again risen this year. The average ransom discovered to date in 2016 stands at US$679, up from $294 in 2015. The steady rise in ransom demands indicates that attackers may think there is more to be squeezed from victims.

This year has also seen a new record in terms of ransom demand, with a threat known as 7ev3n-HONE$T (Trojan.Cryptolocker.AD) requesting a ransom of 13 bitcoin per computer ($5,083 at the time of discovery in January 2016). This amount is the highest Symantec has seen to date.

Figure 13. Average Ransom Amount in US Dollars, by Year



Scale of Losses

It is impossible to accurately measure how much money ransomware victims have paid to attackers. Few victims disclose whether they have paid the ransom. Attackers rarely disclose how much money they have made and payments are difficult to trace since each infection usually has a unique cryptocurrency wallet. Ransom payments are frequently siphoned through a chain of wallets and "tumbler" services before the attackers cash out.

However, some law enforcement agencies have published statistics that provide an insight in the scale of losses. The FBI has reported that it received more than 2,400 complaints regarding ransomware in 2015, with a reported loss of more than $24 million. This was up from 2014 when over 1,800 complaints were filed and losses were reported at $23 million.

Given US estimates alone, it is reasonable to conclude attackers behind major ransomware variants are earning tens of millions of dollars per year. Additionally, significant proportions of victims seem willing to pay, possibly because they have no alternative.

A recent study from IDT911 in the US among small and mid-sized businesses revealed that 84 percent said they would not pay a ransom during an attack. Another report in Germany showed that 32 percent of the surveyed enterprises experienced a ransomware case in the last six months. Out of these businesses, 95 percent said they did not pay a ransom to the attacker.

The True Cost of an Attack

In early February 2016, the Hollywood Presbyterian Medical Center (HPMC) in the US was compromised with ransomware. The hospital admitted to paying the attackers' demand of US$17,000 to restore its systems, some of which provided access to patient medical records. However, $17,000 is likely a small fraction of the potential costs, both monetary and reputational, that an organization could incur for this type of incident.

Some of the potential impacts that an organization could face after a ransomware attack include the following:

- **Downtime costs:** Organizations may be forced to shut down systems to deal with the infection. Customers may be affected as the targeted organization's services may be impacted. Because of this downtime, the company could experience financial losses and reputational damage. In the case of utility companies, loss of power or water can potentially impact millions of people and may cause accidents leading to injury or, even worse, deaths.
- **Financial cost:** Companies may have to pay for incident response and other security-related solutions in response to ransomware. Organizations could also be hit with large legal bills if customers are affected. Fines and other penalties may also apply. For example, US hospitals that violate the Health Insurance Portability and Accountability Act (HIPAA) can be charged up to $1 million.
- **Data loss:** Loss of data due to files being encrypted and/or stolen can have a huge impact on businesses. The loss of company records, customers' personally identifiable information (PII), or intellectual property can significantly impact the organization's finances, brand, and reputation. The cybercriminals behind the attack may threaten to publish stolen data online in an attempt to extort more money from the victim (we have already seen this tactic used by the authors of Chimera). Even if a victim pays the ransom and the cybercriminals decrypt the files, there is still a risk that data may be corrupted in the decryption process.
- **Loss of life:** In the case of a hospital or other medical organization, patients' lives may be put at risk as essential medical equipment may be affected. Patient records including medical history may also be inaccessible, leading to delays in treatment or even incorrect medication being administered.

A ransomware attack can impact business continuity, productivity, company finances, reputation, and even safety at an organization. While the initial impact may be considerable, the long-term effects of an attack may be far more costly. ■

PROTECTION

Adopting a multilayered approach to security minimizes the chance of infection. Symantec has a strategy that protects against ransomware in three stages:

1. Prevent
2. Contain
3. Respond

1. PREVENT

Preventing infection is by far the best outcome so it pays to pay attention to how infection can be prevented. Email and exploit kits are the most common infection vectors for ransomware. Adopting a robust defense against both these infection vectors will help reduce the risk of infection.

Email Security

Email-filtering services such as Symantec Email Security.cloud can help to stop malicious emails before they reach users. Symantec Messaging Gateway's Disarm technology can also protect computers from this threat by removing malicious content from attached documents before they even reach the user.

Email.cloud technology includes Real Time Link Following (RTLF) which processes URLs present in attachments, not just in the body of emails. In addition to this, Email.cloud has advanced capabilities to detect and block malicious JavaScript contained within emails through code analysis and emulation.

Intrusion Prevention

Symantec intrusion prevention system (IPS) technology can detect and block malicious traffic from exploit kit activity, preventing the installation of ransomware.

Download Insight

Symantec Download Insight technology examines files that are downloaded through or launched by web browsers, messaging clients, and other portals. Download Insight determines whether a file is a risk based on reputation.

Browser Protection

Symantec's Browser Protection solution analyzes the web browser's state and blocks websites from delivering exploits.

Exploit Protection

Symantec exploit protection technology recognizes a range of malicious behaviors that are common in exploit attacks and blocks them from executing.

Best Practice

End users are advised to immediately delete any suspicious emails they receive, especially those containing links and/or attachments.

Be wary of Microsoft Office attachments that prompt users to enable macros. While macros can be used for legitimate purposes, such as automating tasks, attackers often use malicious macros to deliver malware through Office documents. To mitigate this infection vector, Microsoft has disabled macros from loading in Office documents by default. Attackers may use social-engineering techniques to convince users to enable macros to run. As a result, Symantec recommends that users avoid enabling macros in Microsoft Office.

2. CONTAIN

In the event of an infection, a critical step is to limit the spread of the attack. Symantec's file-based technologies ensure that any payload downloaded on the computer will not be able to execute its routines.

Symantec has a 24/7 Security Technology and Response (STAR) team responsible for ongoing development and improvement of generic signatures for ransomware. The team carries out continuous monitoring of ransomware families and their delivery chain in order to harvest new samples and ensure robust detection.

Advanced Antivirus Engine

Symantec uses an array of detection engines including an advanced signature-based antivirus engine with heuristics, just-in-time (JIT) memory-scanning, machine-learning engines and Malheur.

PROTECTION

SONAR Behavior Engine

SONAR is Symantec's real-time behavior-based protection that blocks potentially malicious applications from running on the computer. It detects malware without requiring any specific detection signatures. SONAR uses heuristics, reputation data, and behavioral policies to detect emerging and unknown threats. SONAR can detect encryption behaviors common to ransomware.

Machine Learning Technology

Symantec's enhanced machine learning heuristic technology has been trained to specifically target ransomware. This powerful technology can identify new ransomware without requiring additional signatures.

Emulator

The emulator enables the engine to heuristically detect encryption behavior without needing a signature.

Best Practice

Perform a full network scan to identify all infected computers. Compromised computers should be isolated from the network until they have been fully cleaned and restored.

3. RESPOND

There are a number of steps organizations can take to ensure a speedy recovery from ransomware infections.

Incident Response

Symantec Incident Response (IR) can help organizations with responding to attacks and with making decisions on what to do next.

Help identify the primary infector and contain further spread: Determining the primary attack is critical to understanding what the attacker's primary campaign is targeting and ensures that you aren't missing the actual attack by focusing solely on the ransomware.

Provide incident-specific recommendations to prevent success of future similar attacks: We can assist the customer with implementing controls to prevent any further outbreaks as well as assisting them to enhance their endpoint protection environment. In previous incidents, it has taken us as little as 72 hours to significantly improve the security environment at organizations who've been repeat victims of ransomware attacks.

We can analyze the malware to determine how data was encrypted to help victims create a data recovery plan: In many cases, the malware writer makes mistakes in implementation that can be exploited by incident responders to recover data more easily. A skilled malware analyst can reverse engineer the ransomware to identify any weaknesses in implementation and help the user recover their data.

Work with the customer's data recovery provider to help determine the best plan, based on the specific threat: In many cases, customers hire a data recovery service to assist in the ransomware recovery process. The recovery process is unique to each individual situation and can depend heavily on the sophistication of the malware used. After analyzing the malware to understand how it encrypts and erases data, Symantec IR can work with the data recovery provider to develop an efficient and effective data recovery plan.

Best Practice

Backing up important data is one of the key pillars of combating ransomware infections. However, as there has been cases of ransomware encrypting backups, it should not be a replacement for a robust security strategy.

Victims need to be aware that paying the ransom does not always work. Attackers may not send a decryption key, could poorly implement the decryption process and damage files, and may deliver a larger ransom demand after receiving the initial payment. ■

APPENDIX:
SYMANTEC DETECTIONS FOR COMMON RANSOMWARE FAMILIES

The following is a list of commonly known names of recent ransomware families, along with Symantec's detection names for them. The ransom demands priced in US dollars reflect the currency value at the time that the ransomware was released:

Table. Common Ransomware Families' Detection Names, Discovery Months, and Ransom Prices

Discovered	Type	Common Name/Alias	Ransom Demand	Symantec Detection
May 2016	Crypto	Mischa	Approx. 2 BTC	Trojan.Cryptolocker.AP
May 2016	Crypto	Alpha Locker	$400 in iTunes credit	Trojan.Ransomcrypt.AM
May 2016	Crypto	MM Locker	Approx. $400 in BTC	Trojan.Ransomcrypt.AN
May 2016	Crypto	Bucbi	5 BTC	Trojan.Ransomcrypt.AO
May 2016	Crypto	Enigma	0.42 BTC	Trojan.Ransomcrypt.AP
May 2016	Crypto	Mobef/Yakes	4 BTC	Trojan.Ransomcrypt.AQ
May 2016	Crypto	Shujin	Unknown	Trojan.Ransomcrypt.AR
May 2016	Crypto	CryptoHitman	$150 in BTC	Trojan.Ransomcrypt.AS
April 2016	Crypto	Nemucod 7-Zip	0.52985 BTC	JS.Ransomcrypt
April 2016	Crypto	KimcilWare	1 BTC	PHP.Ransomcrypt.B
April 2016	Crypto	Rokku	0.24 BTC	Trojan.Cryptolocker.AK
April 2016	Crypto	Zeta/CryptoMix	Unknown	Trojan.Cryptolocker.AL
April 2016	Crypto	Kovter	Unknown	Trojan.Cryptolocker.AM
April 2016	Crypto	CryptXXX	$500 in BTC	Trojan.Cryptolocker.AN
April 2016	Crypto	Yougothacked	0.5 to 1.5 BTC	Trojan.Cryptolocker.AO
April 2016	Crypto	Sanction/Rush	3 BTC	Trojan.Ransomcrypt.AH
April 2016	Crypto	CryptoHost/Manamecrypt/ROI Locker	0.3 BTC	Trojan.Ransomcrypt.AI
April 2016	Crypto	Jigsaw	0.4 BTC	Trojan.Ransomcrypt.AJ
April 2016	Crypto	AutoLocky	0.75 BTC	Trojan.Ransomcrypt.AK
April 2016	Crypto	TrueCrypter	0.2 BTC	Trojan.Ransomcrypt.AL
April 2016	Locker	BrLock	Unknown	Trojan.Ransomcrypt.AQ
April 2016	Locker	Rasith	$4	W32.Ransomlock.AP
March 2016	Locker	AndroidOS_Locker	10,000 yen	Android.Lockdroid.H
March 2016	Crypto	KeRanger	1 BTC	OSX.Keranger

Discovered	Type	Common Name/Alias	Ransom Demand	Symantec Detection
March 2016	Crypto	PHP CTB-Locker	0.4 to 0.8 BTC	PHP.Cryptolocker.G
March 2016	Crypto	Cerber	1.24 to 2.48 BTC	Trojan.Cryptolocker.AH
March 2016	Crypto	Maktub	1.4 to 3.9 BTC	Trojan.Cryptolocker.AI
March 2016	Crypto	Petya	0.99 BTC	Trojan.Cryptolocker.AJ
March 2016	Crypto	Samas/SamSam	1.5 BTC	Trojan.Ransomcrypt.AE
March 2016	Crypto	Coverton	1 BTC	Trojan.Ransomcrypt.AF
March 2016	Crypto	Cryptohasyou	$300	Trojan.Ransomcrypt.AG
March 2016	Locker	Homeland Security Screen Locker	$500	Trojan.Ransomcrypt.AN
February 2016	Crypto	HydraCrypt/UmbreCrypt	0.5 to 1.5 BTC	Trojan.Cryptolocker.AE
February 2016	Crypto	Locky	0.5 to 1 BTC	Trojan.Cryptolocker.AF
February 2016	Crypto	PadCrypt	0.8 BTC	Trojan.Cryptolocker.AG
February 2016	Crypto	Job Crypter	€300	Trojan.Ransomcrypt.AC
February 2016	Crypto	RackCrypt/MVP Locker	1.3 BTC	Trojan.Ransomcrypt.AD
January 2016	Crypto	CryptoJoker	Unknown	Trojan.Cryptolocker.AC
January 2016	Crypto	7ev3n/HONE$T	13 BTC	Trojan.Cryptolocker.AD
January 2016	Crypto	DMA-Locker	1.5 to 15 BTC	Trojan.Ransomcrypt.AA
January 2016	Crypto	LeChiffre	Unknown	Trojan.Ransomcrypt.AB
January 2016	Crypto	Ransom32	0.1 BTC	Trojan.Ransomcrypt.Y
January 2016	Crypto	NanoLocker	0.1 to 1 BTC	Trojan.Ransomcrypt.Z
December 2015	Crypto	Radamant	0.5 BTC	Trojan.Ransomcrypt.W
December 2015	Crypto	Hi Buddy!	0.3 to 0.7 BTC	Trojan.Ransomcrypt.X
November 2015	Crypto	Mabouia	none	OSX.Ransomcrypt
November 2015	Crypto	CryptoWall 4.0	1.56 BTC	Trojan.Cryptodefense.B
November 2015	Crypto	CryptInfinite/DecryptorMax	$500	Trojan.Cryptolocker.AB
November 2015	Crypto	Linux.Encoder.1	Unknown	Unix.Ransomcrypt
November 2015	Crypto	Linux.Encoder.2	1 BTC	Unix.Ransomcrypt.B
October 2015	Locker	RansomFake	Unknown	JS.FakeRansom
October 2015	Crypto	Chimera	0.93 to 2.45 BTC	Trojan.Ransomcrypt.V
September 2015	Crypto	Cryakl/Vipasana	Unknown	Trojan.Ransomcrypt.U
August 2015	Crypto	ORX-Locker	0.525 BTC	Trojan.Cryptolocker.AA
August 2015	Crypto	Safefiles32	Unknown	Trojan.Cryptolocker.X
August 2015	Crypto	Hidden Tear/EDA2/Magic/Surprise	Unknown	Trojan.Cryptolocker.Y
August 2015	Crypto	CryptoApp	1 BTC	Trojan.Cryptolocker.Z
August 2015	Locker	Department of Justice (DOJ) new variant	Unknown	W32.Ransomlock.AQ!inf

Discovered	Type	Common Name/Alias	Ransom Demand	Symantec Detection
July 2015	Crypto	Encryptor RaaS	0.174 BTC	Trojan.Cryptolocker.W
June 2015	Crypto	Troldesh/Shade	1 BTC	Trojan.Ransomcrypt.T
May 2015	Crypto	Breaking Bad/El-Polocker	$450 to $1000	Trojan.Cryptolocker.S
May 2015	Crypto	Pollcrypto	1 to 2 BTC	Trojan.Cryptolocker.T
May 2015	Crypto	Tox	Random	Trojan.Cryptolocker.U
May 2015	Crypto	Locker	0.1 BTC	Trojan.Cryptolocker.V
April 2015	Crypto	PClock2	0.5 BTC	Trojan.Cryptolocker.Q
April 2015	Crypto	Kriptovor	Unknown	Trojan.Cryptolocker.R
April 2015	Crypto	Threat Finder	1.2 BTC	Trojan.Ransomcrypt.S
March 2015	Crypto	CryptoFortress	1 BTC	Trojan.Cryptolocker.H
March 2015	Crypto	Pacman	Unknown	Trojan.Cryptolocker.P
March 2015	Crypto	BandarChor	Unknown	Trojan.Ransomcrypt.Q
March 2015	Crypto	VaultCrypt/XRTN	Unknown	Trojan.Ransomcrypt.R
February 2015	Crypto	TeslaCrypt	2 BTC	Trojan.Cryptolocker.N
January 2015	Crypto	Ransomweb	Unknown	PHP.Ransomcrypt.A
January 2015	Crypto	CryptoTorLocker2015	$100 in BTC	Trojan.Cryptolocker.M
January 2015	Crypto	Pclock	1 BTC	Trojan.Ransomcrypt.P

CREDITS

Dick O'Brien, Editor
John-Paul Power, Assistant Editor
Scott Wallace, Graphics & Design

Contributors

Asim Rab
Alan Neville
Ayush Anand
Candid Wueest
Dennis Tan
Hon Lau
Jon DiMaggio
Joseph Graziano
Laura O'Brien
Orla Cox
Peter Coogan
Steve Meckl
Yek Loong Chong

Special Thanks To

Jennifer Duffourg
Mara Mort
Matt Nagel
Steve Meckl
William Wright

CHANGE LOG

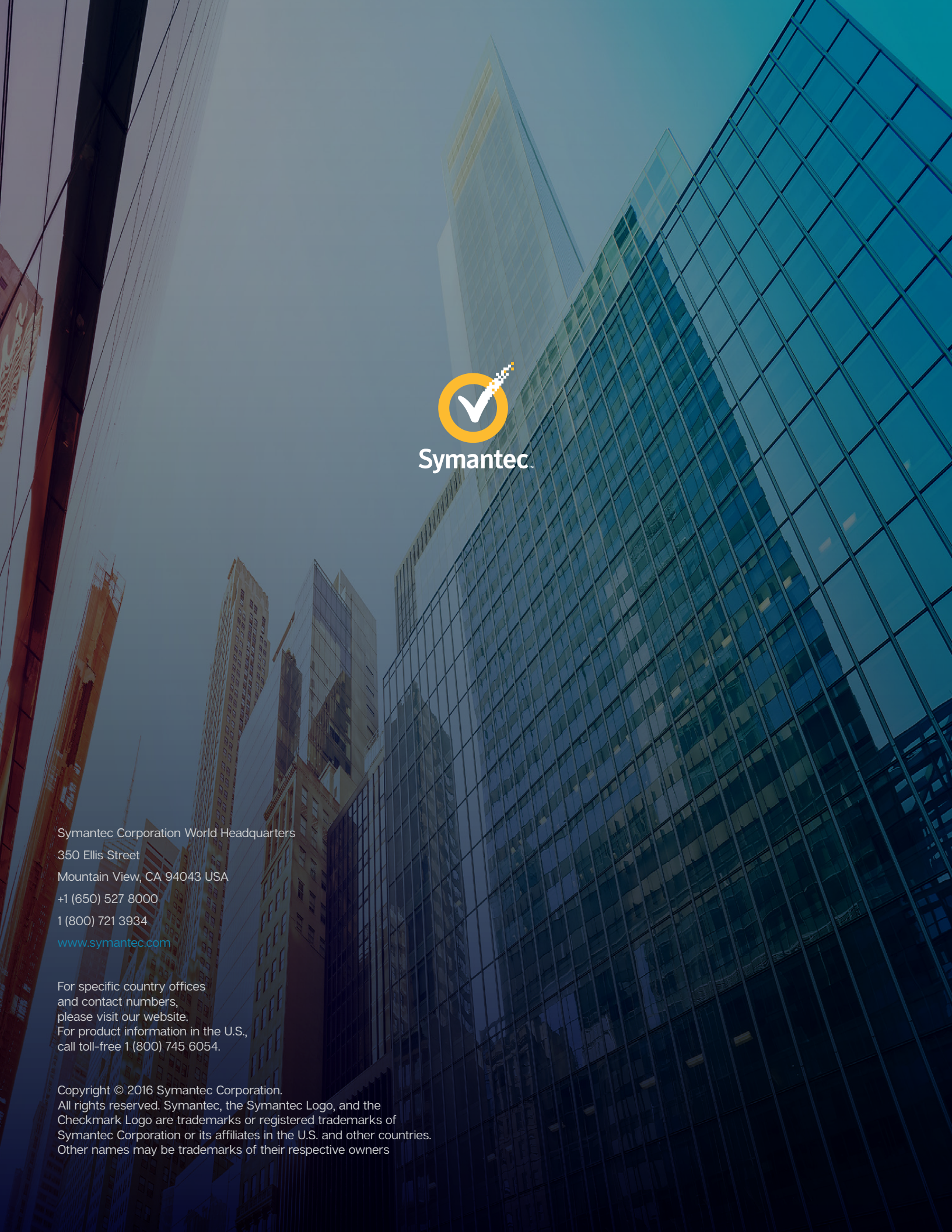
- August 10, 2016: Revised region and infection data.
- July 19, 2016: Initial publication.

ABOUT SYMANTEC

Symantec Corporation is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

MORE INFORMATION

- Symantec Worldwide: http://www.symantec.com/
- ISTR and Symantec Intelligence Resources: http://www.symantec.com/threatreport/
- Symantec Security Response: http://www.symantec.com/security_response/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/



Symantec Corporation World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

For specific country offices
and contact numbers,
please visit our website.
For product information in the U.S.,
call toll-free 1 (800) 745 6054.

Copyright © 2016 Symantec Corporation.
All rights reserved. Symantec, the Symantec Logo, and the
Checkmark Logo are trademarks or registered trademarks of
Symantec Corporation or its affiliates in the U.S. and other countries.
Other names may be trademarks of their respective owners