Internet Security Threat Report

ISTR

Ransomware 2017

An ISTR Special Report

Analyst: Dick O’Brien

July 2017

Contents

Symantec™

Internet Security Threat Report

Contents

Figures and Tables

Symantec™

Internet Security Threat Report

Executive summary and key findings

Section

00

Executive Summary

The ransomware landscape shifted dramatically this year with the appearance of two new self-propagating threats in the form of WannaCry and Petya. Both outbreaks caused global panic, catching many organizations off-guard, with infections spreading rapidly across corporate networks.

Prior to these outbreaks, the main threat posed by ransomware was from widescale malicious spam campaigns, capable of sending ransomware to millions of email addresses on a daily basis, in addition to a growing number of targeted attacks directed at organizations.

The arrival of WannaCry and Petya illustrates how malicious threats can suddenly and unexpectedly evolve and catch unprepared organizations by surprise.

The impact of these incidents will not go unnoticed on the cyber crime underground and it's likely that other groups may attempt similar tactics. Because of the nature of these attacks, organizations are particularly at risk (and were the main victims of both WannaCry and Petya). Businesses need to educate themselves about this new avenue of attack and ensure they have defenses in place.

At the same time, traditional mass-mailing ransomware attacks remain an ongoing threat; and while some spamming operations were disrupted this year, they nevertheless pose a significant risk.

Targeted ransomware attacks, involving the compromise of an organization's network and infection of multiple computers continue to pose a threat. Although less prevalent than mass mailed threats, the damage caused by a targeted attack is potentially much higher.

Ransomware is now one of the key cyber threats facing organizations and can have a major impact on their bottom line, from financial losses, disruption, and reputational damage. Attacks where dozens or even hundreds of computers are infected can leave businesses with enormous cumulative ransom demands.

However, ransom demands are not the only potential source of losses. Over the past year, a growing number of firms have gone on the record about the impact of ransomware on their businesses, with a range of major corporations citing ransomware attacks as materially affecting earnings.

Key findings

- The advent of worm-type ransomware is a new and highly disruptive avenue of attack.
- Businesses in particular are most at risk to worm-type threats, which can spread in minutes across poorly secured networks.
- During the first six months of 2017, organizations accounted for 42 percent of all ransomware infections, up from 30 percent in 2016 and 29 percent in 2015. This shift was mainly accounted for by WannaCry and Petya.
- Overall ransomware infection numbers are continuing to trend upwards, powered by the WannaCry and Petya outbreaks.
- The average ransom demand seen in new ransomware families appears to have stabilized at US$544 indicating attackers may have found their sweet spot.
- The U.S. is still the country most affected by ransomware, followed by Japan, Italy, India, Germany, Netherlands, UK, Australia, Russia, and Canada.
- After a dramatic increase in 2016, when the number of new ransomware families more than tripled, the number of new families appearing slowed in the first six months to 16.
- The drop-off in 2017 may indicate that the "gold rush" mentality among cyber criminals is beginning to abate somewhat, leaving the market to be dominated by professional ransomware gangs.

Internet Security Threat Report

Ransomware: An overview

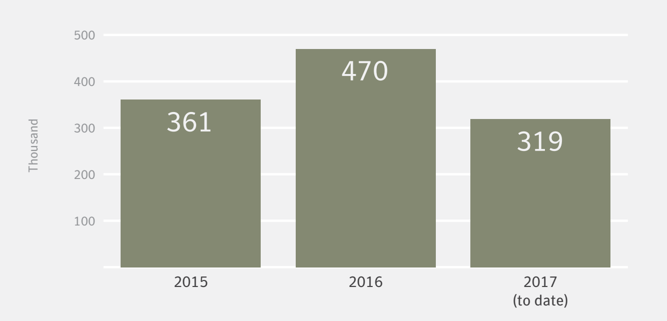
Section

01

After an increase of 36 percent between 2015 and 2016, the rate of ransomware infections seen by Symantec has continued to increase. In the first six months of 2017, Symantec blocked just over 319,000 ransomware infections. If this infection rate continued for the full year, 2017 would be a significant increase over 2016, when a total of 470,000 infections were blocked.

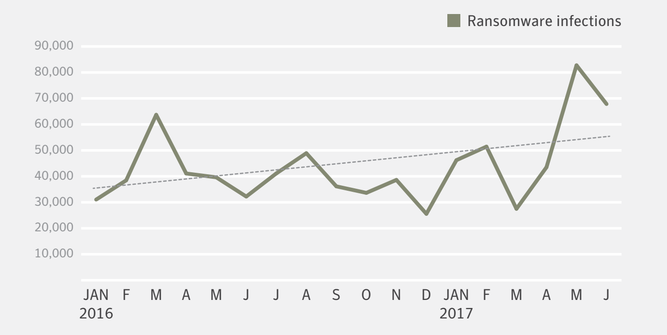
It is important to note that these detection figures represent a small fraction of the total amount of ransomware being blocked by Symantec, with the majority of attacks being blocked earlier in the infection process. For example, virtually all WannaCry infection attempts were blocked at exploit level by Symantec's Intrustion Prevention System (IPS), which prevented the ransomware from reaching the computer.

Ransomware infections by year



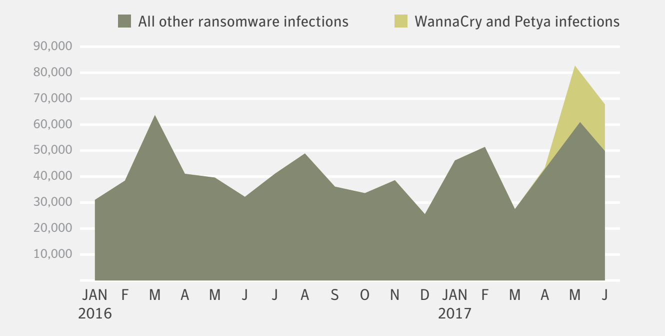
When broken down by months, the rate of infection has trended upwards between January 2016 and June 2017, with a notable increase in infections occurring in May and June 2017.

Ransomware infections by month



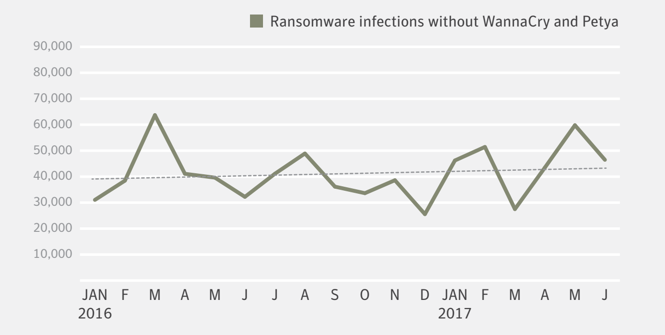
This spike in infections was in a large part due to the WannaCry and Petya outbreaks, which accounted for 28 percent of infections in May and 21 percent of infections in June.

Impact of WannaCry and Petya outbreaks on monthly infection rate

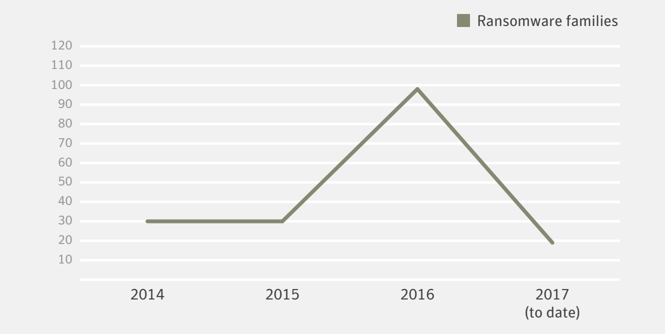


If WannaCry and Petya infection numbers were stripped out of monthly figures, the infection rate would still be moving upwards between January 2016 and June 2017, albeit at a much more gradual rate.

Monthly ransomware infection numbers without WannaCry and Petya



New ransomware families by year



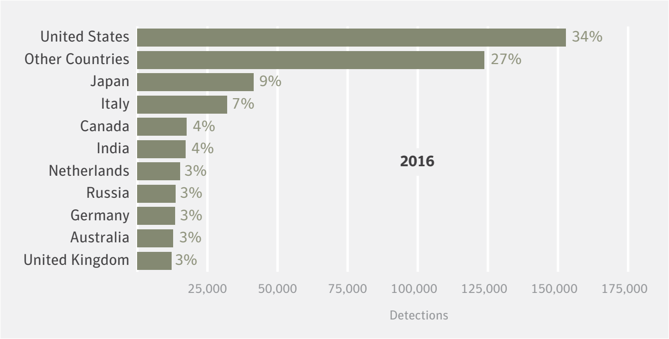
After a dramatic increase in 2016, when the number of new ransomware families more than tripled, the number of new families appearing slowed in the first six months to 16. If this rate continues for the full year, it will be a decline on 2016, but still higher than 2014 and 2015, when both years saw the emergence of 30 new ransomware families.

The number of new threats emerging in 2016 suggested that a large number of attackers were attempting to jump on the ransomware bandwagon by developing their own threats. The drop-off in 2017 may indicate that this "gold rush" mentality is beginning to abate somewhat. That doesn't mean that the threat of ransomware has reduced in any significant way, rather that many of the more opportunistic efforts at exploiting it have run their course. There are still a large number of highly active, professional ransomware developers who continue to pose a threat.

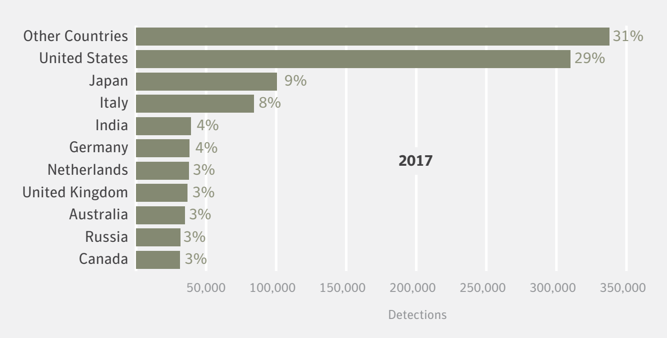
The U.S. has continued to be the region most affected by ransomware during 2017 to date, accounting for 29 percent of all infections. Japan (9 percent), Italy (8 percent), India (4 percent), and Germany (4 percent) were also heavily affected. The top 10 regions were rounded out by Netherlands (3 percent), UK (3 percent), Australia (3 percent), Russia (3 percent), and Canada (3 percent).

The top 10 regions most affected by ransomware in the first half of 2017 were identical to the top 10 in 2016. The only major difference is that the U.S. share of ransomware infections fell from 34 percent in 2016 to 29 percent in the first half of 2017. Aside from this decline, there were no other major changes and no other region moved more than one percent.

Ransomware detections by region, 2016

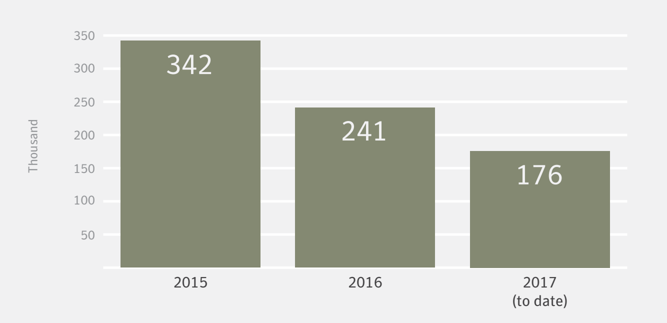


Ransomware detections by region, 2017 (to date)



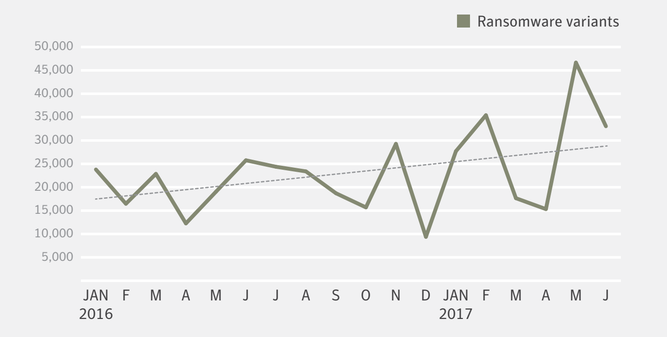
After falling between 2015 and 2016, the number of ransomware variants (i.e. distinct variants of ransomware families seen for the first time) has begun to increase again. Symantec logged 176,000 new ransomware variants in the first six months of 2017, compared to 241,000 for all of 2016.

New ransomware variants by year



The number of new ransomware variants seen has been trending upwards as the year goes on, with a notable increase particularly in May and June, the same months which saw the WannaCry and Petya outbreaks.

New ransomware variants by month



A new breed of threat: WannaCry and Petya

Section

02

On Friday May 12 2017, a new variant of the WannaCry ransomware (Ransom.Wannacry) suddenly appeared, infecting thousands of computers worldwide within a matter of hours. It was a new and particularly dangerous form of threat because of its ability to self-propagate and spread itself across an organization's network and on to other organizations via the internet.

WannaCry was not the first case of ransomware using a worm-like infection vector. For example, ZCryptor (W32.ZCrypt) was the first to display self-propagation behavior on the Windows platform. It infects all removable drives with a copy of itself before it begins encrypting, increasing its chances of spreading to other computers. A number of Android ransomware families also display worm-like behavior by spreading to all contacts on a device's address book using SMS messages.

What was significant about WannaCry was not the fact that it was a worm, rather the means it employed to spread itself—exploiting critical vulnerabilities in Windows, which had been patched two months beforehand by Microsoft.

The exploit used was known as "EternalBlue" and had been released in April, part of a series of leaks by a group known as the Shadow Brokers, who said the data had been stolen from the Equation cyber espionage group.

What is EternalBlue?

EternalBlue is the name for an exploit of a vulnerability in the Windows implementation of the Server Message Block (SMB) protocol (CVE-2017-0144). The vulnerability was the result of a flaw which allowed a remote attacker to execute arbitrary code on a targeted computer sending it specially crafted data packets.

The exploit was allegedly developed by the Equation cyber espionage group, but was part of a trove of data acquired by a mysterious group known as the Shadow Brokers, which began leaking the data in August 2016. To date there have been five separate leaks and EternalBlue was released as part of the most recent leak, on April 14, 2017.

The vulnerability was patched by Microsoft on March 13, 2017 (MS17-010), a month before EternalBlue was leaked. Nevertheless, a significant number of unpatched computers remained and were exposed to the exploit.

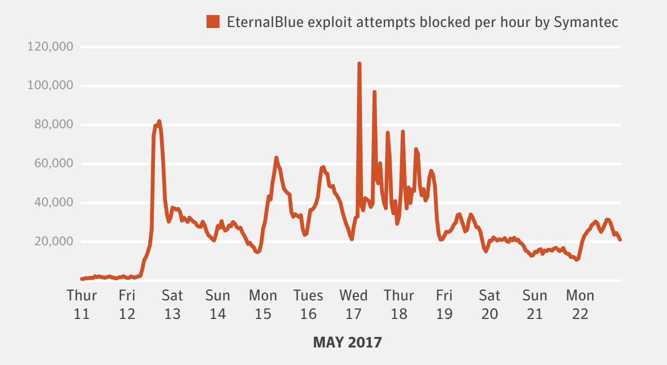
How WannaCry spread and how it was stopped

The version of WannaCry that incorporated EternalBlue first appeared on May 12 at around 6 a.m. UTC and began spreading immediately. Once it installed itself on a computer, it attempted to use the EternalBlue exploit to spread to other computers on the local network.

In addition to this, it would attempt to spread itself across the internet by scanning random IP addresses in an attempt to find other vulnerable computers. The propagation mechanism explains how WannaCry heavily affected some organizations and how it managed to jump from one organization to another.

Symantec products proactively blocked any attempt to exploit the vulnerabilities used by WannaCry, meaning customers were fully protected before WannaCry first appeared. Observing the number of exploit attempts blocked per hour gave some indication of the immediate impact. In the day leading up to the outbreak, barely any blocked exploits were registered. However, from midday on May 12, the number of exploits blocked jumped almost immediately to a rate of around 80,000 per hour.

Number of EternalBlue exploit attempts blocked by Symantec per hour



The number of exploit attempts began to drop after the first 24 hours, largely because of the discovery of a "kill switch", which effectively halted the spread of WannaCry. When it is installed on a computer, WannaCry attempts to contact a specific domain. If it the domain is unavailable, it continues with its encrypting files and attempting to spread to other computers. However, if the domain is contactable, the malware halts installation.

This kill switch feature was discovered later on May 12 by a security researcher, who promptly registered the domain and caused WannaCry to stop spreading. Triggering the kill switch resulted in an immediate drop in exploit attempts blocked by Symantec, which quickly fell off to between 20,000 and 30,000

Who was behind the WannaCry attacks?

In the days and weeks following the WannaCry outbreak, evidence began to emerge as to who was behind the attack. While most ransomware is spread by ordinary cyber criminal gangs, it became apparent that WannaCry may have come from a different source.

Some key evidence emerged from investigation of an earlier version of WannaCry, which was used in a small number of targeted attacks in February, March, and April. This earlier version was quite similar to one used in May, the main difference being that it didn't use EternalBlue as a propagation mechanism, but instead relied on stolen credentials to spread across infected networks.

The tools and infrastructure used in those early attacks in particular were found to have strong links to Lazarus, a group that has been involved in a string of operations in recent years, including the destructive attacks on Sony Pictures in November 2014 and the theft of US$81 million from the Bangladesh Bank, the nation's central bank, in February 2016.

After the first WannaCry attack in February, three pieces of malware linked to Lazarus were discovered on the victim's network: Trojan.Volgmer and two variants of Backdoor.Destover, a disk-wiping tool also used in the Sony Pictures attacks.

The March and April attacks yielded further links to Lazarus. In these attacks, two different backdoors were used to deploy WannaCry: Trojan.Alphanc and Trojan.Bravonc. Alphanc is a modified version of Backdoor.Duuzer, which has previously been linked to Lazarus. Bravonc meanwhile used the same IP addresses for command and control as Duuzer and Destover.

There were also commonalities between WannaCry itself and other known Lazarus tools. For example, Bravonc and Infostealer.Fakepude (which has also been linked to Lazarus) used similar code obfuscation to WannaCry. There was also shared code between WannaCry and another Lazarus tool: Backdoor.Contopee.

While Lazarus was originally linked to cyber espionage type attacks, it appears to have branched out in recent years to include financially motivated attacks. While the attack on the Bangladesh Bank was highly lucrative, the group's venture into ransomware was less so and managed to generate more publicity than profits.

attempts, likely mostly accounted for by existing WannaCry infections. The number of exploit attempts spiked periodically again in subsequent days as copycat attacks began to be seen.

Poor implantation, poor returns

Making the kill switch so easy to find was one of a series of mistakes the attackers made which served to limit the damage caused by WannaCry and limit their profits. The ransomware was configured to generate a unique Bitcoin wallet address for each infected computer. However due to a race condition bug this code did not execute correctly. WannaCry defaulted to using three hardcoded Bitcoin addresses for payment. This meant the attackers were unable to identify which victims have paid.

> Making the kill switch so easy to find was one of a series of mistakes the attackers made which served to limit the damage caused by WannaCry and limit their profits.

The three wallets accumulated more than US$140,000 in payments but were left untouched for almost three months after the attack. Since Bitcoin payments are publicly recorded and anyone who knows a wallet's address can see what payments enter and leave a wallet, there was some speculation that the glare of publicity had prompted the attackers to abandon the money.

However, the wallets were eventually emptied in early August. It is not clear yet where the money was moved to.

Petya: Different threat, similar tactics

Given the impact of the WannaCry outbreak, it was only a matter of time before similar attacks were attempted and that eventually happened on June 27, when a new variant of the Petya ransomware (Ransom.Petya) appeared and managed to infect hundreds of organizations.

Although not identical, the tactics used in this Petya outbreak were quite similar to WannaCry and likely inspired by the earlier outbreak. Petya also used the EternalBlue exploit as a propagation mechanism, but also incorporated other SMB network spreading techniques, which meant it could spread within organizations to computers that have been patched against EternalBlue.

While WannaCry was designed to spread indiscriminately, Petya was far more targeted. It appeared to be designed to mainly affect organizations in Ukraine and, while it spread to other countries, this appears to be more collateral damage rather than by design.

How Petya was spread

Petya is not a new threat and earlier versions were circulating for at least a year before the June 2017 attack. The version used in these most recent attacks was adapted to include a self-propagation mechanism.

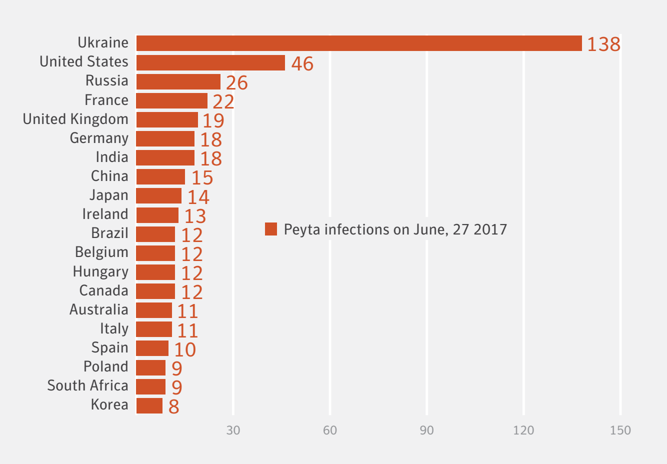
The initial means of infection was via a Trojanized version of MEDoc, a tax and accounting software package that is widely used in Ukraine. The attackers managed to compromise the MEDoc website and Trojanized a software update.

Once installed on a computer within an organization, Petya began building a list of IP addresses to spread to. This mainly involved internal addresses, but also included external IP addresses:

- All IP addresses and DHCP servers of all network adaptors
- All DHCP clients of the DHCP server if ports 445/139 are open
- All IP addresses within the subnet as defined by the subnet mask if ports 445/139 are open
- All computers you have a current open network connection with
- All computers in the ARP cache
- All resources in Active Directory
- All server and workstation resources in Network Neighborhood
- All resources in the Windows Credential Manager (including Remote Desktop Terminal Services computers)

While WannaCry attempted to spread to random external IP addresses, Petya selected external IP addresses that were in some way linked to the organization already infected. This, combined with the initial MEDoc infection vector, ensured that Ukraine was the country most affected by the attack.

Petya infection numbers on June 27 2017, with Ukraine the most heavily affected country



With a list of IP addresses compiled, Petya then attempted to build a list of credentials (user names and passwords) that it can use to spread to these IP addresses. It built the list by stealing credentials, both from the Windows Credential Manager and also by dropping and executing a credential dumper.

Armed with this information, Petya then began spreading itself, using two methods. The first was through the aforementioned EternalBlue exploit and the related EternalRomance SMB exploit, also patched by Microsoft on March 13 2017 (MS17-010). The second method involved copying itself to targeted computers using the stolen credentials. This second means of spreading meant that Petya could also copy itself to computers that were patched against EternalBlue. Interestingly, Petya actually checked for the presence of Symantec and Norton software on targeted computers and, if found, didn't attempt to use EternalBlue and EternalRomance, indicating the attackers were aware that the exploits wouldn't work on computers secured by Symantec products.

Ransomware or wiper?

Once it spread to other computers, Petya began the encryption process. It first modified the master boot record (MBR), allowing it to hijack the normal loading process of the infected computer during the next system reboot.

It then scanned the disk for 65 different file types and encrypted any it found. The key was encrypted with an embedded public key, Base64 encoded, and appended to a README.TXT file.

After a system reboot occurs, a second form of encryption takes place. Here the infected MBR is loaded and encryption of the entire disk begins, followed by display of a ransom note to the user. This ransom note displays an "installation key" which is a randomly generated string. A randomly generated Salsa20 key is then used for disk encryption.

However, the disk can never be decrypted, since there is no actual relationship between the “installation key” and Salsa20 key. Petya, in effect, is disk-wiping malware rather than classic ransomware. Even if the victim paid the ransom, they wouldn’t recover their files.

Ransomware as a political tool

With the arrival of WannaCry, it became apparent that ransomware was no longer solely the preserve of cybercrime groups. Petya provided further evidence of this. From the outset, there were signs that the attack wasn’t financially motivated. To start with, the attack appeared designed to mainly target Ukraine, whereas a conventional cyber crime operation would attempt to spread the ransomware as widely as possible. Secondly, the timing of the attack was interesting, occurring on June 27, the day before Ukraine’s Constitution Day, a national holiday.

This information, combined with the fact that Petya wasn’t really ransomware (since the infected computers could never be decrypted), led Symantec to conclude that the Petya outbreak was politically motivated, designed to cause disruption in Ukraine.

This was not the first time Ukraine was targeted with destructive malware attacks. Disk-wiping malware was used against targets in Ukraine in January 2016 and again in December of that year, attacks which also resulted in power outages.

Petya was also not the first time that ransomware was used as “cover” for a different sort of attack. Symantec Incident Response last year investigated what appeared to be a mass ransomware infection at a large company. Initially it appeared that hundreds of the firm’s computers had been infected with a variant of Ransom.Cryptowall.

When 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, named Trojan.Phonywall, wasn’t real ransomware and was instead a disk wiper.

It transpired that the fake ransomware attack was staged to cover up a cyber espionage attack. The attackers had compromised the company five months previously, stealing thousands of files before attempting to cover up their activity with a fake ransomware attack.

A new template for attacks?

The rapid spread and publicity generated by both WannaCry and Petya make it quite likely that more attackers will attempt to the replicate tactics used by deploying ransomware as a worm.

Straightforward copycat attacks are unlikely to have as wide an impact as WannaCry and Petya. This is largely down to the fact that awareness of the threat posed by the EternalBlue exploit is now quite high and most organizations will have patched any vulnerable computers.

However, that is not to say that there is a significant potential threat from ransomware attackers adopting similar tactics. While EternalBlue made self-propagation quite easy, the Petya attacks proved that there are alternative methods of self-propagation. Although these methods may not be quite as easy or as effective as EternalBlue, in the hands of skilled attackers, they nevertheless could cause significant disruption to unprepared organizations.

> With the arrival of WannaCry, it became apparent that ransomware was no longer solely the preserve of cybercrime groups. Petya provided further evidence of this.

Internet Security Threat Report

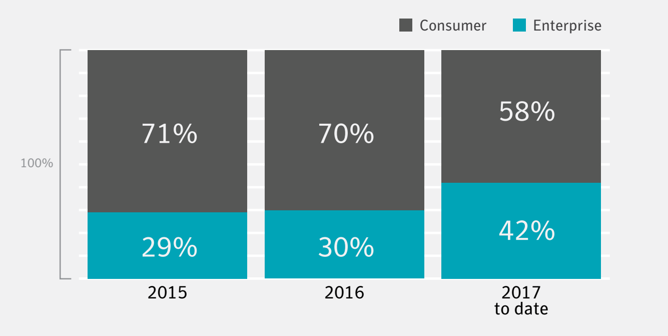
Businesses in the crosshairs

Section

03

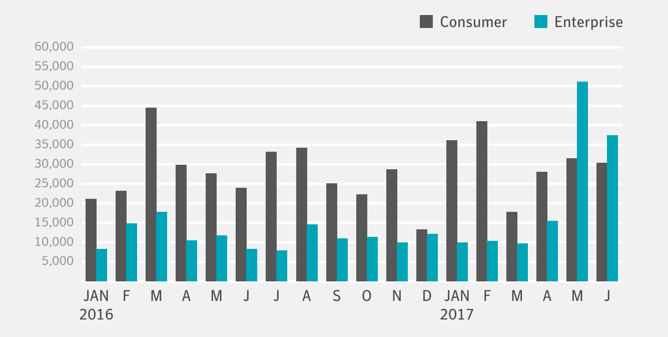
For the past number of years consumers are the most likely victims of ransomware, usually accounting for two-thirds of all infections. For example, in 2015 the proportion of consumer infections was 71 percent. This fell only marginally to 70 percent in 2016. That balance has shifted dramatically during 2017, with enterprises now far more exposed to ransomware. In the first six months of this year, 42 percent of all ransomware infections blocked by Symantec occurred at enterprises.

Consumer vs enterprise, blocked ransomware infections, 2015–2017 to date



The reason for this major increase in the number of blocked enterprise infections can be seen when the figures are broken down on a monthly basis. Enterprise infections jumped dramatically during May and June of 2017, the months when WannaCry and Petya hit.

Consumer vs enterprise ransomware infections, 2017 to date



Why were enterprises and other organizations disproportionally affected by WannaCry and Petya? The worm-like propagation mechanisms employed by both ransomware families (see previous chapter) were designed to enable the ransomware to spread quickly across an entire computer network. Many consumer computers are not connected to a network, unlike those found in organizations.

While WannaCry and Petya also did have the ability to spread across the internet to other vulnerable computers, this means of transmission again largely affected other organizations. Most home internet routers would have blocked infection attempts involving the EternalBlue exploit.

Organizations need to be aware of the threat posed by this new breed of ransomware. The Petya outbreak demonstrated that even without the shortcut of an exploit like EternalBlue, attackers can create self-propagating ransomware that is capable of spreading across an entire network. It does require the use of additional tools, such as credential stealers, which will yield the user names and passwords needed to spread to other computers on a network. This requires more skill and time on the part of attackers, but the potential rewards are much greater. Encrypting hundreds of computers in a single organization, particularly if they aren't backed up, could prove crippling for the victim, who may be faced with a steep ransom demand.

Worms are not the only threat

While worm-type ransomware such as WannaCry and Petya has dominated the headlines this year, it is far from the only ransomware threat affecting businesses. The most prevalent form of ransomware continues to be traditional crypto ransomware delivered through massive spam campaigns (see "How ransomware is spread" chapter).

Most of these spam campaigns are indiscriminate and are simply sent to as many email addresses as possible, regardless of whether they're owned by individuals or organizations. Many campaigns are disguised as routine correspondence, such as invoices or delivery notifications. Since most businesses receive a high volume of similar, albeit legitimate emails from customers and suppliers, malicious emails could be inadvertently opened if they aren't blocked by email security software. While the majority of campaigns are indiscriminate, some are targeted, such as to certain organizations or to individual countries.

Targeted ransomware attacks

Another threat which specifically affects organizations is targeted ransomware attacks, where the attackers select their target in advance and attempt to cause the maximum disruption possible in the hope of a big ransom payout.

Many of these targeted ransomware attacks display a high degree of technical competence and use similar tactics to those used by cyber espionage groups, such as:

- "Living off the land"—using freely available, legitimate network administration software and operating system features to help gain a foothold and move through a network
- Stealing credentials and using them for lateral movement
- Conducting advance reconnaissance to learn more about the target's network in order to spread the infection as widely as possible

Perhaps the most notable example of targeted ransomware attacks to emerge in recent years is SamSam (Ransom.SamSam). The attackers behind SamSam will generally attempt to gain a foothold on the victim's network by finding a weak spot in its defenses, such as an unpatched vulnerability on a public-facing web server.

Once the attackers are on the network, they use publicly available tools, such as Microsoft Sysinternals utilities to traverse it and map every accessible computer and identify the most valuable assets to target.

The attackers will then use a batch script to deploy SamSam, along with a public encryption key to each targeted computer. The attackers also go to great lengths to remove any backups that may exist, thus maximizing the potential impact of the attack. The script will delete volume shadow copies from targeted computers, preventing any files from being restored from them following infection. The attackers may also distribute a tool called sqlsrvtmg1.exe, which searches for any running backup processes and stops them. It also deletes any backup-related files it finds.

Finally, another batch script is used which begins the encryption process on all infected computers before the ransomware deletes itself, leaving only the encrypted files and a ransom note demanding a ransom of 1.5 Bitcoin (US$5,324 at the time of writing) for each infected computer. With SamSam capable of infecting hundreds of computers in a targeted organization, the total ransom demand will quickly add up.

SamSam is not the only targeted ransomware group in operation. Mamba (Ransom.HDDCryptor) has a similar modus operandi and attackers compromise the victim's network before infecting selected computers (for more details see "Major Ransomware Threats" chapter).

Another targeted threat is Bucbi (Ransom.Bucbi), which has been used to compromise RDP servers. Once the attackers gain access to a victim's network, they use the RDP server for lateral movement and can spend some time on reconnaissance, learning about the organization's backup policies, for example.

Once 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 by leaving a note and is instead done using email, allowing the criminals to negotiate a higher amount by leveraging the information they obtained during their reconnaissance.

> Many of these targeted ransomware attacks display a high degree of technical competence and use similar tactics to those used by cyber espionage groups

Some targeted ransomware threats are designed specifically to compromise servers. For example, Ransomweb (PHP.Ransomweb) will wait for several months post-compromise before it demands payment. The delay occurs because it 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.

Prevention is possible, a cure may not be

One of the key messages organizations should take from the wave of recent attacks is to avoid complacency. For example, simply patching against EternalBlue may not block all worm-type threats. Similarly, backing up doesn't inoculate you against the threat of ransomware, since attackers may play the long game and attempt to encrypt all backups as well.

Organizations need to adopt a multi-layered approach to security in order to best ensure that any point of failure is mitigated by other defensive practices. That should include not only regularly patching vulnerabilities and ensuring critical systems are backed up, but also employing multiple, overlapping, and mutually supportive defensive systems to guard against singlepoint failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability with malware protection, and web security gateway solutions throughout the network.

Internet Security Threat Report

Affecting the bottom line: Impact of ransomware

Section

04

Symantec.

Ransomware is one of the most costly threats that can affect an organization. Modern crypto ransomware families use strong encryption that puts any encrypted files out of reach unless a decryption key is obtained, leaving any organization without back-ups with the unpalatable choice of losing important data or paying a ransom to cyber criminals (with no guarantee that the attackers will keep their promise and provide a decryption key).

The potential costs don't stop there. A ransomware attack, particularly one that affects multiple computers on a network, can cause significant disruption, resulting in lost productivity, missed deadlines, and cleanup costs. This can result in reputational damage, particularly if the cause of the disruption becomes public, leading to lost business. In some cases, organizations have acknowledged that ransomware attacks have had a material impact on their bottom line.

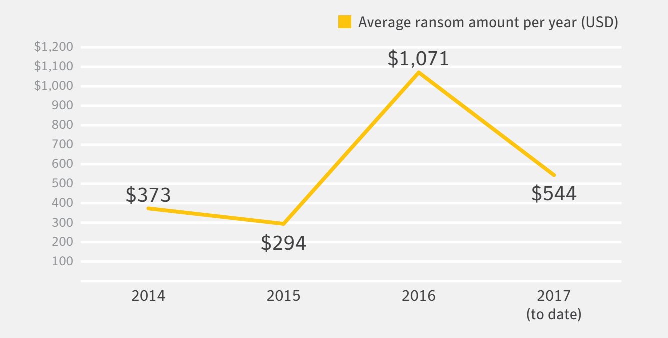
A ransom demand of $500 may not sound like a lot to even a small company, but organizations need to bear in mind that the average demand relates to a single infection. Attacks where dozens or even hundreds of computers are infected will have a far higher cumulative ransom demand.

Ransom demands stabilize

During 2016, the average ransom demand seen in new ransomware families increased dramatically, rising more than threefold from US$294 to $1,077. Perhaps motivated by the belief that that much more could be extracted from potential victims, attackers appeared to up the ante during 2016 in search of the highest possible return.

Since then, the average ransom demand has declined and, for the first six months of 2017, the average demand seen in new ransomware families was $544. Although considerably down from the 2016 figure, it is still nevertheless 85 percent up on the 2015 figure and, after a period of trial and error, attackers may be settling on around $500 as the "sweet spot" for ransom demands.

Average ransom amount in US dollars, by year



A ransom demand of $500 may not sound like a lot to even a small company, but organizations need to bear in mind that the average demand relates to a single infection. Attacks where dozens or even hundreds of computers are infected will have a far higher cumulative ransom demand.

Financial and reputational damage

As the ransomware epidemic grew, there was no shortage of anecdotal evidence about firms opting to pay ransom demands. However, over the past year, a growing number of companies have gone on the record to publicly acknowledge the impact of ransomware on their businesses.

For example, earlier this year South Korean web hosting firm Nayana was hit with a Linux version of the Erebus (Ransom.Erebus) ransomware that saw more than 153 Linux servers encrypted. As a result, more than 3,400 customer websites were knocked offline. Acknowledging the attack, Nayana said that the attackers had demanded a ransom of 550 Bitcoin (approximately US$1.62 million at the time). Several days later, Nayana said that it had negotiated the ransom down with the attackers, agreeing to pay 397 Bitcoin (approximately $1 million). It is believed to be the largest reported ransomware payout to date.

Nayana has not been alone in feeling the brunt of ransomware attacks. Delivery giant FedEx announced in July that the Petya outbreak will have an impact on its full year results. The company's stock price fell by over three percent immediately after the announcement.

FedEx said its Netherlands-based subsidiary TNT Express was heavily hit by Petya and was still experiencing delays as the cleanup operation continued. As a result, TNT was processing decreased volumes and incurring increased costs from remediation. FedEx added that it didn't have insurance to cover losses from a cyber attack. The company is due to report full year results in September.

Petya in particular appeared to have a heavy impact on corporates. Danish shipping giant AP Moller-Maersk said that Petya will cost it up to US$300 million in lost revenues. Announcing second quarter results on August 16, the company warned that its third quarter numbers would be affected by Petya.

"Business volumes were negatively affected for a couple of weeks in July and as a consequence, our Q3 results will be impacted. We expect that the cyber-attack will impact results negatively by $200 million to $300 million," said AP Moller-Maersk Group CEO Søren Skou.

German consumer products maker Beiersdorf said the attack had impacted its half-year results, due to delays in shipping and production caused by the attack. It estimated that €35 million (US$41 million) in second-quarter sales were delayed to the third quarter as a result.

Meanwhile, chocolate maker Mondelez International, which is known for Oreos and Cadbury chocolates, estimated that the attack would shrink second quarter sales growth by three percent (subscription link) due to disruptions to shipping and invoices.

Pharmaceutical firm Reckitt Benckiser said it expected sales would be reduced by approximately £110 million (US$142 million) this year. It was projecting a second quarter sales drop of two percent, cutting annual revenue growth by a full percentage point.

How many people pay?

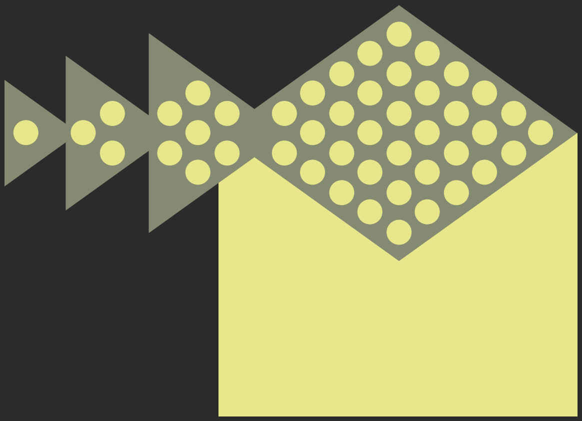
According to research carried out by the Norton Cyber Security Insight team, 34 percent of victims will pay the ransom. This proportion rises to 64 percent of victims in the U.S., providing some indication as to why the country is so heavily targeted.

Willingness to pay the ransom is likely a factor in the growth and persistence of ransomware. Ransom payment has also become easier to manage. To encourage victims to pay, attackers often now offer support on how to pay the fee—and the wider availability of payment broker services makes it even easier to use Bitcoin—especially now that Bitcoin is not as obscure as it used to be.

> According to research carried out by the Norton Cyber Security Insight team, 34 percent of victims will pay the ransom. This proportion rises to 64 percent of victims in the US, providing some indication as to why the country is so heavily targeted.

Internet Security Threat Report

How ransomware is spread



Section

05

Ransomware is spread through a range of different means, aka infection vectors. Despite some disruptions to malicious distribution services, email continues to be the primary distribution channel for ransomware. Exploit kits and, more recently, self-propagation in the form of worm-type ransomware are also used along with a range of more niche vectors. Understanding where ransomware comes from is a key step in building an organization's defenses against it. Blocking threats at the source, before they have an opportunity to download themselves to computers inside a network, is one of the most effective means of protection.

Email: Main source of menace

One of the main distribution channels for ransomware is through massive malicious spam campaigns. This spam is distributed using botnets—networks of compromised computers, ranging from hundreds to millions of infected computers. Many of these botnets are capable of sending out large spam runs on a daily basis, most of which use simple 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, which subsequently downloads and installs the ransomware. JavaScript downloaders which launch malicious PowerShell commands have been widely used this year, but other forms of downloader, including Office macros are also used.
- Clicks a link that initiates a download and installation of the ransomware. Social engineering is usually used to trick the user into clicking the link.
- Clicks a link that points to an exploit kit which will ultimately lead to the malware being installed on the computer

Disruption

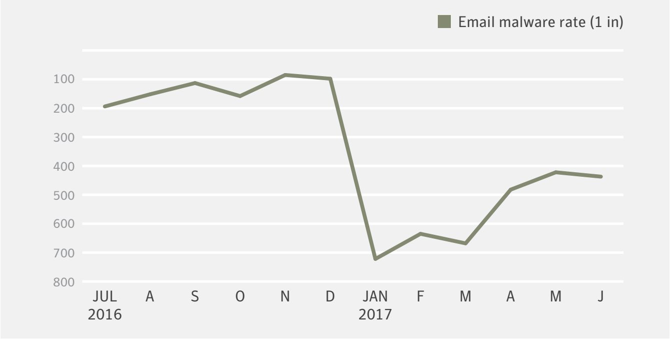
With well-resourced botnets pumping out millions of spam emails daily, email was the dominant source of ransomware during 2016. While it remains a major threat during 2017, malicious email distributors have experienced some disruption in the first half of the year, meaning activity is behind 2016 levels.

One of the main disruptions seen was to the Necurs botnet (Backdoor.Necurs), which was one of the biggest distributors of malware during 2016, running massive spam campaigns spreading the Locky ransomware (Ransom.Locky), among other threats. Necurs ceased operating on December 24 2016 and, initially it appeared that its controllers were taking a break for the holiday period (not uncommon among cyber criminals). However, Necurs remained silent for almost three months, leading to some speculation that it had disappeared entirely. The botnet resumed operations in late March 2017. When it returned, it was involved in pump-and-dump stock scams, although by April, the botnet was once again distributing ransomware. The reason for its long absence remains unknown.

> With well-resourced botnets pumping out millions of spam emails daily, email was the dominant source of ransomware during 2016.

The impact of Necurs going silent was immediately apparent. During December 2016, the last month Necurs was active, one in 98 emails blocked by Symantec contained malware. In January 2017 the email malware rate dropped precipitously to one in 772. Since Necurs resumed operations in March, the email malware rate has steadily climbed and the increase may be linked to Necurs' return. However, email malware rates are still not at the same level as seen in the latter part of 2016.

Email malware rate (one in) seen by Symantec, which dropped significantly after Necurs went offline in late December 2016



Exploit kits

Second only to email, exploit kits were, for a long time, one of the main infection vectors for ransomware. However, exploit kit operators have suffered a series of setbacks in recent times and the proportion of ransomware being delivered by exploit kits has fallen.

Exploit kits work by exploiting 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 exploit kits in a number of different ways:

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

During 2016, there was a significant drop in exploit kit activity. Symantec logged a 60 percent decrease in exploit kit detections, a fall which was driven, in part, by the disappearance of a number of major exploit kit operators during the year.

The Angler exploit kit, which was the most widely seen exploit kit at the beginning of 2016, suddenly dropped off the map from June 2016 onwards. This development coincided with the arrest of 50 people in Russia accused of involvement with the Lurk banking fraud group. Although not confirmed, it is widely believed that the two events were linked.

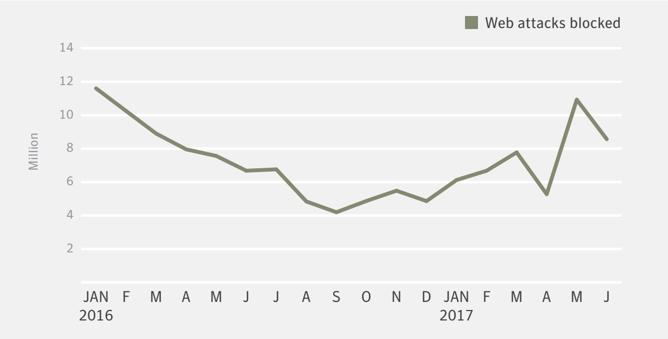
Angler wasn't the only exploit kit to disappear. Another major operator, the Nuclear exploit kit, also disappeared at around the same time, most likely due to research that was published which shed light on the toolkit's infrastructure and likely led to disruptions.

Neutrino, which was for a brief period of time one of the most widely used exploit kits, disappeared completely in April 2017. Its disappearance was prefigured by a decision in September 2016 to scale back activity and only work with selected customers.

Despite numerous disruptions, exploit kit activity has by no means ceased completely and, at the time of writing, the RIG exploit kit was one of the most active exploit kit operations involved in spreading ransomware.

The number of web attacks blocked by Symantec declined during 2016, indicative of the fall in exploit kit activity. Web attack activity has begun to rise again during May and June of 2017. At present it is too early to say how much of this recent increase involves ransomware being spread by exploit kits.

Web attacks blocked by Symantec per month



Despite numerous disruptions, exploit kit activity has by no means ceased completely and, at the time of writing, the RIG exploit kit was one of the most active exploit kit operations involved in spreading ransomware.

Other infection vectors

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

- **Self-propagation:** As discussed earlier, new variants of WannaCry and Petya employed self-propagation to dramatic effect. They were not the first ransomware families to employ this technique and it has previously been used by ZCryptor (W32.ZCrypt), which infects all removable drives with a copy of itself before it begins encrypting files. In addition to this, a number of Android ransomware families display worm-like behavior by spreading to all contacts on a device's address book using SMS messages.
- **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.
- **Brute-forcing passwords:** An emerging tactic for spreading ransomware is by way of brute-forcing login credentials for software used on servers. The attackers behind Bucbi (Ransom.Bucbi) use this method to gain a foothold on remote desktop protocol (RDP) servers. Bucbi then encrypts files on computers and other servers that the RDP server has access to.
- **Exploiting server vulnerabilities:** Attackers have also been seen targeting vulnerable software running on servers to gain access to an organization's network.
  The gang behind the SamSam ransomware (Ransom.SamSam) use freely available tools to find and exploit vulnerabilities to spread their malware throughout the network.
  In addition to this, the Linux.Encoder (Unix.LinuxEncoder) ransomware family targets Linux web servers. 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.
- **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.

Major ransomware threats

Section

06

Cerber

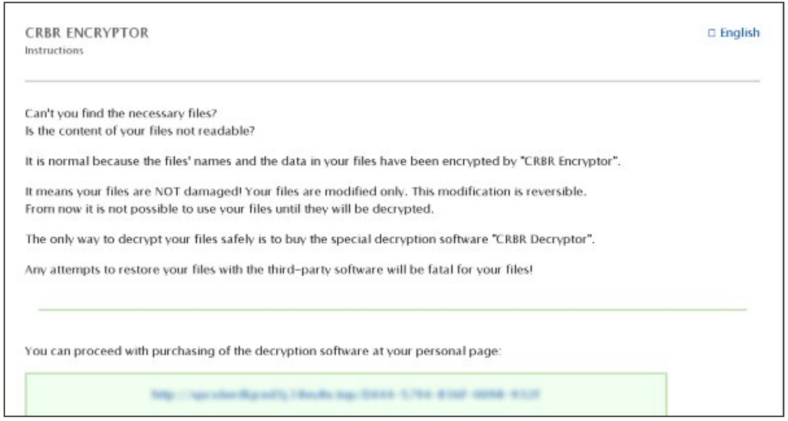
Detection name: Ransom.Cerber

Most recently seen ransom amount: 0.5 bitcoin ($2,000 on August 2017 rates. Ransom demands vary over time.)

Discovery: March 2016

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

Appearing first in March 2016, Cerber has emerged as one of the most widely spread ransomware families over the past year, distributed through spam and exploit kit campaigns. Spam campaigns have employed JavaScript (JS.Downloader) and Word macro (W97M.Downloader) downloaders, in addition to a number of campaigns where Cerber was delivered directly as a zipped attachment. Recent variants have incorporated additional functionality in the form of a Bitcoin wallet-stealing feature.



CRBR ENCRYPTOR
Instructions

□ English

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "CRBR Encryptor".

It means your files are NOT damaged! Your files are modified only. This modification is reversible.
From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "CRBR Decryptor".

Any attempts to restore your files with the third-party software will be fatal for your files!

You can proceed with purchasing of the decryption software at your personal page:

[redacted]

Cerber ransom note

Jaff

Detection name: Ransom.Jaff

Most recently seen ransom amount: 0.356 bitcoin ($1,467 on August 2017 rates. Ransom demands vary over time.)

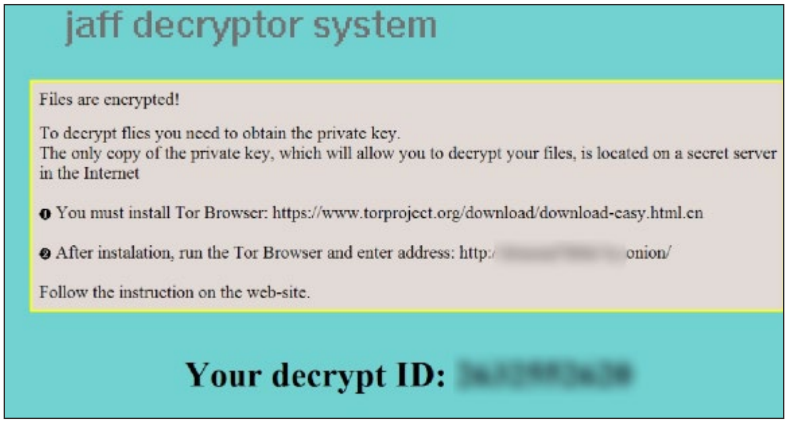
Discovery: May 2017

Known infection vectors: Spam campaigns

Jaff is a relatively recent arrival on the ransomware landscape but made an immediate impact. It is being spread by major malicious spam campaigns mounted via the Necurs botnet. The ransomware is downloaded by a malicious macro which is itself dropped by a .pdf file attached to the spam email.

Early variants of the ransomware appended encrypted files with a .jaff file extension. More recent variants use an extension of .sVn.

Interestingly, before it begins encrypting files, Jaff checks the language setting of the infected computer. If it finds that it is Russian, it will delete itself.



jaff decryptor system

Files are encrypted!

To decrypt flies you need to obtain the private key.
The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet

❶ You must install Tor Browser: https://www.torproject.org/download/download-easy.html.en

❷ After instalation, run the Tor Browser and enter address: http:/[redacted]onion/

Follow the instruction on the web-site.

Your decrypt ID: [redacted]

Jaff ransom note

Sage

Detection name: Ransom.Cry

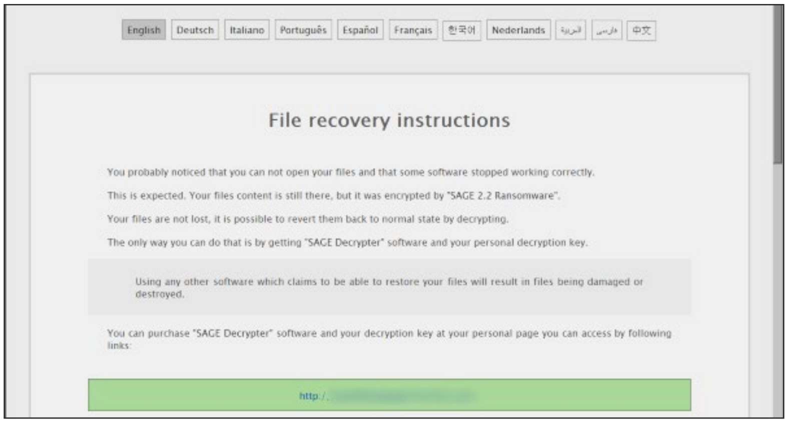
Most recently seen ransom amount: $2,000 in bitcoin

Discovery: September 2016

Known infection vectors: Spam campaigns, botnets, RIG exploit kit

Sage is an evolution of older ransomware known as CryLocker. It has been highly active over the past year and has been distributed through a wide variety of channels including the Trojan.Pandex spamming botnet, the Trik botnet, and the RIG exploit kit.

Ransom demands have varied over time, but recent versions have requested the equivalent of $2,000 in bitcoin. Like Cerber, it offers multiple-language support in its ransom note.



File recovery instructions

You probably noticed that you can not open your files and that some software stopped working correctly.

This is expected. Your files content is still there, but it was encrypted by "SAGE 2.2 Ransomware".

Your files are not lost, it is possible to revert them back to normal state by decrypting.

The only way you can do that is by getting "SAGE Decrypter" software and your personal decryption key.

Using any other software which claims to be able to restore your files will result in files being damaged or destroyed.

You can purchase "SAGE Decrypter" software and your decryption key at your personal page you can access by following links:

http:/. [redacted]

Sage ransom note

GlobeImposter

Detection name: Ransom.GlobeImposter

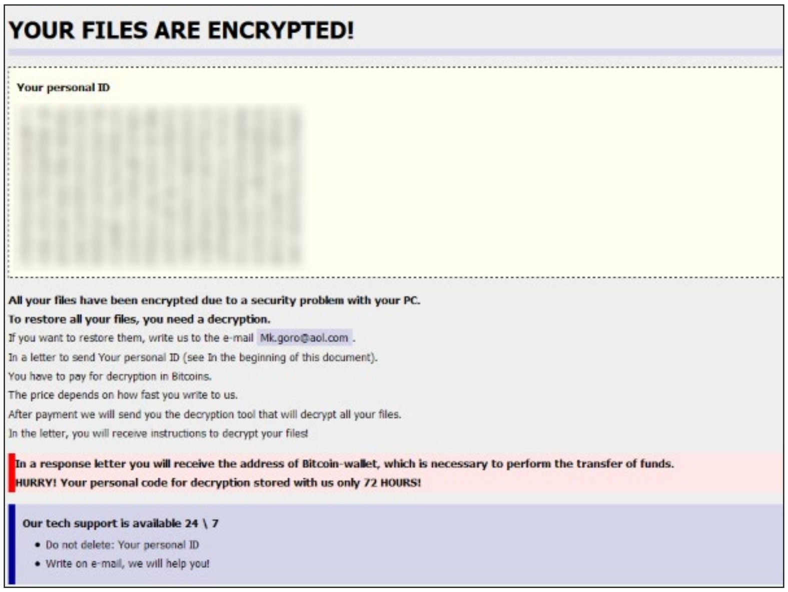
Most recently seen ransom amount: 0.35 bitcoin ($1,401 on August 2017 rates. Ransom demands vary over time.)

Discovery: May 2017

Known infection vectors: Spam campaigns

Another recent arrival, GlobeImposter has managed to make an impact due to its being distributed by a major malicious spamming operation known as Blank Slate, which has been linked in recent times to a number of ransomware families.

GlobeImposter began by encrypting files with the .crypt file extension, but reports indicate that it is now using as many as 20 different file extensions.



YOUR FILES ARE ENCRYPTED!

Your personal ID

[redacted]

All your files have been encrypted due to a security problem with your PC.
To restore all your files, you need a decryption.
If you want to restore them, write us to the e-mail Mk.goro@aol.com .
In a letter to send Your personal ID (see In the beginning of this document).
You have to pay for decryption in Bitcoins.
The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.
In the letter, you will receive instructions to decrypt your files!

In a response letter you will receive the address of Bitcoin-wallet, which is necessary to perform the transfer of funds.
HURRY! Your personal code for decryption stored with us only 72 HOURS!

Our tech support is available 24 \ 7

- Do not delete: Your personal ID
- Write on e-mail, we will help you!

GlobeImposter ransom note

Locky

Detection name: Ransom.Locky

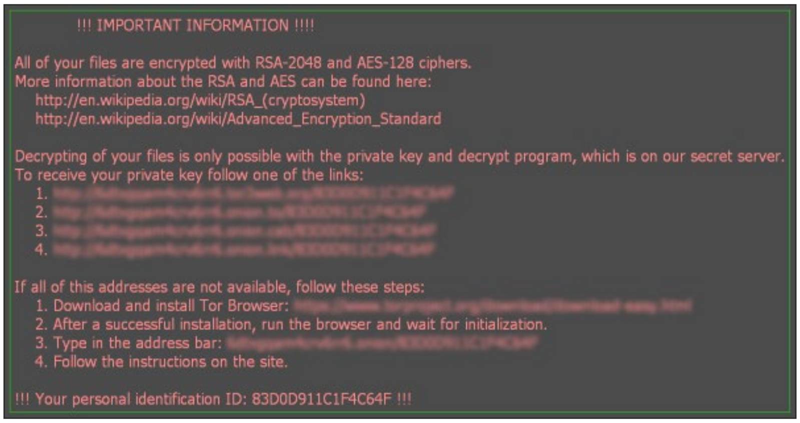
Most recently seen ransom amount: 0.49 bitcoin ($1,963 on August 2017 rates. Ransom demands vary over time.)

Discovery: February 2016

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

Appearing first in early 2016, Locky has been an ongoing ransomware menace. The malware is mainly spread through major spam campaigns, but Locky has also been distributed through a number of exploit kits at times.

Locky has experienced periodic dips in activity, such as when the Necurs spamming botnet went quiet in early 2017, but invariably reappears with new campaigns seen as recently as August 2017.



```
          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. [redacted]
    2. [redacted]
    3. [redacted]
    4. [redacted]

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: [redacted]
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: [redacted]
    4. Follow the instructions on the site.

!!! Your personal identification ID: 83D0D911C1F4C64F !!!
```

Locky ransom note

Mamba

Detection name: Ransom.HDDCryptor

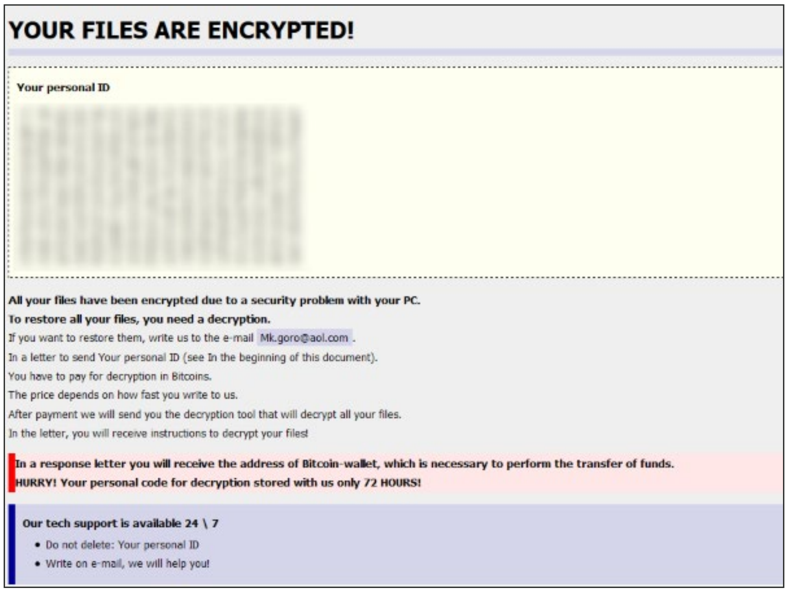
Most recently seen ransom amount: Variable

Discovery: September 2016

Known infection vectors: Targeted attacks involving network compromise

An example of the kind of targeted ransomware being deployed against organizations, the attackers first compromise the victims network before using publicly available tools, such as Microsoft Sysinternals utilities to traverse it and install Mamba on targeted computers. Rather than encrypt selected files, Mamba instead opts for encryption of the entire hard disk.

Mamba was linked to the attack on San Francisco's light rail system, Muni in November 2016, where attackers reportedly demanded $73,000. The ransomware is reportedly still being used in targeted attacks during 2017.



YOUR FILES ARE ENCRYPTED!

Your personal ID

[redacted]

All your files have been encrypted due to a security problem with your PC.
To restore all your files, you need a decryption.
If you want to restore them, write us to the e-mail Mk.goro@aol.com .
In a letter to send Your personal ID (see In the beginning of this document).
You have to pay for decryption in Bitcoins.
The price depends on how fast you write to us.
After payment we will send you the decryption tool that will decrypt all your files.
In the letter, you will receive instructions to decrypt your files!

In a response letter you will receive the address of Bitcoin-wallet, which is necessary to perform the transfer of funds.
HURRY! Your personal code for decryption stored with us only 72 HOURS!

Our tech support is available 24 \ 7

- Do not delete: Your personal ID
- Write on e-mail, we will help you!

Mamba ransom note

Internet Security Threat Report

Protection and best practices

Section

07

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

01 Prevent

02 Contain

03 Respond

01 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 among the most common infection vectors for ransomware, but organizations must also be aware of the new generation of self-propagating ransomware which spreads across networks using stolen credentials and exploiting vulnerabilities. Adopting a robust defense against all of 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 endpoints from this threat by removing malicious content from attached documents before they even reach the user. Disarm is particularly effective against targeted attacks, sterilizing all active content in emails. It removes all active content from attachments such as Microsoft Office documents and PDFs, including macros and JavaScript. A digital carbon copy of the active content is created and attached to the email instead, meaning the endpoint is never exposed to the original malicious conent.

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 exploiting vulnerabilities, preventing the installation of ransomware. Symantec Endpoint Protection (SEP) and Norton with IPS enabled proactively blocked any attempt to exploit the vulnerabilities used by WannaCry and Petya, meaning customers were fully protected even before WannaCry first appeared.

Proactive Exploit Protection

Symantec Proactive Exploit Protection (PEP) recognizes a range of malicious behaviors that are common in exploit attacks and blocks exploit activity.

In addition, Memory Exploit Mitigation (MEM) further enhances zero-day protection capabilities by hardening the operating system.

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.

Download Insight automatically computes reputation and rating of files, URLs, and websites using the 'wisdom of crowds' (analytics). It classifies every program that it encounters as either good or bad.

Browser Protection

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

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.

02 Contain

In the event of a payload arriving on a computer, 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 is investing in Response Operations to specifically address ransomware and now has a dedicated team focused on ransomware protection.

Advanced antivirus engine

Symantec uses an array of detection engines including an advanced antivirus engine with heuristics, just-in-time (JIT) memory scanning, machine-learning engines, and emulator. The emulator enables the engine to heuristically detect encryption behavior without needing a signature. Together with Auto Protect, it will detect ransomware files when they hit the disk, bypassing the packers and encryptors employed to evade static detection technologies.

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. It also employs machine learning to block programs that exhibit combinations of thousands of different suspicious behaviors.

Sapient – machine learning

Sapient is Symantec's enhanced machine learning heuristic technology. It has been trained to specifically target ransomware. Sapient automatically blocked 92 percent of ransomware samples seen in the last year without cloud support enabled and that figure increased to 100 percent blocked with cloud support. In the case of brand-new ransomware families, Sapient blocked 40 percent without cloud support enabled and 100 percent with cloud support.

Symantec's machine learning proved its worth during the WannaCry outbreak. In cases where customers didn't have IPS enabled (which blocked the exploit used), Symantec Endpoint Protection (SEP) 14 proactively blocked all WannaCry infections on day zero, without requiring any updates.

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.

Ongoing development

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.

03 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 which have been repeat victims of ransomware attacks.

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 practices

Backing up important data is one of the key pillars of combating ransomware infections. However, as there have 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 discovered since January 2016, along with Symantec's detection names for them. Note that ransom demands are those logged at time of discovery.

Discovered	Type	Common name/Alias	Ransom demand	Symantec detection
July 2017	Crypto	Karo	Ransom.Karo	$500 in BTC
July 2017	Crypto	FakeCry	Ransom.Fakecry	0.1 BTC
July 2017	Crypto	HakunaMatata / NM4 / Nmoreira	Ransom.Haknata	Unknown
June 2017	Crypto	BTCWare	Ransom.BTCware	Unknown
June 2017	Crypto	Sorebrect / XDATA / AES-NI	Ransom.Sorebrect	Unknown
June 2017	Crypto	Erebus	Ransom.Erebus	1 BTC
May 2017	Crypto	GlobeImposter	Ransom.GlobeImposter	0.085 BTC
May 2017	Crypto	Jaff	Ransom.Jaff	0.356 BTC
May 2017	Crypto	UIWIX	Ransom.Uiwix	$200 in BTC
May 2017	Crypto	WannaCry	Ransom.Wannacry	$300 in BTC
April 2017	Crypto	Mole	Ransom.Mole	Unknown
March 2017	Crypto	Vortex	Ransom.Vortex	$199
February 2017	Crypto	OSX Patcher	OSX.Ransom	0.25
February 2017	Crypto	Ishtar	Ransom.Ishtar	Unknown
February 2017	Crypto	Hermes	Ransom.Hermes	Unknown
February 2017	Crypto	Lambda	Ransom.Lambdalocker	0.5 BTC
January 2017	Crypto	Spora	Ransom.Spora	Unknown
January 2017	Crypto	Evil	Ransom.Evil	Unknown
January 2017	Crypto	FireCrypt / BleedGreen	Ransom.Firecrypt	$500
December 2016	Crypto	Goldeneye	Ransom.Goldeneye	1.33 BTC
November 2016	Locker	YeeScrLocker	Ransom.YeeScrLocker	Unknown
November 2016	Crypto	OzozaLocker	Ransom.OzozaLocker	1 BTC
November 2016	Crypto	PrincessLocker	Ransom.PrincessLocker	3 BTC
November 2016	Crypto	Crypton	Ransom.Crypton	0.2 to 2 BTC
November 2016	Locker	Ransoc	Ransom.Ransoc	Amount varies
November 2016	Locker	Survey Ransomware	Ransom.PCsurveyLocker	To complete a survey
November 2016	Crypto	Telecrypt	Ransom.Telecrypt	5000 RUB
November 2016	Crypto	MasterBuster	Ransom.MasterBuster	$52 = 3500 Rupees
October 2016	Crypto	JapanLocker / shc Ransomware	Ransom.SHCLocker	Unknown
October 2016	Crypto	Google Go Ransomware	Ransom.Googo	0.0523 BTC

Discovered	Type	Common name/Alias	Ransom demand	Symantec detection
October 2016	Crypto	CryPy	Ransom.CryPy	Unknown
October 2016	Crypto	DXXD	Ransom.DXXD	Unknown
October 2016	Crypto	HadesLocker	Ransom.HadesLocker	1 BTC
September 2016	Crypto	Xpan	Ransom.Xpan	1 BTC
September 2016	Crypto	Nagini	Ransom.Nagini	asks for CC number
September 2016	Crypto	MarsJoke	Ransom.MarsJoke	0.6 BTC
September 2016	Crypto	HDDCrypto/ Mamba	Ransom.HDDCryptor	Unknown
September 2016	Crypto	Philadelphia	Ransom.Philadelphia	0.3 BTC
September 2016	Crypto	Kawaii	Ransom.Kawaii	$100 / 6000 Roubles
September 2016	Crypto	Cry	Ransom.Cry	1.13 BTC
September 2016	Crypto	FSociety	Ransom.Fsociety	n/a
September 2016	Crypto	Serpico / Detox	Ransom.Serpico	$56 / 50 Euro
August 2016	Crypto	Domino	Ransom.Domino	1 BTC
August 2016	Crypto	Fantom	Ransom.Fantom	Unknown
August 2016	Crypto	KaoTear	Ransom.KaoTear	Unknown
August 2016	Crypto	Globe / Purge	Ransom.Purge	Unknown
August 2016	Crypto	AlmaLocker	Ransom.AlmaLocker	Unknown
August 2016	Locker	Hitler-Ransomware	Ransom.Hit	25 Euro Vodafone Card
August 2016	Crypto	Shark RaaS / Atom	Ransom.SharkRaaS	Unknown
August 2016	Crypto	Smrss32	Ransom.SMRSS32	1 BTC
August 2016	Locker	Fake Windows Activation Scam	Ransom.SupportScam.C	n/a
July 2016	Crypto	PowerWare new variant	Ransom.PowerWare.B	0.74 BTC
July 2016	Crypto	Stampado	Ransom.Stampado	Unknown
July 2016	Crypto	HolyCrypt	Ransom.HolyCrypt	Unknown
July 2016	Crypto	LEIA / Brazilian Ransomware	Ransom.LEIA	Unknown
July 2016	Crypto	JuicyLemon	Ransom.JuicyLemon	2.5 BTC
June 2016	Crypto	Pizzacrypt	Ransom.Pizzacrypt	Unknown
June 2016	Crypto	Apocalypse	Ransom.Apocalypse	Unknown
June 2016	Crypto	Satana	Ransom.Satana	0.5 BTC
June 2016	Crypto	MIRCOP / Guy Fawkes	Ransom.MIRCOP	48.48 BTC
June 2016	Crypto	BART	Ransom.BART	3 BTC
June 2016	Crypto	DEDCryptor	Ransom.DEDCryptor	2 BTC
June 2016	Crypto	RAA	JS.RansomRAA	0.39 BTC

Discovered	Type	Common name/Alias	Ransom demand	Symantec detection
June 2016	Crypto	My-Little-Ransomware / cuteRansomware	Ransom.MyLittleRansom	n/a
June 2016	Crypto	Zyklon / Wildfire	Ransom.Zyklon	0.5 BTC
June 2016	Crypto	Nemucod Ransomware	Ransom.Nemucod.B	0.32 BTC
June 2016	Crypto	Crysis	Ransom.Crysis	€400 to €900 in BTC
June 2016	Crypto	ODCODC	Ransom.ODCODC	$500
June 2016	Crypto	BlackShades	Ransom.BlackShades	0.07 BTC
May 2016	Crypto	zCrypt	W32.Zcrypt	1.2 BTC
May 2016	Crypto	Bloccato	Ransom.Bloccato	5 BTC
May 2016	Crypto	BadBlock	Ransom.BadBlock	2 BTC
May 2016	Crypto	777 / Ninja.Gaiver	Ransom.777	Unknown
May 2016	Locker	Rogue.TechSupportScam	Ransom.SupportScam.B	Unknown
May 2016	Crypto	CryptoHitman	Ransom.CryptoHitman	$150 in BTC
May 2016	Crypto	Shujin	Ransom.Shujin	Unknown
May 2016	Crypto	Mischa	Ransom.Mischa	1.93 BTC
May 2016	Crypto	Mobef / Yakes	Ransom.Mobef	4 BTC
May 2016	Crypto	Enigma	Ransom.Enigma	0.42 BTC
May 2016	Crypto	Bucbi	Ransom.Bucbi	0.5 BTC
May 2016	Crypto	MM Locker	Ransom.MMLocker	1.01 BTC
May 2016	Crypto	Alpha Locker	Ransom.AlphaLocker	$400 in iTunes Card
April 2016	Locker	BrLock	Ransom.BrLock	Unknown
April 2016	Crypto	TrueCrypter	Ransom.TrueCrypter	0.2 BTC
April 2016	Crypto	Yougothacked	Ransom.Yougothacked	0.5 BTC
April 2016	Crypto	Nemucod 7-Zip	Ransom.Nemucod	0.52 BTC
April 2016	Crypto	CryptXXX / UltraDeCrypter / CrypMic	Ransom.CryptXXX	$500 in BTC
April 2016	Crypto	Kovter	Ransom.Kovter.B	Unknown
April 2016	Crypto	AutoLocky	Ransom.AutoLocky	0.75 BTC
April 2016	Crypto	Jigsaw	Ransom.Jigsaw	$40 in BTC
April 2016	Crypto	CryptoHost / Manamecrypt / ROI Locker	Ransom.CryptoHost	0.3 BTC
April 2016	Crypto	Sanction / Rush	Ransom.Sanction	3 BTC
April 2016	Crypto	KimcilWare	PHP.KimcilWare	1 BTC
April 2016	Crypto	Zeta / CryptoMix / CryptFile2	Ransom.CryptoMix	Unknown
April 2016	Crypto	Rokku	Ransom.Rokku	0.24 BTC
April 2016	Locker	Rasith	W32.Rasith	$4

Back to Table of Contents

Discovered	Type	Common name/Alias	Ransom demand	Symantec detection
March 2016	Crypto	Cryptohasyou	Ransom.Cryptohasyou	$300
March 2016	Crypto	Petya	Ransom.Petya	0.99 BTC
March 2016	Crypto	Coverton	Ransom.Coverton	1 BTC
March 2016	Locker	Homeland Security Screen Locker	Ransom.FakeDHS	$500 in BTC
March 2016	Crypto	Maktub	Ransom.Maktub	1.4 BTC
March 2016	Locker	AndroidOS_Locker	Android.Lockdroid.H	10.000 Japanese yen
March 2016	Crypto	KeRanger	OSX.Keranger	1 BTC
March 2016	Crypto	Cerber	Ransom.Cerber	1.24 BTC
March 2016	Crypto	PHP CTB-Locker	PHP.CTBLocker	0.4 BTC
March 2016	Crypto	Samas / SamSam	Ransom.SamSam	1.5 BTC
February 2016	Crypto	PadCrypt	Ransom.PadCrypt	0.8 BTC or Ukash/PaySafeCard
February 2016	Crypto	Locky / Zepto	Ransom.Locky	1 BTC
February 2016	Crypto	HydraCrypt / UmbreCrypt	Ransom.UmbreCrypt	1.5 BTC
February 2016	Crypto	RackCrypt / MVP Locker	Ransom.MVPLocker	1.3 BTC
February 2016	Crypto	Job Crypter	Ransom.JobCrypter	€300 Pay Safe Card
January 2016	Crypto	7ev3n / HONE$T	Ransom.Seven	13 BTC
January 2016	Crypto	LeChiffre	Ransom.LeChiffre	Unknown
January 2016	Crypto	DMA-Locker	Ransom.DMALocker	15 BTC
January 2016	Crypto	NanoLocker	Ransom.NanoLocker	1.01 BTC
January 2016	Crypto	CryptoJoker	Ransom.CryptoJoker	Unknown
January 2016	Crypto	Ransom32	Ransom.Ransom32	1 BTC

Back to Table of Contents

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure.

Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats.

Symantec Worldwide: http://www.symantec.com

ISTR and Symantec Intelligence Resources: https://www.symantec.com/security-center/threat-report

Symantec Security Center: https://www.symantec.com/security-center

Norton Security Center: https://us.norton.com/security-center

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043
United Stated of America

+1 650 527–8000
+1 800 721–3934

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.

08/17