Internet Security Threat Report

ISTR

April 2017

Volume

22

Contents

Contents

Symantec

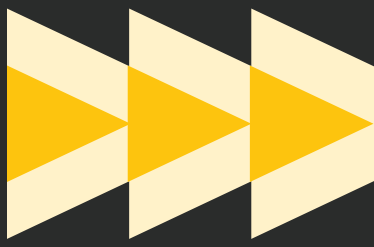
Graphics, tables, and charts

Symantec

Introduction

Section

00



Symantec

Symantec has established the largest civilian threat collection network in the world, and one of the most comprehensive collections of cyber security threat intelligence through the Symantec Global Intelligence Network™. The Symantec Global Intelligence Network tracks over 700,000 global adversaries and records events from 98 million attack sensors worldwide. This network monitors threat activities in over 157 countries and territories through a combination of Symantec products, technologies, and services, including Symantec Endpoint Protection™, Symantec DeepSight™ Intelligence, Symantec Managed Security Services™, Norton™ consumer products, and other third-party data sources, generating more than nine trillion rows of security data.

In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 88,900 recorded vulnerabilities (spanning more than two decades) from 24,560 vendors representing over 78,900 products.

Analysis of spam, phishing, and email malware trends is gathered from a variety of Symantec security technologies processing more than 2 billion emails each day, including: Skeptic™, Symantec Messaging Gateway for Service Providers, Symantec CloudSOC, and the Symantec Probe Network. Skeptic™ is the Symantec Email and Web Security.cloud™ proprietary heuristic technology, filtering more than 336 million emails, and over 2.4 billion web requests each day. Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and partners.

Symantec Cloud Threat Labs provides the detailed analysis of cloud-based threats and risks, and is developed using data from Symantec CloudSOC security technology, which in 2016 safeguarded more than 20,000 cloud apps, 176 million cloud documents, and 1.3 billion emails. Symantec CloudSOC is the company's Cloud Access Security Broker (CASB) solution, and is designed to provide visibility, control, and protection for cloud-based apps and data.

Symantec Web Application Firewall & Reverse Proxy scans one billion previously unseen web requests daily.

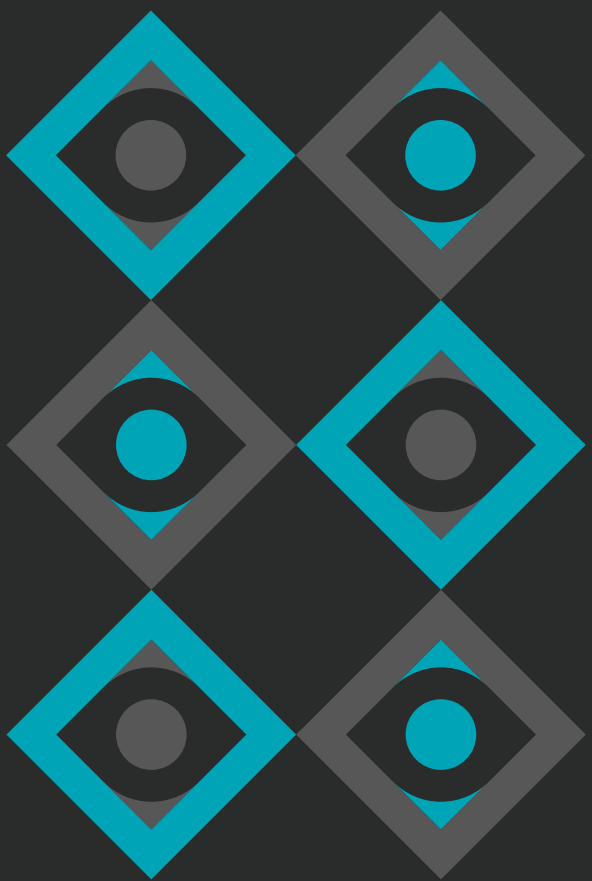
Symantec Website Security secures 1.4 million web servers worldwide with 100 percent availability since 2004. The validation infrastructure processes over 15.7 billion Online Certificate Status Protocol (OCSP) look-ups per day, which are used for obtaining the revocation status of X.509 digital certificates around the world.

These resources give Symantec analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec Internet Security Threat Report™, which gives enterprises, small businesses, and consumers essential information to secure their systems effectively now and into the future.

Executive summary

Section

01



Symantec

Cyber attackers revealed new levels of ambition in 2016, a year marked by extraordinary attacks, including multi-million dollar virtual bank heists, overt attempts to disrupt the US electoral process by state-sponsored groups, and some of the biggest distributed denial of service (DDoS) attacks on record powered by a botnet of Internet of Things (IoT) devices.

While cyber attacks managed to cause unprecedented levels of disruption, attackers frequently used very simple tools and tactics to make a big impact. Zero-day vulnerabilities and sophisticated malware now tend to be used sparingly and attackers are increasingly attempting to hide in plain sight. They rely on straightforward approaches, such as spear-phishing emails and "living off the land" by using whatever tools are on hand, such as legitimate network administration software and operating system features.

Mirai, the botnet behind a wave of major DDoS attacks, was primarily composed of infected routers and security cameras, low-powered and poorly secured devices. In the wrong hands, even relatively benign devices and software can be used to devastating effect.

Targeted attacks: Subversion and sabotage come to the fore

The world of cyber espionage experienced a notable shift towards more overt activity, designed to destabilize and disrupt targeted organizations and countries. Cyber attacks against the US Democratic Party and the subsequent leak of stolen information were one of the major talking points of the US presidential election. With the US Intelligence Community attributing the attacks to Russia and concluding the campaign would have been judged a success, it is likely these tactics will be reused in efforts to influence politics and sow discord in other countries.

Cyber attacks involving sabotage have traditionally been quite rare, but 2016 saw two separate waves of attacks involving destructive malware. Disk-wiping malware was used against targets in Ukraine in January and again in December, attacks which also resulted in power outages. Meanwhile the disk-wiping Trojan Shamoon reappeared after a four-year absence and was used against multiple organizations in Saudi Arabia.

The upsurge in disruptive attacks coincided with a decline in some covert activity, specifically economic espionage, the theft of intellectual property, and trade secrets. Following a 2015 agreement between the US and China, which saw both countries promise not to conduct economic espionage in cyber space, detections of malware linked to suspected Chinese espionage groups dropped considerably. However, this does not mean economic espionage has disappeared entirely and comes at a time when other forms of targeted attack, such as subversion or high-level financial attacks, have increased.

Financial heists: Cyber attackers chase the big scores

Until recently, cyber criminals mainly focused on bank customers, raiding accounts or stealing credit cards. However, a new breed of attacker has bigger ambitions and is targeting the banks themselves, sometimes attempting to steal millions of dollars in a single attack. Gangs such as Carbanak have led the way, demonstrating the potential of this approach by pulling off a string of attacks against US banks.

During 2016, two other outfits upped the ante by launching even more ambitious attacks. The Banswift group managed to steal US$81 million from Bangladesh's central bank by exploiting weaknesses in the bank's security to infiltrate its network and steal its SWIFT credentials, allowing them to make the fraudulent transactions.

Another group, known as Odinaff, was also found to be mounting sophisticated attacks against banks and other financial institutions. It too appeared to be using malware to hide customers' own records of SWIFT messages relating to fraudulent transactions carried out by the group.

While Banswift and Odinaff demonstrated some technical expertise and employed tactics associated with advanced groups, much less sophisticated groups also stole massive sums of money. Business email compromise (BEC) scams, which rely on little more than carefully composed spear-phishing emails, continue to cause major losses; more than $3 billion has been stolen in the past three years.

Living off the land

Attackers ranging from cyber criminals to state-sponsored groups have begun to change their tactics, making more use of operating system features, off-the-shelf tools, and cloud services to compromise their victims. The most high-profile case of a living off the land attack took place during the US elections. A simple spear-phishing email provided access to Hillary Clinton's campaign chairman John Podesta's Gmail account without the use of any malware or vulnerabilities.

"Living off the land"—making use of the resources at hand rather than malware and exploits—provides many advantages to attackers. Identifying and exploiting zero days has become harder as improvements in secure development and bounty programs take hold. Web attack toolkits have fallen out of favor, likely due to the effort required in maintaining fresh exploits and a backend infrastructure.

Powerful scripting tools, such as PowerShell and macros, are default features of Windows and Microsoft Office that can facilitate remote access and malware downloads without the use of vulnerabilities or malicious tools. Despite existing for almost 20 years, Office macros have reemerged on the threat landscape as attackers use social engineering techniques to easily defeat security measures that were put in place to tackle the erstwhile problem of macro viruses.

When executed well, living off the land approaches can result in almost symptomless infections, allowing attackers to hide in plain sight.

Resurgence of email as favored attack channel

Malicious emails were the weapon of choice for a wide range of cyber attacks during 2016, used by everyone from state-sponsored cyber espionage groups to mass-mailing ransomware gangs. One in 131 emails sent were malicious, the highest rate in five years.

Email's renewed popularity has been driven by several factors. It is a proven attack channel. It doesn't rely on vulnerabilities, but instead uses simple deception to lure victims into opening attachments, following links, or disclosing their credentials. Spear-phishing emails, such as spoofed emails instructing targets to reset their Gmail password, were used in the US election attacks.

Malicious emails disguised as routine correspondence, such as invoices or delivery notifications, were meanwhile the favored means of spreading ransomware. The availability of spam botnets-for-hire, such as Necurs, allowed ransomware groups to mount massive email campaigns during 2016, pumping out hundreds of thousands of malicious emails daily.

Ransomware squeezing victims with escalating demands

Ransomware continues to plague businesses and consumers, with indiscriminate campaigns pushing out massive volumes of malicious emails. In some cases, organizations can be overwhelmed by the sheer volume of ransomware-laden emails they receive. Attackers are demanding more and more from victims with the average ransom demand in 2016 rising to $1,077, up from $294 a year earlier.

Attackers have honed a business model that usually involves malware hidden in innocuous emails, unbreakable encryption, and anonymous ransom payment involving cryptocurrencies. The success of this business model has seen a growing number of attackers jump on the bandwagon. The number of new ransomware families uncovered during 2016 more than tripled to 98 and Symantec logged a 36 percent increase in ransomware infections.

New frontiers: IoT and cloud move into the spotlight

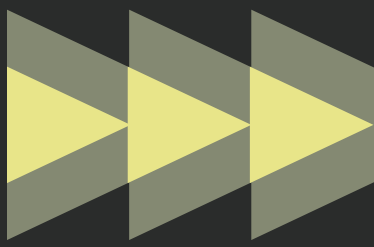
While ransomware and financial fraud groups continue to pose the biggest threat to end users, other threats are beginning to emerge. It was only a matter of time before attacks on IoT devices began to gain momentum, and 2016 saw the first major incident with the emergence of Mirai, a botnet composed of IoT devices such as routers and security cameras. Weak security made these devices easy pickings for attackers, who constructed a botnet big enough to carry out the largest DDoS attack ever seen. Symantec witnessed a twofold increase in attempted attacks against IoT devices over the course of 2016 and, at times of peak activity, the average IoT device was attacked once every two minutes.

Several of Mirai's targets were cloud-related services, such as DNS provider Dyn. This, coupled with the hacking of millions of MongoDB databases hosted in the cloud, shows how cloud attacks have become a reality and are likely to increase in 2017. A growing reliance on cloud services should be an area of concern for enterprises as they present a security blind spot. Symantec found that the average organization was using 928 cloud apps, up from 841 earlier in the year. However, most CIOs think their organizations only use around 30 or 40 cloud apps, meaning the level of risk could be underestimated, leaving them open to attack from newly emergent threats.

Big numbers

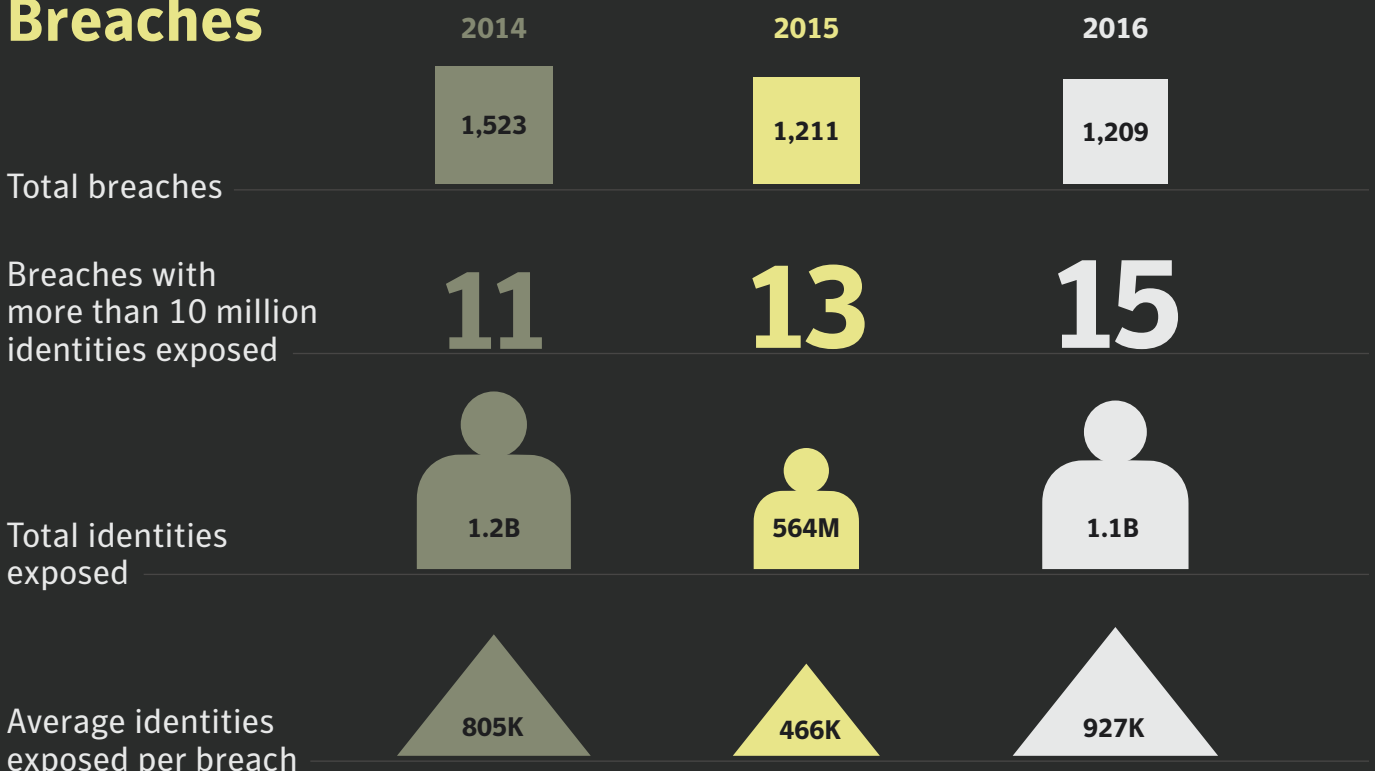
Section

02



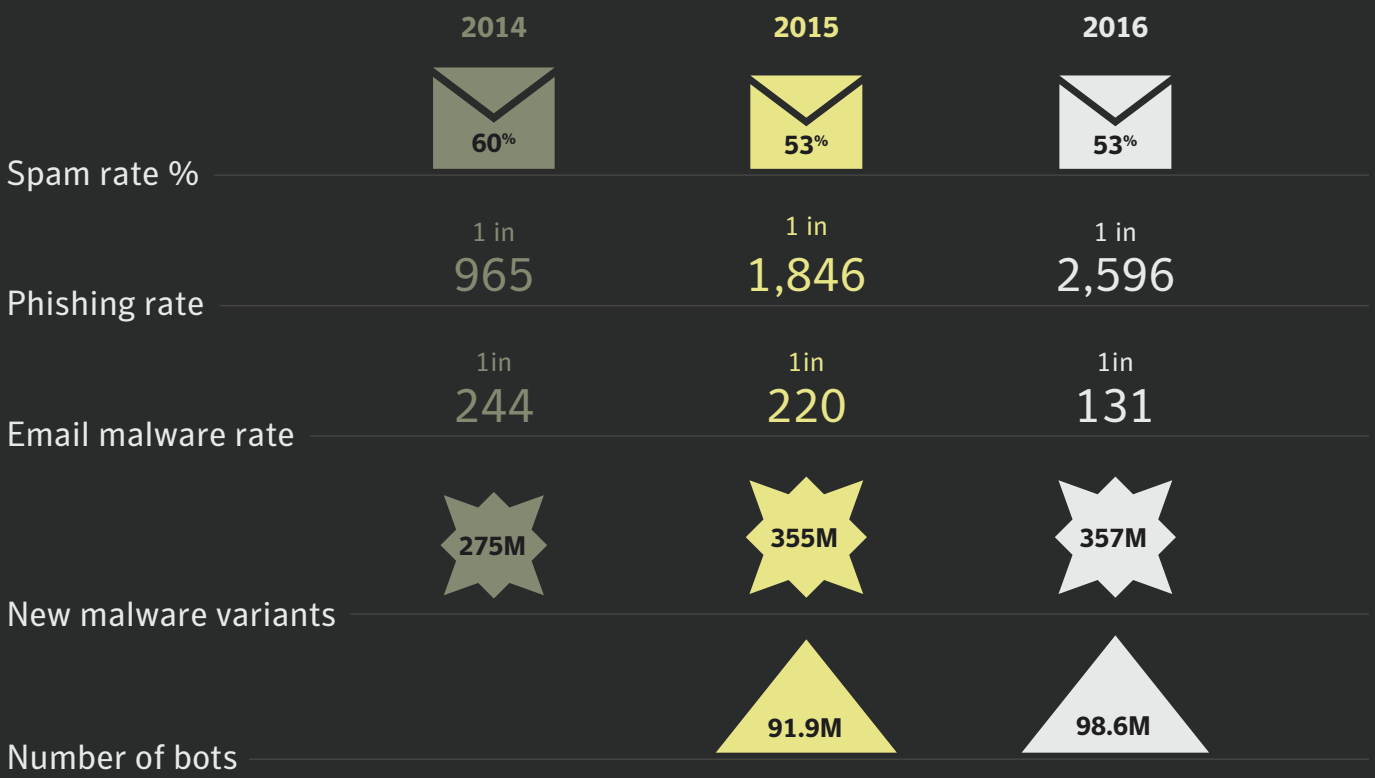
Symantec

Breaches

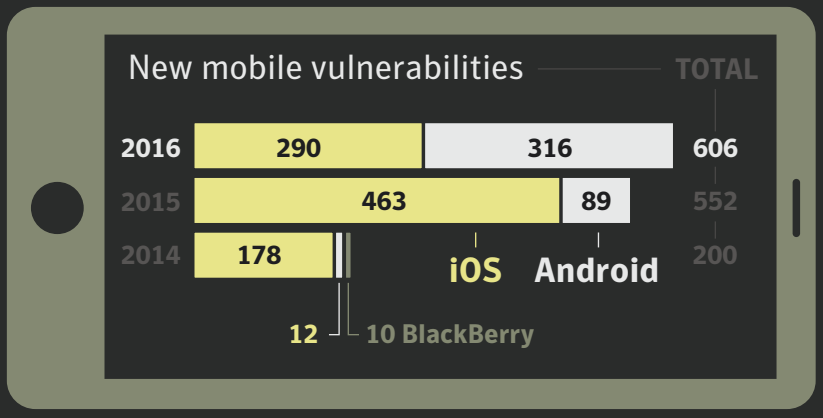


In the last **8** years more than **7.1 billion** identities have been exposed in data breaches

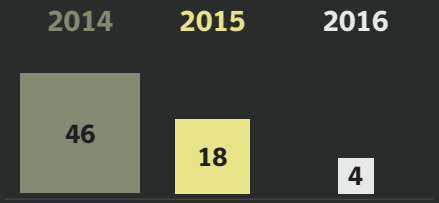
Email threats, malware, and bots



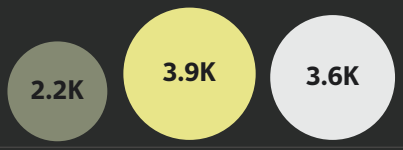
Mobile



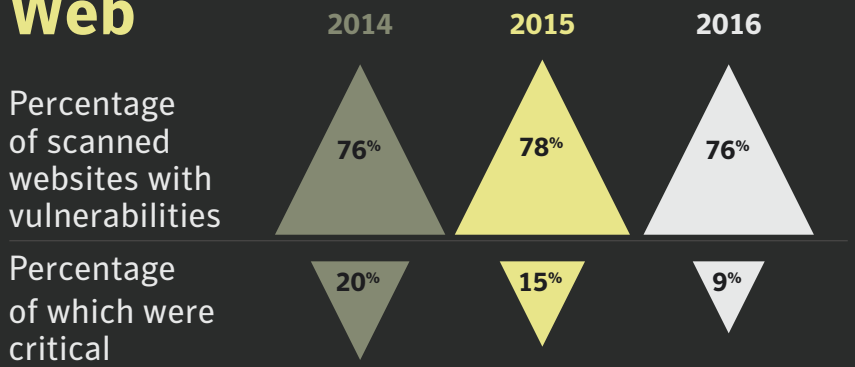
New Android mobile malware families



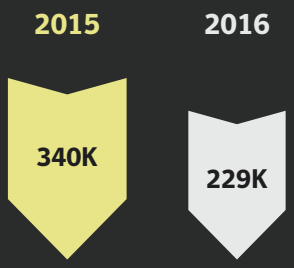
New Android mobile malware variants



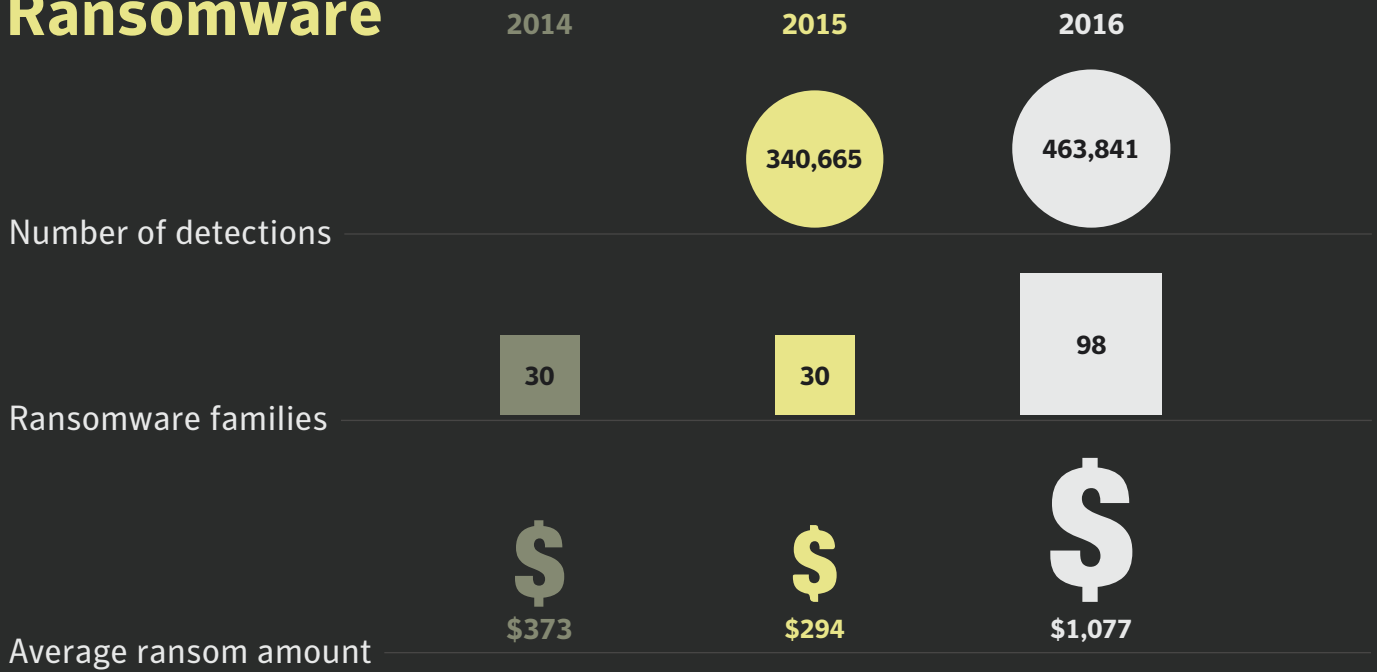
Web



Average number of web attacks blocked per day



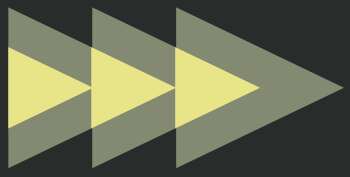
Ransomware



Cloud

	JUL-DEC 2015	JAN-JUN 2016	JUL-DEC 2016
Average number of cloud apps used per organization	774	841	928
Percentage of data broadly shared	25%	23%	25%

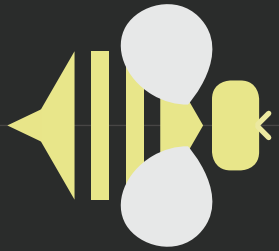
Internet of Things



Speed of attack

2 minutes: time it takes for an IoT device to be attacked

Number of attacks against Symantec honeypot **per hour**



JAN|**2016** DEC|**2016**

Targeted attacks: Espionage, subversion, & sabotage

Section

03

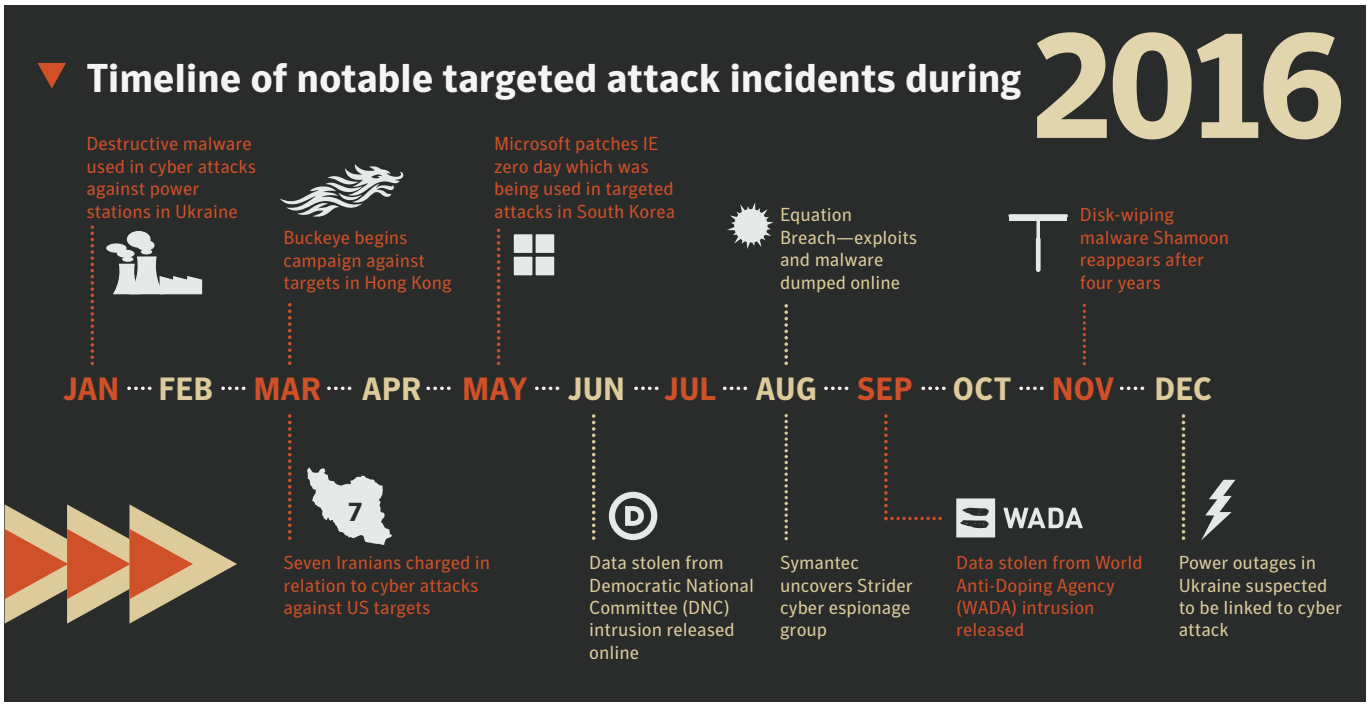
Symantec

Introduction

The targeted attack landscape shifted considerably during 2016, with several groups emerging from the shadows and engaging in more public, politically subversive activities. The ongoing conflict in Ukraine, the US election, and the Olympics were all affected by campaigns designed to steal and leak data in order to influence public opinion, create an atmosphere of distrust, and possibly influence political outcomes. Due to these recent successes and, with key elections approaching in a number of countries in 2017, it is likely these kinds of activities will continue. Groups have meanwhile continually refined their tactics, with several moving away from customized malware and relying more on legitimate software tools to compromise targeted networks.

Key findings

- Attacks for subversive purposes, in particular those during the US elections, have come to the fore and represent a new form of high-profile targeted attack.
- Targeted attacks involving destructive malware have increased in some regions, such as the reemergence of disk-wiping malware Shamoon in the Middle East and attacks against targets in Ukraine involving the KillDisk Trojan.
- Economic espionage such as stealing trade or commercial secrets, one of the traditional forms of targeted attack, has dropped off in some cases. Detections of Chinese espionage malware dropped considerably following a mutual agreement with the US to not target intellectual property. However, economic espionage hasn't disappeared by any means and the drop comes at a time when other types of targeted attack, such as sabotage and subversion, have been on the increase.
- Zero-day vulnerabilities have become less important and some adversaries are no longer as reliant on malware, increasingly "living off the land"—making use of the resources to hand including legitimate administrative and penetration testing tools to carry out attacks.



Notable targeted attack groups

Sandworm

est. 2014

Possible region of origin: **Russia**

Aliases / *Quedagh, BE2 APT*

Tools, tactics, & procedures (TTP)
Spear phishing, vulnerabilities, zero-days, custom back door programs, destructive payloads

Motives
Espionage, sabotage

Target categories & regions
Governments, international organizations, energy, Europe, US

Recent activities
Linked to destructive attacks against Ukrainian media and energy targets

Housefly

est. 2001

Possible region of origin: **US**

Aliases / *Equation*

Tools, tactics, & procedures (TTP)
Watering holes, infected CD-ROMs, infected USB keys, vulnerabilities, zero-days, custom back door and information-stealing programs, worm programs

Motives
Espionage

Target categories & regions
Targets of interest to nation-state attackers

Recent activities
Breached in 2016, with tools and exploits leaked

Fritillary

est. 2010

Possible region of origin: **Russia**

Aliases / *Cozy Bear, Office Monkeys, EuroAPT, Cozyduke, APT29*

Tools, tactics, & procedures (TTP)
Spear phishing, custom back door programs

Motives
Espionage, subversion

Target categories & regions
Governments, think tanks, media, Europe, US

Recent activities
Associated with Democratic National Committee (DNC) attacks

Strider

est. 2011

Possible region of origin: **Western**

Aliases / *Remsec*

Tools, tactics, & procedures (TTP)
Advanced surveillance tool

Motives
Espionage

Target categories & regions
Embassies, airlines, Russia, China, Sweden, Belgium

Recent activities
Uncovered by Symantec in 2016

Swallowtail

est. 2007

Possible region of origin: **Russia**

Aliases / *Fancy Bear, APT28, Tsar Team, Sednit*

Tools, tactics, & procedures (TTP)
Spear phishing, watering holes, infected storage devices, vulnerabilities, zero-days, custom back door and information-stealing programs

Motives
Espionage, subversion

Target categories & regions
Governments, Europe, US

Recent activities
Associated with WADA and DNC hacks

Suckfly

est. 2014

Possible region of origin: **China**

Aliases / *None*

Tools, tactics, & procedures (TTP)
Custom back door programs signed using stolen certificates

Motives
Espionage

Target categories & regions
E-commerce, governments, technology, healthcare, financial, shipping

Recent activities
Targeted attacks using multiple stolen code-signing certificates

Cadelle

est. 2012

Possible region of origin: **Iran**

Aliases / *None*

Tools, tactics, & procedures (TTP)
Custom back door programs

Motives
Espionage

Target categories & regions
Airlines, telecommunications, Iranian citizens, governments, NGOs

Recent activities
Surveillance on domestic targets in Iran and orgs in the Middle East

Buckeye

est. 2009

Possible region of origin: **China**

Aliases / *APT3, UPS, Gothic Panda, TG-0110*

Tools, tactics, & procedures (TTP)
Spear phishing, zero-days, custom back door programs

Motives
Espionage

Target categories & regions
Military, defense industry, media, education, US, UK, Hong Kong

Recent activities
Shifted focus from Western targets to Hong Kong

Appleworm

est. 2012

Possible region of origin: **North Korea**

Aliases / *Lazarus*

Tools, tactics, & procedures (TTP)
Spear phishing, DDoS attacks, disk wiping, zero-days, custom back door and information-stealing programs, destructive payloads

Motives
Espionage, sabotage, subversion

Target categories & regions
Financial, military, governments, entertainment, electronics

Recent activities
Subject to disruption operations in early 2016. Links with Bangladesh Bank attackers

Tick

est. 2006

Possible region of origin: **China**

Aliases / *None*

Tools, tactics, & procedures (TTP)
Spear phishing, watering holes, custom back door programs

Motives
Espionage

Target categories & regions
Technology, broadcasting, aquatic engineering, Japan

Recent activities
Long-standing campaigns against targets in Japan

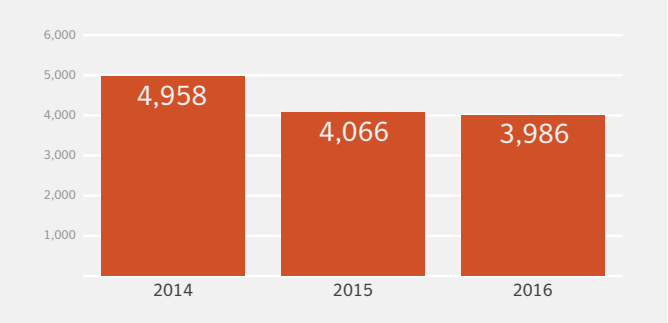
The targeted attack landscape in 2016

2016 was an exceptionally active year for targeted attack groups, with notable incidents occurring in Europe, the US, Asia, and the Middle East. As the year progressed, the level of high-profile activity appeared to escalate, with politically subversive incidents directed at the United States and destructive malware targeting Saudi Arabia and Ukraine.

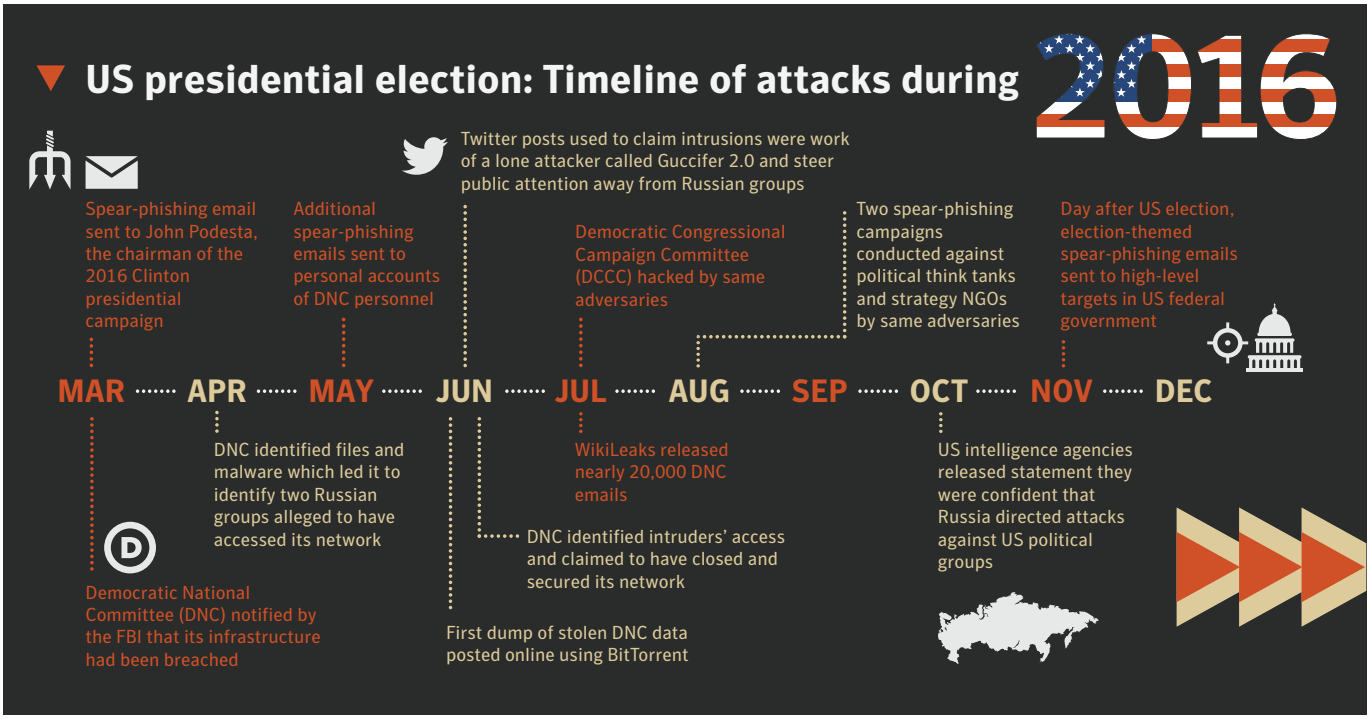
A wide range of targeted attack groups is in operation today. While the global powers all have a long-standing ability to conduct a variety of cyber operations, regional powers have also moved into cyber space with their own cyber espionage operations directed at rival countries and internal opposition groups. The Notable targeted attack groups graphic lists 10 of the most significant groups that were active in 2016 and that have been publicly connected to nation states.

Zero-day vulnerabilities, annual total

Zero-day vulnerabilities (vulnerabilities not discovered by the software's vendor) declined marginally from 4,066 in 2015 to 3,986 in 2016.



Previous editions of the Internet Security Threat Report focused on the number of exploits of zero-day vulnerabilities. This year, we have opted to analyze the total number of zero days, i.e. vulnerabilities not discovered by the software's vendor. Under this metric, zero days found during 2016 fell once again, declining marginally from 4,066 to 3,986. This stagnation suggests that the growing popularity of "bug bounty" programs and a greater focus on security as part of the product development process may mean that zero-day vulnerabilities are becoming harder to find for attackers, forcing them to move away from using them and broadening their range of tactics (see Living off the land below).

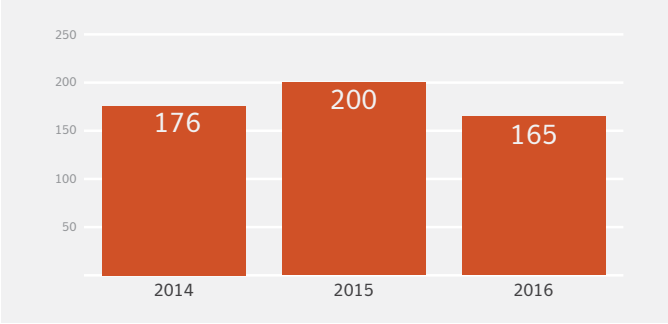


The decline in zero-day discovery comes after the underground market for vulnerabilities came under the spotlight in 2015, following the Hacking Team breach. Multiple zero-day exploits were leaked as part of the breach, in addition to information on how much money these exploits were changing hands for.

Nevertheless, there were a number of instances of zero-day vulnerabilities being exploited in targeted attacks during 2016. For example, in October, Adobe issued a patch for Flash Player following discovery of a zero day that was being actively exploited in the wild. Three vulnerabilities in Apple iOS, collectively known as Trident, were disclosed and patched in August after they were found to have been used in a cyber attack against a UAE-based human rights activist. In May, Microsoft patched an Internet Explorer zero-day which was exploited in targeted attacks in South Korea.

Vulnerabilities disclosed in industrial control systems

The number of industrial control system (ICS) vulnerabilities discovered fell compared to 2015.



Similarly, the number of industrial control system (ICS) vulnerabilities discovered during 2016 fell compared to 2015, providing further evidence to suggest vulnerabilities are becoming harder to find for attackers.

Trends and analysis

Subversion emerges as a new motive for targeted attacks

One of the most eye-catching developments in 2016 was the prominence of operations attempting to influence political events in targeted countries. Traditionally, targeted attack groups have focused on espionage and maintained a low profile in order to avoid detection, but a number of groups added more overt operations to their repertoire during 2016.

In August 2016, a trove of data linked to the Equation cyber espionage group was leaked online by a group calling itself "Shadow Brokers." The leak contained tools and exploits used by Equation, and Shadow Brokers claimed it was a fraction of what it had obtained, offering to auction off the rest to the highest bidder.

Most of the leaked files appear to be several years old, dating back to between 2010 and 2013. How they came into the hands of the leakers remains unknown. The Shadow Brokers group was unknown prior to this incident, but it could also have been a cover name for another group.

Given that the Shadow Brokers' attempts to sell the stolen data appeared half-hearted, it seems likely that discrediting the Equation group rather than monetary gain was the primary motive behind the leak.

The most high-profile, subversive incident of the year was a series of intrusions against the Democratic Party, which occurred in the run-up to the 2016 US presidential election. A joint investigation by the US Intelligence Community concluded that two groups linked to Russia's intelligence services were responsible for the campaign.

Both groups were previously known to Symantec and have been active for a number of years, engaging in espionage against a range of targets in the US and Europe. Fritillary (aka APT29 and Cozy Bear) has been active since at least 2010 and was known for using the Duke family of Trojans against its targets, e.g. Cozyduke (Trojan.Cozer) and Seaduke (Trojan.Seaduke). Swallowtail (aka APT28 and Fancy Bear) has been active for at least 10 years and usually uses the Sofacy Trojan (Infostealer.Sofacy) as one of its main malware tools. Fritillary is known to target very high-profile individuals and organizations in government, international policy, and research institutes in the European Union and the United States while Swallowtail primarily targets military, government, embassy, and defense contractor personnel in Eastern European countries.

In September, Swallowtail was also implicated in the leak of medical records stolen from the World Anti-Doping Agency (WADA). Data relating to American Olympic athletes, British cyclists, and athletes from a number of other countries was released following an intrusion.

According to WADA, Swallowtail was responsible for the intrusion. The group took the unusual step of creating its own website (using the Fancy Bear moniker) to publish the stolen data along with claims it contained proof the athletes had broken anti-doping rules.

The DNC and WADA intrusions were a major change in tactics by both groups, both of whom hadn't previously engaged in this kind of subversive activity. The US intelligence community's report into the DNC data thefts and subsequent public disclosures assessed that they were part of an influence campaign conducted by the Russian Government aimed at

the 2016 US presidential election. It also concluded that the campaign would have been seen as a success in Russia and that these activities will likely be used to inform future influence operations.

Given the proven potential for sowing discord and confusion, there is a strong likelihood that these tactics may be used again in a bid to destabilize other countries. France and Germany are both holding elections this year and already Bruno Kahl, the head of Germany's foreign intelligence service, has said the same kind of attacks have already begun against Germany. "We have evidence of cyber attacks that have no other purpose than triggering political uncertainty," he said. "The perpetrators are interested in delegitimizing the democratic process as such, no matter who that subsequently helps."

Sabotage attacks make a comeback

There was a resurgence in sabotage attacks during 2016, beginning with a number of attacks against Ukraine involving the use of disk-wiping malware. The attacks were linked to another possibly Russian cyber espionage group known as Sandworm and involved a highly destructive Trojan (Trojan.Disakil). Attacks in late 2015 and early 2016 hit media organizations and the energy sector in Ukraine, with the latter being linked to power outages in the country.

Disakil returned at the end of 2016, when a new version was circulated disguised as ransomware. The malware was reportedly used in a number of attempted attacks against the financial sector in Ukraine.

The variant was designed to run on Linux computers and, if run, rendered them unusable by encrypting key operating system files. Once the encryption has finished, it displayed a message demanding a ransom of 222 Bitcoin (approximately US$210,000 at the time of the attacks). Paying the ransom would not decrypt the affected files, with the encryption keys generated on the infected computer not saved locally nor to a command and control (C&C) server. The malware was likely disguised as ransomware in order to trick victims into not investigating attacks thoroughly.

Sabotage attacks also occurred in other regions, one of the most notable of which was the reemergence of the Shamoon disk-wiping malware (W32.Disttrack) after an absence of five years. First used in attacks against the Saudi Arabian energy sector in 2012, a new variant (W32.Disttrack.B) was used against targets in Saudi Arabia in November 2016 and January 2017.

In the first wave of new attacks, the malware was configured to launch its disk-wiping payload at 8:45 p.m. local time on Thursday, November 17. The Saudi Arabian working week runs from Sunday to Thursday. Thus, the attack was timed to occur after most staff had gone home for the weekend in the hope of reducing the chance of discovery before maximum damage could be caused.

The Shamoon malware was configured with passwords that appeared to have been stolen from the targeted organizations. These passwords were likely used to allow the malware to spread across an organization's network.

The attacks were likely politically motivated. In the 2012 attacks, infected computers had their master boot records wiped and replaced with an image of a burning US flag. The latest attacks instead used a photo of the body of Alan Kurdi, the three-year-old Syrian refugee who drowned in the Mediterranean in 2015.

The November attacks were linked to a group known as "Greenbug," which was discovered by Symantec during its investigation into the Shamoon attacks. Greenbug has targeted a range of organizations in the Middle East including companies in the aviation, energy, government, investment, and education sectors. Symantec found that Greenbug infected at least one administrator computer belonging to an organization that was subsequently hit by Shamoon.

The January attacks were carried out by a group known as "Timberworm" (see panel How Shamoon attackers used "living off the land" tactics). Although Greenbug and Timberworm appear to be distinct groups, if they are both spreading Shamoon, it is likely at the direction of a single entity.

Living off the land

Attackers have begun to change their tactics, expanding their range of tools and many groups are no longer as reliant on the traditional attack toolkit of malware and zero-day vulnerabilities. While not a new technique, groups are increasingly "living off the land," using operating system features, legitimate tools, and cloud services to compromise networks. This tactic can make attacks more difficult to detect, since it's harder to spot the malicious use of legitimate tools compared to the presence of malware.

How Shamoon attackers used "living off the land" tactics

One prominent exponent of living off the land during 2016 was Timberworm, a cyber espionage group linked to the resumption of attacks involving the destructive malware Shamoon (W32.Disttrack.B). Shamoon reappeared in November 2016 following a four-year absence, with a series of attacks against targets in Saudi Arabia. Two more waves of attack occurred later in November 2016 and again in January 2017.

While the November attacks were linked to a group known as "Greenbug," the January attacks were launched by Timberworm, a cyber espionage group responsible for a string of attacks across the Middle East.

To spread Shamoon, Timberworm first sent spear-phishing emails to individuals at targeted organizations. In some cases, the emails contained Microsoft Word or Excel files as attachments. In others, the emails contained malicious links, which if clicked, downloaded similar Word or Excel files.

If the file was opened, a macro ran a PowerShell script that provided remote access and performed basic reconnaissance of the compromised computer. If a computer was of interest, they then installed malware (Backdoor.Mhretriev).

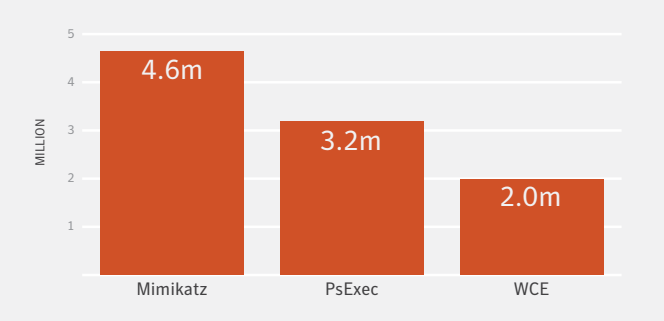
From there, the attackers used a cornucopia of legitimate administrative and penetration testing tools to traverse the target's network and identify computers for infection. These included:

- PsExec, a tool for executing processes on other systems from Microsoft Sysinternals
- PAExec, a free reimplementation of PsExec from Poweradmin
- Netscan, a multipurpose IPv4/IPv6 network scanner
- Samdump, a hacking tool that dumps Windows password hashes
- Mimikatz (Hacktool.Mimikatz), a hacking tool used to harvest credentials
- TightVNC, an open-source remote desktop access application
- Plink, a command line network connection tool supporting encrypted communications
- Rar, archiving utility for compressing files before exfiltration

Once the reconnaissance operation was complete, Shamoon (W32.Disttrack.B) was installed on pre-selected computers. The malware was configured to trigger its disk-wiping payload at a set time on all compromised computers, maximizing the impact of the attacks.

Most commonly seen tools that can be misused by attackers

According to Symantec file reputation telemetry, the most widely seen legitimate tools that can be misused by attackers during 2016 were Mimikatz, PsExec, and WCE.



According to Symantec file reputation telemetry, the most widely seen legitimate tool that can be misused by attackers during 2016 was Mimikatz (Hacktool.Mimikatz)—a tool capable of changing privileges, exporting security certificates, and recovering Windows passwords in plaintext—followed by the Microsoft Sysinternals tool PsExec and Windows Credential Editor. Given the sheer number of instances and the fact that all three tools have legitimate uses (even Mimikatz can be used for penetration testing), it is easy to see the appeal of these tools to attackers, since their use may go unnoticed.

Malicious PowerShell scripts have also been widely used in targeted attacks, with attackers exploiting the framework's flexibility to download payloads, traverse compromised networks, and carry out reconnaissance. Recent research by Symantec demonstrated PowerShell's popularity as an attack tool. Of all of the PowerShell scripts analyzed through Symantec's Blue Coat Malware Analysis sandbox, 95.4 percent were malicious.

This practice has been used extensively by a range of groups in recent times. A prominent case in point was the aforementioned intrusions on the DNC in the run-up to the US presidential election. One of the initial points of compromise according to the FBI was a spear-phishing email sent to campaign chairman John Podesta's email account on March 19, 2016. The email was crafted to appear as though it originated from an official Gmail administrative account and suggested that his email had been compromised and directed him to reset his password. It included a shortened URL which obfuscated a malicious URL. Once clicked, the victim was directed to a fake password reset page masquerading as a legitimate Gmail account reset page. No malware or exploits were needed to perform the attack. Instead, simple social engineering was used to obtain a password.

Spear-phishing email used in DNC attacks

Text of spear-phishing email sent to John Podesta, the chairman of the 2016 Clinton presidential campaign.

From: Google <no-reply@accounts.googlemail.com>
Date: March 19, 2016 at 4:34:30 AM EDT
To: [redacted]@gmail.com
Subject: *Someone has your password*

Someone has your password
Hi John

Someone just used your password to try to sign in to your Google Account [redacted]@gmail.com.

Details:
Saturday, 19 March, 8:34:30 UTC
IP Address: 134.249.139.239
Location: Ukraine

Google stopped this sign-in attempt. You should change your password immediately.

CHANGE PASSWORD <https://bit.ly/1PibSU0>

Best,
The Gmail Team
You received this mandatory email service announcement to update you about important changes to your Google product or account.

Another example of living off the land is provided by the Chafer cyber espionage group, which appears to be based in Iran. One of its attack vectors is to compromise web servers, exploiting vulnerabilities identified through web scanning tools. In a recent intrusion against a target in Turkey, Symantec discovered that Chafer had used a software tool called JexBoss to identify an older, unpatched, community version of JBoss Application Server belonging to the target. The group then deployed a web shell to the server, a script which permits remote administration, in addition to a copy of the software tool Mimikatz.

From there, they were able to use native operating system tools such as Qwinsta and Whoami to extract information about the compromised server. Within 20 minutes of the initial compromise, the group had used the Microsoft Sysinternals tool PsExec to spread to two other computers on the target's network.

Another actor which has made use of this tactic in recent times is the China-based group Tick, which has targeted mainly Japanese organizations for at least 10 years. Recent campaigns have seen it use spear-phishing emails and compromise Japanese websites in order to infect targets.

One of Tick's main tools is its own custom-developed malware (Backdoor.Daserf), but it also uses a range of tools such as the aforementioned Mimikatz, Windows Credential Editor, and GSecdump (Gsecdump), a hacking tool that may be used to steal hashes from Security Accounts Manager (SAM), Active Directory, and active logon sessions.

There are also instances of attackers using basic cloud services rather than command and control servers for data exfiltration. For example, Fritillary, one of the groups which attacked the DNC, was found to have used approximately 200 Microsoft OneDrive accounts to exfiltrate stolen data. The goal here appeared to be to hide in plain sight and the attackers may have decided that data being moved to OneDrive may have been mistaken for legitimate activity.

Economic espionage

In September 2015, the US and China reached an agreement that neither country would conduct economic espionage in cyber space. Under the terms of the agreement, the two countries agreed that neither government would "conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."

Given the nature of such espionage operations, establishing whether this agreement is working can be difficult. However, analysis by Symantec has found strong evidence that there has been a marked decline in activity by groups probably associated with China since the agreement was signed.

Reviewing detections of malware families used by cyber espionage groups, which Symantec believes are China-based, provided an insight into activity levels over time. Almost immediately after the agreement was signed, the number of infections dropped considerably. Infection rates continued to fall in the following months and remained low at year-end.

In tandem with this trend, some individual Chinese groups have also exhibited changing patterns of activity. For example, the Buckeye group (aka APT3 or Gothic Panda) had conducted cyber espionage operations against organizations in the US, UK, and other countries for at least half a decade. However, the group's focus began to shift in the run-up to the US-China agreement.

From June 2015 onwards the group began compromising political entities in Hong Kong. By March 2016 Buckeye had almost fully migrated its focus to organizations in Hong Kong. While there is no definitive proof that the shift in focus was motivated by the agreement, it was consistent with the overall trend of a reduction in cyber espionage activity against targets in other countries. While the US-China agreement has caused a shift in focus for some cyber attack groups, it does not necessarily mean a wholesale cessation of operations.

New threats emerge

In addition to ongoing activity from known targeted attack groups, other threats emerged from the shadows during 2016. In August, Symantec shone the spotlight on a previously unknown group called Strider, which has been mounting attacks against selected targets in Russia, China, Sweden, and Belgium.

Strider's main tool is a stealthy Trojan known as Remsec (Backdoor.Remsec), which appears to be of such high sophistication that we assess it was primarily designed for espionage purposes. Active since at least 2011, Strider maintained a low profile, partly because it was highly selective in its choice of targets, with Symantec finding evidence of infections on 36 computers across seven separate organizations.

Remsec exhibited a high degree of technical competence, containing a number of advanced features designed to help it evade detection. Several components were in the form of executable blobs (Binary Large Objects), which are more difficult for traditional, signature-based antivirus software to detect. In addition to this, much of the malware's functionality is deployed over the network, meaning it resides only in a computer's memory and is never stored on disk—again making it more difficult to detect.

Remsec illustrates the levels of skill and resources that nation-state groups can now bring to bear on targets. As vendors become more effective at uncovering targeted attack groups, which has led some groups to move away from sophisticated tools, there are still some operations that are in a league of their own.

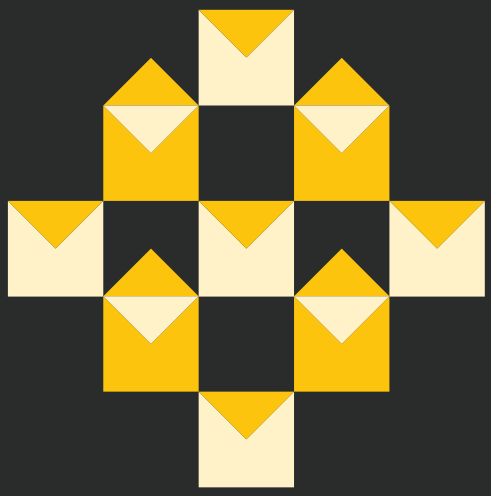
Further reading

- Buckeye cyber espionage group shifts gaze from US to Hong Kong
- Equation: Has secretive cyber espionage group been breached?
- Strider: Cyber espionage group turns eye of Sauron on targets
- Patchwork cyber espionage group expands targets from governments to wide range of industries
- Tick cyber espionage group zeros in on Japan
- Taiwan targeted with new cyber espionage back door Trojan
- Suckfly: Revealing the secret life of your code signing certificates
- Collaborative Operation Blockbuster aims to send Lazarus back to the dead
- Destructive Disakil malware linked to Ukraine power outages also used against media organizations
- Shamoon: Back from the dead and destructive as ever
- Greenbug cyber espionage group targeting Middle East, possible links to Shamoon
- Shamoon: Multi-staged destructive attacks limited to specific targets

Best practices

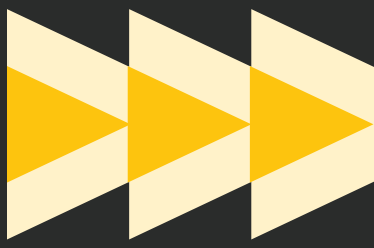
- Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls as well as gateway antivirus, intrusion detection or protection systems (IPS), website vulnerability with malware protection, and web security gateway solutions throughout the network.
- Exploitation of vulnerabilities is a commonly used tactic by targeted attack groups. Receive alerts for new vulnerabilities and threats across vendor platforms and patch known vulnerabilities as soon as possible.
- Implement and enforce a security policy whereby any sensitive data is encrypted at rest and in transit. Ensure that customer data is encrypted as well. This can help mitigate the damage of potential data leaks from within an organization.
- Attackers frequently use stolen or default credentials to traverse a network. Ensure passwords are strong. Important passwords, such as those with high privileges, should be at least 8-10 characters long (and preferably longer) and include a mixture of letters and numbers. Encourage users to avoid reusing the same passwords on multiple websites and sharing passwords with others should be forbidden. Delete unused credentials and profiles and limit the number of administrative-level profiles created.
- Educate employees on the dangers posed by spear-phishing emails, including exercising caution around emails from unfamiliar sources and opening attachments that haven't been solicited. A full protection stack helps to defend against emailed threats, including Symantec Email Security.cloud which can block email-borne threats and Symantec Endpoint Protection, which can block malware on the endpoint. Symantec Messaging Gateway's Disarm technology can also protect computers from threats by removing malicious content from attached documents before they even reach the user.

Email: Malware, spam, & phishing



Section

04



Symantec

Introduction

Although a vital communication tool, email is also one of the prime sources of disruption for end users and organizations. This disruption can range from unwanted emails in the form of spam to more dangerous threats, such as the propagation of ransomware or targeted spear-phishing campaigns.

While just over half of all emails (53 percent) are spam, a growing proportion of that spam contains malware. This increase in email-borne malware is driven largely by a professionalization of malware-spamming operations. Malware authors can outsource their spam campaigns to specialized groups who conduct major spam campaigns. The sheer scale of email malware operations indicates that attackers are making considerable profits from these kinds of attacks and email is likely to continue to be one of the main avenues of attack in 2017.

Key findings

- The email malware rate increased significantly during 2016, from 1 in 220 emails sent containing malware in 2015, to 1 in 131 emails in 2016. This increase was driven primarily by botnets, which are used to deliver massive spam campaigns related to threats such as Locky (Ransom.Locky), Dridex (W32.Cridex), and TeslaCrypt (Ransom.TeslaCrypt).
- Targeted spear-phishing campaigns, especially in the form of Business Email Compromise (BEC) scams, rather than the mass-mailing phishing campaigns of old, are now favored by attackers. This is reflected in the drop in phishing rates, which fell from 1 in 1,846 emails to 1 in 2,596 emails.
- Major email threat groups are relying primarily on the use of first-stage downloaders to install their final payload, typically ransomware. At the beginning of 2016, Office documents containing malicious macros were the most common form of downloader being used in spam campaigns. However, a shift occurred in March and, since then, JavaScript downloaders have dominated.

Trends and analysis

Email data gathered throughout 2016 demonstrates that email has become the main vector for malware propagation.

Malware menace

The most noteworthy trend observed through 2016 was the uptick in email malware rates. The rate jumped from 1 in 220 emails in 2015 to 1 in 131 emails in 2016.

Overall email malware rate

2014	2015	2016
1 in 244	1 in 220	1 in 131

This increase in email malware can probably be linked to ongoing activity during 2016 by mass-mailing malware groups, primarily spreading Locky, Dridex, and TeslaCrypt. One of the major distributors of malware is a botnet known as Necurs (Backdoor.Necurs). Necurs is responsible for massive campaigns that spread malware through JavaScript and Office macro attachments. These downloaders subsequently install the final payload, which in 2016 was typically ransomware threats such as Locky.

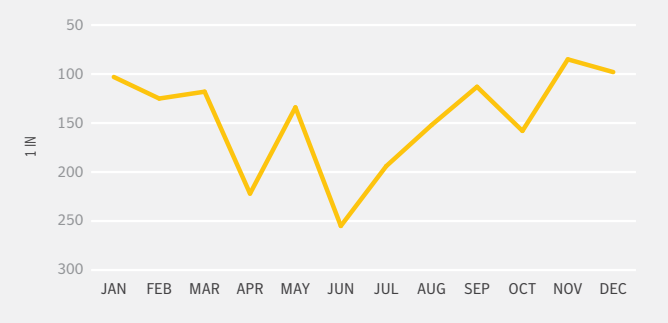
Necurs was inactive between December 24, 2016 and March 20, 2017, meaning there was a significant decline in the email malware rate in January and February 2017. While it is not unusual for malware groups to take a break during Christmas, these breaks usually only last around a week. The reason for Necurs ceasing operations remains unknown, but the group was able to immediately resume mass-mailing campaigns on its return. Symantec blocked almost two million malicious emails on March 20 alone, the day of its return.

Dridex is a financial Trojan used to steal end users' banking credentials. The attackers behind Dridex are professionals who put a lot of effort into continually refining the malware and making the emails used to distribute it appear as legitimate as possible. TeslaCrypt and Locky are both ransomware, with Locky having appeared in February 2016. Ransomware was one of the major themes of cyber security in 2016.

Monthly telemetry collected by Symantec showed a strong start to the year for email malware, with sharp drops in April and June, times when decreases in activities by the groups behind Locky, Dridex, and others were reported.

Monthly email malware rate

The monthly email malware rate shows sharp drops in April and June, which may be linked to law enforcement activity against several cyber crime groups.



Symantec believes that this drop in activity may have been linked to law enforcement activity, with the drop in activity in June coming in the aftermath of the arrest of 50 people in Russia allegedly connected to the Lurk banking fraud group.

However, this drop in activity was only temporary and malware spam campaigns quickly scaled up again. Campaigns involving Dridex and Locky resumed, while incidents of the Kovter family of threats (Trojan.Kovter) started increasing in August and maintained this growth for the rest of the year. For more details on mass-mailing ransomware campaigns, see our Ransomware chapter.

Email malware rate by industry

Wholesale Trade and Agriculture were the classified industry sectors most affected by email-borne threats in 2016.

Industry	Email Malware Rate (1 in)
Nonclassifiable Establishments	103
Agriculture, Forestry, & Fishing	111
Wholesale Trade	111
Services	121
Manufacturing	130
Retail Trade	135
Mining	139
Public Administration	141
Transportation & Public Utilities	176
Construction	179
Finance, Insurance, & Real Estate	182

With the exception of Retail Trade, which saw a drop in its email malware rate (from 1 in 74 emails in 2015 to 1 in 135 emails in 2016), every industry saw an increase in email malware in 2016. The biggest increases were in the industries of Transport (from 1 in 338 emails to 1 in 176), Finance (from 1 in 310 to 1 in 182), and Mining (from 1 in 304 to 1 in 139). Healthcare Services saw a jump from 1 in 396 emails to 1 in 204.

Email malware hit businesses of all sizes in 2016. However, small- to medium-sized businesses (with 251 to 500 employees) were the most impacted, according to our figures.

Email malware rate by company size

The highest rate of malware in email traffic was in the 251-500 company size grouping, with 1 in 95 emails received containing malware.

Company Size	Email Malware Rate (1 in)
1-250	127
251-500	95
501-1000	139
1001-1500	224
1501-2500	104
2501+	170

Phishing

Phishing rates have been in decline for the last several years, and they dropped again in 2016, falling from 1 in 1,846 emails to 1 in 2,596 emails.

Overall phishing rate

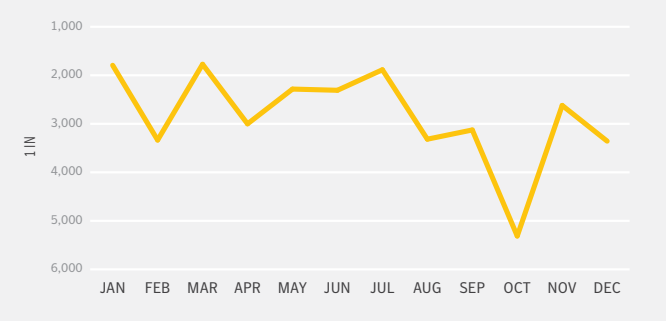
2014	2015	2016
1 in 965	1 in 1846	1 in 2596

There was a noticeable drop in October, which had a phishing rate of just 1 in 5,313 emails, before the rate returned to a more "average" figure of 1 in 2,621 emails for November.

There was a lot happening in the information security world in October, including the Mirai botnet coming to increased prominence following a distributed denial of service attack (DDoS) on DNS provider Dyn, which affected a number of high-profile websites, including Spotify, Netflix, and PayPal. There were also reports of an increase in activity surrounding the Kovter (Trojan.Kotver) family of threats. However, there is no single clear reason why the phishing rate dropped so sharply that month.

Monthly phishing rate

The monthly phishing rate figures show a noticeable drop in October, but there was no single clear reason for such a significant drop that month.



It's likely there are myriad reasons behind the decrease in phishing activity. Consumers are increasingly aware of the dangers of clicking unknown links or downloading suspicious attachments, meaning that it's possible the "standard," indiscriminate, mass-mailing phishing campaigns are becoming less effective for scammers.

Phishing rate by industry

Agriculture was the industry sector most affected by phishing in 2016, with 1 in 1,815 emails classed as phishing attempts.

Industry	Phishing Rate (1 in)
Agriculture, Forestry, & Fishing	1815
Finance, Insurance, & Real Estate	1918
Mining	2254
Public Administration	2329
Retail Trade	2419
Nonclassifiable Establishments	2498
Services	3091
Manufacturing	3171
Wholesale Trade	4742
Construction	4917
Transportation & Public Utilities	6176

Phishing rate by company size

The highest rate of phishing occurred in the 251-500 company size grouping, with 1 in 2,554 emails received classed as phishing attempts.

Company Size	Phishing Rate (1 in)
1-250	2897
251-500	2554
501-1000	4023
1001-1500	6640
1501-2500	2610
2501+	3323

However, spear phishing continues to grow. There were many high-profile cases over the course of 2016, such as the hacking of the emails of Hillary Clinton campaign chairman John Podesta and former US Secretary of State Colin Powell, where spear-phishing emails were used.

BEC scams

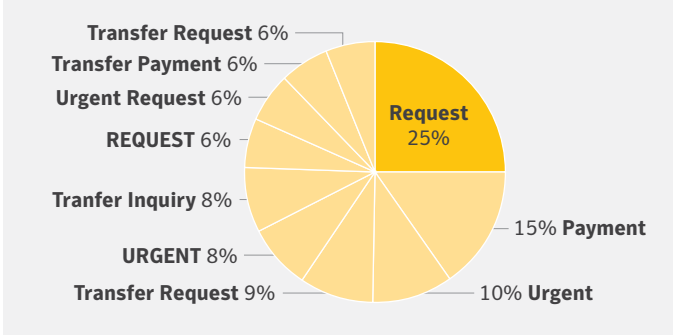
BEC scams, which rely on spear-phishing emails, came to increased prominence in 2016. Also known as CEO fraud or "whaling," BEC scams are a form of low-tech financial fraud where spoofed emails are sent to financial staff by scammers pretending to be the CEO or senior management. The scammers then request a large money transfer. These scams can be damaging as they require little technical expertise but can reap huge financial rewards for the criminals and significant losses for the companies involved. For example, early in 2016, an Austrian aerospace company fired its CEO after it lost almost US$50 million to BEC scammers.

Symantec research in the first half of 2016 found that more than 400 businesses are targeted by BEC scams every day, with small- and medium-sized businesses the most targeted. Estimates from the FBI indicate that more than $3 billion may have been lost to BEC scams in the past three years, with more than 22,000 victims worldwide.

Symantec research found these scams to be an evolution of the famous Nigerian 419 scams; almost half of the email addresses analyzed by Symantec had Nigerian IP addresses. Emails are sent Monday to Friday, following a standard working week, and generally contain innocuous subject lines, featuring words such as "Request," "Payment," "Urgent," etc.

BEC scams: Common subject lines

"Request" was the most popular keyword used in subject lines for BEC scam emails. It was followed by "Payment" (15 percent) and "Urgent" (10 percent).



BEC scammers' techniques continue to evolve in order to ensure the success of the scam. Symantec research in November found that, rather than asking for a money transfer straight away, scammers used informal language to check if a victim was at their desk or to find out more information before requesting the cash.

A new technique recently observed by our researchers is the "hijacking" of legitimate invoices sent by companies so that the account number is changed to that of the scammer. Some cases we have seen involved scammers attacking the email server to change the details on the invoice. Others were just fake invoice emails sent without the need to hack the email server, but which were effective provided they went out before the legitimate invoices.

With BEC scams proving hugely lucrative, they are likely to continue to be a strong trend in 2017.

Spam stays steady

Spam rates remained steady at 53 percent in 2016 after declining in recent years.

However, this figure does still mean that the majority of inbound business emails sent in 2016 were spam. Spam is generally considered to be any unsolicited email that is sent in bulk and in some cases may not contain malicious threats. Spam emails can just be annoying or unwanted or they may lead to sites that carry out click fraud.

Overall spam rate

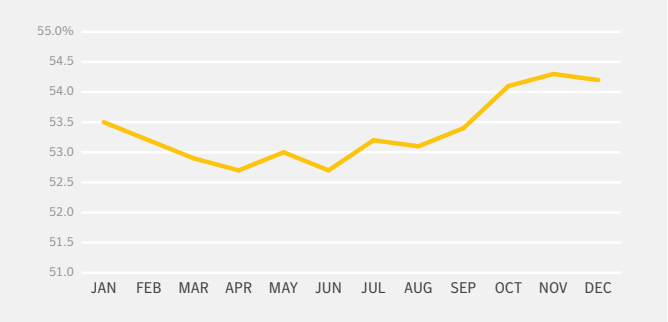
The spam rate between 2015 and 2016 has remained fairly steady.

2014	2015	2016
60%	53%	53%

Spam fell to its lowest level since 2003 in 2015, and it maintained this low figure in 2016. This is likely influenced by the previously mentioned growth in ransomware and more targeted spear-phishing campaigns such as BEC scams. The profitability of these campaigns may be turning attackers away from the old-school spam campaigns to these new methods.

Monthly spam rate

The spam rate increased slightly towards the end of 2016. In November, the spam rate hit 54.3 percent, the highest rate seen since March 2015.



While the overall spam rate remained stagnant for the year, there was a spike in spam being sent in the last quarter of 2016. In November, the spam rate hit 54.3 percent, the highest rate seen since March 2015.

A couple of factors influenced this jump. The US presidential election, which took place at the beginning of November, caused a spike in election-related spam. Symantec blocked almost 8 million emails related to the presidential election in the period from mid-September to mid-October.

Also in October, two significant campaigns impacted Symantec customers. An adult-themed spam attack that started in Spain impacted users in EMEA as it quickly spread into several different European languages. The second campaign, a significant snowshoe attack (see Ice-cold panel) sent emails related to spam products and services. The attackers sent a low volume of email to probe detections and aborted the spam run within minutes if the messages were blocked.

Spam related to Black Friday and Cyber Monday was also behind the high volumes of spam in November, with one campaign being used to spread the Locky ransomware. In December there were reports of the hailstorm spam technique being used to spread Dridex and Locky, but the spam rate held steady.

Spammers appear to be non-discriminatory when it comes to the size of the companies they target. The difference between the most-targeted small businesses and least-targeted larger businesses was just over a percentage point.

Spam rate by company size

There was little difference between the most targeted and least targeted company sizes, with the spam rate varying between 52.6 percent and 54.2 percent.

Company Size	Spam Rate (%)
1-250	54.2
251-500	53.1
501-1000	53.4
1001-1500	53.2
1501-2500	52.6
2501+	52.8

Spam rate by industry

Some industry sectors receive more spam than others, but the range is only approximately 8 percent.

Industry	Spam Rate (%)
Construction	59.5
Mining	57.1
Retail Trade	54.9
Manufacturing	54.4
Agriculture, Forestry, & Fishing	54.0
Nonclassifiable Establishments	53.0
Services	53.0
Finance, Insurance, & Real Estate	52.9
Transportation & Public Utilities	52.9
Wholesale Trade	52.6
Public Administration	51.6

Case studies/investigations

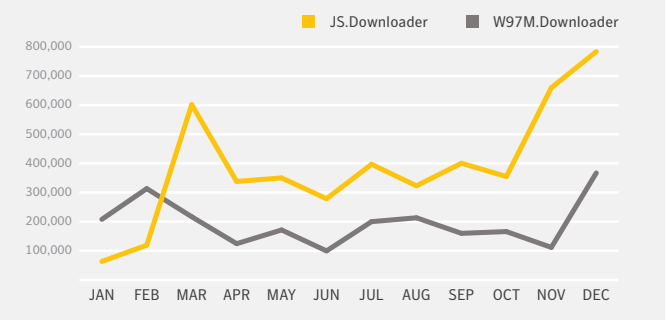
The groups involved in mass-mailing campaigns continually refine their tactics in a bid to stay one step ahead of email security systems.

Changing tactics

A notable trend during 2016 was a shift in the type of downloader used to deliver some of the most prolific threats. At the beginning of the year, Office documents with malicious macros (W97M.Downloader and variants) were the most popular form of downloader and were used in campaigns delivering threats such as Dridex (W32.Cridex). During March 2016, a shift occurred and the use of JavaScript downloaders (JS.Downloader and variants) increased significantly.

Downloader detections by month

Office macro downloaders (W97M.Downloader and variants) and JavaScript downloaders (JS.Downloader and variants) are the most commonly used downloaders that spread malware via email. JavaScript downloader activity increased during 2016, while Office macros experienced a resurgence in December 2016.



Symantec believes that spamming operations using JavaScript and Office macro downloaders are operated by different cyber criminal groups. Malware groups can hire either (or both) channels to deliver their threats. If this is the case, the trend is down to malware groups that favor spamming operations using JavaScript downloaders in the latter end of 2016.

While the propagation of Office macro downloaders has been lower throughout the year, Symantec doesn't believe that this vector will disappear. In fact, we can see that W97M.Downloader detections spiked in December, although JS.Downloader continues to dominate. This spike could possibly be attributed to the previously mentioned hailstorm campaign (see Ice-cold panel) that was being used to spread Locky and Dridex, which can be spread through malicious macros in Word documents.

Ice-cold: Snowshoe and hailstorm techniques

Snowshoe spamming distributes a broad load of spam across an array of IP addresses in order to increase the chances of some getting through. Snowshoe spammers anticipate that some emails will be trapped by spam filters. However, this technique of sending emails from a large number of IP addresses increases the chances of them avoiding spam filters and reaching a computer user's inbox. Snowshoe spammers send a low amount of spam from each IP address in order to stay under the radar.

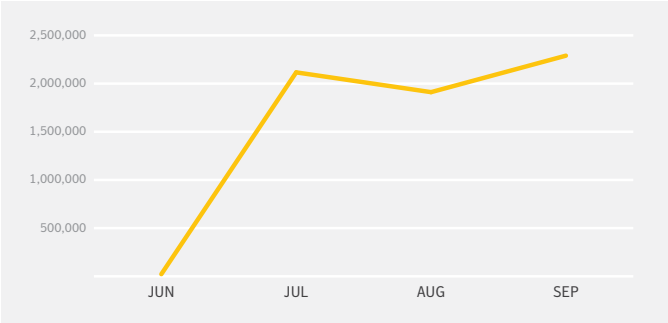
The hailstorm spam technique is an evolution of the snowshoe spam technique, and both have been around for many years. Hailstorm spam is also sent using a large number of sender IP addresses, but hailstorm campaigns are sent out in very high volume over a very short period of time. Hailstorm spammers can send thousands of emails very quickly, and then suddenly stop. Some hailstorm spam attacks take place over such a short period of time that they often end before the fastest traditional anti-spam defenses can update in response to them.

Within the shift to JavaScript downloaders, Symantec saw a significant increase in the use of malicious Windows Script File (WSF) attachments (detected as JS.Downloader) from July onwards. WSF files are designed to allow a mix of scripting languages within a single file. They are opened and run by the Windows Script Host (WSH). Their use as malicious attachments may be due to the fact that files with the .wsf extension are not automatically blocked by some email clients and can be launched like an executable file.

Ransomware, in particular, has been distributed employing this new tactic. In the second half of 2016, Symantec blocked a range of major campaigns distributing Locky (Ransom.Locky) that involved malicious WSF files.

Blocked emails with WSF attachments

The number of blocked emails containing malicious WSF attachments jumped significantly between June and September 2016.

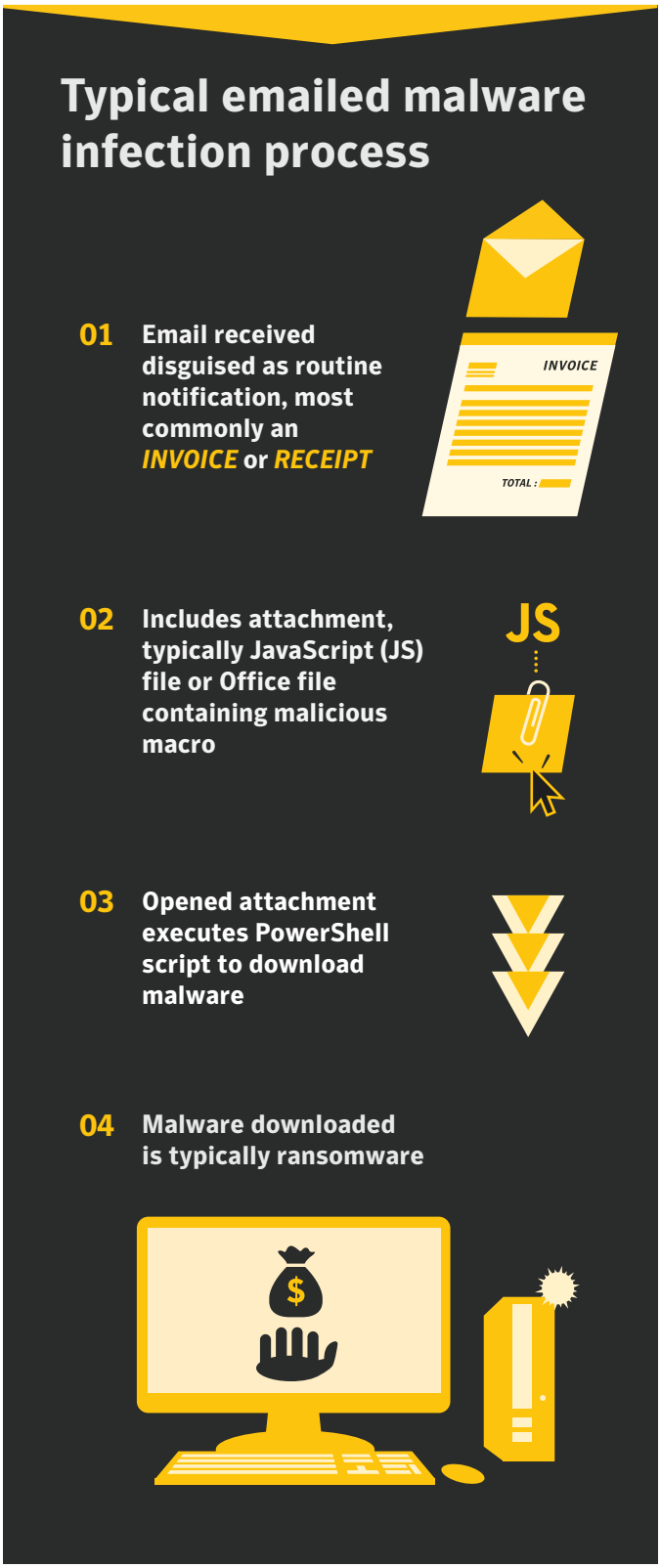


Tried and tested social engineering

While spam campaigns spreading malware rely on a range of tactics, the largest malware spamming operations tend to rely on social engineering tricks. Threats such as Locky ransomware or the Dridex financial Trojan may be spread through emails disguised as financial transaction confirmations.

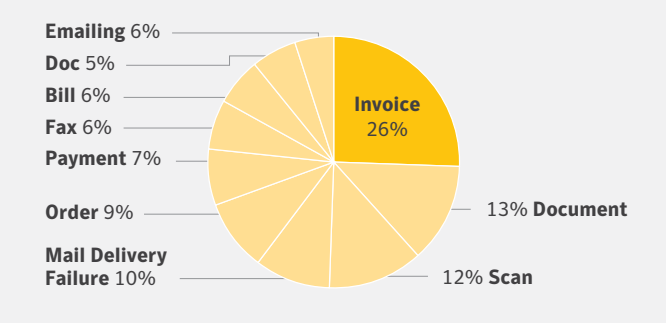
Analysis of 623 major malware spam campaigns logged by Symantec during 2016 found that "Invoice" was the most commonly used keyword in subject lines. Other financial terms such as "Order," "Payment," and "Bill" also figured in the top 10.

The use of financial keywords has been an unchanging feature of malware spam campaigns throughout the year, indicating that attackers are having a high degree of success with this tactic. Since most businesses receive a high volume of routine legitimate emails from customers and suppliers, malicious emails could be inadvertently opened if they aren't blocked by email security software. Consumers, meanwhile, may also be tricked into opening these emails, fearing they have been charged for goods they didn't order.



Keywords used in malware spam campaigns

The top 10 subject line keywords seen in major malware spam campaigns during 2016.

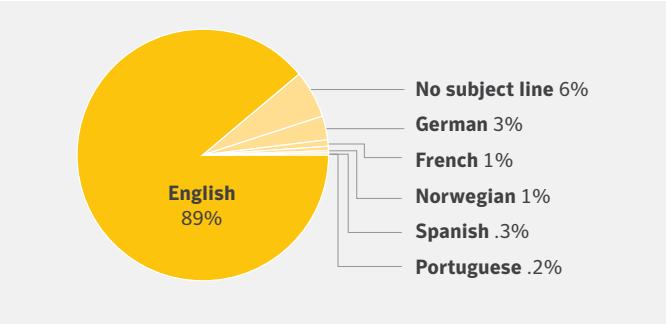


Another common tactic is to disguise emails as coming from a scanner, printer, or multifunction device (MFD). Emails containing the keywords "Scan," "Document," and "Fax" were usually disguised as coming from such devices.

A third tactic seen during 2016 was to disguise malicious spam campaigns as some kind of email delivery failure message. Ten percent of the major spam campaigns analyzed had some form of delivery failure message in the subject line.

Preferred languages used in spam campaigns

The language used in subject lines in major malware spam campaigns, 2016



The vast majority (89 percent) of the major malware spam campaigns analyzed had English-language subject lines. German was a distant second, accounting for three percent, with small proportions of French, Norwegian, Portuguese, and Spanish emails. Interestingly, attackers adopted similar tactics regardless of language, with many non-English campaigns also employing a financial theme. For example, the most popular keyword used in German campaigns was "Rechnung," the German word for invoice.

Social engineering and new messaging platforms

As businesses and consumers move to newer messaging platforms beyond traditional email, attackers will likely seek to leverage these platforms for malicious purposes.

Businesses are increasingly using collaborative tools such as Slack for both internal communication and interactions with customers. In China, WeChat has dominated the messaging space, where it offers extensive features, including a payment system. Where financial transactions go, cyber criminals are likely to follow. WeChat will likely serve as a model for other messaging applications. Facebook Messenger has already increased its focus on the use of automated bots to allow brands to insert themselves into users' conversations.

While some of the techniques used in typical malicious emails are not transferable to other messaging platforms, at the root of email campaigns is the use of social engineering. The lessons learned from the success of email scams and campaigns will likely be applied to messaging platforms as they become more widely adopted by businesses and consumers.

Further reading

- Dridex: Financial Trojan aggressively spread in millions of spam emails each day
- Locky ransomware on aggressive hunt for victims
- Locky, Dridex, and Angler among cyber crime groups to experience fall in activity
- Surge of email attacks using malicious WSF attachments
- Necurs: Mass-mailing botnet returns with new wave of spam campaigns

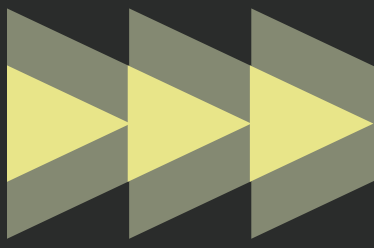
Best practices

- A full protection stack helps to defend against emailed threats. Symantec Email Security.cloud can block email-borne threats and Symantec Endpoint Protection can block malware on the endpoint.
- Delete any suspicious-looking emails you receive, especially if they contain links or attachments.
- Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.
- Always keep your security software up to date to protect yourself against any new malware variants.
- Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by attackers.
- Be suspicious of emails that demand some action without following usual procedures.
- Draft a reply with the supposed sender's email obtained directly from the corporate address book, instead of simply hitting the Reply button, to ensure that a scammer is pushed out of the reply thread.
- Do not reply to suspicious emails and do not give out sensitive information.
- Report suspicious or obviously bogus emails to the proper authorities.
- Enforce an effective password policy on all your employees to ensure passwords are strong and changed regularly.
- Never use links in an email to connect to a website unless you are sure they are genuine. Type URLs directly into the address bar to ensure you are connecting to a legitimate site and not one with an address that simply looks similar.

Web attacks, toolkits, & exploiting vulnerabilities online

Section

05



Symantec

Introduction

A distinct shift in the cyber security landscape occurred in 2016, as web attacks fell by almost a third year-on-year. The shift involved a move away from exploit kits being used as the primary infection vector, to email being the favored threat delivery method of attackers. This is a distinct contrast with 2015, when the number of web attacks doubled from the previous year.

However, this shift from exploit kits to email may not be permanent. Attackers have regularly switched between email and exploit kits and are likely to continue to do so.

Key findings

- Web attacks have dropped by a third (32 percent) year-on-year. However, web attacks are still a big problem, with an average of more than 229,000 being detected every single day in 2016. More than three-quarters (76 percent) of scanned websites in 2016 contained vulnerabilities, nine percent of which were deemed critical.
- Malicious activity from exploit kits dropped by 60 percent in 2016, with our research indicating that attackers are now favoring email as a primary infection vector. The drop in exploit kits is significant, but it does not necessarily mean the threat from attackers is decreasing, rather they are using different methods to spread threats.
- The RIG exploit kit was the most active exploit kit at the end of 2016. It was responsible for 35 percent of all web attacks in December, distributing mainly Ransom.Cerber.
- On average there were 2.4 browser vulnerabilities discovered per day in 2016, a slight drop from 2015, when approximately three browser vulnerabilities were discovered every day.

Trends and analysis

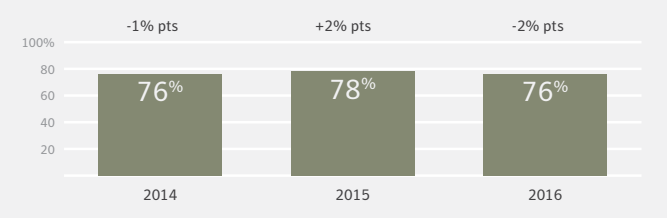
While the web attack and exploit kit figures have fallen, the percentage of websites scanned that contained vulnerabilities remained at the same high level it has been at for the last number of years.

Vulnerability assessment

Our data found that 76 percent of websites scanned contained vulnerabilities—the same percentage as 2014 and just two percent less than the 2015 figure.

Scanned websites with vulnerabilities

Seventy-six percent of scanned websites were found to have vulnerabilities in 2016, down two percent from 2015.

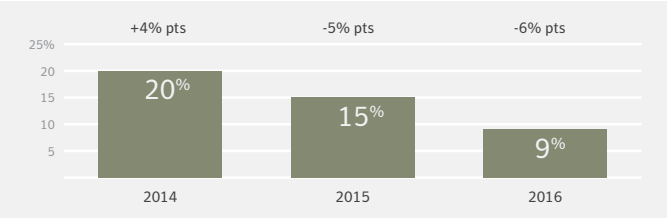


Critical vulnerabilities were down by six percent year-on-year. Nine percent of the websites scanned were found to contain critical vulnerabilities. This compares to 20 percent in 2014, and 15 percent in 2015, appearing to show a trend of steady decline in the number of websites with critical vulnerabilities.

A critical vulnerability is one which, if exploited by attackers, may allow malicious code to be run without user interaction, potentially resulting in a data breach and further compromise of visitors to the affected websites.

Percentage of vulnerabilities which were critical

The percentage of vulnerabilities found to be critical has fallen steadily in the last three years and now stands at nine percent.



Exploit kits

Undoubtedly, the biggest takeaway for web threats in 2016 was the phenomenal drop in exploit kit activity. Exploit kit detections dropped by 60 percent, with some of the most prominent exploit kit families disappearing during the course of the year.

There are a few reasons behind this fall in exploit kit detection numbers. As previously mentioned, and as discussed in depth in the Email: malware, spam, & phishing chapter, our data indicates that over the course of 2016 email became the preferred infection vector for attackers. The email malware rate increased in 2016, from 1 in 220 emails to 1 in 131 emails.

The disappearance of many exploit kit families over the course of the year can also be observed, as analysis of our month-on-month data shows.

The largest percentage of exploit kits detected in 2016, as in 2015, were unclassified. This category is comprised of lots of different, small, unrelated exploit kits that don't fall under the definition of a known exploit kit family.

The Angler exploit kit continued to be the most detected exploit kit family in 2016, dominating for the first half of the year and accounting for more than 50 percent of all exploit kit activity in May. However, Angler activity dropped by nearly 30 percentage points in June and continued to fall to almost non-existent levels by year-end.

This sharp drop in Angler activity coincided with the arrest of 50 people in Russia accused of involvement with the Lurk banking fraud group, and it is widely speculated that this takedown was the reason for the disappearance of this previously dominant exploit kit. For more details, see the case study later in this chapter.

The disappearance of Angler led to a spike in activity for the Neutrino exploit kit in the following months, with its activity jumping by 10 percentage points in June immediately following the drop in activity from Angler. However, by year-end Neutrino's activity levels were largely the same as they were at the start of the year.

Nuclear and Spartan are two other toolkits that largely disappeared in 2016. An exposé on the Nuclear exploit kit that revealed a lot about how it worked is believed to be the reason behind its disappearance. In contrast, the disappearance of Spartan seems to simply be a case of the criminal or criminals behind it deciding to "retire" the exploit kit. Symantec telemetry shows Spartan being extremely active up to the end of March 2016, which is why it appears in the top 10 for the year, but it then disappears.

The disappearance of so many high-profile exploit kits may mean that they are no longer seen as a reliable option. Cyber criminals may not want to purchase an "exploit kit as a service" for fear the exploit kit could simply disappear from circulation in a month's time.

There was an uptick in RIG exploit kit activity in the last quarter of the year, which is probably related to the disappearance of so many other high-profile exploit kit families. The RIG exploit kit was the most active exploit kit at the end of 2016, and was responsible for 35 percent of all attacks in December. These attacks were mainly distributing the Ransom.Cerber ransomware.

Top 10 exploit kits

The Angler exploit kit was the most common exploit kit in use during 2016, and accounted for 22 percent of all exploit kit web attacks. However, Angler activity dropped by nearly 30 percentage points in June and continued to fall to almost non-existent levels by year-end. The RIG exploit kit was the most active exploit kit at the end of 2016, and was responsible for 35 percent of all attacks in December.

Rank	Exploit Kit	2015 (%)	2016 (%)	Percentage Point Difference
1	Unclassified	38.9	37.9	-1.0
2	Angler	13.3	22.2	8.9
3	Spartan	7.3	11.9	4.6
4	RIG	2.0	7.9	5.9
5	Magnitude	1.1	5.8	4.7
6	Neutrino	1.3	5.8	4.5
7	VIP	24.8	3.2	-21.6
8	Nuclear	4.0	1.6	-2.4
9	Fiesta	2.5	1.0	-1.5
10	G01 Pack	2.2	0.8	-1.4

Web attacks

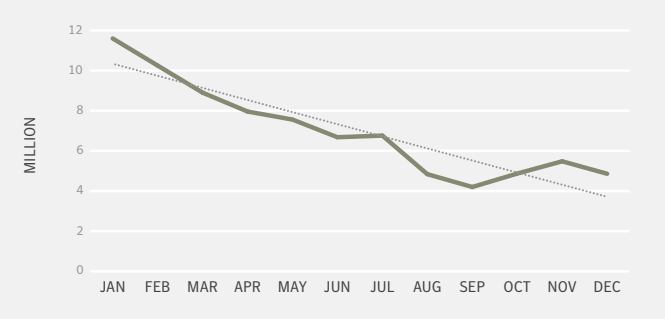
Overall, web attacks dropped more than 30 percent year-on-year between 2015 and 2016. This drop can be explained by attackers moving to email as the primary infection vector. As previously mentioned, email is an easier way for attackers to distribute malware and, in the current climate, is also more reliable. Exploit kits require maintenance of a backend infrastructure and are simply more work for attackers than sending an email.

The important takeaway from this, though, is not that the threats have lessened, rather that attackers are simply using different tactics to spread threats.

Symantec telemetry shows that the drop in web threats was almost continuous for the 12 months of 2016. They reached their lowest point in September, increasing slightly in October and November, before falling back again in December.

Web attacks blocked per month

The number of web attacks per unique system fell steadily throughout 2016.



Despite this general drop in web threat activity, it is still a major threat, with Symantec blocking an average of more than 229,000 *unique* web attacks on endpoint computers every day in 2016. Data from Blue Coat web gateway products that operate at the network level shows that, by the end of 2016, the number of web threats blocked at the gateway grew by 24 percent compared with the same period in 2015. However, the rate of increase is down, when compared to a growth of 124 percent from 2014 to 2015.

Technology- and business-related websites were the most frequently exploited website categories in 2016. Technology websites were exploited nearly twice as much as business-related websites. Search, which was the third-most frequently exploited category in 2015, dropped out of the top 10 in 2016.

Classification of most frequently exploited websites

Technology- and business-related websites were the most popular for hosting malicious content and malvertising in 2016.

Rank	Domain Categories	2015 (%)	2016 (%)	Percentage Point Difference
1	Technology	23.2	20.7	-2.5
2	Business	8.1	11.3	3.2
3	Blogging	7.0	8.6	1.6
4	Hosting	0.6	7.2	6.6
5	Health	1.9	5.7	3.8
6	Shopping	2.4	4.2	1.8
7	Educational	4.0	4.1	< 0.1
8	Entertainment	2.6	4.0	1.4
9	Travel	1.5	3.6	2.1
10	Gambling	0.6	2.8	2.2

Browser vulnerabilities

On average, there were 2.4 browser vulnerabilities discovered per day in 2016. The number of publicly announced browser vulnerabilities dropped during the year, with Microsoft Internet Explorer/Edge experiencing the biggest drop in vulnerabilities. This may be explained by the fact that there was no new version of Explorer released in 2016, with Microsoft essentially ending its development. Usage of the Explorer browser also plummeted during the year. Microsoft's new browser, Edge, is only available to people using Windows 10, and its new security architecture makes it more difficult to successfully exploit.

The number of vulnerabilities in Firefox and Safari also dropped, while Symantec measured a slight increase in the number of Google Chrome vulnerabilities. However, an unusually high number of browser vulnerabilities were discovered in 2015, partially due to the high number of zero-day vulnerabilities discovered that year. In 2016, the figures for browser vulnerabilities really just returned closer to "normal" levels, but are still quite high.

Case study

Angler: The rise and fall of an exploit kit

The Angler exploit kit first appeared on the threat landscape in late 2013, following the demise of the Blackhole exploit kit in October that year. It became fairly popular straight away, but it really took off in 2015, when it dominated the exploit kit landscape.

Angler was a sophisticated exploit kit that pioneered many technical advances that other exploit kits subsequently followed, such as including the use of anti-cyber security countermeasures. Angler was able to download and execute malware from memory, without needing to write any files to disk, in an attempt to evade detection by traditional security technology. It was also very fast at integrating new zero-day exploits into its arsenal, which would account for its growth in popularity in 2015. There were a lot of zero-day vulnerabilities discovered in 2015, including a number in Adobe Flash Player, which was commonly targeted by Angler.

One of Angler's big advantages over other exploit kits was that it could bypass many traditional security countermeasures. It used a number of techniques to evade detection, including switching host names and IP numbers rapidly, and it also used domain shadowing—registering domain names that look like they belong to legitimate websites—to piggyback on legitimate domains.

Angler was one of the most active exploit kits throughout 2015. Symantec's intrusion protection system blocked hundreds of thousands of attacks by it on a daily basis. Total blocks on Angler-based attacks numbered more than 19.5 million in 2015 alone. Angler's primary delivery mechanism was malvertisements, and it mostly exploited Adobe Flash vulnerabilities. Computers running Windows, particularly Windows 7, were its favored targets.

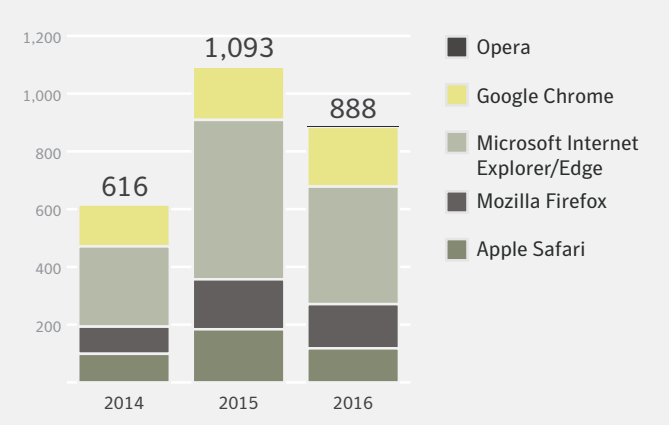
Angler was primarily used to spread ransomware. Its demise in June 2016 coincided with a decline in detections of CryptXXX ransomware (Ransom.CryptXXX), which was primarily spread using Angler.

Angler suffered a decline in activity at the beginning of 2016 but quickly ramped up again before disappearing completely in June. Its demise followed the arrest of 50 people by authorities in Russia who were allegedly associated with the Lurk banking fraud group. It's widely believed these arrests are the reason behind Angler's demise.

The demise of such a previously dominant exploit kit has left something of a gap in the market, which was temporarily filled by a rise in activity by the Neutrino exploit kit. Cyber criminals are sure to find a way to fill that gap before long.

Browser vulnerabilities

The number of browser vulnerabilities discovered dropped from 1,093 in 2015 to 888 in 2016.



Another possible reason behind the fall in browser vulnerabilities is that, due to an increased number of bug bounty programs, and the increased participation of security researchers in them, many browser vulnerabilities have been discovered and patched in previous years and the "low-hanging fruit" that may once have been exploited by malicious actors is no longer there.

Further reading

Locky, Dridex and Angler among cyber crime groups to experience fall in activity

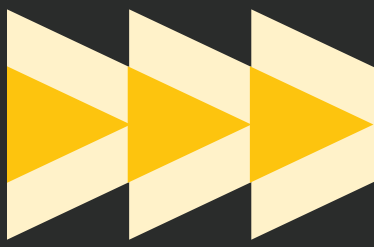
Best practices

- Regularly assess your website for any vulnerabilities.
- Scan your website daily for malware.
- Set the secure flag for all session cookies.
- Secure your websites against man-in-the-middle (MITM) attacks and malware infection.
- Choose SSL Certificates with Extended Validation to verify protection and display the green browser address bar to website users.
- Display recognized trust marks in highly visible locations on your website.
- Be picky about your plugins. The software you use to manage your website may come with vulnerabilities too. The more third-party software you use, the greater your attack surface, so only deploy what's absolutely necessary.

Cyber crime & the underground economy

Section

06



Symantec

Introduction

Two distinct sides to cyber crime emerged in 2016. Traditional mass-market cyber crime groups carried out large-scale email campaigns to distribute "commodity" malware such as ransomware and online banking threats. While their motivations and payloads remained largely the same, their distribution methods have shifted away from web-based exploit kits to more traditional methods, in particular the use of email attachments.

The other side of cyber crime is made up of organized criminal groups, responsible for a number of sophisticated financial heists. However, it wasn't just professional criminals conducting these campaigns—there has been evidence of nation-state involvement as well.

Both mass-market and targeted cyber crime groups have adopted tactics referred to as "living off the land." This trend, as discussed in the Targeted attacks chapter, shows attackers leveraging operating system and application features coupled with publicly available tools in lieu of exploiting vulnerabilities and developing custom tools.

Key findings

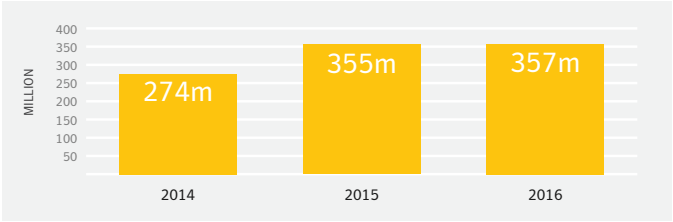
- Cyber crime hit the big time in 2016, with high-profile victims and bigger-than-ever financial rewards. The Banswift (Trojan.Banswift) attacks that took place in 2016 were also the first time there were strong indications of state involvement in financial cyber crime.
- Mass-market cyber crime remains strong despite disruption efforts. Attackers adapted their methods for distributing traditional cyber crime malware. In particular the use of JavaScript downloaders and malicious macro downloaders in Office files was widespread and accounted for just over 7 million attempted infections in 2016.
- While the number of data breaches in 2016 remained steady compared to 2015, the number of identities stolen increased significantly. Almost 1.1 billion identities were stolen in 2016, a big jump from the 563.8 million stolen in 2015.
- Nearly 100 million bots were observed in 2016, an increase of seven percent from 2015.

Malware

Malware continues to be a blight on the threat landscape with more than 357 million new variants observed in 2016. However, for the first time, the rate of new malware seen on the endpoint has remained largely stagnant in 2016 – increasing by half a percent.

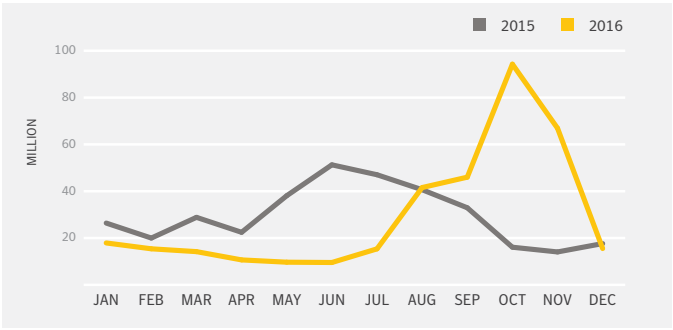
Unique malware variants detected for the first time

There was a slight (0.5 percent) increase between 2015 and 2016 in unique malware variants detected for the first time.



Monthly count of unique malware variants first seen in 2016

In this month-by-month measure of unique malware variants first seen in 2016, a clear spike can be seen in October.

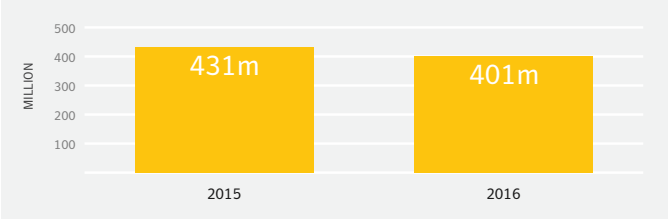


While the rate of new malware variants was stable for the early part of 2016, the latter half of the year saw an explosion in new variants. This was driven mainly by the high volume of ransomware downloaders propagated over email by the Necurs (Backdoor.Necurs) botnet, which is discussed in further detail later in this chapter.

In previous reports, Symantec took a slightly different approach to counting malware variants, focusing on variants unique for that year only, rather than malware first seen in that year. Using this legacy methodology on 2016 data shows a slightly higher volume of variants but a seven percent decline in new variants year on year.

Unique malware variants detected

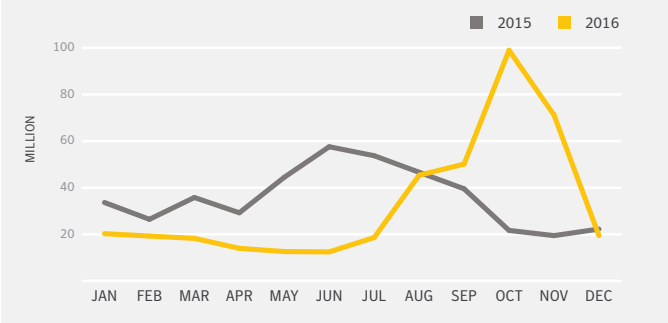
There was a slight drop between 2015 and 2016 in the number of unique malware variants detected.



Breaking the data down month by month shows an almost identical trend with a notable uptick in variants towards the end of the year.

Monthly count of unique malware variants in 2016

The count of unique malware variants also shows a spike in October.



Looking at this data in isolation, it may appear that the malware problem is stabilizing or even improving; however, looking at the bigger picture, it is clear this isn't the case. Many attacks are blocked earlier in the attack chain and aren't represented in malware volume numbers, which focus primarily on the final or close-to-final payloads. As discussed in the Email chapter, email accounted for a large volume of malware distributed in 2016. Symantec has also continued to block a large number of web attacks. This leads to fewer final payloads being delivered and, therefore, a lower total number of variants seen.

There are other explanations too: a lower incidence of polymorphic threats and attackers relying less on malware to carry out their deeds. This is a phenomenon referred to as "living off the land."

Living off the land: PowerShell, macros, and social engineering

A trend emerged in 2016 that saw attackers use legitimate Windows programs to download and execute payloads. This tactic of "living off the land" is discussed in greater detail in the Targeted Attacks chapter; however, the techniques used by advanced attackers have also been seen in the cyber crime world.

PowerShell, a powerful scripting language and shell framework, has become a mainstay of the infection chain and appeals to attackers for a number of reasons. It is installed by default on most Windows computers, and most organizations do not have extended logging enabled for it, making malicious PowerShell activities largely invisible. Scripts can also easily be obfuscated, which hides their malicious intent. It allows for payloads to be executed directly from memory, meaning that attackers leave fewer traces behind.

An analysis by Symantec in late 2016 showed that 95.4 percent of inspected PowerShell scripts were found to be malicious. Malicious PowerShell scripts are primarily used as downloaders during the initial infection phase, but can also be used for lateral movement across a network. This lateral movement is typically seen in targeted attacks to enable a threat to execute code on a remote computer when spreading inside the network. When it comes to cyber crime attacks, PowerShell is used to facilitate the download and execution of the final payload.

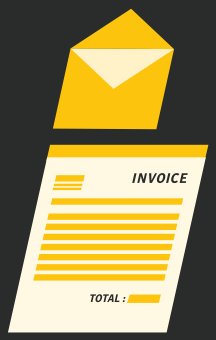
The use of PowerShell increased sharply during 2016. Blue Coat's Malware Analysis sandbox received 22 times as many samples using PowerShell in the third quarter of 2016 compared to the second quarter. This was likely due to increased activity associated with JavaScript downloaders and Trojan.Kotver in this time period. Overall, our analysis found PowerShell was used most frequently with W97M.Downloader (9.4 percent of samples), followed by Kovter (Trojan.Kotver) at 4.5 percent, and JS.Downloader (4 percent). Kovter is notable for its use of PowerShell to create a fileless infection completely contained in the registry.

More advanced targeted cyber crime groups also leveraged PowerShell in 2016. The Odinaff group used malicious PowerShell scripts to attack financial organizations. These attacks are discussed later in this chapter.

Malicious Office macros continue to be popular with attackers as evidenced by the prevalence of detections (discussed below). Office macros don't run by default, so these attacks rely on social engineering to convince users to launch the macro when opening an Office attachment. By using features like PowerShell and macros, attackers don't need to rely on software exploits or custom tools that are more likely to arouse suspicion while requiring more time and skill to use.

Typical attack scenario in 2016 took the following steps:

01 An attacker sends an email, typically masquerading as an ***INVOICE*** or ***BILL***



02 The email contains an attachment, usually an office file, JavaScript (JS), or another scripting type

03 When the file is launched, it will either prompt users to execute a macro or will launch PowerShell to download and execute the final payload

04 The final payload is typically ransomware but may also be an online banking threat such as Dridex

There are also attacks which don't rely on any malicious code or system features. Business Email Compromise (BEC) attacks, discussed in-depth in the chapter on email, rely solely on social engineering to trick victims into giving up large sums of money.

While this trend shows a movement away from exploits and custom tools, it's important to note that there is a malware component to almost every attack. This means that malware will continue to persist as a problem. Additionally, this shift doesn't mean that attackers are becoming less sophisticated. In fact, it demonstrates an increase in efficiency and an ability to hide in plain sight.

Malware prevalence and trends

Generic detections dominated the most prevalent malware detected on the endpoint in 2016.

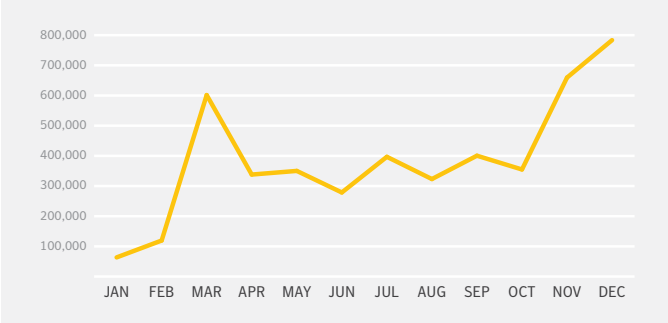
Rank	Detection	Number of Infections
1	Heur.AdvML.B	5,648,434
2	JS.Downloader	3,487,119
3	Packed.Dromedan!lnk	2,615,857
4	W97M.Downloader	2,199,083
5	Heur.AdvML.C	2,039,212
6	SMG.Heur!cg1	1,291,550
7	W32.SillyFDC	1,019,644
8	Trojan.Startpage	908,429
9	W32.Downadup.B	814,687
10	Infostealer	753,783

Looking at the most prevalent malware highlights, the impact of generic or heuristic malware detections is notable. They account for nine out of the top 10 types of malware detected on the endpoint in 2016. However, it's important to note the prominence of JS.Downloader and W97M.Downloader, which are new entries in 2016's prevalence list.

In 2016, Symantec observed a large number of email campaigns distributing ransomware and online banking threats via malicious Office macro (W97M.Downloader and variants) and JavaScript downloader files (JS.Downloader and variants). Between them they have accounted for 7 million detections on the endpoint in 2016 and have dominated the cyber crime threat landscape, particularly in the latter half of the year.

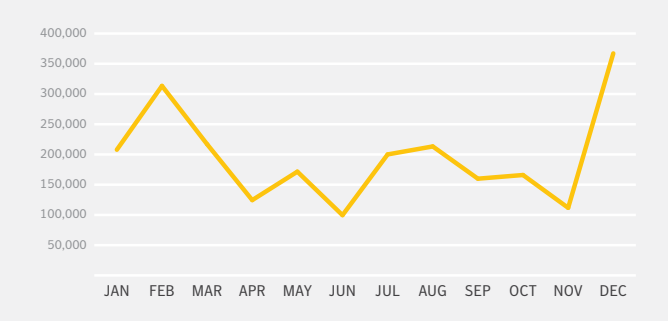
JavaScript downloader detections per month

JavaScript downloader detections (JS.Downloader and variants) increased in the second half of 2016.



Office macro downloader detections per month

There was a spike in Office macro detections (W97M.Downlader and variants) in December 2016.



These downloaders are favored by attackers for a variety of reasons. Businesses are unlikely to block all Office files at the email gateway as it could affect legitimate emails, which accounts for the popularity of Office macro downloaders. Meanwhile, ease of obfuscation in an attempt to evade detection has contributed to the increase of JavaScript downloaders. As previously discussed, JS.Downloader will typically use PowerShell or a Visual Basic Script (VBS) to execute the final payload in an attempt to fly below the radar.

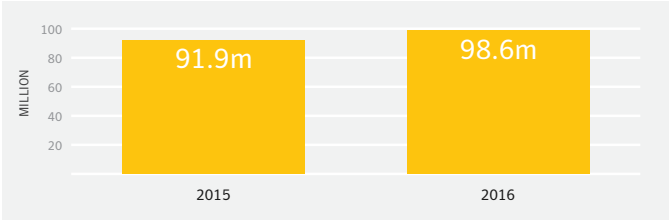
Symantec research indicates that some groups favor W97M.Downloader, while others prefer JS.Downloader. Activity around W97M.Downloader dropped in the second half of 2016, but Symantec believes the groups using it are likely to increase activity again. In fact, an increase in W97M.Downloader detections was observed in the final month of 2016.

Many of these threats are being primarily propagated by spam botnets.

Symantec observed an uptick in bot numbers in 2016. The figure jumped from 91.9 million to 98.6 million bots making up various botnets.

Bot activity numbers

Symantec observed 6.7 million more bots in 2016 than 2015.



Some malware took further precautions in order to be even stealthier. Twenty percent of malware is now routinely able to detect and identify the presence of a virtual machine environment, an increase from 16 percent in 2015.

Blue Coat's Malware Analysis sandbox tracked an increased use of the SSL protocol for communication with command and control (C&C) servers, making it more difficult to inspect network traffic. Such behavior increased by 79 percent, resting at 3.1 percent at the end of 2016. This was probably due to SSL certificates becoming more easily available in 2016, and attackers realizing that they had an improved chance of passing through the gateway undetected if they used SSL encryption. Furthermore, the communication to cloud services doubled to more than four percent in 2016.

One percent of all threats used the Tor network. In those cases, it was primarily used by ransomware to deliver payment instructions.

Botnet case study: Necurs

The Necurs botnet was one of the main distributors of malware in 2016 and was responsible for massive email campaigns distributing JavaScript, VBS, and Office macro downloaders. Necurs' primary payload in 2016 was Ransom.Locky. Other major botnets observed by Symantec were used to spread threats such as Dridex (W32.Cridex), Cerber (Ransom.Cerber), and Kotver (Trojan.Kotver), as well as Locky.

Necurs was one of the most active botnets distributing malware in 2016. The operators behind Necurs stuck to the average working week. Threats were distributed Monday through Friday and there was little activity on weekends.

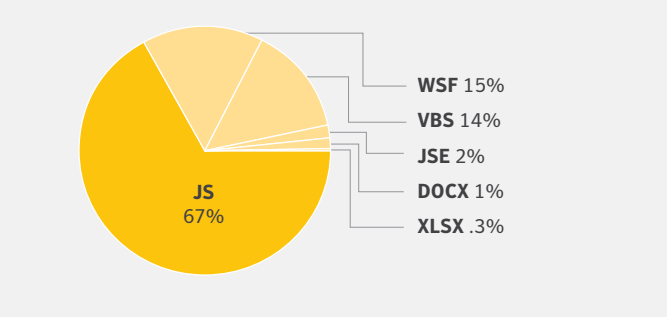
Looking at just one day of Necurs activity, the scale of it is clear. On November 24, 2016, Necurs sent five spam campaigns—two delivering JavaScript downloaders, two delivering .wsf attachments, and one delivering a VBS attachment. These five spam runs sent out more than 2.3 million spam emails—more than 1.8 million used JS downloaders, while just under 465,000 used VBS.

Research by Symantec into 146 email runs carried out by Necurs in the last quarter of the year found that it was responsible for sending out an average of 525 unique malware samples in every email run.

Looking at spam runs primarily involving JS, VBS, and WSF downloaders, our research found that JavaScript downloaders were by far the most popular type of downloader distributed by Necurs.

Downloaders delivered by Necurs spam botnet

In the period observed by Symantec, Necurs predominantly sent spam campaigns involving JS.Downloader.



When this study of Necurs began at the end of October, threats were primarily being spread using VBS, but in November and December JavaScript downloaders dominated.

This use of different downloaders indicates that Necurs was a "botnet for hire" that was being used by different attack groups.

Interestingly, Symantec observed Necurs' activity ceasing for almost three months from the end of December. Its last spam run started on December 22 and ended on December 24. While it was first thought that this was just a case of the group behind Necurs taking a break for the holidays, the botnet remained quiet until March 20, 2017.

Necurs' disappearance led to a big drop in the volume of malicious email being sent in late 2016 and early 2017. The reason behind its disappearance remains a mystery. Symantec blocked almost two million malicious emails on March 20, the day of its return. The fact that Necurs was able to resume massive spam campaigns on its return indicates that, whatever the reason for its absence, it appears to have lost none of its capabilities.

It's all about the money: Financial malware

Financial malware, specifically threats targeting online banking, has historically been a large driver of cyber crime. However, a number of arrests and takedowns, coupled with the continued success of ransomware, means that it has become less dominant.

Infection data shows that this area is dominated by five families, while activity outside of this top five is negligible.

Top 10 financial Trojans

The list of top 10 financial Trojans shows that a handful of financial Trojans dominated the landscape in 2016.

Rank	Financial threats	Impacted machines
1	Ramnit	460,673
2	Bebloh	310,086
3	Zbot	292,160
4	Snifula	121,624
5	Cridex	23,127
6	Dyre	4,675
7	Shylock	4,512
8	Pandemiya	3,330
9	Shifu	2,177
10	Spyeye	1,480

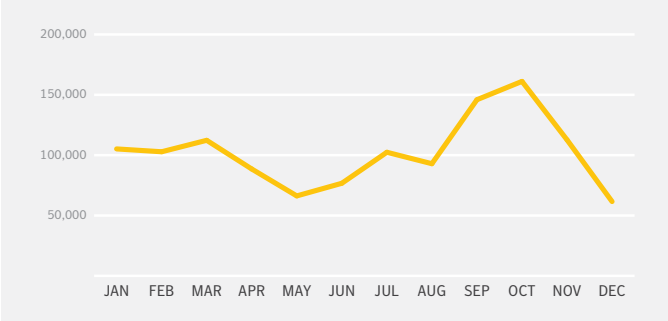
Ramnit (W32.Ramnit) made a triumphant return to the world of financial fraud in 2016. Ramnit has been in operation since 2010 but a takedown of the cyber crime gang behind it in February 2015, which Symantec assisted in, was believed to have shut down the botnet's operations. It is believed that the botnet was made up of 350,000 computers at the time of the takedown. Ramnit disappeared for some time, but a new variant was observed in December 2015.

Ramnit went on to dominate financial Trojans in 2016 and was detected at a high rate consistently for the whole year. Interestingly, as Ramnit was often distributed via the Angler exploit kit in the past, it did not show any drop in activity following the disappearance of Angler in the middle of the year. This indicates the actors behind it may have adjusted their infection techniques, and there were reports of Ramnit being spread through email in the UK. The fact that some Ramnit variants self-replicate contributed to its prevalence.

There were reports in 2016 of Bebloh (Trojan.Bebloh), which occupies the second spot in the financial Trojans list, undertaking aggressive campaigns in Japan, targeting small banks and credit unions. Bebloh also drove a big spike in financial Trojan activity in September and October. Bebloh was part of the Avalanche malware-hosting network, which was taken down in 2016, and saw a sharp drop in activity in November and December.

Financial Trojan activity by month

The downturn in activity after October 2016 reflects the impact of a number of high-profile takedowns.



The alleged hacker behind the Neverquest banking malware, which Symantec detects as Trojan.Snifula, was also arrested in January 2017. All these factors could mean the financial Trojans top five could look very different at the end of 2017.

The impact of takedowns, covered in more detail later in this chapter, is reflected in the downturn in infection numbers after October 2016. Significant drops in activity from Dridex (which dominated the threat landscape in 2015), Dyre, and Shylock (Trojan.Shylock) can all be attributed to takedowns.

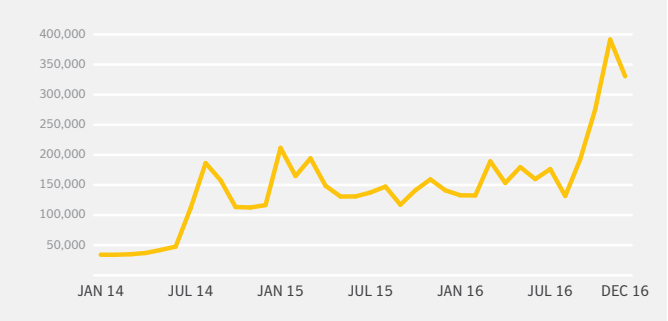
Up to the Mac

Apple's operating system, which was once seen as being almost impregnable, saw an increasing amount of malware being detected on it over the course of 2016.

A steady increase in malware being detected on Macs began in September and continued through the last quarter of the year; almost three times as many malware detections occurred in November 2016 compared to the start of the year.

Mac malware distribution per month, 2014-2016

The growth in Mac malware in the second half of 2016 can clearly be seen.



However, these figures do not necessarily mean that attackers are increasingly targeting the Mac ecosystem.

Looking more closely at the malware blocked on OS X endpoints, JavaScript downloaders (JS.Downloader) and Office macro downloaders (W97M.Downloader) are two of the main infection vectors, accounting for three of the top five. JS.Nemucod, which delivers Locky ransomware, also features in the top 10.

It's more likely that Mac users are being caught up in email campaigns spreading threats using JS.Downloader, W97M.Downloader, and JS.Nemucod rather than that threat actors are increasingly targeting Mac users.

This is also evident in an uptick in malware detected on Mac in November and December, a time when an increase in incidents of JS.Downloader and W97M.Downloader also took place.

The other detections that make up the top five, OSX.Malcol and OSX.Malcol.2, are generic detections that protect against many individual but varied OS X Trojans.

Top 10 malware blocked on OS X endpoints as percentage of total infections

JS.Downloader and W97M.Downloader both feature in the top five for malware blocked on OS X endpoints in 2016.

Rank	Detection	Total Infections(%)
1	OSX.Malcol	6.88
2	JS.Downloader	5.76
3	OSX.Malcol.2	5.73
4	W97M.Downloader	5.11
5	JS.Downloader.D	1.87
6	JS.Nemucod	1.09
7	VBS.Downloader.B	1.04
8	VBS.Downloader.Trojan	0.83
9	Trojan.Malscript	0.59
10	SMG.Heur!cg1	0.57

Odinaff and Banswift: The year of the targeted financial heist

While the cyber crime threat landscape is typically dominated by indiscriminate, mass attacks, 2016 saw the emergence or reemergence of more sophisticated and elite cyber crime groups. While traditional cyber crime takes a more "smash and grab" approach, the elite criminals leverage techniques typically seen in advanced targeted attacks. The resources, patience, and sheer bravado needed to execute these attacks demonstrates how cyber crime is potentially entering a new era.

The emergence of two groups targeting the inner workings of the international financial system, while traditional online banking threats declined, shows how financial institutions are facing a much different kind of threat in 2017.

Banswift

A cyber heist on Bangladesh's central bank in early 2016 was one of the most audacious bank heists ever. The criminals successfully got away with US$81 million and, but for a typo and the suspicions of eagle-eyed bank officials being raised, could have made off with $1 billion.

The criminals exploited weaknesses in the Bangladesh Bank's security to infiltrate its system and steal the bank's SWIFT credentials, which allowed them to make the fraudulent transactions.

The criminals then used malware to cover their tracks. The malware was able to doctor the Bangladesh Bank's printed transaction confirmation messages in order to delay discovery of the fraud. The attackers also carried out the attack at the start of a long weekend in Bangladesh, to further reduce the chance of the thefts being discovered.

Using the stolen SWIFT credentials from the Bangladesh Bank, the criminals made several transfer requests to the Federal Reserve Bank of New York for it to transfer the Bangladesh bank's money, primarily to locations in the Philippines and Sri Lanka. Four requests to transfer a total of $81 million to entities in the Philippines successfully went through, but a request to transfer $20 million to a non-profit "foundation" in Sri Lanka raised suspicions because foundation was spelled incorrectly. This led to the transfers being suspended and clarification being sought from Bangladesh, which uncovered the fraud. However, by then the $81 million had disappeared, primarily into accounts related to casinos in the Philippines.

Most of that $81 million remains unrecovered, however, $15 million was returned by a casino in the Philippines to the Bangladesh Central Bank in November.

The methods used in this attack, in particular the in-depth knowledge of the SWIFT systems and the steps taken to cover tracks, are indicative of highly proficient actors. This was an incredibly audacious hack, and was also the first time strong indications of nation-state involvement in financial cyber crime had been observed. The attack was linked to nation-state actors in North Korea.

Symantec's analysis of the malware (Trojan.Banswift) used in the attack on the Bangladesh bank found evidence of code sharing between this malware and tools used by Lazarus—which the FBI claims has links to the North Korean government. The Lazarus group was associated with the infamous Sony hack in 2014, and has been linked to a string of attacks against the US and South Korea since 2009.

This same group was also linked to two other bank heists targeting banks that make transfers using the SWIFT network, though the SWIFT network itself was not compromised in any of these attacks.

Vietnam's Tien Phong Bank revealed that it had intercepted a fraudulent transfer of more than $1 million in the fourth quarter of 2015. Research by Symantec also uncovered evidence that another bank was targeted by the same group in October 2015.

A third bank, Banco del Austro in Ecuador, was also reported to have lost $12 million to attackers using fraudulent SWIFT transactions, although no definitive link could be made between that fraud and the attacks in Asia.

Symantec believes the Lazarus group may have reappeared in 2017 with further attacks against financial institutions.

Odinaff

A campaign involving Trojan.Odinaff was discovered to be targeting financial organizations worldwide in 2016. The attacks leveraging Odinaff were sophisticated and clearly carried out by a professional cyber criminal gang. While also targeting users of SWIFT, there is no evidence linking these attacks with the Banswift attacks.

Symantec research indicates that campaigns using Odinaff began in January 2016 and were focused on organizations in the banking, securities, trading, and payroll sectors. The Odinaff Trojan was typically deployed in the first stage of an attack to gain a foothold on the network.

Attacks involving Odinaff were highly sophisticated, requiring a large amount of hands-on involvement, with methodical deployment of a range of lightweight back doors and purpose-built tools onto computers of specific interest.

The Trojan was most commonly deployed in documents containing malicious macros, while botnets were also used to deploy it. The attacks were carefully managed, with the threat actors maintaining a low profile on the targeted organization's network, only downloading and installing new tools when necessary.

Tools used in the Odinaff attacks bear the hallmarks of the infamous Carbanak group, which has been targeting the financial sector since 2013.

Carbanak's activities were discovered in late 2014 and the group is believed to have targeted hundreds of banks in multiple countries. Some members of the cyber security community estimate that they may have stolen up to $1 billion. Symantec discovered multiple links between Carbanak and the Odinaff attackers, however, the infrastructure crossover is atypical, meaning Odinaff could be operating in loose cooperation with Carbanak if it is not part of the wider Carbanak organization.

The Odinaff and Banswift attacks demonstrated that, while in 2016 many attackers moved back to utilizing existing tools and techniques, there are still cohorts of extremely sophisticated cyber criminals deploying advanced campaigns for big financial reward.

Data breaches and the underground economy

Data breaches

In the last eight years, more than seven billion online identities have been stolen in data breaches, which is almost the equivalent of one for every person on the planet.

In 2016, more than 1.1 billion identities were stolen in data breaches, almost double the number stolen in 2015, when just over 563 million identities were stolen. This is the despite the fact that the number of data breaches actually fell between 2015 and 2016—dropping from 1,211 to 1,209.

The average number of identities stolen per breach in 2016 jumped to almost 1 million—the highest average of the last three years.

In 2016, there were 15 mega breaches—breaches in which more than 10 million identities were stolen—an increase from 11 in 2014 and 13 in 2015.

Data breaches, 2014-2016

While the number of data breaches in 2016 remained fairly steady, the number of identities stolen increased significantly.

Year	Breaches	Identities stolen	Average per breach	Mega breaches
2014	1523	1,226,138,929	805,081	11
2015	1211	563,807,647	465,572	13
2016	1209	1,120,172,821	926,528	15

Data breaches also hit the headlines in 2016—primarily due to Yahoo. In September, the company revealed that a breach in 2014 led to 500 million of its user accounts being compromised. Then, in December, it revealed that in August 2013, more than 1 billion user accounts were compromised—making it the largest data breach that has ever been reported.

The company said it believes the two breaches are connected and that the attacks are state-sponsored. The revelations have had serious implications for the company, which is in the midst of being sold to Verizon, and it has seen its value plummet as a result of these revelations.

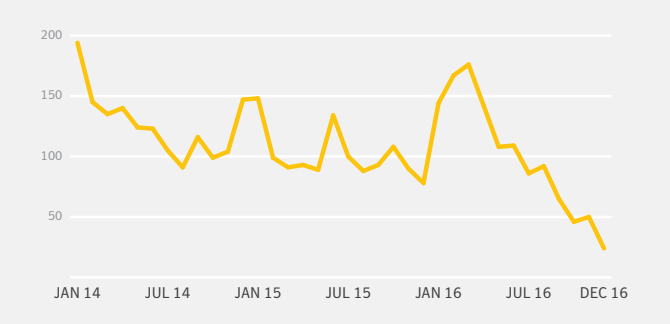
Year in review

While news of the Yahoo data breaches broke in 2016, they are not included in Symantec's telemetry for the year, as Symantec records a data breach when it takes place, rather than when it is reported.

The number of breaches per month in 2016 was highest at the start of the year and then tapered off towards the end of the year. This is fairly typical for data breaches as often there is a gap between a data breach occurring and it being reported, as can clearly be seen in the case of the Yahoo breaches, so data breaches that took place towards the end of 2016 may not have been reported yet.

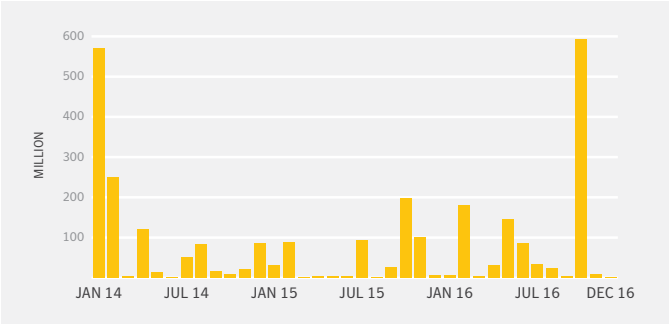
Data breaches per month, 2014-2016

The number of data breaches per month tapered off at the end of 2016. It is likely that data breaches that occurred in November and December have not yet been reported.



Identities stolen by month, 2014-2016

There was a spike in identities stolen in October 2016, which was largely caused by a breach of Friend Finder Networks.



While the number of data breaches tapered off towards the end of the year, the number of identities stolen peaked in October, rising to almost 600 million. This surge can be largely attributed to a data breach of Friend Finder Networks, which exposed the private details of 412 million user accounts.

Friend Finder Networks is an adult dating and pornography site company that operates sites including Adult Friend Finder and Cams.com, as well as some other smaller websites. It also ran Penthouse.com, which it sold in February 2016. Despite this, Adult Friend Finder still had Penthouse.com user details stored and, as a result, these were also exposed in the breach.

The breach saw email addresses, passwords (which were stored in either plain visible format or SHA1 hashed), dates of last visits, browser information, IP addresses, and site membership status exposed. It was the second hack on the organization in just over a year.

Types of data lost in breaches in 2016

Personally Identifiable Information was still the most common form of data to be lost in 2016, but Personal Financial Information was not far behind.

Type	2015 (%)	2016 (%)	Percentage point difference
Personally Identifiable Information (PII)	54.5	42.9	-11.6
Personal Financial Information (PFI)	32.9	39.2	6.3
Other information	1.6	11.1	9.5
Personal Health Information (PHI)	11.0	6.8	-4.2

Almost 40 percent of information lost in data breaches in 2016 was Personal Financial Information, which could include credit or debit card details or banking financial records. This figure increased by more than six percentage points from 2015.

The exposure of financial data in data breaches is serious as those affected have a direct risk of financial loss if this data is exploited.

Data breach causes

Theft of Data was the cause behind the highest percentage (36 percent) of data breaches in 2016, as it was in 2015. It was followed by Improper Use of Data, Unclassified or Other Cause (where the cause could not be determined), and Phishing, Spoofing, or Social Engineering.

Top 10 causes of data breaches in 2016

Theft of Data led the way as the main cause of data breaches in 2016, accounting for more than a third of breaches.

Rank	Cause	2015 (%)	2016 (%)	Percentage point difference
1	Theft of Data	42.4	36.2	-6.2
2	Improper Use of Data	20.4	19.3	-1.1
3	Unclassified or Other Cause	11.9	19.2	7.3
4	Phishing, Spoofing, or Social Engineering	21.8	15.8	-6.0
5	Accidental Data Loss	1.7	3.2	1.5
6	Loss or Theft of Device	0.6	3.1	2.5
7	IT Errors Leading to Data Loss	0.5	1.6	1.1
8	Network Disruption or DDoS	0.3	1.6	1.3
9	Extortion, Blackmail, or Disruption	0.1	0.2	0.1
10	Identity Theft or Fraud	0.1	0	-0.1

While Theft of Data is the cause of just over a third of data breaches when looking at number of breaches, when measuring by the number of identities stolen, more than 91 percent of breaches fall into this category.

Top 10 causes of data breaches by identities stolen in 2016

Theft of Data was responsible for the vast majority of identities stolen in 2016.

Rank	Cause	2015 (%)	2016 (%)	Percentage point difference
1	Theft of Data	85.3	91.6	6.3
2	Phishing, Spoofing, or Social Engineering	9.8	6.4	-3.4
3	Accidental Data Loss	1.1	1.0	-0.1
4	IT Errors Leading to Data Loss	< 0.1	0.9	0.9
5	Network Disruption or DDoS	< 0.1	< 0.1	< 0.1
6	Improper Use of Data	3.3	< 0.1	-3.3
7	Loss or Theft of Device	< 0.1	< 0.1	< -0.1
8	Unclassified or Other Cause	0.4	< 0.1	-0.4
9	Extortion, Blackmail, or Disruption	< 0.1	< 0.1	< 0.1
10	Identity Theft or Fraud	< 0.1	0	< -0.1

Industries exposed

Services was the industry most affected by data breaches during 2016, with almost 45 percent of breaches occurring in that sector, followed by the Finance, Insurance, and Real Estate sector at 22 percent. This is the same top two as 2015. Looking at a more detailed breakdown into sub-sectors, the Business Services industry had the highest percentage of data breaches (24 percent), followed by Health Services (11 percent).

Due to the sensitivity of the information that could be revealed, there are strict rules about reporting data breaches in the Health Services industry, which would account for it appearing so high on the list.

Top 10 sectors breached by number of incidents

Services was the industry most affected by data breaches in 2016.

Rank	Industry	Breaches	Percent
1	Services	452	44.2
2	Finance, Insurance, & Real Estate	226	22.1
3	Manufacturing	116	11.3
4	Retail Trade	84	8.2
5	Transportation & Public Utilities	75	7.3
6	Wholesale Trade	32	3.1
7	Construction	20	2.0
8	Mining	8	0.8
9	Public Administration	6	0.6
10	Nonclassifiable Establishments	3	0.3

Top 10 sub-sectors breached by number of incidents

Business Services was the most affected sub-sector, followed by Health Services.

Rank	Industry	Breaches	Percent
1	Business Services	248	24.2
2	Health Services	115	11.2
3	Depository Institutions	71	6.9
4	Nondepository Institutions	62	6.1
5	Communications	42	4.1
6	Insurance Carriers	41	4.0
7	Engineering & Management Services	38	3.7
8	Miscellaneous Retail	34	3.3
9	Wholesale Trade - Durable Goods	25	2.4
10	Holding & Other Investment Offices	23	2.2

The top 10 sectors and sub-sectors breached by number of identities stolen largely reflects the above figures, with Services (90 percent) at the top of the sectors list, and Business Services (78 percent) top in sub-sectors.

Health Services represents a much smaller percentage when looking at data breaches by number of identities stolen—it is ninth on the list of sub-sectors, accounting for less than one percent of identities stolen.

Top 10 sectors breached by number of identities stolen

The Services sector accounted for more than 90 percent of the identities stolen in 2016

Rank	Industry	Identities	Percent
1	Services	914,382,512	90.1
2	Manufacturing	56,782,089	5.6
3	Retail Trade	13,173,167	1.3
4	Mining	9,758,832	1.0
5	Construction	7,963,470	0.8
6	Transportation & Public Utilities	6,243,712	0.6
7	Finance, Insurance, & Real Estate	3,554,225	0.4
8	Wholesale Trade	2,051,635	0.2
9	Public Administration	1,198,971	0.1
10	Nonclassifiable Establishments	685	< 0.1

Top 10 sub-sectors breached by number of identities stolen

Business Services was the sub-sector most affected in terms of identities stolen, accounting for nearly 78 percent.

Rank	Industry	Identities	Percent
1	Business Services	786,918,569	77.5
2	Motion Pictures	85,200,000	8.4
3	Printing & Publishing	49,299,205	4.9
4	Personal Services	27,001,398	2.7
5	Miscellaneous Retail	10,694,512	1.1
6	Coal Mining	9,746,241	1.0
7	Engineering & Management Services	8,216,181	0.8
8	Special Trade Contractors	7,932,817	0.8
9	Health Services	6,838,017	0.7
10	Communications	5,304,054	0.5

One interesting feature in the sub-sectors list is the presence of Motion Pictures in second place with 85.2 million identities (8 percent) stolen. This figure can be attributed to a single data breach, the hack of French online video-sharing website Dailymotion, which falls under the Motion Pictures classification.

The data breach of Dailymotion took place in October, but was not made public until December. The breach led to the exposure of 85.2 million unique email addresses and user names from the company's systems. However, roughly one-fifth of the accounts exposed had associated passwords that were scrambled with the strong bcrypt hashing function, making them difficult to crack.

Country data

The United States was at the top of the list for both the number of breaches by country and the number of identities stolen by country. This is an unsurprising finding for several reasons. The US has a large population, high adoption of technology, and a large number of companies based there. There are also strict legal requirements in the US around reporting data breaches. Data breaches are often underreported in territories where there are no legal requirements in place.

Top 10 countries by number of data breaches

The United States was the country most heavily affected by data breaches in 2016

Rank	Country	Breaches
1	United States	1023
2	United Kingdom	38
3	Canada	19
4	Australia	15
5	India	8
6	Ireland	8
7	Japan	7
8	Israel	6
9	Germany	5
10	Thailand	5

Top 10 countries by number of identities stolen

Once again, the United States leads the way in terms of identities stolen in 2016.

Rank	Country	Identities
1	United States	791,820,040
2	France	85,312,000
3	Russia	83,500,000
4	Canada	72,016,746
5	Taiwan	30,000,051
6	China	11,344,346
7	South Korea	10,394,341
8	Japan	8,301,658
9	Netherlands	6,595,756
10	Sweden	6,084,276

Looking at identities stolen in the US, one interesting finding is that the identities were mainly exposed in mega breaches. Ninety percent of identities stolen in the US were exposed in just eight mega breaches.

There were only four data breaches in France in 2016, but it appears in the second spot on the list for identities stolen due to the previously discussed Dailymotion breach that saw more than 85 million identities stolen.

Similarly, in Russia, two data breaches were responsible for the bulk of exposed identities. Both breaches occurred at Mail.Ru. One breach revealed 57 million email addresses, while the second saw 25 million user accounts from an online forum compromised.

Underground Economy

While the underground economy is typically associated with credit card details and stolen personal information, Symantec researchers observed cyber criminals showing an increasing interest in selling media accounts such as Netflix and Spotify, with prices ranging from 10 cents to US$10 per account. While the prices they can charge for these accounts are low, if an attacker has compromised a device it is likely they will have this account information anyway, so they attempt to sell it on in an effort to maximize their profits.

The 2016 underground economy has something for everybody: from accounts for ride-hailing apps such as Uber for $1, to distributed denial of service (DDoS) services that could cost up to $1,000.

Restaurant gift cards, hotel bookings, and airline frequent flyer miles were also among the services for sale. Online banking accounts were also for sale, alongside PayPal accounts, and retail shopping accounts for Amazon and Walmart.

When it came to malware, ransomware toolkits could command up to $1,800, and were often sold as Crimeware-as-a-Service (CaaS), while Android banking Trojans were being sold for $200.

Symantec observed an increase in offers for money transfer services, which were being sold for around 10 percent of their value, e.g. pay $100 in bitcoins for a money transfer of $1,000. This indicates that the process of cashing out the stolen money is still the most difficult step in the chain for cyber criminals.

The prices observed, on publicly accessible underground forums and dark web Tor sites, have remained somewhat stable since 2015. Credit cards are still the most sold digital good on underground forums.

The prices for credit cards varied greatly depending on the country they were from (credit cards from the EU being more expensive than those from the US), the company, the level (Gold, Platinum, etc), and the extra information provided. Credit cards with full details commanded a higher price than those without, while if a personal identification number (PIN) was included, the price could be 10 times higher.

Underground marketplace price list

Payment cards	Price
Single credit card	$0.5 - $30
Single credit card with full details (Fullz)	$20 - $60
Dump of magnetic strip track 1&2 & PIN	$60 - $100
Malware	
Basic banking Trojan kit with support	$100
Password stealing Trojan	$25 - $100
Android banking Trojan	$200
Office macro downloader generator	$5
Malware crypter service (make hard to detect)	$20 - $40
Ransomware kit	$10 - $1800
Services	
Media streaming services	$0.10 - $10
Hotel reward program accounts (100K points)	$10 - $20
Airline frequent flyer miles account (10K miles)	$5 - $35
Taxi app accounts with credit	$0.5 - $1
Online retail gift cards	20% - 65% of face value
Restaurant gift cards	20% - 40% of face value
Airline ticket and hotel bookings	10% of face value
DDoS service, < 1hr duration, medium target	$5 - $20
DDoS service, > 24hr duration, medium & strong target	$10 - $1000
Dedicated bulletproof hosting (per month)	$100 - $200
Money transfer services	
Cash-out service	10% - 20%
Accounts	
Online bank accounts	0.5% - 10% of account balance
Retailer accounts	$20 - $50
Cloud service provider accounts	$6 - $10
Identities	
Identity (Name, SSN & DOB)	$0.1 - $1.5
Scanned passports and other documents (e.g. utility bill)	$1 - $3

The underground marketplace

Ransomware toolkit

$10 – $1,800

DDoS short duration
(< 1 hr)

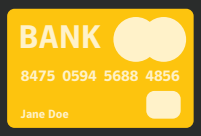
$5 – $20

Documents
(Passports, utility bills)

$1 – $3

Android banking Trojan

$200



Credit cards

$0.5 – $30

Cloud service account

$6 – $10

Gift card

20%– 40%
(of face value)

Cash-out service

10%– 20%
(of acct. value)

Where *everything* has a price

Disruptions and takedowns

While cyber crime continues to be profitable, there were a number of significant disruptions, including several high-profile takedowns, which helped put a dent in activity and send out a warning signal.

Avalanche

The Avalanche takedown dealt a severe blow to the cyber criminal community following the takedown of infrastructure used by at least 17 malware families. The takedown was a combined effort by multiple international law enforcement agencies, public prosecutors, and security and IT organizations, including Symantec. It resulted in the seizure of 39 servers and several hundred thousand domains that were being used by the criminal organization behind the Avalanche network.

Symantec's research into the Avalanche network began in 2012 when it published research on ransomware that was predominantly targeting German speakers in Germany, Austria, and parts of Switzerland. At the same time, German police were carrying out an investigation into the Bebloh malware (Trojan.Bebloh), which featured in Symantec research. Symantec researchers provided technical assistance to the police investigation, and these combined efforts eventually led to the discovery of the Avalanche botnet. Avalanche was a massive operation responsible for controlling a large number of compromised computers across the world.

The investigation culminated on November 30, 2016, and resulted in the takedown of infrastructure providing support for at least 17 different malware families, as well as the arrests of multiple individuals suspected of participating in the operation.

Bayrob

The Bayrob takedown was the culmination of an eight-year FBI investigation that was assisted by Symantec. It saw the arrest and extradition to the US of three Romanian men who may have stolen up to US$35 million from victims over several years.

The career cyber criminals behind Bayrob (Trojan.Bayrob) started out by creating fake online vehicle auctions to con victims out of tens of thousands of dollars, before diversifying into other fraudulent and malware operations, including credit card theft and cryptocurrency mining.

During its investigation, Symantec discovered multiple versions of the Bayrob malware, collected intelligence data, and witnessed Bayrob as it morphed from online fraud to a botnet of over 300,000 computers used for cryptocurrency mining. Symantec succeeded in exposing the gang's operations, gaining insight into its key players, tactics, malware, and the potential impact and criminal activity undertaken.

Symantec first wrote about the Bayrob gang in 2007, when it exposed its highly sophisticated fake motor sales eBay scam. This public attention did not deter the cyber criminals, however, and the gang continued its criminal activities, carrying out more online auction fraud, as well as diversifying into credit card fraud. It also recruited a network of money mules in the US and Europe in order to move the proceeds of its scams back to Romania.

In recent years, the group had turned its attention to building a botnet for cryptocurrency mining, and by 2016 its botnet had grown to more than 300,000 computers.

Over the years, Symantec continuously monitored the group's activities, allowing it to keep improving protection for customers, as well as assisting with the FBI's investigation. This cooperation eventually led to the arrests in late 2016.

Lurk/Angler

Russian security forces cracked down on the Lurk banking group in June 2016, arresting 50 people in Moscow.

The Lurk banking Trojan targeted Russian financial institutions and the group behind it is believed to have stolen more than US$25 million from the accounts of various Russian financial institutions.

These arrests coincided with a drop in activity from a number of threat groups—including Locky, Dridex, and the Angler exploit kit. However, while Locky and Dridex experienced a surge in activity again in the second half of 2016, Angler did not. This led to speculation that the same people were behind both the Lurk banking Trojan and the Angler exploit kit.

Since the Lurk arrests, Angler has disappeared from the threat landscape, a development covered in depth in the Web Attacks chapter.

Dyre

One of the major takedown stories to break in early 2016 surrounded the Dyre financial fraud Trojan.

Reports emerged in February that a Russian law enforcement operation in November 2015 coincided with a virtual cessation in activity around the financial Trojan. Symantec telemetry confirmed this drop in activity. Dyre (Infostealer.Dyre) was spread through email spam campaigns, and no Dyre-related spam campaigns have been observed by Symantec since November 18, 2015.

The Dyre takedown was significant because it had grown to become one of the most active financial fraud tools in operation. Dyre targeted Windows computers to steal banking and other credentials; it could also be used to infect victims with other types of malware and add them to spam botnets.

Dyre spam campaigns contained a malicious attachment that, if opened, would install the Upatre downloader (Downloader.Upatre) on a victim's computer. Detections of Upatre hit a high of more than a quarter of a million in July 2015. Detections of both Upatre and Dyre dropped sharply after November 2015.

The circumstances surrounding the Dyre takedown are unclear, with no definitive evidence emerging relating to who or how many people were arrested. Reports in late 2016 claimed that new banking Trojan Trickbot (Trojan.Trickybot) was a rewrite of Dyre. Fidelis researchers said they believed "with moderate confidence" that one or more of Dyre's original developers was involved with Trickbot.

Further reading

- SWIFT attackers' malware linked to more financial attacks
- Odinaff: New Trojan used in high level financial attacks
- Avalanche malware network hit with law enforcement takedown
- Bayrob: Three suspects extradited to face charges in US
- PowerShell threats surge: 95.4 percent of analyzed scripts were malicious
- Necurs: Mass mailing botnet returns with new wave of spam campaigns

Best practices

- Regularly back up any files stored on your computer or any other devices.
- Always keep your security software up to date, on all your devices, including mobile, to protect yourself against any new variants of malware.
- Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by attackers.
- Delete any suspicious-looking emails you receive, especially if they contain links or attachments.
- Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.
- On mobile devices, refrain from downloading apps from unfamiliar sites and only install apps from trusted sources. Also, pay close attention to the permissions requested by apps.
- Make sure passwords you use for your online accounts are unique and strong. Do not reuse passwords across multiple accounts, and enable two-factor authentication if available.
- Sign up to alerts from your bank so that you will be alerted if any suspicious transactions are made on your account.

Ransomware: Extorting businesses & consumers

Section

07

Symantec

Introduction

During 2016, ransomware was one of the most significant threats facing both individuals and organizations. Attackers have honed and perfected the ransomware business model, using strong encryption, anonymous Bitcoin payments, and vast spam campaigns to create dangerous and wide-ranging malware. The increasing number of new ransomware families signals that more and more attackers are jumping on the bandwagon. While consumers in particular (69 percent of all infections) are at risk from ransomware, this year saw evidence that ransomware attackers may be branching out and developing even more sophisticated attacks, such as targeted ransomware attacks on businesses that involved initial compromise and network traversal leading to the encryption of multiple machines. Ransomware looks set to continue to be a major source of concern globally in 2017.

Key findings

- Due to its prevalence and destructiveness, ransomware remained the most dangerous cyber crime threat facing consumers and businesses in 2016.
- The average ransom amount has shot upwards, jumping 266 percent from US$294 in 2015 to $1,077. Attackers clearly think that there's more to be squeezed from victims.
- Detections of ransomware increased by 36 percent in 2016.

Trends & analysis

The number of detections of ransomware increased by 36 percent during 2016, from 340,000 in 2015 to 463,000 during 2016. The daily rate of antivirus detections for ransomware also increased during 2016, averaging at approximately 846 per day at the beginning of the year and rising to more than 1,539 a day at year end.

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.

Ransomware is spread in a number of different ways and, generally speaking, the infection process involves a number of different stages at which the attack can be blocked. For example, in the case of ransomware distributed via email, most attacks (hundreds of thousands per day) are blocked by anti-spam defenses. Most ransomware emails come with a downloader hidden in a malicious attachment. The downloader is used to download and install the ransomware on the victim's computer and a significant number of attacks are blocked at this stage, before the ransomware can be downloaded to the target's computer.

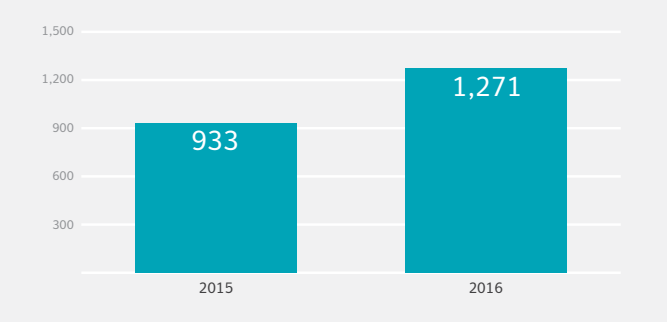
In the case of web attacks, a significant number of ransomware attacks are performed using exploit kits, malicious web pages designed to exploit vulnerabilities on the victim's computer to install malware. A large number of ransomware attacks are blocked at exploit kit stage, before the ransomware can be installed on the victim's computer.

In addition to attacks which are blocked early in the infection process, ransomware is often detected and blocked by generic detection technologies, which identify malicious behavior common to malware.

While antivirus detections of ransomware amount to a small percentage of the overall number of attacks, the notable uptick in detections during the year suggests that ransomware activity increased during 2016.

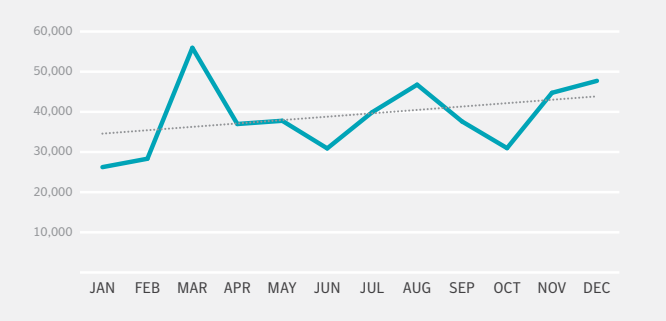
Average global ransomware detections per day

Ransomware antivirus detections increased by 36 percent compared to 2015, rising from an average of 933 per day in 2015 to 1,270 per day in 2016.



Global ransomware detections by month

Ransomware antivirus detections by month increased over the course of 2016 averaging at approximately 35,000 per month at the beginning of the year and rising to more than 40,000 per month by the end of the year.

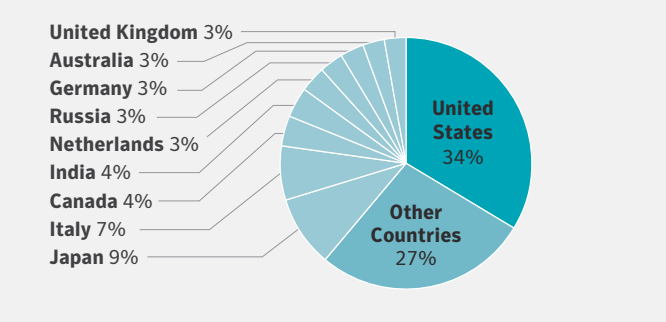


With more than a third of all infections logged in 2016, the US continues to be the region most affected by ransomware. Japan (nine percent), Italy (seven percent), Canada (four percent), and India (four percent) are also heavily affected. European nations such as the Netherlands (three percent), Russia (three percent), Germany (three percent), and the UK (three percent) figure highly in infection statistics. The other country to figure in the top 10 is Australia (three percent).

The statistics indicate that attackers are largely concentrating their efforts on developed, stable economies.

Ransomware detections by country

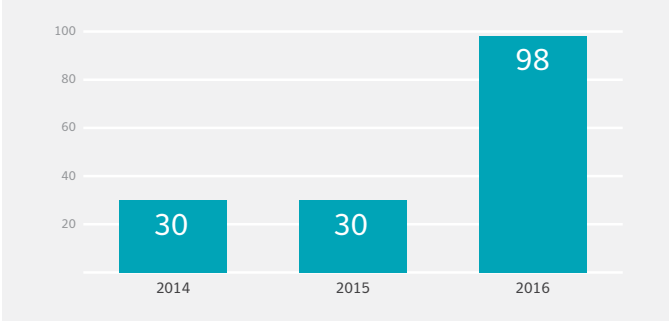
Ransomware antivirus detections by country, 2016. The US continues to be the region where ransomware is most prevalent.



The number of new ransomware families emerging shot up during 2016. With 30 new families appearing each year for 2014 and 2015, the number more than tripled to 98 in 2016. The trend suggests that more and more attackers are now jumping on the ransomware bandwagon and creating new ransomware families or modifying existing ones.

New ransomware families

New ransomware families discovered by year. The number more than tripled to 98 in 2016, suggesting more and more attackers are now jumping on the ransomware bandwagon.

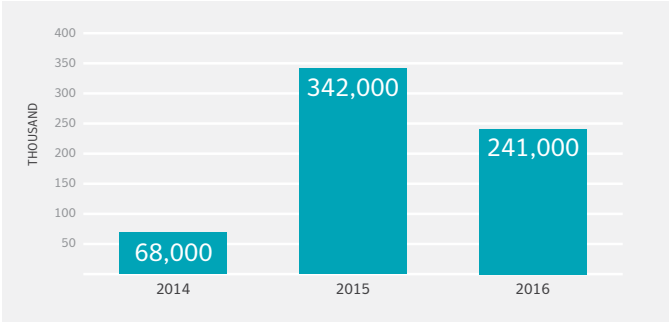


The number of ransomware variants (i.e. distinct variants of ransomware families) was down year-on-year, falling by 29 percent from 342,000 in 2015 to 241,000 in 2016. That downward trend was reflected in monthly numbers of new ransomware variants, where the average number fell from more than 20,000 in January to below 20,000 by year-end.

The number of new variants is another indicator of overall ransomware activity, where attackers will create new variants of their threats in the hope of evading detection. The fall in the number of variants could be explained when put alongside the major increase in new ransomware families in 2016. It suggests that more attackers are opting to start with a clean slate by creating a new family of ransomware rather than tweaking existing families by creating new variants.

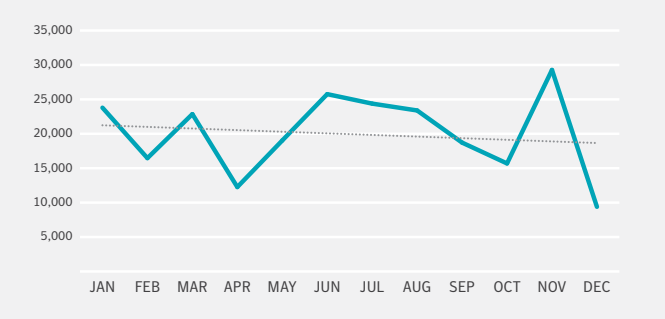
New ransomware variants

New ransomware variants (number of unique, individual examples) by year. The number of new variants fell by 29 percent from 342,000 in 2015 to 241,000 in 2016.



Ransomware variants by month

New ransomware variants by month. The average number fell from more than 20,000 in January 2016 to below 20,000 by year-end.

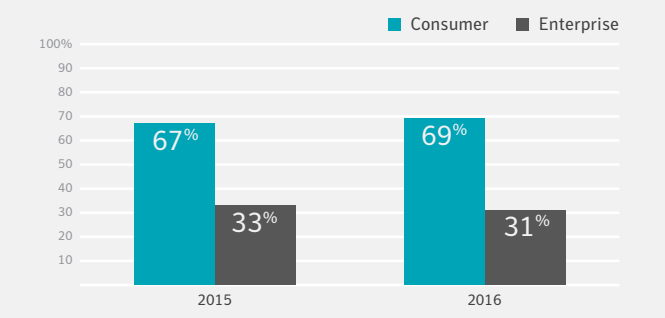


The majority of ransomware infections during 2016 occurred on consumer computers (69 percent). This is marginally up from 2015, when the proportion of ransomware infections occurring on consumer computers was 67 percent.

The proportion of consumer infections vs infections in enterprises and other organizations remained relatively stable for much of 2016, with consumer infections accounting for between 59 percent and 79 percent each month. The sole exception was December 2016, when there was near parity, with the proportion of consumer infections falling to 51 percent.

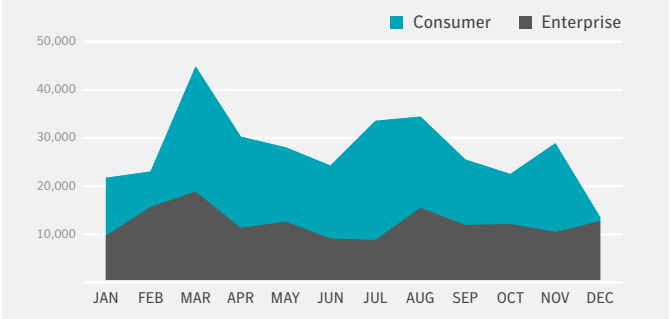
Consumer vs enterprise infections

Enterprise versus consumer ransomware infections. The majority of ransomware infections during 2016 occurred on consumer computers. The proportion of consumer infections (69 percent) was only marginally up from 2015, when it was 67 percent.



Consumer vs enterprise infections by month

The proportion of consumer infections vs infections in enterprises and other organizations remained relatively stable for much of 2016.



Case studies/investigations

How ransomware can affect consumers

There are now hundreds of different ransomware families, which are spread through a variety of methods, but the most active ransomware threats seen in 2016 were usually spread via email. In many cases, the victim would receive a spam email designed to appear like an invoice or receipt from a company. The email would be written in a way to lure the recipient into opening a malicious attachment, e.g. “Here is the details for you recent purchase, for more details see the attached receipt.”

Opening the attachment can set in train the process of infection. It can run a small piece of malware, known as a downloader, which will download the ransomware and install it on the victim’s computer. Once installed, the ransomware will then begin encrypting a pre-programmed range of files on the computer (either files in certain folders or files with certain extensions or both). Most newer ransomware families employ strong encryption, meaning the victim has no hope of opening encrypted files without an encryption key.

Often the victim will be unaware of anything untoward until a ransom message is displayed on their screen. The message will usually explain what has happened to the victim’s files and how the ransom can be paid, which is often done via websites on the anonymous Tor network.

How ransomware can affect businesses

Most ransomware threats are indiscriminate and the infection experience is similar for businesses and consumers. However, a small number of groups have begun to specifically target businesses with ransomware attacks designed to infect multiple computers on a single network and encrypt valuable data.

In the case of SamSam (Ransom.SamSam) the attackers' initial point of entry was a public-facing web server. They exploited an unpatched vulnerability to compromise the server and get a foothold on the victim's network. From there, the attackers used multipurpose tools such as Microsoft Sysinternals to traverse the victim's network. This enabled them to map every accessible computer on the organization's network and identify the most valuable assets.

The attackers then 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. They next distributed a tool called sqlsrvtmg1.exe. This executable searched for any running backup processes and stopped them. It also deleted any back-up-related files it found.

The last stage 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 finished, 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$1,587 at the time of writing) for each compromised computer.

Ransom demands soar

The mean average ransom demanded by attackers increased dramatically during 2016. After declining slightly during 2015, the average ransom demand seen in new families discovered in 2016 rose from $294 to $1,077.

The increase in the average ransom demand was, in part, affected by the highest ransom seen during 2016, an unusually high $28,730, which was demanded by the MIRCOP ransomware (Ransom.Mircop). However, even if MIRCOP were excluded, the mean average ransom would still have more than doubled to $678. Attackers clearly think there is more to be squeezed from victims.

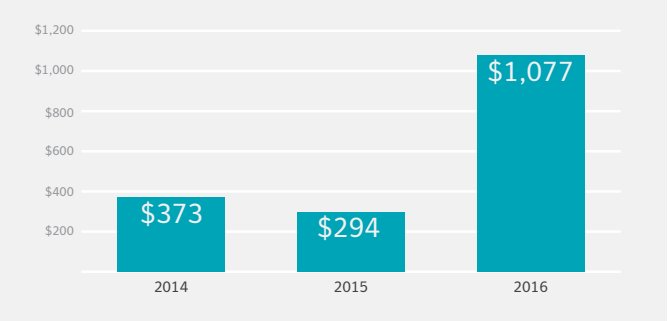
According to research carried out by the Norton Cyber Security Insight team, 34 percent of victims will pay the ransom. This proportion rises to 64 percent of victims in the US, providing some indication as to why the country is so heavily targeted. Willingness to pay the ransom has to be a major reason for the increase in ransom demands.

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.

However, paying the ransom doesn't guarantee decryption of the victim's files. According to the Norton Cyber Security Insight team, only 47 percent of victims who paid the ransom reported getting their files back.

Average ransom demand

The average mean ransom demand seen in new families discovered in 2016 rose from $294 to $1,077.



Attackers have also become more creative in their attempts to extract more from victims, with several newer ransomware families featuring variable ransom demands. For example, Cerber (Ransom.Cerber) will double its ransom demand from 1.25 bitcoin (US$1,255) to 2.5 bitcoin after five days if the ransom remains unpaid.

There is also some evidence that ransomware attackers have begun tailoring their ransom demands on the basis of the type and volume of data they have encrypted. The attackers behind HDDCryptor (Ransom.HDDCryptor) reportedly demanded $70,000 following an attack on San Francisco's Municipal Transportation Agency, which resulted in disruption of the city's light rail service (these "custom" ransom demands aren't factored into our calculations for average ransom amounts).

Infection vectors

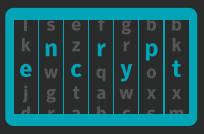
Ransomware is spread using multiple infection vectors. One of the most common vectors used is spam emails, with some of the most widespread threats of 2016, such as Locky (Ransom.Locky), being distributed in this fashion.

Widescale spam runs, some consisting of millions of emails, occur almost daily and are powered by botnets—networks of compromised computers, ranging from hundreds to millions of computers. Most campaigns use social engineering tricks to lure recipients into opening emails and attachments, such as disguising the email as an invoice or a shipping notification.

Major ransomware threats

Locky

Cerber



CryptXXX

Approx. Ransom:

Locky	Cerber	CryptXXX
$965	$1,200	$500

Discovery:

Locky	Cerber	CryptXXX
February 2016	March 2016	April 2016

Spread through:

Locky	Cerber	CryptXXX
Email campaigns Neutrino exploit kit Nuclear exploit kit RIG exploit kit	Email campaigns RIG exploit kit Magnitude exploit kit	Angler exploit kit Neutrino exploit kit
One of the most widely spread ransomware threats in 2016 Spread via massive email campaigns powered by Necurs botnet Significant drop in Locky prevalence in early 2017 due to reduction in Necurs activity since late December 2016	Very widespread in late 2016 as a result of extensive email and RIG exploit kit campaigns Email campaigns primarily use JavaScript and Office macro downloaders but may also be attached as a zip file	Disappearance of Angler in early June 2016 prompted a drop in activity Reemerged in early 2017 delivered via Neutrino exploit kit Early variants used weak encryption which could be broken. Newer versions employ stronger encryption, making decryption impossible

The most common infection method involves a malicious attachment that contains a downloader—usually a JavaScript downloader (JS.Downloader) or Word Macro downloader (W97M.Downloader)—which subsequently downloads and installs the ransomware. In some cases, no downloader is used and the malicious attachment directly installs the ransomware. In others, the spam email will contain a link that points to an exploit kit which will lead to the ransomware being installed on the recipient's computer. Some links do not lead to an exploit kit and instead lead directly to a downloader or ransomware payload.

Exploit kits by themselves are another major infection vector and have been utilized to spread major ransomware threats such as Cerber (Ransom.Cerber) and CryptXXX (Ransom.CryptXXX). Exploit kit attackers usually compromise third-party web servers and insert malicious code into the web pages hosted on them. This enables them to direct browsers to the exploit kit servers.

Aside from links distributed via spam campaigns or social media posts, attackers can use a number of other methods for redirecting traffic to exploit kit servers, such as malicious advertisements (known as malvertising) or redirecting traffic from traffic distribution services.

Exploit kits rely on exploiting vulnerabilities. Users running outdated or unpatched software are at most risk. Users with up-to-date software will only be exposed in cases where a zero-day vulnerability is used by an exploit kit. At the end of 2016, Symantec was blocking around 388,000 attacks per day from exploit kits.

While spam campaigns and exploit kits are the main infection vectors, a number of other tactics have also been used to spread ransomware, including:

- **Secondary infections:** In some cases malware that has already infected a computer can be used to download more malware, including ransomware. A case in point was the original CryptoLocker ransomware, with some victims reportedly infected following earlier infection from one of several botnets.
- **Brute-forcing passwords:** Some families of ransomware are spread through brute-forcing login credentials for software used on servers. One example is Bucbi (Ransom.Bucbi), which uses this method to gain a foothold on remote desktop protocol (RDP) servers.
- **Exploiting server vulnerabilities:** A number of ransomware groups have targeted vulnerable software running on servers to gain access to an organization's network. The group behind the SamSam ransomware (Ransom.SamSam) finds and exploits vulnerabilities to spread their malware through a network.
- **Self-propagation:** While a few Android ransomware display worm-like behavior by spreading to all contacts via SMS, 2016 saw the first Windows ransomware to use self-propagation. ZCryptor (W32.ZCrypt) infects all removable drives with a copy of itself before it begins encrypting, increasing its chances of spreading to other computers.
- **Third-party app stores:** Some mobile ransomware may be spread via untrusted third-party app stores. One example is Android.Lockdroid.E, which poses as a pornographic video player on third-party app stores.

Arrival of Ransomware-as-a-Service

One factor that may have influenced the increase in ransomware activity during 2016 was the advent of Ransomware-as-a-Service (RaaS). This involves malware developers creating ransomware kits, which can be used to easily create and customize their new ransomware variants. The developers usually provide the kits to attackers in exchange for a percentage of the proceeds.

One example of RaaS is Shark (Ransom.SharkRaaS), which emerged during 2016. Shark is distributed through its own website and allows users to customize the ransom amount and which files it encrypts. Payment is automated and sent directly to Shark's creators, who retain 20 percent and send the remainder on to the attackers.

New techniques: Targeted attacks and "living off the land"

While ransomware attacks to date have been largely indiscriminate, there is evidence that attackers have a growing interest in hitting organizations with targeted attacks. Although relatively small in number compared to the mass-mailed threats, these can be devastating for organizations affected, with potentially hundreds of computers encrypted.

One of the most dangerous examples of this new breed of targeted attacks is SamSam (Ransom.SamSam). SamSam targets servers running older, unpatched community versions of JBoss Application Server, with the attackers using freely available tools, such as the open-source testing tool JexBoss, to identify vulnerable servers.

Once they have compromised one server, the attackers may steal credentials and use a number of publicly available tools, such as Microsoft Sysinternals utilities, to traverse the victim's network. When computers suitable for infection are identified, the attackers use a batch script to deploy SamSam and a public encryption key on each computer. The script also deletes Volume Shadow Copies from the computers, which prevents any files from being restored following infection. They also search for any running backup processes and stop them, in addition to deleting any backup related files they find.

The techniques used in the SamSam attacks are more commonly seen in cyber espionage campaigns and indicate the level of expertise available to some ransomware groups. Although more difficult to perform, these kinds of targeted attacks could potentially infect thousands of computers in an affected organization, causing massive disruption.

Other platforms now vulnerable

To date, ransomware attackers have largely focused on Windows users, however the breadth of platforms under threat has begun to grow. A number of Android threats have emerged including one crypto-ransomware for Android—the Russian-language Simplocker (Android.Simplocker) and its English-language variant (Android.Simplocker.B). Mobile devices are not the only Android devices that are potentially vulnerable to ransomware. Research by Symantec found that SmartTVs running Android could potentially be affected as well.

During 2016, a threat known as KeRanger (OSX.Keranger) became the first widespread ransomware to target Mac users. KeRanger was briefly distributed in a compromised version of the installer for the Transmission BitTorrent client.

Aside from threats designed specifically for one operating system, a number of ransomware variants are created in JavaScript, meaning they can infect multiple platforms, such as Ransom.Nemucod and Ransom.Ransom32.

Law enforcement takedowns

There were a number of law enforcement operations affecting some of the smaller ransomware groups during 2016. In August, Dutch police seized command and control (C&C) infrastructure belonging to the WildFire group (Ransom.Zyklon).

In December, Symantec assisted in a takedown operation against the Avalanche malware-hosting network. The operation resulted in the seizure of 39 servers and several hundred thousand domains that were being used by the criminal organization to spread at least 17 malware families, including the Trojan.Ransomlock.P ransomware.

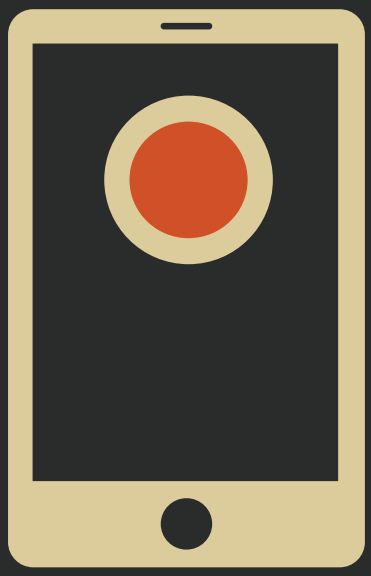
Further reading

- Ransomware and Business 2016
- Locky ransomware on aggressive hunt for victims
- KeRanger: First Mac OS X ransomware emerges
- SamSam may signal a new trend of targeted ransomware

Best practices

- New ransomware variants appear on a regular basis. Always keep your security software up to date to protect yourself against ransomware.
- Keep your operating system and other software updated. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomware attackers.
- Email is one of the main infection methods. Delete any suspicious-looking email you receive, especially if they contain links and/or attachments.
- Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.
- Backing up important data is the single most effective way of combating ransomware infection. Attackers have leverage over their victims by encrypting valuable files and leaving them inaccessible. If the victim has backup copies, they can restore their files once the infection has been cleaned up.
- Using cloud services could help mitigate ransomware infection, since many retain previous versions of files, allowing you to "roll back" to the unencrypted form.

New frontiers: Internet of Things, mobile, & cloud threats



Section

08

Symantec

While attacks against traditional desktops and servers have dominated the threat landscape in terms of numbers, there are other platforms being actively targeted or that are ripe for targeting by threat actors.

The widespread use of mobile devices and the mainstream adoption of cloud and Internet of Things (IoT) technologies has opened up whole new platforms and users for attackers to target, and in 2016 a number of emerging threats against these three increasingly high-profile areas could be observed.

Internet of Things

The rapid increase in profile of the security of IoT devices in 2016 didn't come as a total bolt from the blue. Symantec warned about the "insecurity of the Internet of Things" in the 2015 ISTR. However, it would have been hard to predict the level of attention IoT and its security, or lack thereof, would receive in the last quarter of 2016.

The reason for such attention comes down to one word: Mirai. The Mirai botnet, which is made up of IoT devices, was used in a number of high-profile distributed denial of service (DDoS) attacks towards the end of 2016.

It is difficult to definitively state how many Mirai-infected devices are out there, but many figures quoted are quite staggering. Incapsula research uncovered almost 50,000 unique IPs hosting Mirai-infected devices attempting to launch attacks on its network. Level 3 said it had identified approximately 493,000 Mirai bots: 213,000 before the source code was released, and 280,000 in the last few months of 2016.

Symantec established an IoT honeypot in late 2015 to track attack attempts against IoT devices. Data gathered from this honeypot shows how IoT attacks are gathering steam and how IoT devices are firmly in the sights of attackers.

Key findings

- Attacks on Symantec's Internet of Things honeypot almost doubled from January to December 2016. An average of almost 4.6 unique IP addresses were hitting the honeypot every hour in January, but this increased to an average of just over 8.8 in December. At times of peak activity, when Mirai was expanding rapidly, attacks on the honeypot were taking place every two minutes.
- In 2016, IoT devices were responsible for the biggest DDoS attack ever seen. The attack on the French hosting company OVH, which peaked at 1 Tbps, was the largest DDoS attack ever recorded. It was primarily driven by the Mirai botnet.
- Default passwords are still the biggest security weakness for IoT devices. The password most commonly tried by attackers is "admin."

Trends and analysis

What is the IoT? Many people picture smart thermostats and virtual assistants that will respond to voice commands, but the IoT is primarily composed of commonly used devices. Home routers, DVRs, and internet-connected cameras—which all make up part of the IoT—were the devices most targeted by the Mirai botnet.

A botnet is a "zombie army" of internet-connected devices, infected with malicious software and controlled as a group without their owners' knowledge. The attacker can use the controlled devices to carry out malicious activities such as DDoS attacks or spam campaigns. IoT devices are an attractive target for botnets for three reasons:

01 Security is often not a priority for the device manufacturer. This leads to poor practices such as the use of default passwords and open ports, which the users do not, or cannot, change.

02 They typically don't have built-in mechanisms to receive automatic firmware updates, resulting in vulnerabilities being left unpatched.

03 They are often forgotten about once installed. This means that their owners are unaware when devices are being used for malicious purposes and have little incentive to apply firmware updates.

While Mirai's sole purpose appears to be DDoS attacks, malware on a wireless router could conceivably lead to personal information—including user names, passwords, and financial data—being stolen. Infected IoT devices could also be

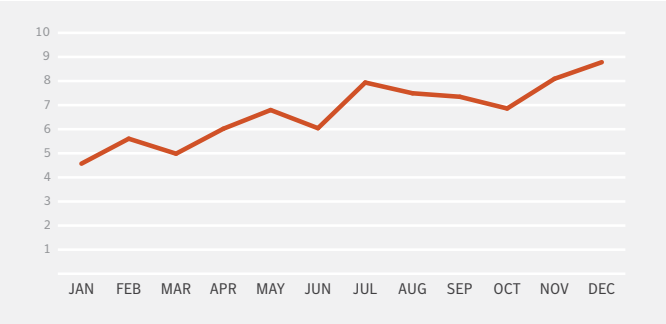
used as a stepping-stone to attack other devices in a private network. It could also mean that a device belonging to you could participate in a global botnet that plays a role in taking down websites or services.

Symantec established an IoT honeypot in 2015 to observe attacks against IoT devices. The honeypot appears as an open router and attempts to connect to the system are logged for analysis. Between January and December 2016, the number of unique IP addresses targeting the honeypot almost doubled.

In January, the average number of unique IPs scanning the honeypot every hour stood at almost 4.6. In December, that figure had grown to an average of just over 8.8. Most of the IPs hitting the honeypot are other IoT devices.

Hourly attacks on the IoT honeypot per month

The growth in hourly attacks on the Symantec honeypot from January to December can be clearly observed, almost doubling over the course of the year.



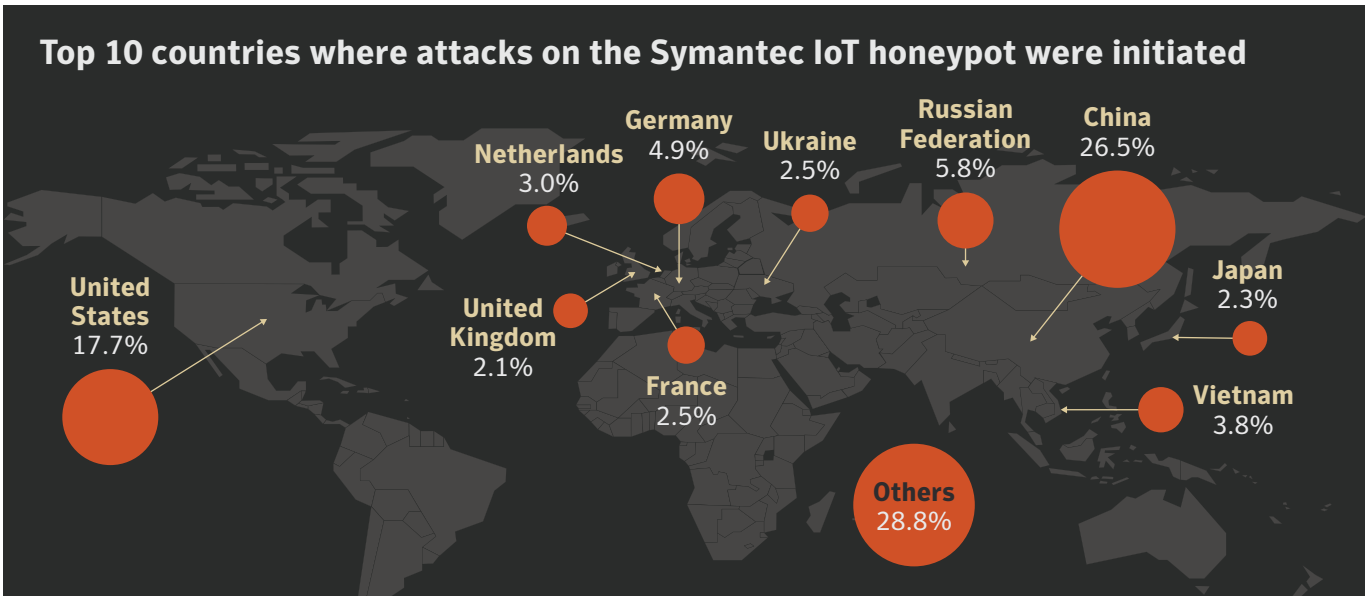
While there was a slight downward trend from July to October, incidents of attacks swung sharply upwards in November and December. The source code for the Mirai botnet was made public on the last day of September, which was likely to have had some influence on this increase.

The source code for Mirai was revealed on a hacking forum by an individual with the user name Anna-senpai. It is not possible to definitively say who is behind Mirai, but security journalist Brian Krebs, one of the first victims of the botnet, wrote a lengthy article about his investigation into the identity of Anna-senpai.

A large-scale attack on DNS provider Dyn, which took place on October 21, received extensive media attention and raised Mirai's profile. It demonstrated how easy it was to create a large botnet and disrupt major websites. The perpetrators of the Dyn attack have not been identified, but it is widely believed they were "script kiddies" (wannabe hackers with few skills) rather than a sophisticated hacking group. The Dyn attack also revealed the existence of Mirai to the world at large, and there were subsequent media reports of so-called "skids" asking for tutorials on hacking forums so they could learn how to use the Mirai source code.

Country data

Analysis of honeypot data also meant it was possible to determine the countries from which attacks on the honeypot were initiated.



China (26.5 percent) and the US (17.7 percent) dominated when it came to attacks, with Russia (5.8 percent), Germany (4.9 percent), and Vietnam (3.8 percent) rounding out the top five.

These metrics measure the countries in which the IP address of the attacking device was based, but this doesn't necessarily mean the attackers themselves were based in these countries.

Passwords

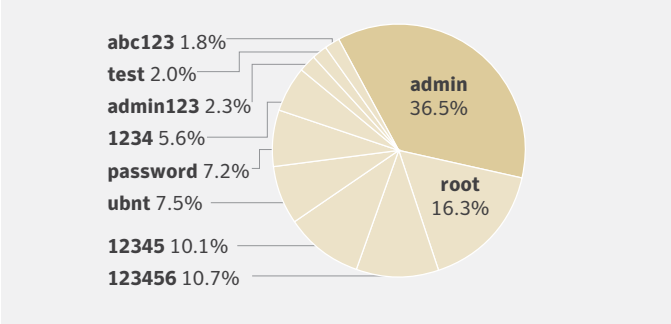
Analysis of the passwords used by IoT malware to attempt to log into devices yielded unsurprising results, revealing that the default user names and passwords of IoT devices are often never changed.

There are many reasons for this. A number of IoT devices have hardcoded user names and passwords that can't easily be changed. Many users are likely unaware of the dangers of default credentials and are therefore unlikely to change them.

Traditional best practice dictates that users should have a unique user name and password combination for all their IoT devices, as is recommended for online accounts. However, unless manufacturers and providers implement changes that force users to select a unique password, then passwords are likely to continue to be a security weak point.

Top 10 passwords used to attempt to log in to the Symantec IoT honeypot

Default passwords dominated the list of top 10 passwords used to log into the Symantec honeypot.



"Admin" (37 percent) and "root" (16 percent) dominate the list of passwords used to attempt to log in to the Symantec honeypot, with the usual suspects of "123456," "12345," "1234," and "password" also featuring. The default password for the Ubiquiti brand of routers, "ubnt," also features in the top 10. It is likely Ubiquiti routers were targeted because it was revealed in May 2016 that an old vulnerability in the routers allowed worms targeting embedded devices to spread across thousands of Ubiquiti Networks routers running outdated firmware.

While Ubiquiti released a firmware update in mid-2016 that patched this vulnerability, the worm was still able to exploit the weakness in cases where the firmware update had not been downloaded.

The Mirai botnet

Mirai first came to public attention in September when, as mentioned above, the botnet was used for a huge DDoS attack on Brian Krebs' website. That attack peaked at 620 Gbps, making it the biggest DDoS attack ever reported at that time. However, a few days later, reports emerged about an earlier attack on French hosting company OVH that was reported to have peaked at 1 Tbps.

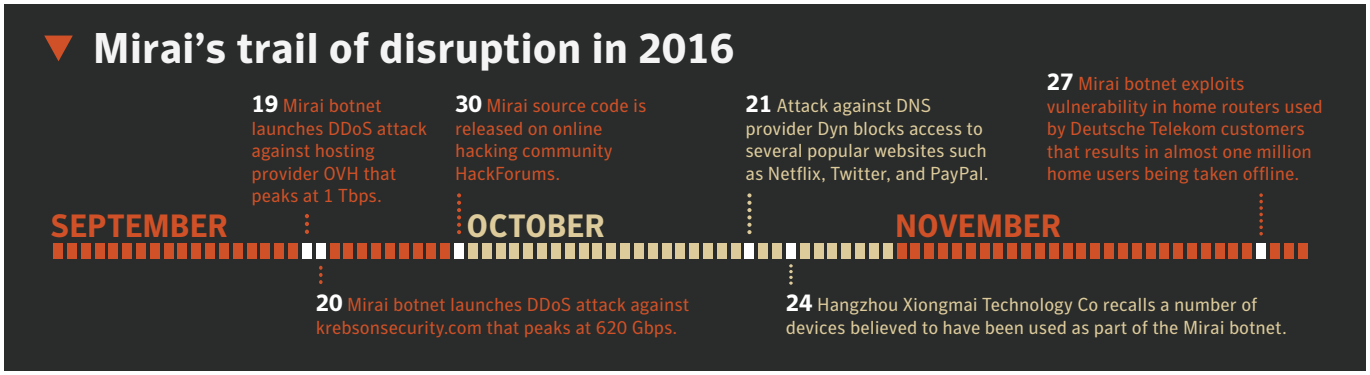
However, it was a DDoS attack on DNS company Dyn in October that put Mirai on the front page. The attack on Dyn disrupted many of the world's leading websites, including Netflix, Twitter, and PayPal.

The attack showed how powerful a DDoS attack using IoT devices could be and raised questions about what it might mean if attackers decided to target industrial control systems or critical national infrastructure.

Mirai works by continuously scanning for IoT devices that are accessible over the internet and protected by factory default or hardcoded user names and passwords. It then infects them with malware that forces them to report to a central control server, turning them into a bot that can be used in DDoS attacks. There are also at least 17 other IoT malware families that are actively compromising devices.

With Gartner predicting that there will be more than 20 billion IoT devices in the world by 2020, it's important that security problems be addressed or campaigns like Mirai could be seen on an even larger scale. Additionally, the profile of IoT devices is likely to change. As connected cars and connected medical devices become more commonplace, attacker motives are also likely to change.

Attacks using IoT devices also lower the barriers to entry for cyber criminals. There is much less security for attackers to overcome when trying to take over an IoT device. Unlike a desktop computer or laptop, which will typically have security software installed and receive automatic security updates, an IoT device's only protection may be an easily guessed default user name and password. Currently, the poor security on IoT devices is just making life easier for cyber criminals.



An evolving story

The source code for Mirai was made publicly available at the end of September. As mentioned, it was posted to HackForums by a user with the handle Anna-senpai on September 30. As expected, the revelation of the source code resulted in the creation of other Mirai variants.

In late November, a variant of Mirai crippled internet access for nearly 1 million home internet users in Germany. This variant attacked a number of routers where TCP port 7547 was accessible remotely on the device, while also exploiting a weakness in the CPE WAN Management Protocol. Similar routers used by Irish company Eir were also believed to have been vulnerable to the same attack.

With this first variant appearing less than two months after the source code was made public, it would be reasonable to assume that it is just the tip of what could be a very large iceberg.

Looking forward

The number of IoT devices will continue to grow and this may lead to increased calls for regulation of the IoT industry as the only way to deal with the security problem. If regulation becomes a possibility, the next question will be whether it would be best applied at the industry level or the government level.

The DDoS attack on US-headquartered Dyn, which was carried out primarily using webcams produced by Chinese electronics firm XiongMai Technologies, emphasizes the difficulty of regulating IoT devices.

Though there is no one way to fix a complex problem like this, risk-based baseline security standards are part of the solution. Individual nation states should consider minimum security regulation, in particular for critical uses, to ensure that security is a core consideration in the design and manufacture of IoT devices.

Of course, manufacturers should take the lead role in the security of the products that they are sending to market. They should provide consumers a level of transparency in the security of IoT devices so that consumers can make an informed decision on purchases. This also allows security to become an inherent feature of a device, which would allow premium manufacturers to differentiate their products based on security.

Whatever happens, IoT security is likely to continue to be much discussed in 2017.

Best practices

- Research the capabilities and security features of an IoT device before purchase.
- Perform an audit of IoT devices used on your network.
- Change the default credentials on devices. Use strong and unique passwords for device accounts and Wi-Fi networks. Don't use common or easily guessable passwords such as "123456" or "password."
- Use a strong encryption method when setting up Wi-Fi network access (WPA2).
- Many devices come with a variety of services enabled by default. Disable features and services that are not required.
- Disable Telnet login and use SSH where possible.
- Modify the default privacy and security settings of IoT devices according to your requirements.
- Disable or protect remote access to IoT devices when not needed.
- Use wired connections instead of wireless where possible.
- Regularly check the manufacturer's website for firmware updates.
- Ensure that a hardware outage does not result in an unsecure state of the device.

Mobile

Symantec has continued to observe an increase in malicious activity related to mobile devices, driven by cyber criminals using tried and trusted methods to monetize attacks. Android continues to be the most targeted mobile platform. However, following an explosive year in 2015, the rate of growth in attacks against Android has slowed for the first time in 2016 as attackers consolidate their activities and contend with improved security architectures.

Key findings

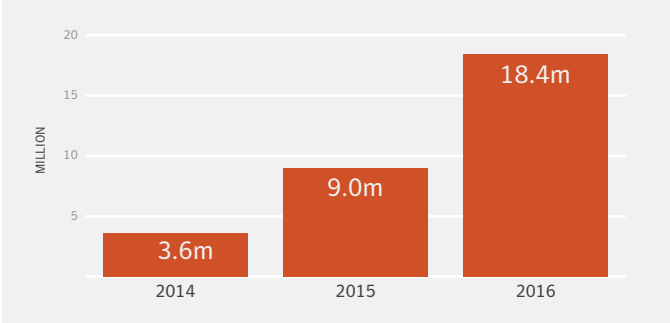
- The Android operating system remains the main focus for mobile threat actors. However, security improvements in Android's architecture have made it increasingly difficult to infect mobile phones or to capitalize on successful infections.
- Attacks on the iOS operating system are still relatively rare. However, three zero-day vulnerabilities in iOS were exploited in targeted attacks to infect phones with the Pegasus malware in 2016.
- The overall volume of malicious Android apps increased significantly in 2016, growing by 105 percent. However, this rate of growth has slowed when compared with the previous year, when the number of malicious apps increased by 152 percent.
- Symantec blocked 18.4 million mobile malware infections in total in 2016. Data from Symantec-protected mobile devices shows that 1 in 20 devices will have experienced an attempted infection in 2016. Similar levels were observed in 2015.

Mobile malware trends

Overall threat detections on mobile devices, including data from Symantec cloud technologies, doubled in 2016, resulting in 18.4 million mobile malware detections in 2016. However, the increase of 105 percent in 2016 was significantly smaller than the 152 percent increase in the previous year, despite the growth in smartphone adoption. This is an indication that there is a transition occurring from a period of explosive growth in the mobile threat landscape, to a phase where attackers are consolidating their activities while coming to grips with the security measures implemented on Android.

Number of overall mobile malware detections per year

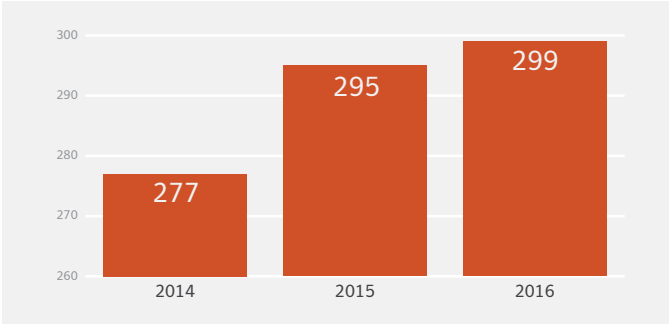
Symantec observed 18.4 million mobile malware detections in total in 2016, an increase of 105 percent on 2015.



Further evidence of the consolidation taking place emerges when looking at families of threats. Threat families are a grouping of threats from the same or similar attack groups. Symantec recorded four new mobile families in 2016, which was a steep drop from 2015, when 18 new families were identified. However, it should be noted that newer detection technologies, such as heuristics, machine learning, and cloud detections, detect threats in a more generic manner, potentially masking the presence of newer families. When analyzing mobile threat characteristics more closely, clusters of 61 distinct new threats that emerged in 2016 can be seen. When compared to the 75 clusters identified in 2015, it shows a drop of almost 19 percent, again pointing to a slowdown in growth or innovation in the mobile threat landscape.

Cumulative number of mobile malware families per year

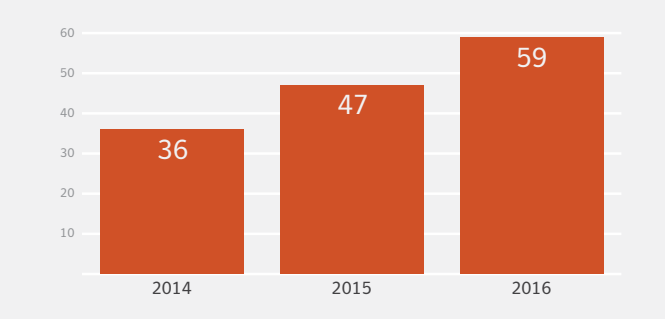
Four new mobile malware families were recorded by Symantec in 2016, a steep drop from 2015, when 18 new families were identified.



Looking more closely at individual threat variants within each family, the number of malicious mobile app variants per family increased by more than a quarter in 2016, just slightly less than the increase in 2015, when the number of malicious mobile variants per family increased by 30 percent.

Mobile variants per family

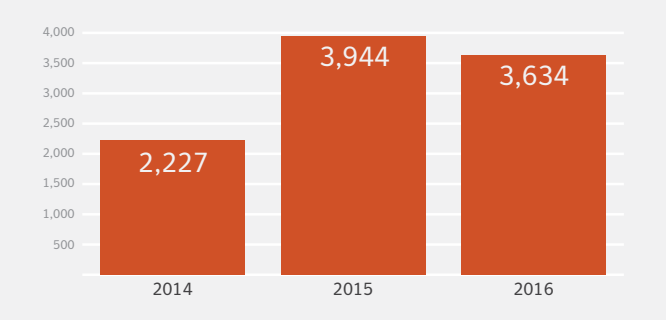
Mobile variants per family increased by more than a quarter in 2016, slightly less than the 30 percent increase in 2015.



Taking a more holistic view, there was a slight decrease in the overall number of malicious mobile app variants detected, with a drop of eight percent between 2015 and 2016. This small decrease followed a huge spike in malicious mobile app variants detected between 2014 and 2015, when it increased by more than three quarters. The figures this year show that activity began to stabilize.

Mobile malware variants by year

The decrease in mobile variants detected in 2016 indicates that activity in the area is beginning to stabilize.



Overall, it can be deduced that attackers are opting to refine and modify existing malware families and types rather than develop new and unique threat types.

Motives and techniques

Mobile malware continues to be financially motivated, using tried and trusted monetization methods, such as sending premium text messages, advertisement click fraud, and ransomware.

When analyzing the malware types detected, the top two detections—Android.Malapp and Android.MalDownloader—account for more than half of total detections for the year. These are generic detections used to detect a wide variety of individual but unclassified threats.

The first interesting detection in the top 10 is Android.Opfake in third place. Opfake detects malware that sends premium text messages, which continue to be a big earner for mobile threat attackers. A second premium text message detection, Android.Premiumtext, appears in fifth place. The Android operating system has added warnings when premium text messages are sent, making it increasingly difficult for threat actors to hide their activities. Some of the other malware in the top 10 (Android.HiddenAds and Android.Fakeapp) use click fraud methods in order to make money and get around the warnings.

Malware that is used to spread ransomware and malware used in attempts to steal victims' banking information also featured in the top 20 detections for 2016.

Top mobile threats in 2016

The two most commonly seen mobile malware detections are generic detection names, used to block a wide range of unclassified Android threats.

Mobile Threat	Percentage
Android.Malapp	39.2
Android.MalDownloader	16.1
Android.Opfake	5.2
Android.HiddenAds	4.8
Android.Premiumtext	4.1
Android.Maldropper	2.1
Android.Mobilespy	1.9
Android.Downloader	1.7
Android.Dropper	1.7
Android.Fakeapp	1.7
Android.Smsstealer	1.7
Android.Rootnik	1.6
Android.Lotoor	1.4
Android.SmsBlocker	1.4
Android.MobileSpy	1.3
Android.RegSMS	1.2
Android.FakeInst	1.2
Android.SMSblocker	0.9
Android.HiddenApp	0.8
Android.Lockdroid.E	0.8

Malware and grayware rates

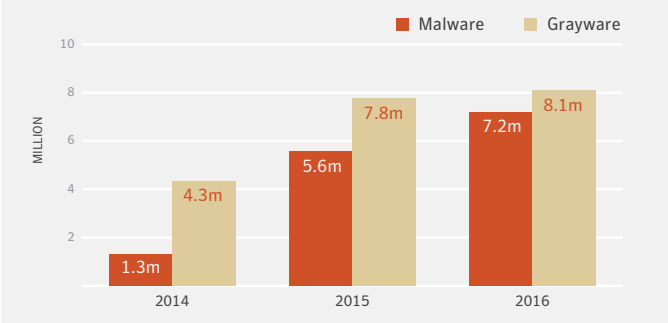
Symantec proactively collates mobile apps that are found to contain grayware or malware.

Grayware is made up of programs that do not contain malware and are not obviously malicious, but can be annoying or harmful for users. Examples include hack tools, accessware, spyware, adware, dialers, and joke programs.

There were significant spikes in both malware and grayware apps between 2014 and 2015, but in 2016 both areas leveled off. Grayware increased by just less than four percent in 2016, while malware increased by around 29 percent, compared to an increase of more than 300 percent in 2015. The levels of grayware and malware identified in 2016 are now almost comparative.

Malware and grayware rates, 2014-2016

There was a levelling off in malware and grayware apps in 2016 following growth between 2014 and 2015.



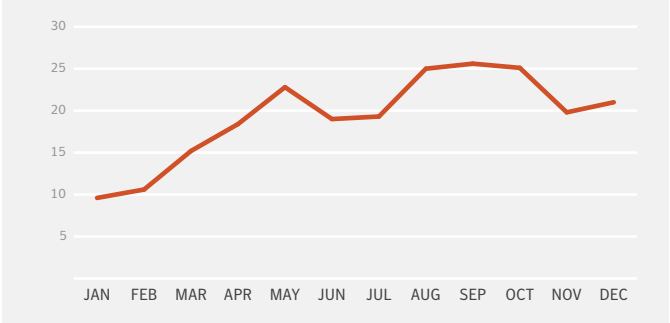
Increase in runtime packers

While mobile attackers may not be demonstrating significant innovations in the types of threat activity they conduct, they are adopting techniques that will increase infection success rates and longevity. Mobile attackers have increasingly adopted the use of runtime packers in an attempt to obfuscate malware, a practice that nearly doubled from the beginning of 2016 to the end of the year.

Runtime packers make it more difficult for malware to be detected and have been used by traditional malware for a number of years. They can allow a malicious app to be repackaged many times so it isn't detected as malicious, but then at runtime it will deploy its malware load.

Percentage of in-field mobile malware that is packed

A rise in the use of runtime packers can be seen in 2016, with the rate more than doubling between January and December.



Mobile vulnerabilities

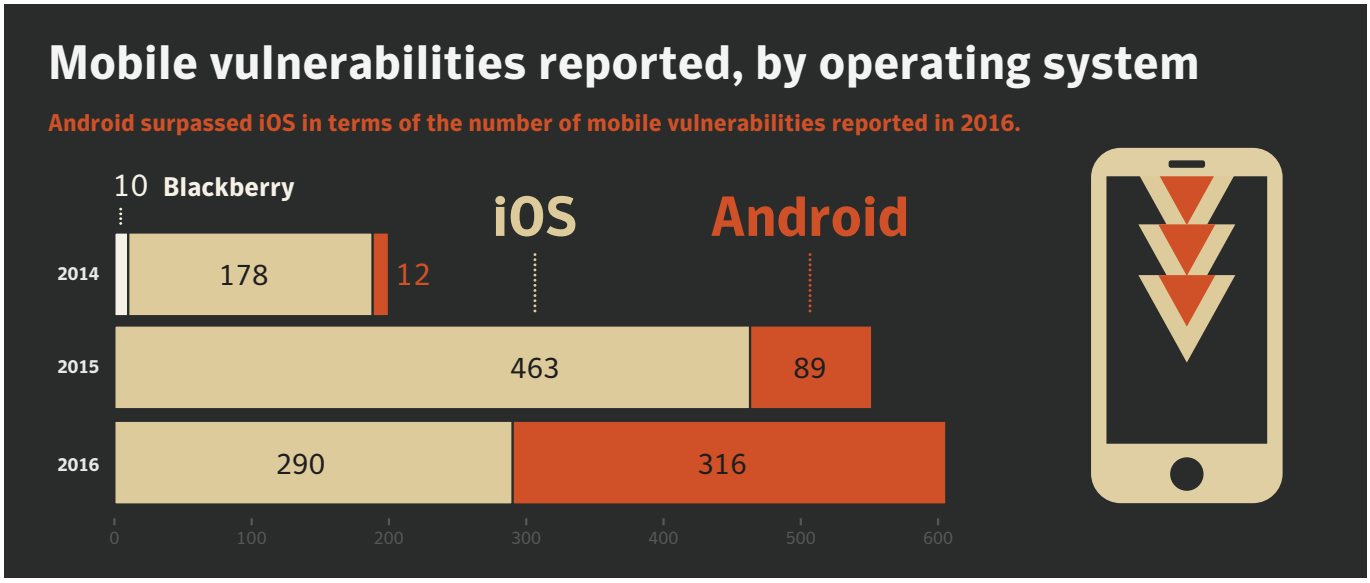
A noteworthy change in 2016 was that Android surpassed iOS in terms of the number of mobile vulnerabilities reported, a stark contrast with previous years, when iOS far outstripped Android in this area. This change may be partially attributed to continuing improvements in the security of the Android architecture and an ongoing interest by researchers in mobile platforms.

Improvements in Android architecture

Android has continually modified its architecture to help improve security. This has impacted cyber criminals by making it more difficult for them to successfully install malware on phones. Even if they do succeed in installing malware on a victim's phone, various developments and improvements in Android have made it increasingly difficult to monetize it.

Symantec data shows that premium text messages are still one of the most effective ways for cyber attackers to make money from mobile malware. However, Android 4.2 (Jelly Bean) incorporated an update in 2012 that undermined the operation of premium SMS Trojans, which were rampant at the time. The update meant the phone would display an alert if there was an attempt to send a message to a premium phone number, greatly reducing the effectiveness of these scams.

Autostart restrictions introduced in Android 3.1 (Honeycomb) in 2011 also presented a challenge to attackers as it blocked silent autostart capabilities, preventing Trojans from silently launching without any front-end activity. While this has been effective, attackers have also devised ways to get around this restriction.



Elsewhere, updates released as part of Android 5.0 (Lollipop) and Android 6.0 (Marshmallow) made life more difficult for attackers attempting to deploy mobile banking malware. Mobile banking malware works by creating overlay injections to phish the current running application, but these updates thwarted malware's ability to find the current running task by deprecating the getRunningTasks() API. Since then, attackers have been engaged in finding workarounds to overcome these additional security measures.

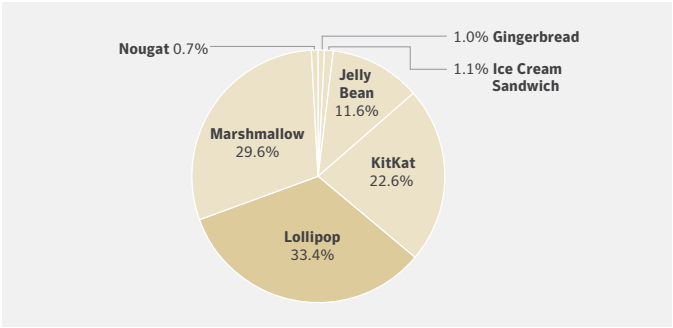
Updates on Marshmallow also attempted to tackle the problem of mobile ransomware. A new permissions model on the updates made it very difficult for ransomware authors targeting Marshmallow to successfully launch their malware on a device by requiring the user to give explicit permission for the ransomware to lock the device.

While these updates and security improvements are welcomed, continuing improvements are only useful if people can download the latest version of Android onto their device, which isn't always the case.

Some manufacturers never roll out the latest version of Android onto their smartphones, or there is a major lag between the latest version being released and it becoming available for all. Figures from Android itself show that, at the start of 2017, the most up-to-date version of its OS, Nougat, had only a tiny market share, as it was not yet available for most phones outside of Google's ecosystem. The next most up-to-date version, Marshmallow, did not have the operating system's biggest market share either, with it around four percentage points behind the previous version, Lollipop. A lack of updates can provide ample opportunities for cyber attackers to target outdated mobile operating systems.

Market share of different versions of Android, January 2017

The most up-to-date version of Android, Nougat, only has a tiny percentage of the operating system's market share.



The prevalence of older operating system versions means attackers can continue using old techniques, which may be unusable on the most up-to-date OS, to carry out attacks without a need for innovation on their parts.

This may go some way to explain the lack of innovation or expansion on the part of mobile attackers—they have a model that works.

Sour taste for Apple

Malware on iOS is still a relatively rare occurrence. However, in August 2016 it was discovered that three zero-day vulnerabilities on iOS, known as Trident, were being exploited in targeted attacks to inject the Pegasus malware onto victims' phones. Pegasus is spyware that can access messages, calls, and emails. It can also gather information from apps including Gmail, Facebook, Skype, and WhatsApp.

The attack worked by sending a link to the victim through a text message. If the victim clicked on the link then the phone was jailbroken and Pegasus could be injected onto it and start its spy work.

The vulnerabilities that allowed this attack to take place included one in the Safari WebKit that allowed the attacker to compromise the device if a user clicked on a link, an information leak in the kernel, and an issue where kernel memory corruption could lead to a jailbreak.

The attack was discovered when a human rights activist handed over his phone to Citizen Lab after he received a suspicious text message. The vulnerabilities only appear to have been exploited in a limited number of targeted attacks.

Pegasus is a spyware developed by the NSO Group, an Israeli firm that reportedly only sells its software to governments. The three vulnerabilities were patched by Apple in iOS version 9.3.5.

This attack showed that while attacks on iOS are rare, the system is not infallible.

Best practices

- Keep your software up to date.
- Refrain from downloading apps from unfamiliar sites and only install apps from trusted sources.
- Pay close attention to the permissions requested by apps.
- Install a suitable mobile security app, such as Norton, to protect your device and data.
- Make frequent backups of important data.

Cloud

As cloud usage by both enterprises and consumers has become mainstream, its appeal to attackers has naturally increased. While cloud attacks are still in their infancy, 2016 saw the first widespread outage of cloud services as a result of a denial of service (DoS) campaign, serving as a warning for how susceptible cloud services are to malicious attack.

Key findings

- Widespread adoption of cloud applications in corporations, coupled with risky user behavior that the corporation may not even be aware of, is widening the scope for cloud-based attacks. At the end of 2016, the average enterprise organization was using 928 cloud apps, up from 841 earlier in the year. However, most CIOs think their organizations only use around 30 or 40 cloud apps.
- Symantec CloudSOC analysis found that 25 percent of all shadow data (business data stored in the cloud without IT's consent or knowledge) is "broadly shared," increasing its risk of exposure. Three percent of this "broadly shared" data is compliance related.
- Several high-profile attacks and campaigns in 2016 took aim against cloud-related services, including the Mirai botnet's distributed denial of service (DDoS) attacks against DNS provider Dyn, and attacks on Mongo DB databases hosted on cloud services.

Trends and analysis

Data gathered by Symantec CloudSOC over the last six months of 2016 showed that the use and abuse of cloud apps and services, as well as the data shared and stored in them, is increasing.

The analysis looked at more than 20,000 cloud apps, 176 million cloud documents, and 1.3 billion emails. It found that the average enterprise has 928 cloud apps in use, an increase of 87 from 841 in the first half of 2016.

While these numbers may seem big, bear in mind that a multitude of commonly used services such as Office 365, Google, Dropbox, and Salesforce are all cloud apps. In fact, Office 365, Google, and Dropbox were found to be the top three most commonly adopted and used collaborative apps in enterprises in both the first and second half of 2016.

Most commonly used cloud apps in enterprises

The average enterprise has 928 cloud apps in use on its systems, but most CIOs think their organizations only use around 30 or 40 cloud apps.

Collaboration	
1H 2016	2H 2016
Office 365	Office 365
Google	Google
Dropbox	Dropbox
Box	Evernote
Evernote	Box
Business enablement	
1H 2016	2H 2016
Salesforce	GitHub
GitHub	Salesforce
Zendesk	Zendesk
ServiceNow	ServiceNow
Amazon Web Services	Amazon Web Services
Consumer	
1H 2016	2H 2016
Facebook	Facebook
Twitter	LinkedIn
LinkedIn	YouTube
YouTube	Twitter
Pinterest	Pinterest

A lack of policies and procedures around how users in an organization use cloud services increases the risk of cloud app use. This analysis found that most CIOs think their organizations only use around 30 or 40 cloud apps, despite most enterprises having adopted an average of 928, a difference of more than 2,000 percent.

Symantec CloudSOC analysis found that 25 percent of all shadow data (business data stored in the cloud without IT's consent or knowledge) is "broadly shared," meaning it is shared internally, externally, and/or with the public.

Even more concerning is that of the 25 percent of files broadly shared, three percent contained compliance-related data such as Personally Identifiable Information (PII), Payment Card Information (PCI), or Protected Health Information (PHI). If this sensitive data leaks, it can lead to substantial compliance penalties and mitigation costs for the affected company. Limiting employees to using secure, popular file-sharing apps like Office 365 and Box cannot fully mitigate risks to this data from employee misuse or account compromise by hackers. Enforcing smart cloud data governance practices, such as identifying, categorizing, and monitoring the use of all cloud data, is critical to prevent data loss.

Alarmingly, Symantec CloudSOC found that 66 percent of risky user activity in the cloud indicated attempts to exfiltrate data. Attempts to exfiltrate data are indicated by frequent sharing of accounts, frequent or excessive downloads, and frequent previewing of documents. Previewing of documents is indicative of exfiltration activity because it can allow attackers to screenshot data. User Behavior Analysis (UBA) is critical to identifying risky users and identifying and preventing exploits such as data exfiltration, data destruction, and account compromise.

Risky business

Increased use of cloud services by organizations and their employees means that companies' data governance is being eroded and they are susceptible to weaknesses that exist outside of their organization.

This could be very serious. Symantec analysis found that 76 percent of websites contain vulnerabilities, nine percent of which are critical. This statistic is explored in more detail in the chapter on Web Attacks.

The Dyn attack, previously covered in the IoT section of this chapter, is an example of attackers targeting one organization, but affecting services provided by numerous enterprises, including Amazon Web Services, SoundCloud, Spotify, and GitHub. It underlined the risks businesses take when using cloud services.

Ransomware danger

A number of ransomware attacks against cloud-based services demonstrated the susceptibility of cloud-based data to cyber crime attacks. A recent high-profile case was when tens of thousands of MongoDB open source databases were hijacked and held for ransom. The incident occurred after older MongoDB databases were left open by users in a default configuration setting.

While there was no inherent security vulnerability in MongoDB itself, and the company alerted users about this issue, numerous older implementations that hadn't applied security best practices remained online, with more than 27,000 databases reportedly being hijacked. These attacks underlined the need for users to remain vigilant and ensure any open source software they are using is secure.

There was also a report in early 2016 from a California firm that ran its entire operation through a managed cloud solutions firm. After one of its employees opened a spam email, it found that no one in the company could access the more than 4,000 files it had stored in the cloud.

The company had fallen victim to ransomware, specifically TeslaCrypt (Ransom.TeslaCrypt). Fortunately, the cloud provider kept daily backups, but it still took a week for the company's files to be restored. This is just one example of the amount of disruption ransomware can cause to businesses.

IoT and cloud: Potential partners in cyber crime

The rush to bring any and all devices online has meant that security is often an afterthought. This was patently evident in the case of CloudPets, internet-connected teddy bears. Spiral Toys' CloudPets are soft toys that allow children and their parents to exchange recorded messages over the internet. However, researcher Troy Hunt found that the company stored customer data in an unprotected MongoDB that was easy to discover online. This exposed more than 800,000 customer credentials, including emails and passwords, and more than 2 million recorded messages. Hunt said that even though the credentials were secured using secure hashing function bcrypt, a large number of the passwords were weak enough to make it possible to decrypt them.

This case illustrates how the combination of IoT and cloud can put customer data at risk. Many IoT devices gather personal data and rely on cloud services to store that data in online databases. If those databases are not adequately secured then customer privacy and security is being placed at risk.

Living off the land

Increased use of cloud services also helps facilitate a trend discussed elsewhere in this report of attackers opting to "live off the land" instead of developing their own attack infrastructure.

Two of the most high-profile cases of 2016—the hacking of the Gmail account of Hillary Clinton's campaign chief John Podesta, and the hacking of the World Anti-Doping Agency (WADA)—were facilitated through the use of cloud services. Attackers used social engineering to acquire the password for John Podesta's Gmail. Additionally, the attackers reportedly used cloud services to exfiltrate the stolen data rather than build custom infrastructure for this purpose. Both of these high-profile cases are covered in depth in the Targeted Attacks chapter.

Cloud is attractive to attackers as, depending on how it is used and configured, it allows them to bypass local security; data stored on the cloud can be more easily accessible to attackers than data stored on local servers. Targeting cloud services also allows attackers to cause maximum disruption with relatively little effort—as seen with the Dyn DNS DDoS attack.

As the usage of cloud services becomes increasingly common, it stands to reason that attacks on such services will also become more commonplace in the future.

Further reading

2H 2016 Shadow Data Report: Companies More Collaborative, More Secure and More in the Cloud than Ever Before

Best practices

- Delete any suspicious-looking emails you receive, especially if they contain links or attachments.
- Be extremely wary of any Microsoft Office email attachment that advises you to enable macros to view its content. Unless you are absolutely sure that this is a genuine email from a trusted source, do not enable macros and instead immediately delete the email.
- Watch out for any updates or patches issued for any open source software you use. Software updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by attackers.
- Ensure that the cloud service you use regularly backs up your files to ensure you can replace them should you become a victim of ransomware.
- Implement smart data governance practices in your business so that you know what business data is being stored on cloud services.

Credits

Team

Kavitha Chandrasekar
Gillian Cleary
Orla Cox
Hon Lau
Benjamin Nahorney
Brigid O Gorman
Dick O'Brien
Scott Wallace
Paul Wood
Candid Wueest

Contributors

Shaun Aimoto
Tareq AlKhatib
Peter Coogan
Mayee Corpin
Jon DiMaggio
Stephen Doherty
Tommy Dong
James Duff
Brian Fletcher
Kevin Gossett
Sara Groves
Kevin Haley
Dermot Harnett
Martin Johnson
Sean Kiernan
Bhavani Satish Konijeti
Gary Krall
Richard Krivo
Yogesh Kulkarni
Matt Nagel
Gavin O'Gorman
John-Paul Power
Nirmal Ramadass
Rajesh Sethumadhavan
Ankit Singh
Tor Skaar
Dennis Tan
Suyog Upadhye
Parveen Vashishtha
William Wright
Tony Zhu

About Symantec

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.

More Information

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

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.

11/17