ISTR

Internet Security Threat Report

Volume

23

Symantec

TABLE OF CONTENTS

Symantec

Intro

Section

01

Executive Summary

From the sudden spread of WannaCry and Petya/NotPetya, to the swift growth in coinminers, 2017 provided us with another reminder that digital security threats can come from new and unexpected sources. With each passing year, not only has the sheer volume of threats increased, but the threat landscape has become more diverse, with attackers working harder to discover new avenues of attack and cover their tracks while doing so.

Coin-mining attacks explode

Cyber criminals who have been firmly focused on ransomware for revenue generation are now starting to explore other opportunities. During the past year, the astronomical rise in cryptocurrency values inspired many cyber criminals to shift to coin mining as an alternative revenue source. This coin mining gold rush resulted in an 8,500 percent increase in detections of coinminers on endpoint computers in 2017.

With a low barrier of entry—only requiring a couple lines of code to operate—cyber criminals are using coinminers to steal computer processing power and cloud CPU usage from consumers and enterprises to mine cryptocurrency. While the immediate impact of coin mining is typically performance related—slowing down devices, overheating batteries and in some cases, rendering devices unusable—there are broader implications, particularly for organizations. Corporate networks are at risk of shutdown from coinminers aggressively propagated across their environment. There may also be financial implications for organizations who find themselves billed for cloud CPU usage by coinminers.

As malicious coin mining evolves, IoT devices will continue to be ripe targets for exploitation. Symantec™ already found a 600 percent increase in overall IoT attacks in 2017, which means that cyber criminals could exploit the connected nature of these devices to mine en masse.

Spike in software supply chain attacks

Despite the EternalBlue exploit wreaking havoc in 2017, the reality is that vulnerabilities are becoming increasingly difficult for attackers to identify and exploit. In response to this, Symantec is now seeing an increase in attackers injecting malware implants into the supply chain to infiltrate unsuspecting organizations, with a 200 percent increase in these attacks—one every month of 2017 as compared to four attacks annually in years prior.

Hijacking software updates provides attackers with an entry point for compromising well-protected targets, or to target a specific region or sector. The Petya/NotPetya (Ransom.Petya) outbreak was the most notable example: after using Ukrainian accounting software as the point of entry, Petya/NotPetya used a variety of methods to spread across corporate networks to deploy the attackers' malicious payload.

Ransomware business experiences market correction

When viewed as a business, it's clear that ransomware profitability in 2016 led to a crowded market with overpriced ransom demands. In 2017, the ransomware "market" made a correction with fewer ransomware families and lower ransom demands—signaling that ransomware has become a commodity. Many cyber criminals may have shifted their focus to coin mining as an alternative to cash in while cryptocurrency values are high. Some online banking threats have also experienced a renaissance as established ransomware groups have attempted to diversify.

Last year, the average ransom demand dropped to $522, less than half the average of the year prior. And while the number of ransomware variants increased by 46 percent, indicating the established criminal groups are still quite productive, the number of ransomware families dropped, suggesting they are innovating less and may have shifted their focus to new, higher value targets.

Drop in zero days can't halt the rise in targeted attacks

Symantec has found that overall targeted attack activity is up by 10 percent in 2017, motivated primarily (90 percent) by intelligence gathering. However, a not-so-insignificant 10 percent of attack groups engage in some form of disruptive activity.

The "Living off the Land" trend continues with attack groups opting for tried-and-trusted means to infiltrate target organizations. Spear phishing is the number one infection vector employed by 71 percent of organized groups in 2017. The use of zero days continues to fall out of favor. In fact, only 27 percent of the 140 targeted attack groups that Symantec tracks have been known to use zero-day vulnerabilities at any point in the past.

Mobile malware continues to surge

Threats in the mobile space continue to grow year-over-year. The number of new mobile malware variants increased by 54 percent in 2017, as compared to 2016. And last year, there were an average of 24,000 malicious mobile applications blocked each day.

While threats are on the increase, the problem is exacerbated by the continued use of older operating systems. In particular, on Android™, only 20 percent of devices are running the newest major version and only 2.3 percent are on the latest minor release.

Mobile users also face privacy risks from grayware, apps that aren't completely malicious but can be troublesome. Symantec found that 63 percent of grayware apps leak the device's phone number. With grayware increasing by 20 percent in 2017, this isn't a problem that's going away.

Big Numbers

Web Threats

More than

1 Billion

Web requests analyzed each day
Up 5% from 2016

1 in 13

Web requests lead to malware
Up 3% from 2016

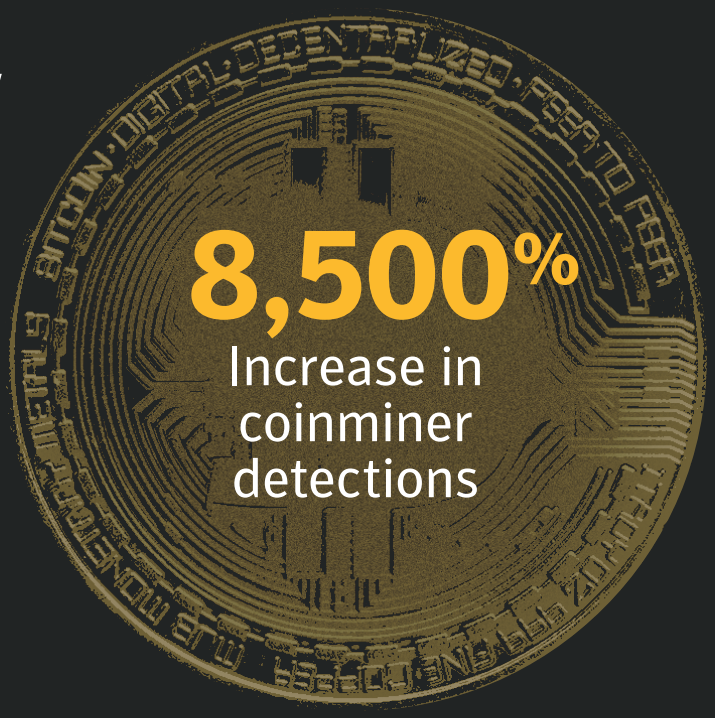
Malware

92%

Increase in new downloader variants

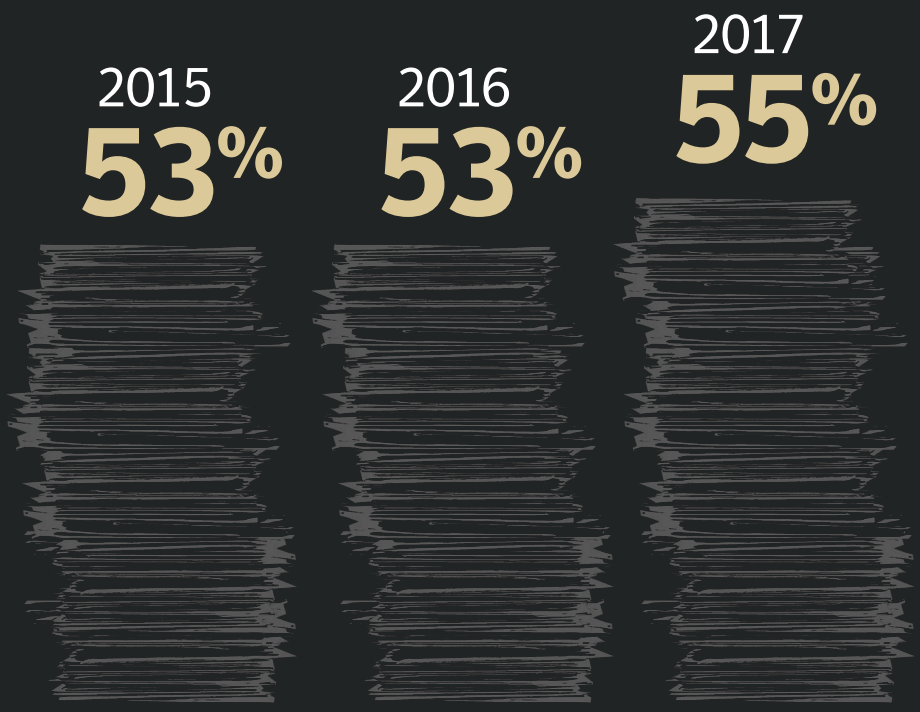
80%

Increase in new malware on Macs



Email

Percentage
Spam Rate



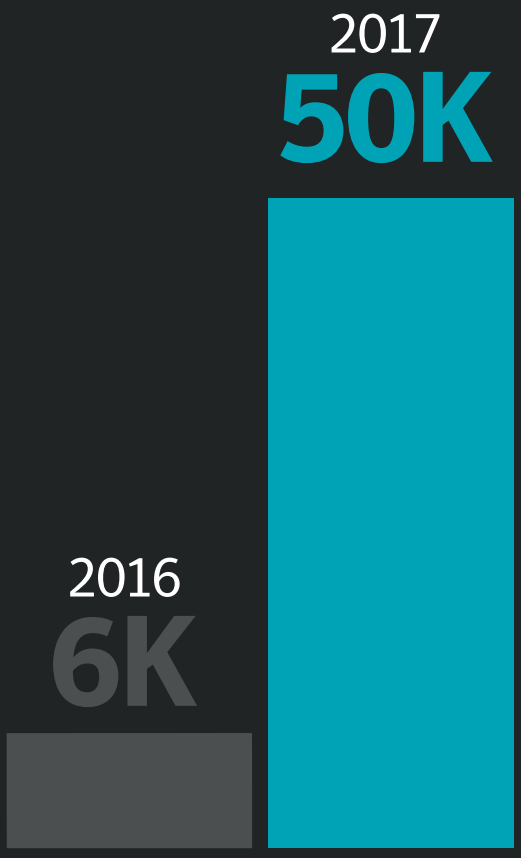
Ransomware

5.4B
WannaCry
attacks blocked

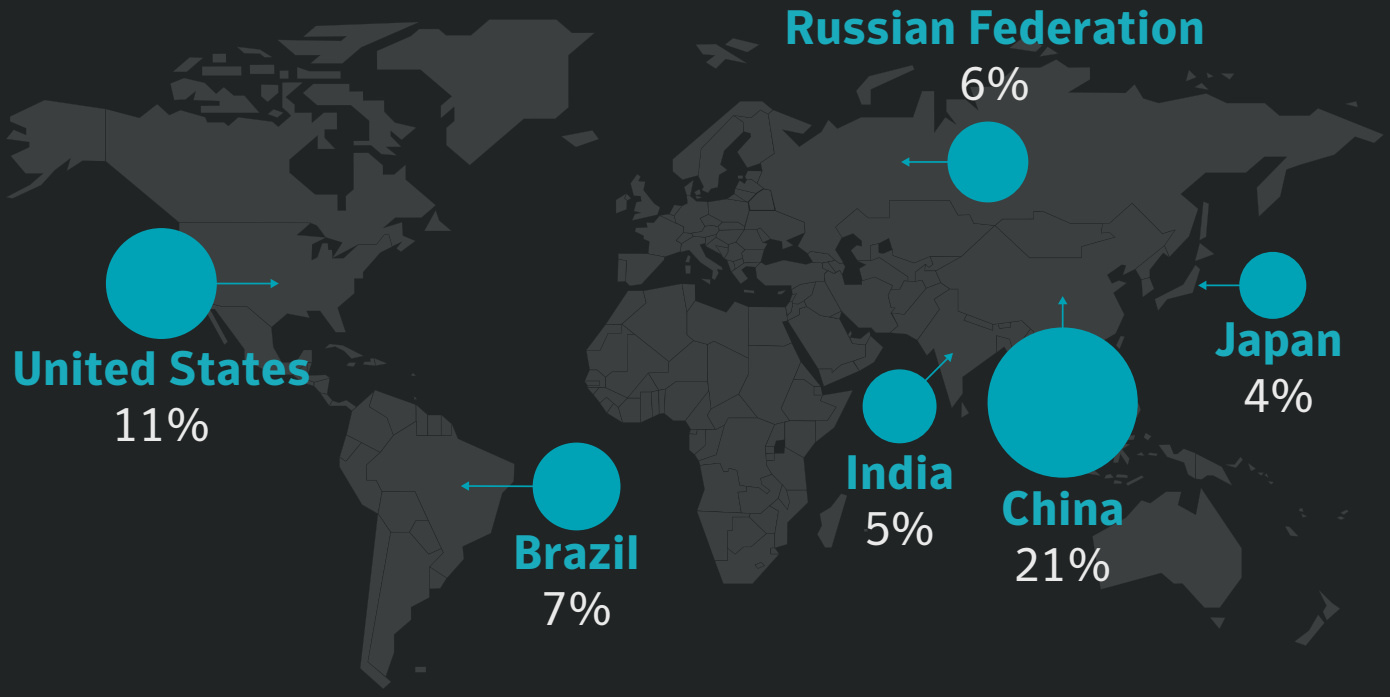
46%
Increase in new
ransomware
variants

IoT

600%
Increase
in Attacks

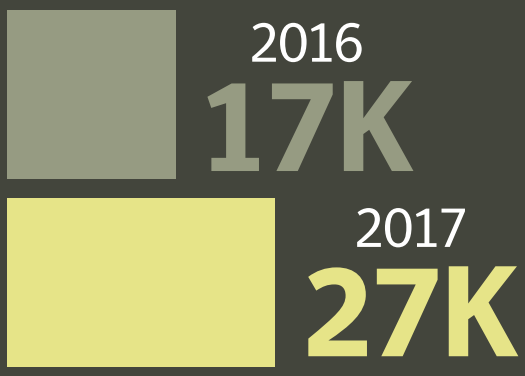


Attack Origin



Mobile

Number of new variants



Increase in mobile malware variants

54%

24,000 Average number of malicious mobile apps blocked each day

App categories that have the most malicious mobile apps are:

27% Lifestyle

20% Music & Audio

Leaky Apps – what sensitive information do they most often leak?

63% Phone Number

37% Device Location

Vulnerabilities

13%

Overall increase in reported vulnerabilities

29%

Increase in industrial control system (ICS) related vulnerabilities

Methodology

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 comprises more than 126.5 million attack sensors, recording thousands of threat events every second, and contains over five petabytes of security threat data. This network also monitors the threat activities for over 175 million endpoints located in 157 countries and territories through a combination of Symantec products, technologies, and services, including Symantec Endpoint Protection™ software, the Symantec DeepSight™ Intelligence service, Symantec Managed Security Services™ offering, Norton™ consumer products, and other third-party data sources.

In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 95,800 recorded vulnerabilities (gathered over more than two decades) from 25,000 vendors representing over 78,700 products.

Analysis of spam, phishing, and email malware trends is gathered from a variety of Symantec email security technologies processing more than 2.4 billion emails each day, including: Symantec Messaging Gateway for Service Providers, Symantec Email Security.cloud, Symantec Advanced Threat Protection for Email, Symantec's CloudSOC™ Service, and the Symantec Probe Network.

Filtering more than 338 million emails, and over 1.8 billion web requests each day, Symantec's proprietary Skeptic™ technology underlies the Symantec Email and Web Security.cloud™ services, utilizing advanced machine learning, network traffic analysis, and behavior analysis to detect even the most stealthy and persistent threats. Additionally, Symantec's Advanced Threat Protection for Email uncovers advanced email attacks by adding cloud-based sandboxing, additional spear-phishing protection, and unique targeted attack identification capabilities. Symantec also gathers phishing information through an extensive anti-fraud community of enterprises, security vendors, and partners.

Over 1 billion URLs are processed and analyzed each day by Symantec's Secure Web Gateway solutions, including ProxySG™, Advanced Secure Gateway (ASG), and Web Security Solution (WSS), all powered by our real-time WebPulse Collaborative Defense technology and Content Analysis System, identifying and protecting against malicious payloads and controlling sensitive web-based content. This is out of a total of 6 billion web analysis requests. The technology is supported by our Global Intelligence Network, featuring web and threat intelligence gained through our partnership with more than 15,000 of the largest global enterprises.

ID Analytics™, and ID:A Labs (our dedicated identity research group), provides comprehensive insights into credit and fraud risks, and is powered by the ID Network™. The ID Network is a unique cross-industry repository of up-to-the-minute consumer information providing a unique perspective on identity and fraud-related risks. The ID Network also receives outcome behavior data from third-party enterprises that confirm when an applicant has been identified as fraudulent within their portfolio. This continuously updated database of cross-industry consumer behavior data allows Symantec to identify the riskiest one percent of all applications, for example, including applications for credit cards, auto loans, and wireless phone service.

Symantec Endpoint Protection Mobile (SEP Mobile) offers unparalleled depth of mobile threat intelligence which is used to predict, detect, and protect against the broadest range of existing and unknown threats. SEP Mobile's predictive technology uses a layered approach that leverages massive crowdsourced threat intelligence, in addition to both device-based and server-based analysis, to proactively protect mobile devices from malware, network threats, and app and OS vulnerability exploits.

The ISTR also includes analysis by industry sector, for which the Standard Industry Classification (SIC) system for identifying the industry sectors for businesses is used. The data relating to Symantec's customers and clients is anonymized prior to analysis and grouped according to key attributes such as industry, company size, and geographical location.

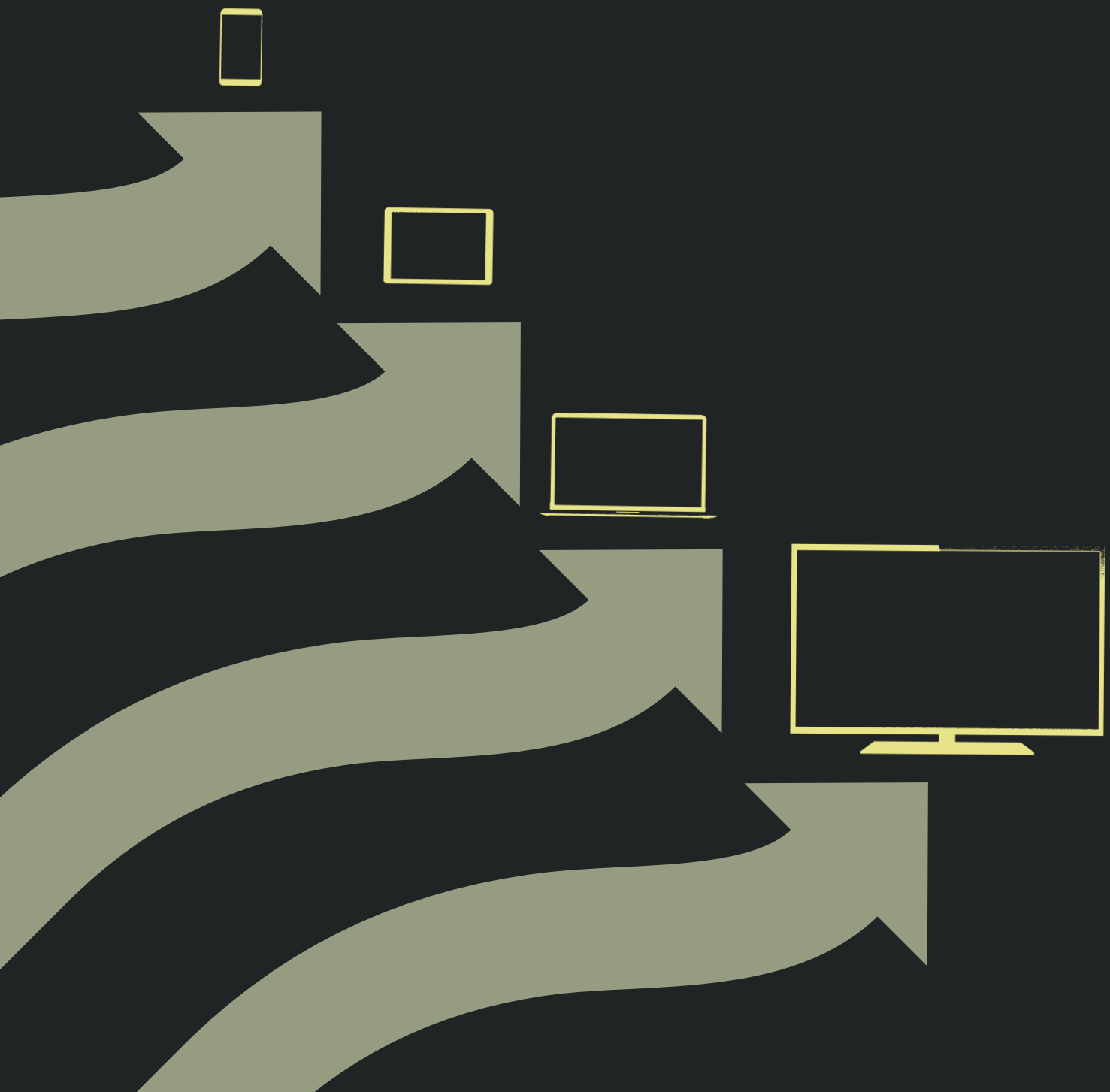
Symantec takes every care and precaution to ensure that all of the data presented in this report is produced to the highest standards and to present an unbiased and objective view of the threat landscape. Occasionally it has been necessary to filter or adjust the data to avoid bias or skewing, and this is stated in the report where required. For further information on the products, services and technologies mentioned, please refer to the Further Information section and Contacts at the back of this report.

These resources give Symantec analysts unrivalled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in cyber 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 help secure their systems effectively now and into the future.

Year in Review

02 Section

The Cyber Crime Threat Landscape



2017 was an interesting year on the cyber crime threat landscape. The WannaCry and Petya/NotPetya attacks made headlines, but they were exceptions and masked the first indications of a shift, in the ransomware landscape in particular. While ransomware remains a major threat, it seems some ransomware criminals have been busy adding more strings to their bow: in some cases distributing financial Trojans and in other cases turning to cryptocurrency coin mining.

Some online banking threats felt the impact of major take-downs that took place in late 2016, but others managed to make a breakthrough. In particular, the Emotet (Trojan.Emotet) banking Trojan reemerged after a long hiatus. Emotet's activity ramped up in the last few months of 2017, with detections increasing by 2,000 percent in this period. At the same time, the growth of coinminers, and their use by cyber criminals, grabbed headlines.

> "The growth in coin mining in the final months of 2017 was immense. Overall coin-mining activity increased by 34,000 percent over the course of the year; while file-based detections of coinminers on endpoint machines increased by 8,500 percent."

The growth in coin mining in the final months of 2017 was immense. Overall coin-mining activity increased by 34,000 percent over the course of the year, while file-based detections of coinminers on endpoint machines increased by 8,500 percent. There were more than 8 million coin-mining events blocked by Symantec in December 2017 alone. These numbers are quite mind-boggling, but this explosion in activity may be short lived. Coin-mining activity is strongly linked to the increase in value of many cryptocurrencies; a sustained drop in their value may lead to this activity going down just as quickly as it went up.

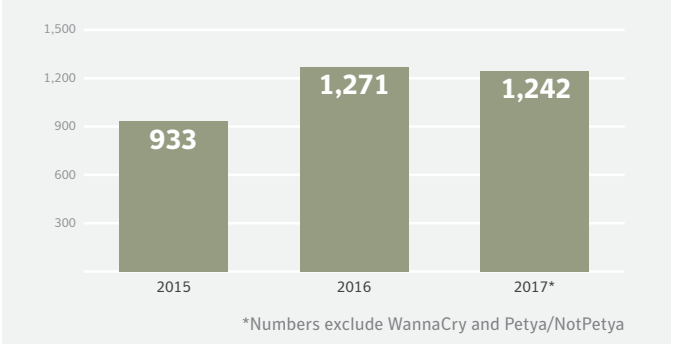
Ransomware

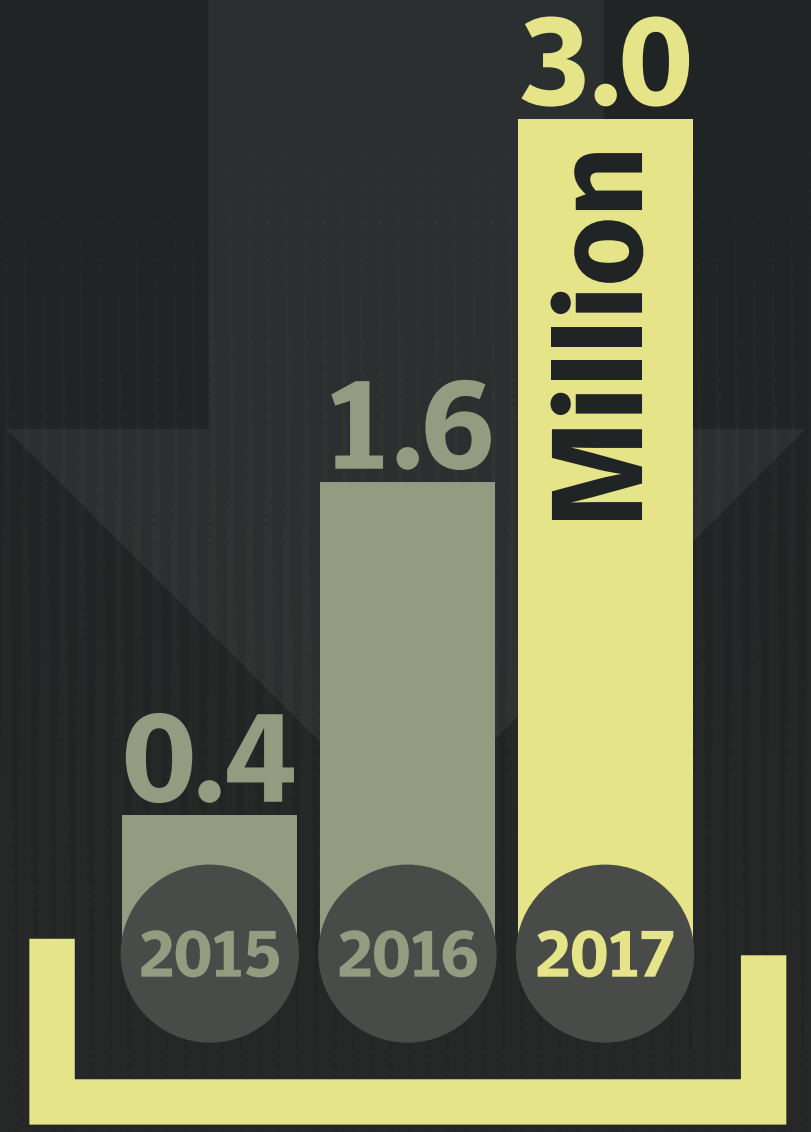
The ransomware landscape in 2017 was dominated by the stories of the WannaCry (Ransom.Wannacry) and Petya/NotPetya (Ransom.Petya) attacks, but they were not "typical" ransomware attacks, and don't represent the overall trend for ransomware in 2017. In fact, Petya/NotPetya was not a real ransomware, it was a destructive wiper that masqueraded as ransomware. For these reasons, we have omitted detections of these threats from our ransomware detection counts in this chapter. The impact and significance of these attacks is covered elsewhere in this report, in the article on Ransomware: More Than Just Cyber Crime.

Ransomware infections had steadily increased year-over-year since 2013, and reached a record high of 1,271 detections per day in 2016. Ransomware detections failed to break that record in 2017, but remained at those elevated levels. With WannaCry and Petya/NotPetya excluded from detection numbers, there were approximately 1,242 average ransomware detections every day in 2017, roughly the same as 2016's record-breaking number.

Ransomware detections per day 2015-2017

If we exclude WannaCry and Petya/NotPetya, ransomware detections were stable between 2016 and 2017.





There was a 92% increase in blocks of downloaders in 2017

"Improved detections earlier in the attack chain by Symantec mean these downloaders are being detected and blocked before they drop their final payload."

A stabilizing of ransomware detections on the endpoint may not necessarily be an indication of drops in activity, but could also be indicative of the impact of improved upstream protection. Effective email filtering, Intrusion Prevention System (IPS) detection, and machine learning technology mean that ransomware activity is being blocked earlier in the infection chain. For example, in 2017 we saw a 92 percent increase in blocks of script and macro downloaders, a major source of ransomware infections. Improved detections earlier in the attack chain by Symantec mean these downloaders are being detected and blocked before they drop their final payload.

Viewing ransomware as a business, it's clear that the profitability of ransomware in 2016 led to a crowded market and clear overpricing of ransom demands from greedy criminals. In 2017, the market made a correction, with fewer new ransomware families and lower ransom demands. Ransomware authors honed their business model in 2017, seeming

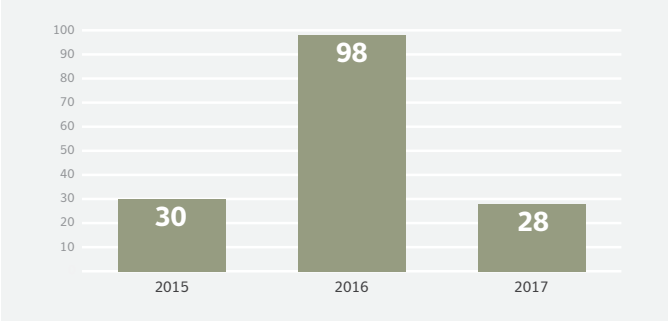
to find the sweet spot victims are willing to pay. The average ransom demand for 2017 was $522, which is less than half of 2016's figure of $1,070, and is also a decrease from the mid-year average, which was $544.

In 2017, 28 new ransomware families appeared, which is on par with 2014 and 2015, but a drop on 2016, when an unprecedented 98 new families were discovered.

> **"There were also declines in activity from some of the big ransomware families in 2017. Cerber, Locky, and TorrentLocker all but disappeared from the scene over the course of the year."**

New ransomware families 2015-2017

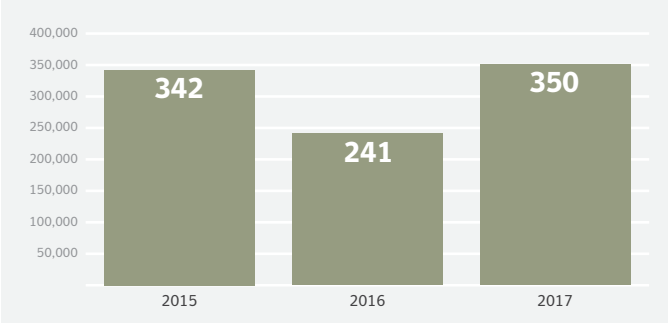
The number of new families observed stabilized in 2017 after a surge in 2016



However, the number of overall ransomware variants increased by 46 percent, indicating that established ransomware groups continue to develop and propagate their wares. The stable number of new families emerging likely indicates a lack of new attack groups, or less innovation on the part of established groups.

New ransomware variants 2015-2017

The number of new ransomware variants seen increased by 46 percent in 2017



There were also declines in activity from some of the big ransomware families in 2017. Cerber (Ransom.Cerber), Locky (Ransom.Locky), and TorrentLocker (Ransom.TorrentLocker) all but disappeared from the scene over the course of the year.

Despite this, the Necurs (Backdoor.Necurs) botnet, one of the main distributors of Locky, had a big impact on the cyber crime threat landscape in 2017. Necurs disappeared for much of the first three months of 2017—reappearing just as suddenly on March 20 when it started sending out stock spam. Its absence was immediately felt, with a major drop in email malware and spam rates for those three months. The rates steadily increased for the rest of the year, though they never quite reached 2016 levels.

Email malware rate 2016-2017 (1 in)

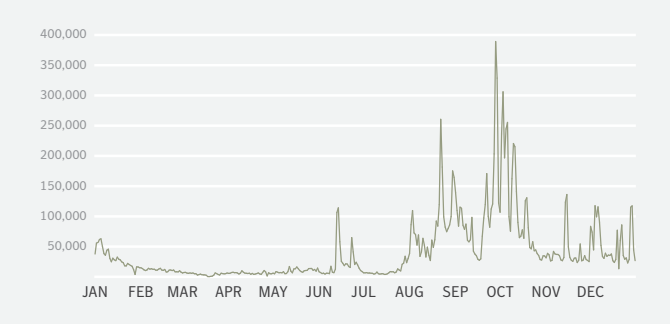
The impact made by Necurs' absence at the start of 2017 is clearly visible

Despite its absence at the beginning of the year, Necurs was still one of the biggest hitters in cyber crime in 2017. If we look at telemetry for the number of email malware campaigns executed by Necurs in 2017 we can see an increase in activity from June, with a notable surge in September and October, and some peaks visible right through to the end of the year.

Necurs sent out almost 15 million malicious emails in 2017, with 80 percent of these sent in the second half of the year. More than 67,000 malicious emails were sent by the Necurs botnet every day in the last six months of 2017.

Necurs email malware campaigns 2017

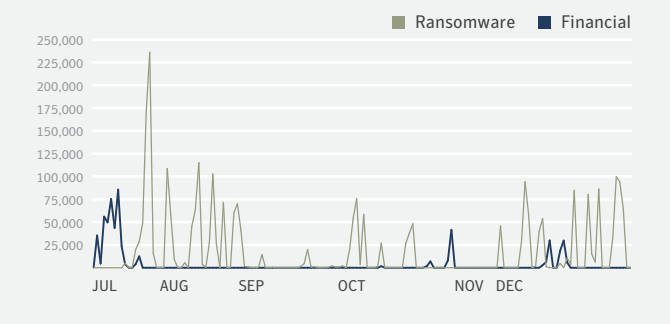
The vast majority of activity occurred in the second half of the year



While the main groups behind ransomware distribution are still very much active, we observed a greater number of email campaigns distributing online banking threats and, in some cases, replacing ransomware campaigns. If we look at Necurs activity for the final six months of the year, we can see that its final payloads alternated between ransomware and financial malware.

Necurs payloads H2 2017

Necurs primarily distributed ransomware, but it also sent out some financial Trojan campaigns

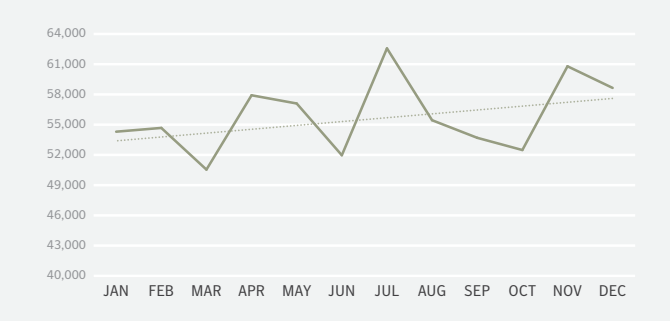


Online banking threats

Despite attention from Necurs, overall financial Trojan activity fell in 2017 compared to 2016, primarily due to law enforcement action. Two financial Trojans that were major players in 2016—Trojan.Bebloh and Trojan.Snifula—largely disappeared in 2017 as the criminal gangs operating them were both hit by takedowns towards the end of 2016. Both of these Trojans were detected on hundreds of thousands of machines in 2016, so their absence had a big impact on financial Trojan numbers overall. A decline in financial Trojan numbers year-over-year is a trend that we have seen in the last couple of years. As well as the takedowns, some of this decline can be explained by better detections being in place further upstream, similar to the situation with ransomware, which means that the final payload of the financial Trojan may never end up on the victim's machine.

Financial Trojans: Month by month counts 2017

Overall, financial Trojan figures in 2017 were down compared to 2016



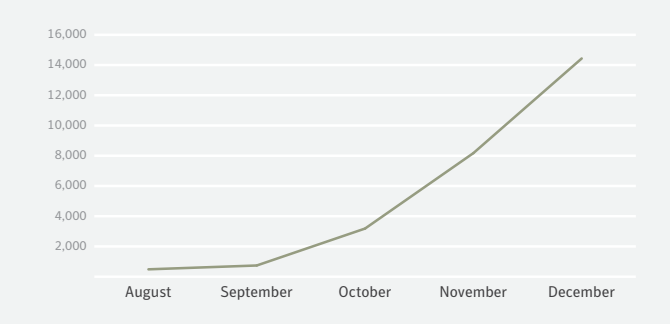
Despite the overall drop, we can see that activity is trending up in the second half of the year. This is primarily due to the Emotet banking Trojan, which had a surge of activity in the last quarter of 2017.

Emotet: Making an impact

Emotet is a financial Trojan that first emerged in 2014 and, after a quiet period, reappeared to make waves in the second half of 2017. Its activity has steadily increased, particularly in the last few months of the year, with its activity increasing by 2,000 percent in the final quarter of 2017. Primarily delivered through large email campaigns, the group behind Emotet appears to be a "professional" cyber crime group, with most campaigns being deployed Monday to Friday, with the group appearing to take the weekend off. The threat is primarily deployed via spam campaigns sent out by the Emotet botnet; as well as stealing information from infected devices, the malware is also capable of adding infected devices to the botnet.

Emotet detections

Emotet detections rose sharply in the final months of 2017



> **"Emotet is a financial Trojan that first emerged in 2014 and, after a quiet period, reappeared to make waves in the second half of 2017."**

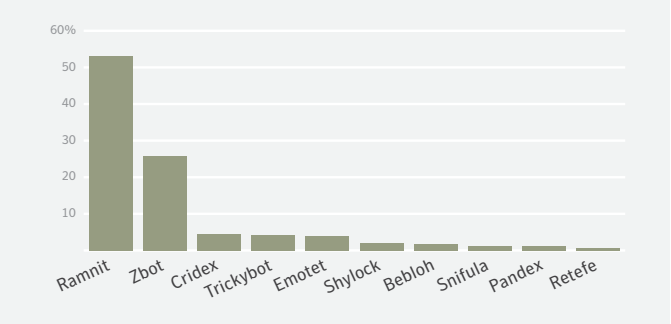
Emotet saw a particular uptick in activity in November and December. While, overall, it's only fifth in our list of top 10 financial Trojans in 2017—and is dwarfed by Ramnit (W32.Ramnit) and Zbot (Trojan.Zbot), which both dominated the financial Trojans list in 2016 too—its reemergence and increasing activity is interesting, and will be significant if it continues into 2018. Emotet's activity did decrease during the December holiday period, but it appears its operators may just have been taking a break, as it returned to its year-end activity levels at the start of 2018. If it maintains those levels of activity for the year it's likely to be higher up our list of top financial Trojans next year.

While the reemergence of Emotet was the most interesting development in this space in 2017, other online banking threats also evolved. Some financial Trojans began stealing not just online banking credentials but cryptocurrency wallet logins and any other account details that may help maximize profits.

Dridex (Trojan.Cridex), which is third in our top 10 list of financial Trojans for 2017, now checks the software installed on the devices it has infected. If it detects accounting software it will enable remote access and attempt to carry out larger fraud, rather than just stealing online banking credentials. In another example of a threat evolving in 2017, Trickybot (Trojan.Trickybot) integrated the EternalBlue exploit to allow it to spread across networks. EternalBlue, of course, was most famously used in the WannaCry and Petya/NotPetya attacks, with Trickybot apparently incorporating it following the Petya/NotPetya outbreak.

Top 10 financial Trojans 2017

Ramnit and Zbot dominated, but Emotet, the fifth most detected, made a big impact towards the end of the year



While some ransomware groups switched to distributing financial Trojans, we also observed many cyber criminals turning to coinminers in 2017, with the growth in coin mining in the last quarter of 2017 undoubtedly one of the stories of the year.

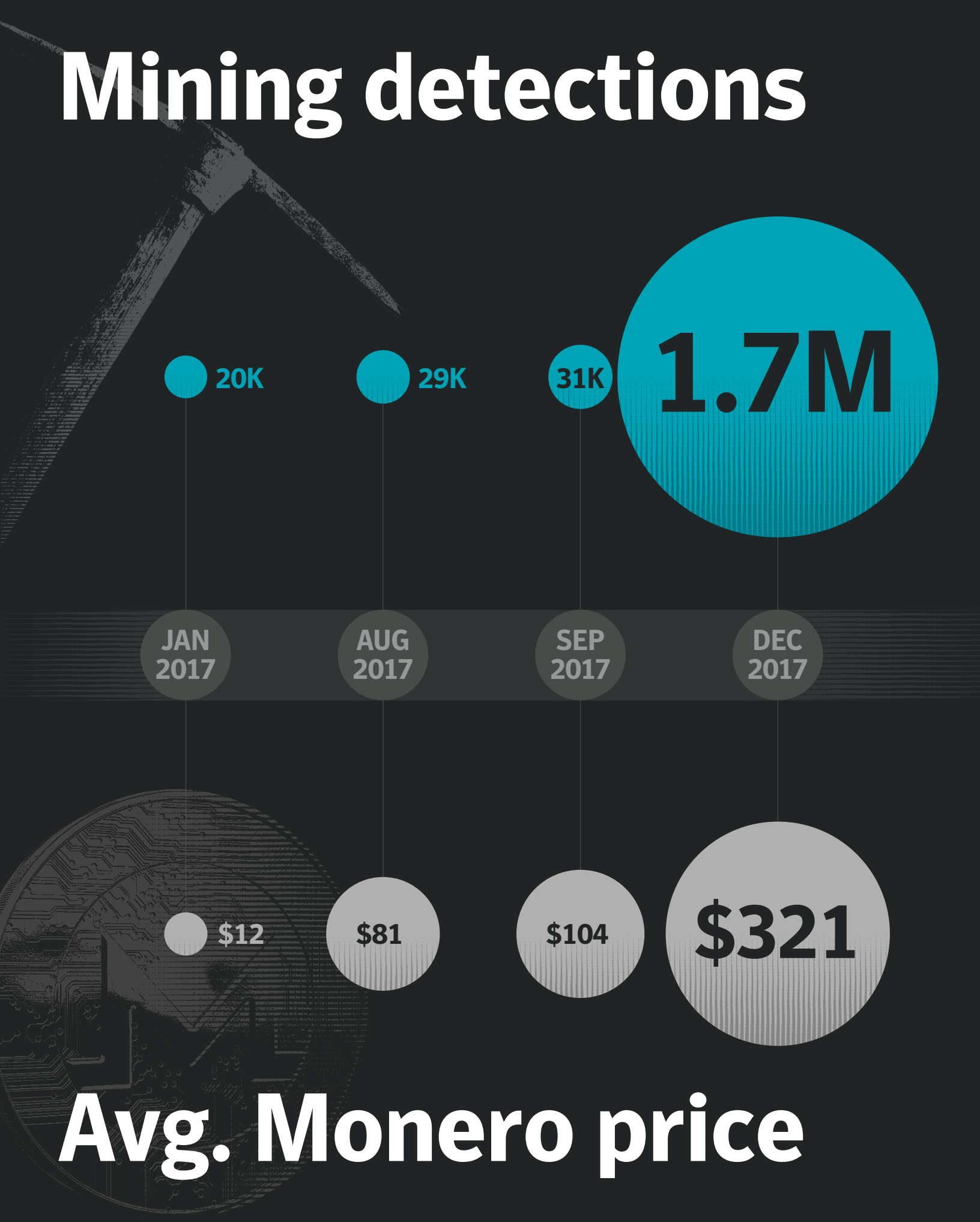
Coin mining: A modern gold rush

Before we examine this growth in coinminers, let us first explain what a coinminer is.

Coinminers are used to mine cryptocurrencies. Cryptocurrencies are digital currencies: they are created using computer programs and computing power, and recorded on the blockchain. Bitcoin was the first cryptocurrency developed on the blockchain, and is still the best known and most highly valued cryptocurrency in existence. However, Bitcoin requires a lot of processing power to mine and so is not a viable option for mining on regular computers. However, other cryptocurrencies have been developed that can more easily be mined using the computing power of regular home computers. Monero is the primary example of this. Monero, unlike Bitcoin, also provides full anonymity.

File-based coin mining involves downloading and running an executable file on your computer. Browser-based coin mining, which saw the biggest jump in prevalence in 2017, takes place inside a web browser and is implemented using scripting languages.

Mining detections



Avg. Monero price

Coin mining is not illegal, and many people are now choosing to run files or scripts on their computers to carry out coin mining. And, indeed, many people may not object to some of their computing power being used to mine cryptocurrency when they visit a particular website. It could be a welcome alternative to watching ads, or paying for the content in other ways. For example, media website Salon.com asked visitors who use an ad blocker to either turn it off or allow their computer to be used to carry out coin mining while they are on the website. The problems arise when people aren't aware their computers are being used to mine cryptocurrency, or if cyber criminals surreptitiously install miners on victims' computers or Internet of Things (IoT) devices without their knowledge.

A few factors can help explain the rise in the popularity of coinminers among cyber criminals in the latter part of 2017:

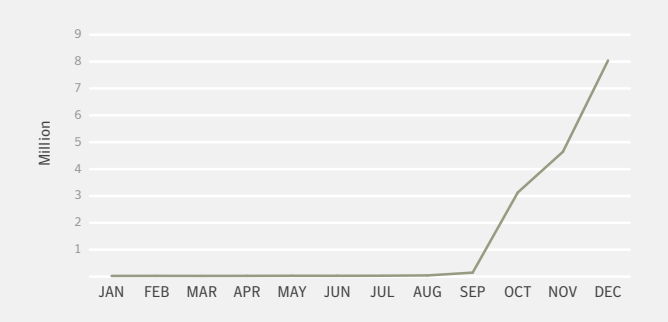
- The main driving force was almost certainly the steep rise in value of many cryptocurrencies in the final months of 2017.
- The launch of a new browser-based mining service in September by Coinhive also led to renewed interest in the area of browser-based mining. We detailed this in a blog published in December 2017. Coinhive is marketed as an alternative to ads for websites seeking to generate revenue. It recommends that its users are transparent with site visitors about its presence, but it is somewhat powerless to prevent unscrupulous operators from using it to carry out secret mining with the hope that users won't notice.
- Carrying out browser-based coin mining does not require the same level of skill as developing an exploit and installing it on victims' computers, and it also means that even people whose machines are fully patched are potential victims.
- It is a less disruptive way to make money. Victims won't necessarily immediately realize they are infected, if they ever do. They may notice that their computer is performing more slowly or that their electricity bill has increased due to their computer using more power, but if the impact is only minor victims may not make the connection to coin mining. This allows cyber criminals to make money without victims even realizing they have something unwanted on their machine or on the website they are visiting. Ransomware does not allow cyber criminals to fly under the radar in this way.

The growth in coin-mining events blocked by Symantec in the last few months of 2017 is stark, with a steep rise in detections in the last quarter of the year. More than 8 million coin mining events were blocked in December—an increase of 34,000 percent since the beginning of the year. File-based detections on the endpoint by Symantec products for these miners jumped by 8,500 percent in 2017. Much of this growth is driven by JS.Webcoinminer which detects activity associated with browser-based coinminers.

> **"Coinminers made up 24 percent of all web attacks blocked in December 2017, and 16 percent of web attacks blocked in the last three months of 2017, demonstrating the big impact of these browser-based coinminers."**

Coin-mining events 2017

Total coin-mining activity blocked by Symantec increased by more than 34,000 percent during 2017



Coinminers made up 24 percent of all web attacks blocked in December 2017, and 16 percent of web attacks blocked in the last three months of 2017, demonstrating the big impact of these browser-based coinminers.

There were twice as many detections of coinminers on consumer machines than enterprise in December, when browser-based coinminers surged, indicating that coinminers are

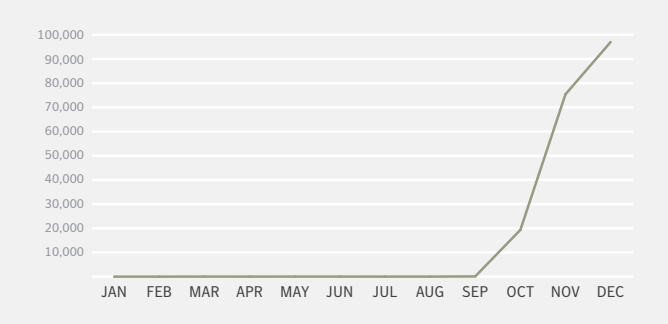
affecting consumers more than enterprise users. In a way this make sense as these miners work best on sites where people spend a long time—such as video streaming sites—which is more likely to occur on consumer rather than enterprise machines.

It's not just Windows® computers that are being impacted either: there was also a sharp increase in miner detections on Mac® computers since October, also driven by JS.Webcoinminer.

"Just as they are not limited to one operating system, cyber criminals distributing coinminers do not seem to be limited to using just one distribution vector. In the latter part of 2017, there were multiple reports of campaigns spreading coinminers."

Coinminer detections per month on Mac

A sharp increase in detections in the last three months of the year is visible



Just as they are not limited to one operating system, cyber criminals distributing coinminers do not seem to be limited to using just one distribution vector. In the latter part of 2017, there were multiple reports of campaigns spreading coinminers.

- The attack group behind the VenusLocker ransomware switched from distributing that malware via email campaigns to distributing a Monero miner.
- The attackers behind the Zealot campaign sought to exploit vulnerabilities in order to install a Monero miner on unpatched machines.
- A massive brute-forcing campaign focused on WordPress sites was used in an attempt to install a Monero miner on compromised sites. This attack had generated at least $100,000 by the time it was discovered.
- There were also examples of coinminers trying to spread via Facebook Messenger.
- The increased prevalence of coinminers has correlated with the increasing value of many cryptocurrencies. The longevity of this activity very much depends on the future value of these currencies.


Targeted
Attacks
by Numbers

How likely is it that your organization will be attacked? And if you are attacked, what are the attackers' likely motives and means?

We spend a lot of time investigating targeted attacks and, over the past number of years, we've regularly shone the spotlight on previously unknown groups. Often we're asked to give an overview of the targeted attack landscape. People want to know what the overall activity level is like, whether it's up or down, who is being targeted and where they are located. It's something we often do with other threat types, such as ransomware or financial Trojans.

However, presenting a macro picture of targeted attacks is a fairly difficult thing to do. Why? For a start, targeted attacks are just that, targeted. Relatively speaking, they're very low in number, which makes it more difficult to crunch the numbers. Even a very small number of attacks can cause big variations in percentage terms.

When we began to think about it a little more, we realized there was an alternative approach. We keep a lot of data on targeted attack groups themselves. By aggregating that data, we could paint a picture of the average targeted attack group. And from that, we could tell people how these groups are most likely to attack an organization and what their primary motivations are.

What do we classify as a targeted attack?

Before we go any further, it's probably worth clarifying what we mean by "targeted attack." While the term does appear to be self-explanatory—an attack directed at a specific target or targets as opposed to widescale indiscriminate campaigns—there are some distinctions to make. The work of individuals usually isn't classed as a targeted attack. For example, if someone decides to hack into the computer of someone they know, this isn't a targeted attack as we'd know it.

Instead, targeted attacks are the work of organized groups. The majority of these groups are state sponsored (although there is a small number of private operators) and they're usually driven by a small number of motivations: intelligence gathering, disruption, sabotage, or financial. Broadly speaking "targeted attacks" corresponds to espionage, although the lines are starting to blur and, in recent times, we've seen a number of groups branch out beyond espionage.

Even within this definition, there are some attacks that don't fit the mold. For example, the Petya/NotPetya (Ransom.Petya) attacks were the work of a state sponsored attacker, but were indiscriminate (although mainly targeted at Ukraine).

Groups

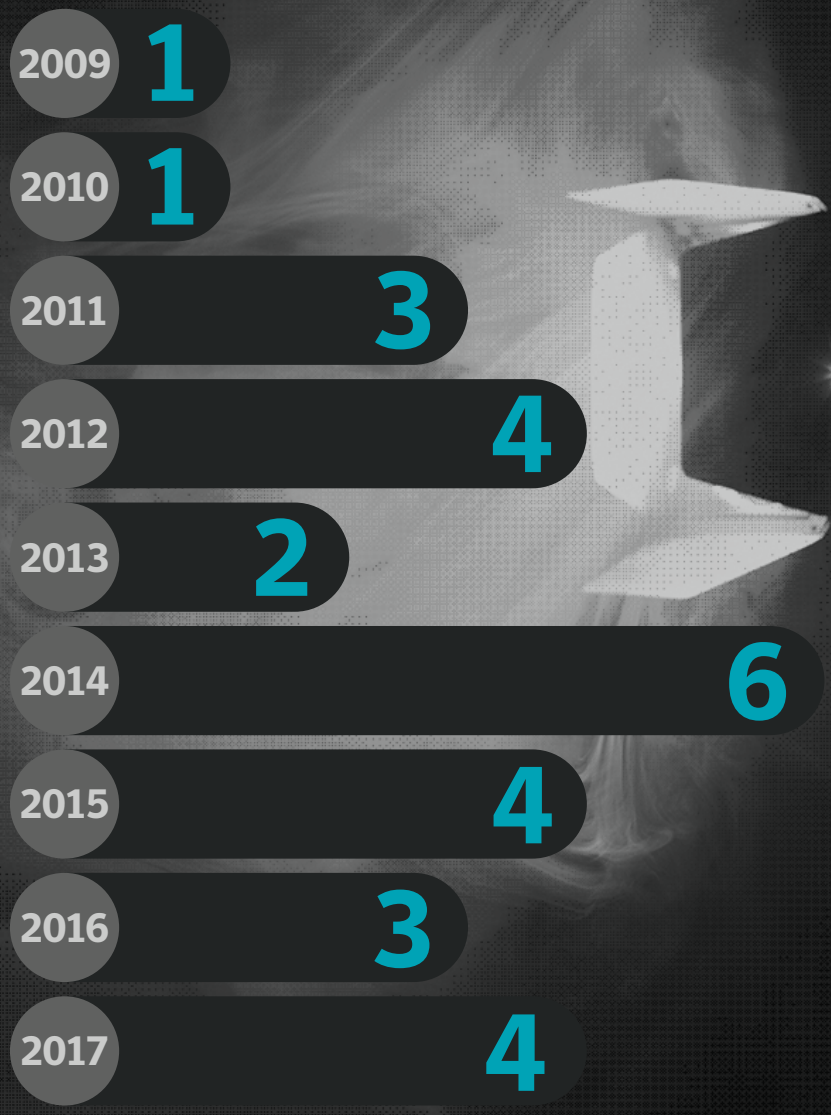
The first thing we looked at was how many groups are operating at present and if that number is growing over time. Currently, there are 140 targeted attack groups known to Symantec. Even that number may require some explanation. What is a targeted attack group? They rarely leave calling cards, meaning it can take some time to piece together the evidence to suggest that certain tools and techniques are all the work of one particular group.

In a world where few things are certain, the lines can be blurred. For example, groups affiliated to a single state are sometimes known to share infrastructure and tools, which can lead to some questions on whether two or more groups are distinct entities or part of the same operation. Vendors will often make different assessments based on the information they have, which means the running total of known groups kept by any two vendors is likely to be different.

> **"Unlike the world of cyber crime, where gangs regularly disappear only to be replaced by new threats, the world of cyber espionage is becoming an increasingly crowded marketplace."**

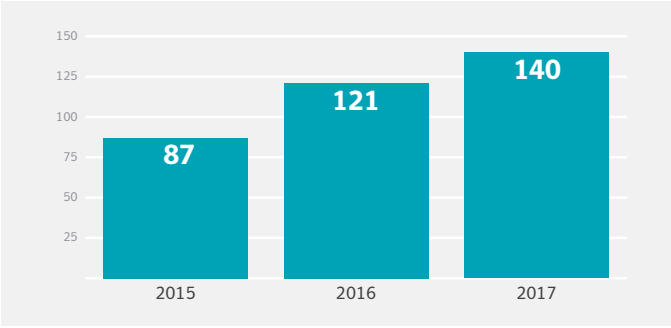
Over the past three years, we've become aware of an average of 29 new groups every year, although the pace of new groups emerging slowed somewhat during 2017, when we logged a total of 19 new groups. Nevertheless, it gives a good idea of the pace of expansion in this sector. When you compare it to the total of known groups, the number of new players appearing on the scene every year is quite significant. What's more, most of the older groups show no sign of going away. What the attackers do once they've compromised an organization, such as what computers they target, and what (if any) information they steal can provide you with further insights.

Symantec has exposed an average of 3 new targeted attack groups every year.



Targeted attack groups known to Symantec

Running total of targeted attack groups known to Symantec. Over the past three years, we've become aware of an average of 29 new groups every year.



One of the most interesting but intensive jobs we do is discovering and investigating new targeted attack groups, in order protect our customers from them and warn the wider world.

Once we have enough data to build up a useful profile, we'll usually publish our research and, of those 140 groups we know about, 28 were first exposed by Symantec. We've exposed an average of three new groups every year.

Motives

While we rarely get an insight into the minds of the attackers, over time we're usually able to come to some conclusions about the motivations behind targeted attack groups. We have a few ways of doing this. Looking at the type of organization targeted by these groups can often tell you a lot about what they're interested in. Analyzing the capabilities and features of the tools will provide further insights. What the attackers do once they've compromised an organization, such as what computers they target, and what (if any) information they steal can provide you with further insights.

ANALYST STORIES

We talked to some of our threat researchers and asked them to tell us about the groups they've worked on.

What's the most interesting group you've encountered?

Gavin O'Gorman

"Butterfly is probably the most interesting group I've worked on. They were one of the few targeted attack groups who didn't appear to be affiliated to any country and were instead involved in corporate espionage, presumably for financial gain. Over the course of a few years, they compromised a range of major corporations, such as Twitter™, Facebook™, Apple®, and Microsoft®.

Every time I go to a conference, people ask me about them, wanting to know if we've seen any more attacks. The answer is that they've disappeared completely. Their operational security was some of the best we've seen. For example, they ran command and control servers on encrypted virtual machines on compromised servers. That's something we don't see every day.

Have they retired? I doubt it. The zero-day vulnerabilities they were using would have required a lot of time and skill to acquire on their own and they were most likely bought instead. Zero days like those cost a lot of money, which means they must have been earning a lot.

If I had to guess, they shut down temporarily and developed a completely new set of tools. They were making too much money to just walk away."

Alan Neville

"Turla was one of the first big investigations I worked on, and it's still one of the most interesting. They used a lot of tools and tricks that I hadn't seen before and really demonstrated the level of sophistication at which these groups operate. Even tracing the development of their tool kit indicated this was a large, well organized group that had money to back their operations. There was obviously a lot of skilled work involved by different people to develop each component.

For example, their Venom watering hole framework is a step above what we usually see. They were one of the first groups to use system fingerprinting techniques, whereby they analyzed visitors to watering holes and collected enough information to determine if the potential victim was of interest to the group, and if so, were able to determine the best exploit to deliver in order to gain a foothold within their target's organization. But alongside that, there was also their ability to compromise multiple servers to host their exploit kit framework as a means of compromising victims. They obviously had such a range of skills available to them and this was demonstrated by the varying level of sophistication of the tools they used, their ability to operate within multiple environments, and the fact they had been active for such a long period of time, compromising multiple governments. To this day, Turla continue their operations and remain one of the most interesting groups to track."

Stephen Doherty

"Dragonfly is definitely the most interesting group I've worked on recently, mainly because they've been targeting critical infrastructure. There was a time when these kinds of attacks were unthinkable, at least until Stuxnet surfaced. But now there's several groups doing it. Dragonfly has been compromising energy companies since at least 2011.

As time goes on, they've begun to use more off-the-shelf tools and Living off the Land tactics, meaning it's become harder to attribute attacks to them. You need to be very precise because, given their targets, if you get it wrong, you're going to create unnecessary alarm.

What are they doing? As far as we can tell, they're focused on getting and maintaining access to energy networks and gathering information on how they operate.

We know they have the ability to cause serious disruption to energy networks, but so far they've never opted to go that far. The danger is that they could, at a time of their choosing. Of all the groups we've looked at, they're probably the ones that have come closest to crossing the line between intelligence gathering and something more hostile, like sabotage."

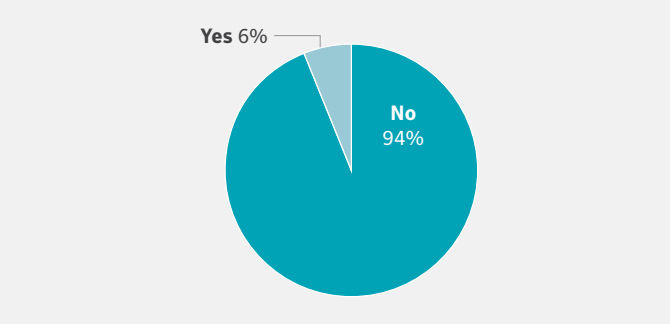
In most cases, we've been able to establish at least one motive for each of the groups we investigate. By far the most prevalent motive is intelligence gathering, with 90 percent of groups being wholly or partly involved in it. Intelligence gathering can include information stealing, spying, and surveillance.

> "Disruptive attacks are also regarded as being far more hostile and aggressive than intelligence gathering and anyone mounting them will risk reprisals."

While disruptive attacks have come to prominence in the past two years, as a motive, disruption is still a distant second to intelligence gathering, with 11 percent of groups engaged in it. This isn't surprising. While there have been a number of high-profile disruptive attacks, they are still a risky proposition. By their very nature, they draw a lot of attention. The exposure makes it more difficult for groups to carry out further attacks, since their tools and techniques will have been thoroughly investigated and as a result organizations are likely to bolster their defenses. Disruptive attacks are also regarded as being far more hostile and aggressive than intelligence gathering and anyone mounting them will risk reprisals. In most cases, particularly when sabotage is involved, they are used sparingly and usually appear calibrated to send a message to the intended target.

Destructive malware

Percentage of groups known to use destructive malware.



While only a small percentage of groups are involved in disruptive attacks, an even smaller percentage are involved in activities that could be classed as destructive, such as disk wiping. Of the groups we've encountered, only six percent have been known to use destructive malware at any point.

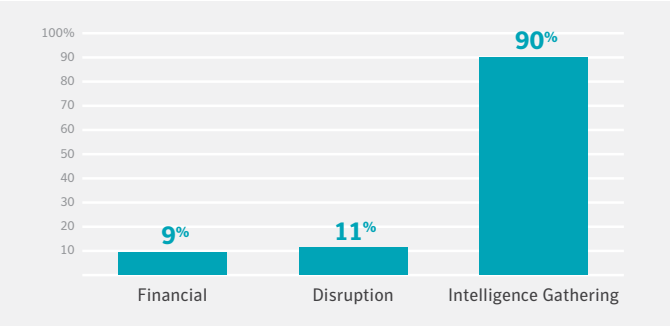
The third category of motive we've seen is financial, seen in just over nine percent of groups. Again, this isn't too surprising. Most targeted attack groups are state sponsored, meaning they have the resources of an entire country behind them. They don't need money. Or, to be precise, they don't need any more money.

There are exceptions. The most notable in recent years is probably the Lazarus group, a large and very active outfit, which made a name for itself from widescale espionage operations and a number of very public disruptive attacks, most notably the 2014 Sony Pictures™ attack which saw large amounts of information, including unreleased films, being stolen and computers wiped by malware.

More recently, Lazarus has also moved into financially motivated operations. The group was linked to the US$81 million theft from the Bangladesh central bank in 2016, along with a string of other virtual heists. Why was Lazarus robbing banks? The FBI has said the North Korean government was responsible for the aforementioned Sony Pictures attack. Subject to ongoing sanctions relating to its nuclear weapons program, North Korea is known to be short of foreign currency and cyber crime may be one way of raising more. Lazarus was also linked to the WannaCry ransomware outbreak in May 2017 (for more about that, see "Ransomware: More Than Just Cyber Crime."

Targeted attack motives

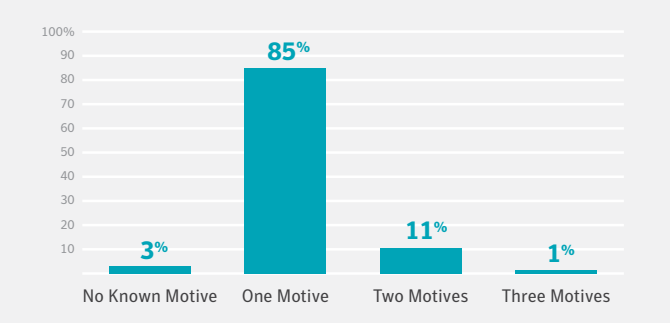
Known motives of targeted attack groups. The majority of groups are focused on intelligence gathering.



While Lazarus has its fingers in many pies, it is an exception to the rule. Most of the targeted attack groups we've encountered are much more tightly focused, with 85 percent having only one clear motive. Just 12 percent of groups have two or more known motives. For a small number of groups (three percent) we've yet to establish a motive.

Number of motives

Number of motives per group. Most (85 percent) have just one known motive.



Vectors: How do groups compromise their victims?

One of the key pieces of information we look for when investigating targeted attacks is the infection vector, namely how the attackers managed to get on the victim's network in the first place. It goes without saying, but blocking attacks at the point of entry is the most effective way of combatting targeted attacks.

Discovering the infection vector can often be quite difficult. Attackers usually attempt to compromise organizations by infecting any available computer in a targeted organization and, once inside, then move on to specific computers of interest by mapping and traversing the organization's network. Groups with good operational security will often clean up as they go along, removing their tools from any computers they no longer need. That means that traces of the initial infection have often been removed by attackers by the time an attack is uncovered.

Spear-phishing emails emerged as by far the most widely used infection vector, employed by 71 percent of groups.

Spear phishing relies on duping the recipient into opening an attachment or following a malicious link and its popularity illustrates how often the person sitting behind a computer can be the weakest link in an organization's security. Alongside a robust email security solution, educating staff about the dangers of spear-phishing emails and how to spot them will go a long way towards minimizing risk of compromise.

> **"Spear-phishing emails emerged as by far the most widely used infection vector, employed by 71 percent of groups."**

The next most popular infection vector is watering holes, websites which have been compromised by the attacker, usually without the knowledge of the website's owner. Attackers will often compromise a website that is likely to be visited by intended targets. For example, if their target is in the aviation sector, they may compromise an aviation forum.

Watering hole attacks tend to be a blunter form of infection method. Attackers can't be guaranteed that the intended target will visit the compromised website. There is also the risk of collateral damage, in the form of unintended infections of victims outside the targeted organization. Attackers will often attempt to reduce the risk of this happening by employing an exploit kit which will only infect users coming from a pre-selected IP range.

Alongside spear phishing and watering holes there are a few, more niche infection vectors. Six percent of groups have been known to use software updates, where legitimate software packages are compromised, usually by uploading a Trojanized version of the software to the unwitting developer's website.

ANALYST STORIES

What groups have the best/worst operational security?

"The groups with the best operational security are probably the ones we don't know about," said Gavin O'Gorman. "If you can identify a distinct group, by tying multiple incidents together, that means that the attackers have made a mistake and done something that allows us to identify them. We see lots of individual incidents. Attribution, tying multiple incidents to the same group is getting increasingly hard because they're getting better at covering their tracks. The increasing use of off-the-shelf tools means attackers leave less distinctive fingerprints behind."

"One of the poorest examples of operational security I've seen was this guy Bachosens," said Stephen Doherty, referring to a lone wolf attacker who was discovered carrying out targeted attacks on organizations for cyber crime purposes. "He made some really fundamental mistakes, such as registering domains using his own name. You could see that he was learning over time and he'd begun to tighten up, but he didn't seem to realize that all of the clues he'd left earlier don't just disappear."

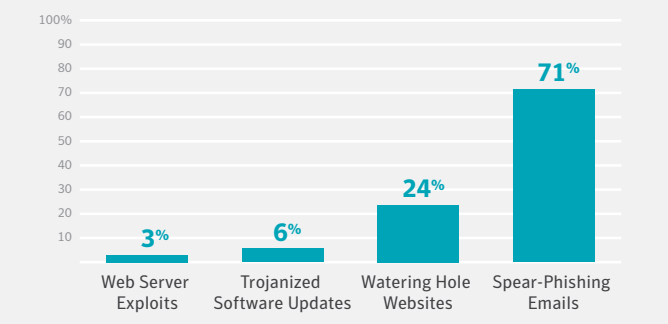
"If you think that's bad, there's one group some Symantec colleagues were working on recently where the researcher found the attacker's CV!" said O'Gorman. "The attacker used some malicious infrastructure for their own personal use, and left a link to their CV on it, publicly accessible."

"Of course, some people don't care as much about operational security as others," said Doherty. "Take Swallowtail [aka APT 28 and Fancy Bear]. Those guys just use the same tools over and over. They don't seem to care too much about people knowing it was them."

A small number of groups (three percent) have been known to use web server exploits to compromise victims, which involves exploiting vulnerabilities in SQL-based applications to send malicious commands to an SQL database.

Targeted attack infection vectors

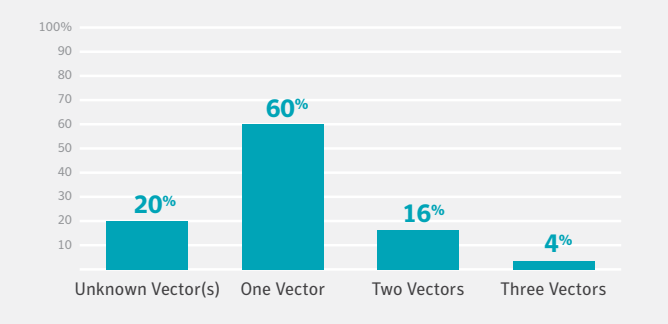
Known infection vectors used by targeted attack groups. Spear phishing is by far the most popular.



The majority of groups we've encountered (60 percent) rely on just one known infection vector. Of the remainder, 20 percent have been known to use two or more infection vectors. For 20 percent of groups, we've yet to discover an infection vector they use.

Number of infection vectors

Number of known infection vectors per group.

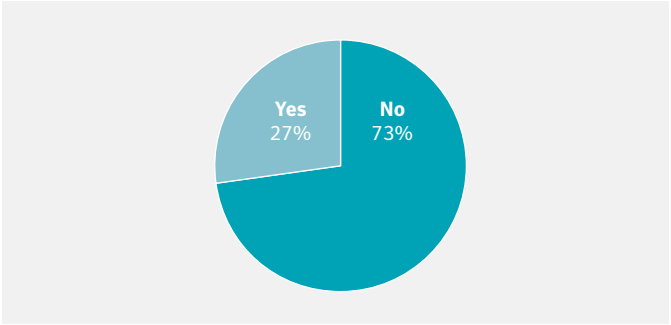


One tactic we've frequently seen used over the years to infect the victims of targeted attacks is the exploitation of zero-day vulnerabilities, software vulnerabilities which were previously unknown and unpatched. However, in the past few years, usage of zero days seems to have declined and this appears to be borne out by our analysis. Only 27 percent of the groups we've investigated have been known to use zero-day vulnerabilities at any point in the past.

There was a time when zero days were a valuable and powerful tool for targeted attack groups. But attackers have begun to eschew them in favor of less conspicuous tactics, namely "living off the land" by using whatever tools are on hand, such as legitimate network administration software and operating system features.

Zero-day vulnerability use

Nearly three quarters of all groups have never been observed exploiting zero-day vulnerabilities.



> "One of the key phases in most targeted attacks is what's known as lateral movement. Attackers rarely luck out and manage to immediately compromise the computers they are interested in."

Lateral movement

One of the key phases in most targeted attacks is what's known as lateral movement. Attackers rarely luck out and manage to immediately compromise the computers they are interested in. Instead they'll usually find a way on to a target's network by infecting any available computer and use these computers as a beachhead. From there, they'll explore the network, identify targets of interest and move across the network to infect those computers.

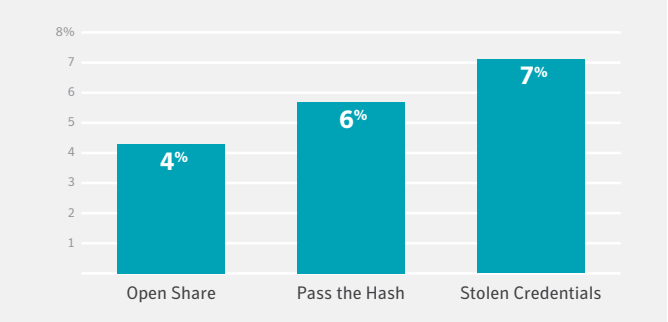
There are many techniques used to perform lateral movement and, in most cases, they leave few traces. There are a few common lateral movement techniques we log.

Of those, stolen credentials were the most commonly seen lateral movement technique employed. Attackers often use hacking software tools to obtain credentials from a compromised computer and then use them to attempt to log into other computers on the network. "Pass the hash"—where attackers steal and reuse the underlying hashed version of a password and, without cracking it, can use it to authentic themselves on other computers or servers—was used by just under six percent of groups.

Another commonly used technique we've seen is exploiting open network shares, which was used by just over four percent of groups.

Lateral movement techniques

Stolen credentials is the most common lateral movement technique we've observed, used by seven percent of groups.

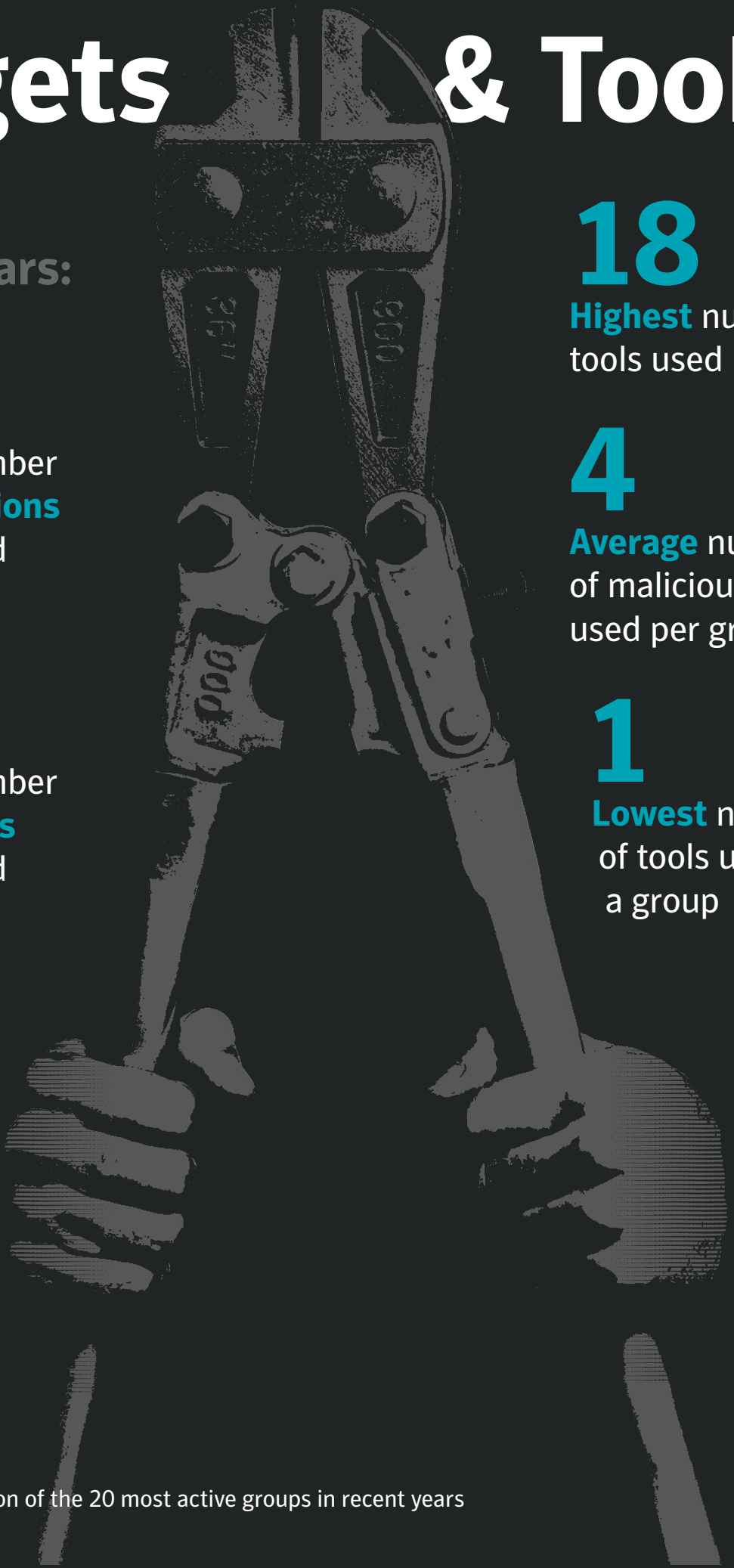


Tools of the trade: The malware behind targeted attacks

Malware continues to be one of the most important tools used by targeted attack groups. Although many groups rely on it less than before (using hacking tools and legitimate software for network traversal for example), malware is still generally used at the "pointy end" of any attack, to achieve the ultimate goal of the attack, whether it's information stealing, spying, sabotage, or any other kind of compromise.

In order to get a picture of how these malicious tools are being used, we picked a selection of 20 of the most active targeted attack groups over the past number of years and drilled down into the numbers (performing this exercise for every group would involve far too much data, so we picked a representative sample).

Targets & Tools*



Over the past 3 years:

42
Average number of **organizations** compromised per group

65
Average number of **individuals** compromised per group

18
Highest number of tools used by a group

4
Average number of malicious tools used per group

1
Lowest number of tools used by a group

*Based on a selection of the 20 most active groups in recent years

What we found was, among these 20 groups, the average number of tools used by each group was 4. The highest number was 18 and this related to the aforementioned Lazarus group. The number reflects the fact that it's something of a sprawling operation with a lot of interests.

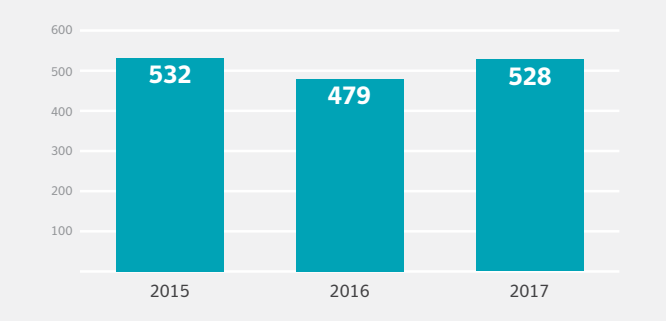
How are these tools being used? Over the past three years, an average of 42 organizations were compromised per group. In the same time period, the same groups each compromised an average of 65 individuals. If our sample of 20 groups is representative, the average targeted attack group will therefore compromise an average of 14 organizations and 22 individuals a year.

Where are the victims?

How common are targeted attacks? And how widespread are they? We took a look at our infection data for malware solely associated with targeted attack groups and found that hundreds of organizations annually, across a fairly broad range of countries, are affected by targeted attacks.

Organizations hit by targeted attacks

Number of organizations affected by targeted attacks per year, 2015 to 2017.



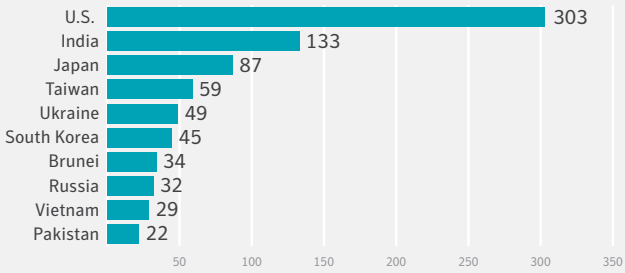
Following a dip in 2016, the number of organizations affected by targeted attacks rebounded in 2017 back to the same levels seen in 2015.

When broken down by geography, it wasn't too surprising to find out that the United States was the country most affected by targeted attacks over the past three years. It's populous, prosperous, and powerful, meaning it's going to be an obvious region of interest for targeted attack groups.

Similarly, large countries such as India, Japan, and Russia are expected inclusions on the list. Another evident trend is that countries that are the focus of regional tensions are often frequently attacked, such as Taiwan, Ukraine, and South Korea.

Top 10 countries affected by targeted attacks

Between 2015 and 2017, the U.S. was the country most affected by targeted attacks.



Analyst stories

What are the biggest/longest running groups?

"It can be hard to say when a group got started, but on the evidence we have, Turla is probably one of the longest running groups out there," said Alan Neville. "They've definitely been around since at least 2005 and there's been some research linking them to attacks as early as the 1990s, which would definitely make them among the first."

"Lazarus is probably the biggest group at the moment," said Gavin O'Gorman. "It's hard to say though whether it's one large team or a cluster of groups with access to the same tools. They probably have so many people working there that it's hard to maintain operational security. You know what it's like with huge teams. People will just go and do their own thing and it's harder to keep control over them."

What can we learn?

Based on the data we've gathered together here, what can we say about targeted attacks? Are you at risk? And, if you are, how are you at risk?

The first thing to say is that while the overall number of organizations affected by targeted attacks is quite low, the risk posed by an attack is quite high. These attackers are skilled, well-resourced, and capable of stealing valuable information or causing serious disruption.

Countries that are politically and economically powerful tend to attract more attacks than most, for obvious reasons. But if you're based in a country that is the focus of regional political tensions, you may be more at risk of attack.

The most likely reason for an attack is intelligence gathering. That could mean theft of documents and intellectual property, or it could involve snooping on your staff and customers. With this in mind, attackers will do everything they can to avoid discovery and can sometimes succeed in staying on a victim's network for months at a time.

If you're going to be attacked, the chances are that initial compromise, the gap in the fence the attackers sneak through, is going to be created by social engineering rather than anything technically sophisticated such as exploit of a zero-day vulnerability. Spear-phishing emails are the number one means of attack we've seen used, meaning a well-crafted email, sent to an unsuspecting staff member is the most likely source of compromise and can be the trigger to a potentially serious security breach.

Further Reading

Greenbug cyberespionage group targeting Middle East, possible links to Shamoon (Blog)

Shamoon: Multi-staged destructive attacks limited to specific targets (Blog)

Longhorn: Tools used by cyberespionage group linked to Vault 7 (Blog)

WannaCry: Ransomware attacks show strong links to Lazarus group (Blog)

Bachosens: Highly-skilled petty cyber criminal with lofty ambitions targeting large organizations (Blog)

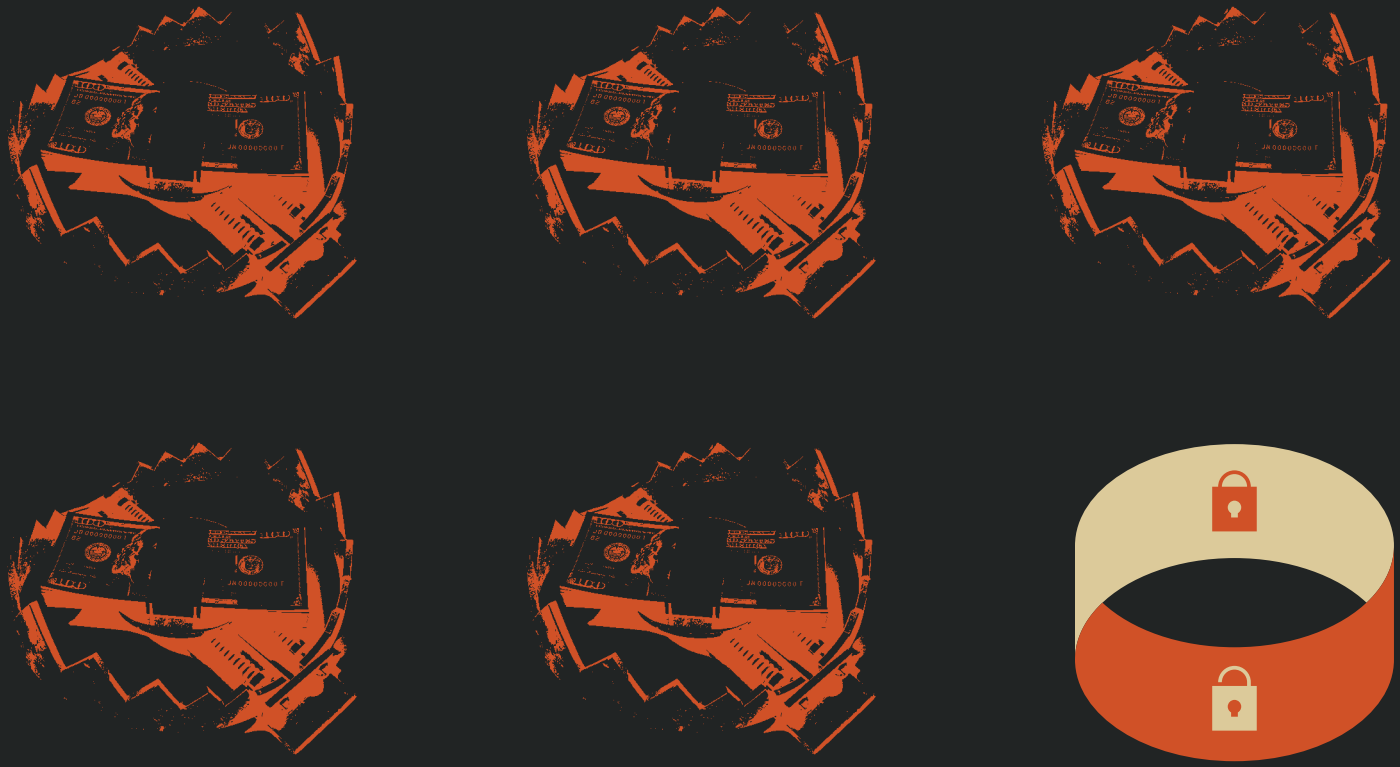
Attackers are increasingly living off the land (Blog)

Dragonfly: Western energy sector targeted by sophisticated attack group (Blog)

Sowbug: Cyber espionage group targets South American and Southeast Asian governments (Blog)

Triton: New Malware Threatens Industrial Safety Systems (Blog)

Ransomware: More Than Just Cyber Crime



Ransomware is no longer just the preserve of the cyber criminal. For a variety of reasons, targeted attack groups are taking an interest too; whether it's to raise foreign currency or use fake ransomware a cover for other types of attacks.

In late 2015, we came across something which, at the time, was very unusual. A major company in South East Asia asked us to investigate a widescale ransomware attack on its network. Hundreds of computers had been hit, all infected with what appeared to be a variant of the CryptoWall (Ransom.Cryptowall) ransomware. Almost immediately though, we realized that there was something very odd about this attack.

When we analyzed samples of the malware, we found that it didn't actually encrypt any files as you would expect ransomware to do. Instead, it just overwrote files on the hard disk with meaningless data. The malware was in fact a disk wiper, disguised as ransomware. Why did the attackers go to the trouble of trying to cover their tracks in this fashion?

When we dug a little deeper we began to piece together what had happened. The organization had been the victim of long running and sophisticated targeted attack. Five months prior to the "ransomware" incident, a number of computers at the organization had been compromised through a combination of spear-phishing emails and watering hole websites.

From this initial compromise, the attackers used a combination of malware and penetration testing tools to steal credentials, map the organization's network, and compromise many more computers, including file, application, and email servers.

The true purpose of the attack was data theft and, over the course of the intervening five months, the attackers managed to steal thousands of files from the organization. When they were finished, the intruders attempted to cover their tracks, deploying the fake ransomware to wipe the disks of infected computers.

Disguising the disk wiper as ransomware was a clever move. At the time, ransomware was beginning to reach epidemic proportions. On cursory examination, the wiper (which we named Trojan.Phonywall) looked a lot like CryptoWall, displaying a ransom note identical to the real CryptoWall message. The only difference was the payment URL. CryptoWall payment URLs were usually unique to each infection but Phonywall's was hardcoded and just copied from a CryptoWall ransom note posted online. If the attack hadn't been investigated properly, the company may have simply assumed that it had been hit with a ransomware attack, accepted its losses, and not investigated any further.

We had seen plenty of cases in the past where attackers have employed DDoS attacks to cover up intrusions. However, in 2015 the use of ransomware as a decoy by a targeted attack group was something completely new. All of that quickly changed and by 2017 it was no longer an outlier. Several targeted attack groups had discovered ransomware. They put it to a range of uses but, in almost every case, it was used to devastating effect.

> "... the intruders attempted to cover their tracks, deploying the fake ransomware to wipe the disks of infected computers."

Revenue-generating attacks

Targeted attack groups don't usually get involved in financially motivated attacks. That's because, in most cases, they have the resources of a nation state behind them and can afford to pay for personnel and pricey tools (such as zero days).

When WannaCry (Ransom.Wannacry) first struck, it seemed unlikely that a targeted attack group was behind it. The attack had the hallmarks of a cyber crime operation, something most targeted attack groups wouldn't stoop to. However, we subsequently uncovered strong evidence that the Lazarus group was behind the threat.

Although it is also possible the attack had a disruptive motive; if the motive was financial, it wouldn't be the first time Lazarus had gotten involved in cyber crime activities, having been linked to the Bangladesh Bank heist and a number of other major bank attacks. The group has been linked by the FBI to North Korea, which is subject to sanctions and known to be short on foreign currency reserves.

WannaCry had a massive impact and, had the potential to be hugely profitable. The main reason for this was that it incorporated the leaked EternalBlue exploit that used two known vulnerabilities in Windows (CVE-2017-0144 and CVE-2017-0145) to turn the ransomware into a worm, capable of spreading itself to any unpatched computers on the victim's

Gathering pace of attacks

network and also to other vulnerable computers connected to the internet. Within hours of its release, WannaCry had infected hundreds of thousands of computers worldwide.

While WannaCry caught the world's attention and caused a significant amount of disruption, from a financial perspective it was a flop. Its authors botched their implementation of the payment mechanism. WannaCry was meant to generate a unique Bitcoin wallet address for each infected computer but, due to a bug, it failed to do so and instead defaulted to three hardcoded Bitcoin addresses for payment. The attackers had no way of knowing which victims had paid using the hardcoded addresses, meaning once this became public knowledge, victims had little incentive to pay the ransom.

Secondly, the authors included a "killswitch" in the malware. This was the address of a non-existent domain. WannaCry checked if the domain was live and, if it was, would cease installing. The feature was obviously intended to allow the attackers to call a halt to the attack. However, it was quickly found by a security researcher who registered the domain themselves, thus limiting the damage of WannaCry on the same day it was released.

Had it been configured correctly, WannaCry could have earned its creators tens of millions of dollars.

"DDoS attacks can knock an organization offline, meaning that its systems admins will be busy trying to stem the DDoS attack and may be too distracted to notice suspicious activity on their network indicating that a targeted attack is underway."

Ransomware as a decoy

Decoy attacks aren't new, but previously targeted attack groups relied on other forms of decoy, usually distributed denial of service (DDoS) attacks. DDoS attacks can knock an organization offline, meaning that its systems admins will be busy trying to stem the DDoS attack and may be too distracted to notice suspicious activity on their network indicating that a targeted attack is underway.

As mentioned earlier, we saw the first case of ransomware being used as a decoy in late 2015. However, by the end of 2016, more targeted attack groups had adopted the tactic. One of the most high-profile examples was the Sandworm cyber espionage group which created a new version of its destructive Disakil Trojan (Trojan.Disakil) which was disguised as ransomware.

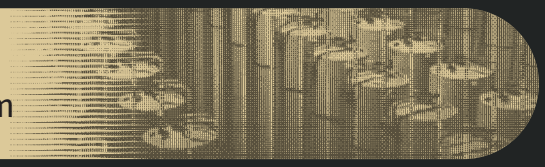
Designed to run on Linux computers, it essentially rendered them unusable by encrypting key operating system files. Once the encryption finished, it displayed a message demanding a ransom of 222 Bitcoin (approximately $250,000 at the time). Paying the ransom would not decrypt the affected files, since the encryption keys generated on the infected computer are not saved locally nor to a command and control (C&C) server.

This version of Disakil was used in a number of attacks against the Ukrainian electricity grid and was also reportedly used in attempted attacks against the financial sector and shipping targets in Ukraine. As with DDoS attacks, using ransomware as a decoy had a similar effect, sowing confusion among the victims and delaying an effective response.

Over the past number of years, the amount of ransomware being distributed has expanded rapidly, making it one of the most common cyber crime threats. Its ubiquity has made it a perfect cover for attacks. It's now so widespread that admins may not be surprised by a ransomware attack or question an apparent ransomware infection.

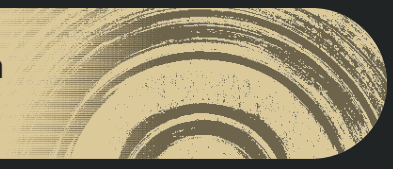
Major destructive malware attacks

JUL 2010 — Discovery of Stuxnet worm, targeting Iranian nuclear program



AUG 2012 — Shamoon disk-wiping Trojan used against targets in Saudi Arabia

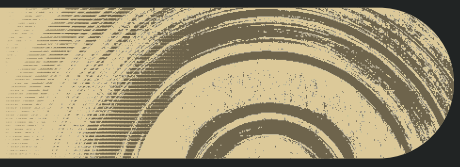
MAR 2013 — Disk-wiping attacks launched against South Korean banks and television broadcasters



DEC 2014 — Disk-wiping malware used in attack on Sony pictures (U.S.)

NOV 2016 — Fresh wave of Shamoon attacks against Saudi Arabia

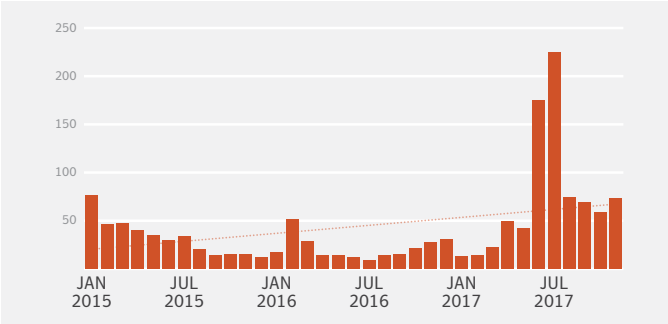
DEC 2016 — Disk-wiping malware used in attacks on Ukraine energy sector



JUN 2017 — Petya/NotPetya hits multiple organizations, mainly in Ukraine

Destructive malware infection attempts

Infection attempts by month involving destructive malware associated with targeted attack groups.



Ransomware as a disruption tool

The advent of ransomware as a decoy, followed by the appearance of WannaCry has led to the arrival of a third type of attack, namely ransomware as a form of disruption.

The first and most notable case of this was Petya/NotPetya (Ransom.Petya). When it emerged, it initially appeared to be a WannaCry copycat.

> **"As with DDoS attacks, using ransomware as a decoy had a similar effect, sowing confusion among the victims and delaying an effective response."**

Like WannaCry, Petya/NotPetya also used the EternalBlue exploit to spread itself, but also incorporated other Server Message Block (SMB) network spreading techniques, which meant it could spread across organizations to computers that had been patched against EternalBlue.

However, Petya/NotPetya contained some key differences to WannaCry which revealed the motive of the attackers. For a start, disks encrypted by Petya/NotPetya could never be recovered. When it ran, it scanned the hard drive for 65 different file types and encrypted any it found. The key was encrypted with an embedded public key and appended to a README.TXT file. When the computer rebooted, it encrypted the entire hard disk and displayed a ransom note to the user. This ransom note displays an "installation key" which was a randomly generated string. A randomly generated Salsa20 key was then used for disk encryption. The problem was that there was no relationship between the "installation key" and Salsa20 key. Since the disk couldn't be decrypted, Petya/NotPetya wasn't really ransomware. It was a disk wiper.

Secondly, unlike WannaCry, Petya/NotPetya wasn't designed to spread indiscriminately. Instead, the attack was designed to mainly affect organizations in Ukraine. The initial infections were spread through a Trojanized version of M.E.doc, a tax and accounting software package that is widely used in Ukraine. The attackers managed to compromise the M.E.doc website and upload a Trojanized version of a software update.

Disruptive attacks are an evolution of decoy attacks. The inclusion of a self-propagation mechanism means that the attack is more widespread. While ransomware still acts as decoy, the end-goal of the attack is not a cover-up, but to disrupt and sow confusion in affected organizations.

Once installed on one computer within an organization, Petya/NotPetya would begin attempting to spread itself to other computers on the network, building a list of IP addresses and using EternalBlue and other SMB spreading techniques to infect them. It did spread to external IP addresses, but only those that were in some way connected to the infected organization. While some organizations outside Ukraine were hit, these were essentially collateral damage, rather than intentional.

The net effect was that Petya/NotPetya was highly targeted against Ukraine and deeply disruptive, because it wiped all infected computers. The timing of the attack also appeared designed to cause maximum disruption, coming on June 27, the day before Ukraine's Constitution Day, a national holiday.

Copycat or retaliation?

Several months after the Petya/NotPetya outbreak, a very similar threat began spreading. BadRabbit (Ransom.BadRabbit) appeared on October 24, 2017 and was highly targeted against Russia (which accounted for 86 percent of infection attempts in the first 24 hours). The initial infection method was via drive-by downloads on compromised websites, with the malware disguised as a fake update for Adobe Flash Player™. By compromising Russian websites, the attackers ensured that victims were mainly concentrated in that country.

Just like Petya/NotPetya, BadRabbit was capable of self-propagation, and tried to spread itself across a victim's network

Why have targeted attack groups started using ransomware?

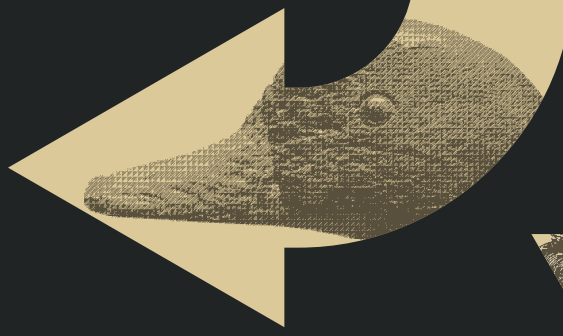
Decoy

Revenue

Disruption

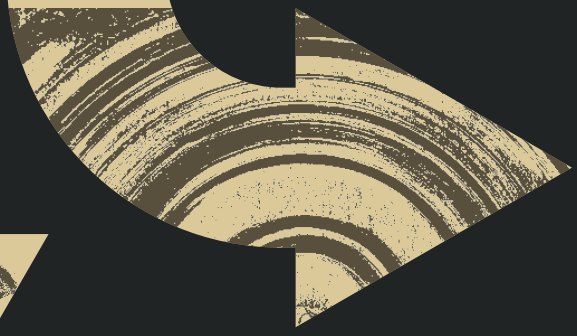
Disakil

- Perfect cover for a targeted attack. Ransomware attacks are quite common and may not arouse suspicion.
- Encrypting or wiping computers can cover evidence of an intrusion.



Petya/ NotPetya

- Making the ransomware impossible to decrypt effectively turned it into a disk wiper.
- Using ransomware disguised true disruptive motive of the attack.



WannaCry

- Possible source of foreign currency for cash-strapped regimes.
- Using EternalBlue exploit turned ransomware into a worm and hit hundreds of thousands of potential victims.

via SMB and Mimikatz (Hacktool.Mimikatz), a hacking tool capable of stealing passwords. The malware also uses a hardcoded list of commonly used default credentials to attempt to guess passwords, along with the EternalRomance exploit, a similar exploit to EternalBlue.

Unlike Petya/NotPetya, BadRabbit was genuine ransomware and decryption was possible. After the system is restarted, a ransom note is displayed, demanding a ransom of 0.05 bitcoin (approximately $280 at the time of the attack).

That fact that it was functional ransomware may mean that the attackers had seen the impact of Petya/NotPetya and opportunistically created a copycat version in the hope of making some money. However, if that was the case, why was BadRabbit largely targeted at Russia? Did a group of attackers in Ukraine think Russia was responsible for Petya/NotPetya? If so, was BadRabbit their retaliation? A lot of unanswered questions remain.

> **"Targeted attack groups using ransomware is a very recent development and it remains to be seen whether it will continue into 2018."**

Short-term phenomenon or long-term trend?

Targeted attack groups using ransomware is a very recent development and it remains to be seen whether it will continue into 2018.

WannaCry was the sole confirmed case of a targeted attack group who dabbled in ransomware for financial purposes. However, from a revenue raising perspective, it was a fiasco. Its botched configuration meant the attackers earned relatively little. Lazarus, the group behind WannaCry, has had much more success with virtual bank heists, meaning it is possible the group will abandon ransomware as a failed experiment.

On the one hand, ransomware is a cheap and easy form of decoy or disruption. Not a lot of development work is required and, in many cases, variants aren't written from scratch and instead adapted from pre-existing threats. Even the incorporation of the EternalBlue exploit into WannaCry was fairly unsophisticated, largely a case of copying and pasting code. By contrast, performing a DDoS attack, the traditional form of decoy, requires a lot more time, effort, and infrastructure.

Ransomware continues to be one of the main online threats faced by organizations and consumers. Our own telemetry suggests that ransomware infections continued to grow during 2017. Its sheer ubiquity means that it may continue to be a perfect cover for other forms of attack.

Further Reading

Destructive Disakil malware linked to Ukraine power outages also used against media organizations (Blog)

What you need to know about the WannaCry Ransomware (Blog)

WannaCry: Ransomware attacks show strong links to Lazarus group (Blog)

Petya/NotPetya ransomware outbreak: Here's what you need to know (Blog)

BadRabbit: New strain of ransomware hits Russia and Ukraine (Blog)

Ransomware 2017: An ISTR special report (white paper)

Infecting the Software Supply Chain

There was at least one large software update supply chain attack reported every month in 2017.

This is a clear sign of an increasing trend considering an average of three similar cases were reported per year between 2013 and 2016. The actual number may even be higher considering some smaller cases may not have been publicly reported. An extension of the recent living-off-the-land trend, this type of attack occurs when sophisticated attackers manipulate software supply chains to infiltrate even the most well-guarded networks. One of the reasons why attackers have chosen to hijack software updates is that it is getting increasingly difficult to find exploitable zero-day vulnerabilities that they can use. Therefore supply chain attacks are an efficient alternative to reach their goals and will most likely continue to grow.

A software update supply chain attack in IT security can be defined as follows:

> *Implanting a piece of malware into an otherwise legitimate software package at its usual distribution location; this can occur during production at the software vendor, at a third-party storage location, or through redirection.*

The typical attack scenario involves the attacker replacing a legitimate software update with a malicious version in order to distribute it quickly and surreptitiously to intended targets. Any user applying the software update will automatically have their computer infected and will give the attacker a foothold on their network. It is not only desktop computers, the same applies to IoT devices and industrial controller components.

Motivations for attackers

There are six main reasons why the software update supply chain is attractive for attackers:

01 Infiltration of well-protected organizations by leveraging a trusted channel

02 Fast distribution: number of infections can grow quickly as users update automatically

03 Targeting of specific regions or sectors

04 Infiltration of isolated targets, such as those in industrial environments

05 Difficult for victims to identify attacks as trusted processes are misused

06 May provide attacker with elevated privileges during installation

Attackers typically use software update supply chain attacks to infiltrate well-protected organizations where traditional infection vectors are unsuccessful. It is especially common for targeted attack groups to search for the weakest link in the chain.

By spreading malware through an already established distribution channel, attackers can compromise a large volume of computers in a short period of time, especially if the compromised software has an automated update mechanism. All this, without the need for an exploit that can be used for network propagation.

“Attackers typically use software update supply chain attacks to infiltrate well-protected organizations where traditional infection vectors are unsuccessful.”

Depending on the software package chosen, supply chain attacks may allow for semi-targeted infections. For example, attackers may target a specific sector by leveraging software that is primarily used in that sector. Trojanized software updates may also allow attackers to penetrate air-gapped networks, as sysadmins will often copy the software update to the separated network or install it from a USB stick.

The Petya/NotPetya incident in June 2017 was an example of how the supply chain can be abused to rapidly deploy malware to a targeted region.

In the Petya/NotPetya (Ransom.Petya) case, Ukrainian accounting software was misused to distribute the payload. It’s therefore not surprising that more than 96 percent of the companies that downloaded the malicious update were located in Ukraine. This figure only includes organizations that got infected directly by downloading the infected software; it does not count companies that were subsequently infected via the EternalBlue exploit or due to the use of stolen credentials.

Software update supply chain attack methods

While attackers cannot fully control who gets infected in a software update supply chain attack, they can still use the first-phase malware to analyze the target and then only deploy the second-phase payload to victims of interest. This was the case during the CCleaner incident.

Well-orchestrated supply chain attacks are difficult to spot for the average user. The Trojanized update is downloaded from a legitimate, trusted domain that might even have been whitelisted in the victim's organization. In addition, the download is started from a trusted application that has the required permission to perform network connections and execute downloaded binaries. In some cases, even the downloaded binary has a valid digital certificate. This can make these types of attacks particularly difficult to stop.

> "The most straightforward attack path is when an attacker is able to compromise the vendor of a software package directly."

Compromising the software supplier directly

The most straightforward attack path is when an attacker is able to compromise the vendor of a software package directly. This method was leveraged with great effect in the Petya/NotPetya attack campaign in June 2017.

In a direct compromise scenario, the attacker switches the update package with a modified malicious version. The simplest way to achieve this is by compromising the web server where the update packages are hosted—for example, through a vulnerability in the content management tool. The attacker hits the jackpot if they manage to get full access to the development environment. This may be achieved through a successful spear-phishing attack against a developer, or by using any of the other common vectors, such as infected websites or credential theft.

Depending on the access obtained, the attacker may also acquire digital certificates allowing them to code-sign the Trojanized update. This results in the malicious update having a legitimate and trusted digital signature that cannot be distinguished by the user. Of course, attackers with such deep access can also modify any information posted on the download website, such as file size, version number, or hash value of the modified update. These attributes are therefore not a guarantee of a legitimate update.

This is very often the most difficult type of attack to conduct, but also the most difficult for the user to detect. It's therefore highly effective.

Hijacking DNS, domains, IP routing or network traffic

Sometimes, even the supply chain target is attacked indirectly—a supply chain attack against the supply chain, so to speak. In today's interconnected IT world there are many interdependencies between companies that can be misused. For example, attackers can try to attack the domain registrar in order to change the registered name servers for a given domain, or even transfer the whole domain. Another method involves compromising a DNS server in order to change the domain resolution to a different IP address under the attacker's control. Both attacks will result in visitors to the domain being redirected to the attacker's server. We have seen a bank's whole online presence being taken over in this manner. While in that case the main goal seems to have been to redirect visitors to phishing websites, it's a technique that could easily be used to push Trojanized updates.

Sometimes, no hacking is involved at all, if the timing is right. Surprisingly, it is not uncommon for organizations to forget to renew domains they acquired some time ago to use for various purposes, such as limited promotions for example. An attacker could then register one of these lapsed domains and potentially use it to control all data sent back to the domain's visitors. There are hundreds of cases of hijacked subdomains of larger companies that pointed to expired domains.

The Border Gateway Protocol (BGP) manages how packets are routed on the internet and is therefore responsible for defining the path through which a resource, such as an IP address, can be reached. Through BGP routing modification, it is possible to redirect IP addresses belonging to other entities to a new destination. A case of BGP hijacking in December 2017 saw some of the IP addresses belonging to Microsoft and Apple, among others, rerouted through Russia. This allows attackers to intercept requests for updates from these IP addresses, and instead send down a Trojanized update. Of course, it is not always that easy. For example, Windows updates have to be signed by Microsoft to get executed, but as we saw in the past with the Flamer threat, vulnerabilities may exist that allow attackers to bypass this security measure.

If the attacker has control over a targeted network, perhaps because they created a rogue Wi-Fi access point or because they have access to the ISP used by the target, then they can attempt to swap any requested file update using a man-in-the-middle (MitM) attack. In September 2017, some variants of the FinFisher malware appear to have used this attack vector to compromise target computers.

Hijacking third-party hosting services

Not all software vendors host software on their own infrastructure. Some use cloud storage distributed around the globe and others, especially open source projects, are often hosted on service providers such as GitHub. Attackers could potentially make subtle changes to the source code that they could exploit in future campaigns. With many projects, such changes are reviewed and may be discovered. A more common method is to steal the credentials of someone that has the permission to upload new binaries. Therefore, it is not surprising that we see many phishing attacks against developer accounts, which could facilitate future software update supply chain attacks.

Other supply chain attack methods

There are other software supply chain attack methods that do not implant a backdoor in a software update, but instead misuse the connection and relationships between companies. The following are examples of how the supply chain can be abused beyond hijacking updates.

Supply chain attacks

2015

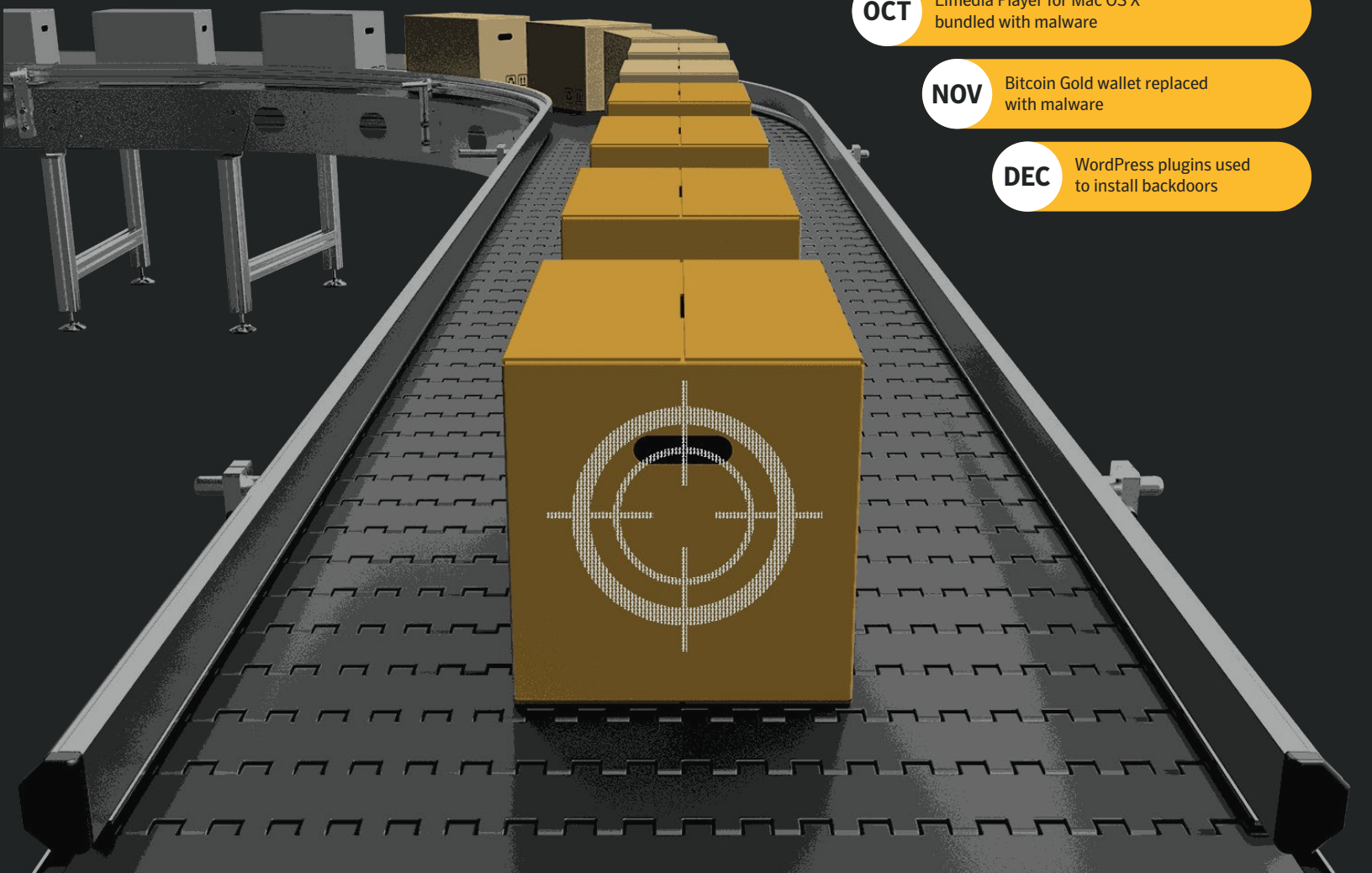
- **APR** EvLog update compromised with malware
- **MAY** Japanese word processor tool used to install malware
- **JUN** XcodeGhost: Malware found in Apple dev environment
- **DEC** Backdoor found in Juniper Networks firewall

2016

- **SEP** S. Korean security software used to install malware
- **OCT** Attackers hijack Brazilian Bank's entire DNS
- **NOV** Ask Network Toolbar used to install malware
- **DEC** Ask Partner Network updater used to install malware

2017

- **FEB**
  - Trojanized version of Yeecall Pro for Android used as a RAT
  - Kingslayer campaign hijacks sysadmin software updates
- **MAR** Adobe Reader installer bundled with malware
- **MAY**
  - HandBrake video tool used to install malware
  - Operation WilySupply compromises editing tool updates
- **JUN** M.E.Doc updater used to distribute Petya/NotPetya
- **JUL**
  - ePrica pharmacy software installs backdoor Trojan
- **AUG**
  - CCleaner tool injected with malware
  - Backdoor found in NetSarang server mgmt. software
- **SEP**
  - Modified Python modules found on official repository
  - "ExpensiveWall" malware found in Android SDK
- **OCT** Elmedia Player for Mac OS X bundled with malware
- **NOV** Bitcoin Gold wallet replaced with malware
- **DEC** WordPress plugins used to install backdoors



Account misuse

These attacks misuse the access permission of service providers or suppliers. Although they are often referred to as supply chain attacks, they are not quite the same thing. One of the most discussed cases is a reported attack against Target™ in 2013 that led to a large data breach. The attackers were allegedly able to misuse stolen credentials from a HVAC systems supplier to gain initial access to the victim's network. There have been numerous similar incidents where attackers stole VPN and SSH credentials of service employees that had remote access to computers of interest in the final target organizations. There have even been cases where a password reset email provider has been compromised in order to take over accounts. Controlling the reset service allowed the attacker to set new passwords for any given account without requiring access to the actual email account.

> "No need to compromise the software vendor if you own the software."

Watering hole attacks

Software update supply chain attacks differ from classic watering hole attacks, where an attacker compromises a website of interest to the victim group and implants an exploit that will compromise the targets' computers. These watering hole attacks, which are often observed during targeted attacks, attempt to exploit a vulnerability rather than hijack the trusted update process.

Process attacks

A similar attack avenue also exists for disruption attacks and hardware attacks. Attackers can block suppliers from providing the right parts for just-in-time manufacturing lines, or worse, switch the order of some parts, resulting in the production process coming to a halt. There is also the chance that newly bought hardware is infected or manipulated by the attacker, before it arrives at the target destination. We have also observed attackers stealing customer data from a supplier as that was easier to compromise than the main target. For large enterprises it is often hard to control what happens with confidential data once it has left their own network.

Deliberate malicious applications

There have even been some attacks where rather than compromising the software vendor, the attacker simply bought the rights to the software package and then sent a malicious update to the existing user base. No need to compromise the software vendor if you own the software. In other cases it was a malicious insider or a former employee that still had access and that deliberately changed the software update.

A similar scenario is when links are sent in spam emails that point to fake websites with cloned software packages. Similarly, opportunistic attacks can occur if a user is searching for a tool, for example for video editing, but lands on a fake site providing an infected version. Such cases can be detected by well-known protection measures and software should only be downloaded from trusted sources. Similar due diligence applies when buying hardware equipment.

Collateral infections

Of course, there are also collateral damage infections that can happen at a software vendor. For example, it is possible for the computer of a developer to get infected with file-infecting malware that then infects the public software package before distribution. Another example is USB drives that get infected at the manufacturing site, because one of the machines was infected with a worm that copied itself to all attached USB drives. Such infections can also spread quickly, but are usually neither intentional nor targeted.

Case studies

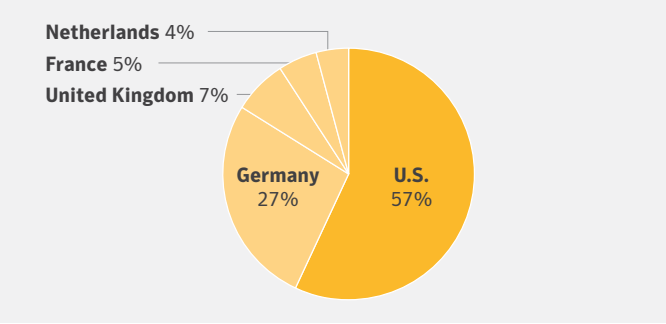
CCleaner

In August 2017, a popular system clean-up tool called CCleaner was targeted by supply chain attackers. An unknown group of attackers gained access to the company's development environment, which allowed them to create and distribute a malicious version of the tool through the update process. The success of the campaign was aided by the fact that the attackers were able to sign the Trojanized update with the manufacturer's official digital signature.

Between August 15 and September 12, the compromised version, CCleaner v5.33.6162, and the cloud version were distributed to customers. According to figures from Avast, the modified version was downloaded 2.27 million times. Our telemetry shows that most downloads happened in the U.S., followed by Germany.

CCleaner infections by country

The U.S. was hit most, followed by Germany



This first-phase backdoor, detected as Trojan.Sibakdi, is a typical reconnaissance tool and gathers system information such as the name of the computer, installed software packages, list of running processes, and other information, and sends it back to the attacker with an HTTPS POST request.

The malware uses classic tricks to avoid automated detection. For example, the malware pings a local multicast IP address using a timeout set to 601 seconds. Consequently, the malware sleeps for 10 minutes in an attempt to evade automated sandbox detection.

The information gathered from the first payload was then used to narrow down the list of interesting targets to a handful of technology companies. These compromised computers then received a second payload (Trojan.Famberp). Analysis of the log files on the command and control (C&C) server revealed that around 20 selected victims around the globe did receive a second payload delivered through the dropped backdoor.

The attacker misused DLLs from older versions of software and modified them with malicious code. On 32-bit systems the VirtCDRDrv32.dll, which was part of an older version of WinZip, and on 64-bit systems the EFACli64.dll, which was part of an older Symantec Endpoint Protection package, was used as a template. These DLLs were modified, Trojanized, and no longer digitally signed. Malicious code was simply injected into them.

Petya/NotPetya and M.E.doc

In June 2017, the Petya/NotPetya wiper Trojan spread rapidly and compromised thousands of computers. Analysis showed that M.E.Doc, a tax and accounting software package, was used for the initial insertion of Petya/NotPetya into corporate networks. After gaining an initial foothold, Petya/NotPetya then used a variety of methods to spread across corporate networks.

Onsite analysis indicates that the attackers used stolen credentials to modify the configuration of the M.E.doc web server. This allowed the attackers to redirect any request for the update server to a malicious server under their control. The analysis further showed that the update process had already been compromised in April 2017. Until June, at least three malicious updates were pushed down. The backdoor then periodically checked back with the same update server for any additional commands to be executed and sent back some system information inside an HTTP cookie, including local proxy settings with passwords, in order to evade detection.

This backdoor mechanism was then finally used to download and execute the Petya/NotPetya wiper malware.

Conclusion

Given the increase in supply chain attacks in 2017 and the success of a number of campaigns, it's likely that attackers will continue to leverage this attack method. Already in 2018 we have seen some attacks where this method was used: one targeting forum software, and another aimed at Mac users.

While supply chain attacks are difficult to protect against, there are some steps that can be taken including testing new updates, even seemingly legitimate ones, in small test environments or sandboxes first, in order to detect any suspicious behavior. However, bear in mind that attackers can apply well-known tricks to delay malicious behavior in order to not attract attention during this kind of analysis.

Behavior monitoring of all activity on a system can also help identify any unwanted patterns and allow you to block a suspicious application before any damage can be done. This is possible as the behavior of a malicious update will be different to that of the expected clean software.

Finally, the producers of software packages should ensure that they are able to detect unwanted changes in the software update process and on their website.

Mobile Threat Landscape

Threats in the mobile space continue to grow year on year. In 2017, there was a 54 percent increase in the number of new malware variants alone and it's not just the volume that's increasing. Attackers have developed new methods of infection and tricks to remain on compromised devices as long as possible. They've also come up with a variety of means of generating revenue from devices, from ransomware to cryptocurrency mining.

But while the attacks continue to evolve and mature, the same can't always be said of the device user. Many users continue to make life easy for attackers by continuing to use older operating systems. In particular, on Android, only 20 percent of devices are running the newest major version.

Mobile threats continue to rise

The number of new mobile malware variants grew by 54 percent in 2017, compared to 2016.

Mobile malware variants by year

The number of new mobile malware variants grew by 54 percent in 2017, compared to 2016.

	2016	2017	Change
Mobile Malware Variants	17,214	26,579	54%

Number of malware blocked per day on mobile devices

An average of 23,795 malicious mobile applications blocked on mobile devices each day.

	2016	2017
Total Mobile Malware Blocked	7,193,927	8,684,993
Average per Day	19,709	23,795

Average number of ransomware blocked per month.

An average of 3,510 mobile ransomware were blocked per month in 2017.

	2017
Mobile Ransomware Blocked	42,118
Average per Month	3,510

Number of new mobile malware families identified

The number of new mobile malware families grew by 12 percent in 2017, compared to 2016.

	2016	2017	Change
New Mobile Malware Families	361	405	12%

> **"Many users continue to make life easy for attackers by continuing to use older operating systems. In particular, on Android, only 20 percent of devices are running the newest major version."**

Top 10 app categories for malware

In 2017, 27 percent of malicious apps were found in the Lifestyle category, followed by Music & Audio with 20 percent.

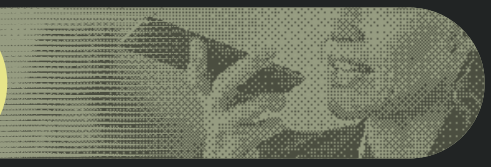
Category	% Malware
Lifestyle	27%
Music & Audio	20%
Books & Reference	10%
Entertainment	6%
Tools	6%
House & Home	5%
Education	4%
Art & Design	4%
Photography	3%
Casual Games	2%

2017 Notable events in the mobile threat landscape

JAN

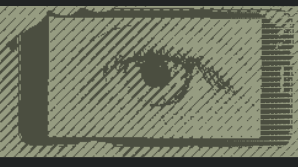
- Ransomware adopted banking malware's social engineering tactics to circumvent new permission model introduced in Android Marshmallow (6.0).

FEB



- Ransomware using voice recognition, forcing victims to speak the unlock code instead of typing the key.
- Ransomware using social messenger apps with integrated payment SDKs to facilitate barcoded payments.

MAR

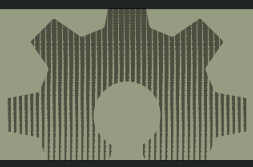


- MobileSpy family of threats using reactive tools to hook into events, such as SMS text received, to trigger other actions and commands remotely.
- Wide availability of mobile malware toolkits help to automate the creation of new variants of malicious mobile apps in large volumes.

APR

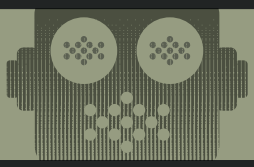
- Rise of WAP billing Trojans spawn the next generation in Premium Service Subscription scams by silently visiting WAP service subscription pages and automating the sign-up process, subscribing the victim to the paid-for services without consent.

JUL



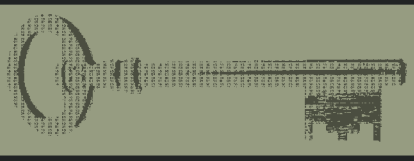
- Rootnik family begins using open-source VirtualApp engine to create a virtual space within the Android device that is used to install and run APKs without any contstraints.

AUG



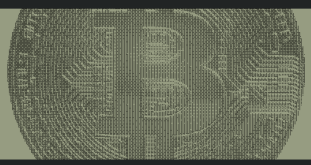
- Devices infected with Adclicker were turned into distributed denial of service (DDoS) bots that were commanded to repeatedly visit specific target URLs.

SEP



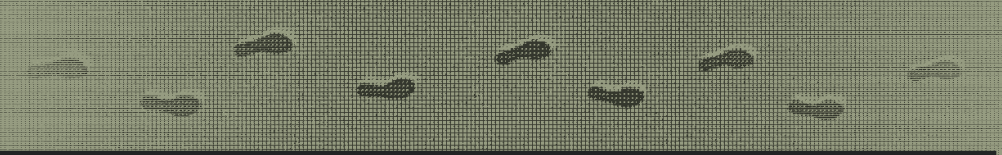
- Banking malware variants found to be using StackTraceElements API to derive decryption keys at runtime.

OCT



- Rise of fake mobile apps with embedded JavaScript-based cryptocurrency miners.

NOV



- Android.Fakeapp variant stealing credentials of online aggregate service providers, covering up the trail by launching legitimate apps using mobile deep-linking URIs.

Notably, with 99.9 percent, the clear majority of discovered mobile malware was hosted on third-party app stores.

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. Like malware, grayware has also continued to increase in volume in 2017.

Number of mobile grayware variants identified

	2016	2017	Change
New Mobile Grayware Variants	3,055	3,655	20%

Number of mobile grayware families identified

The number of new mobile grayware families grew by 5 percent from 188 in 2016 to 198 in 2017.

	2016	2017	Change
New Mobile Grayware Families	188	198	5%

Percentage of apps that leak sensitive information

While not considered malicious, grayware nevertheless presents potential privacy issues for users. We found that 63 percent of the grayware apps in 2017 leaked the phone number and 37 percent revealed the phone's physical location.

Type of Information Leaked	Percentage
Phone Number	63%
Location Info	37%
Installed App Info	35%

Cryptocurrencies and other new vectors for monetization

The goal of the vast majority of mobile malware is revenue generation. Traditional means of revenue generation have included premium rate SMS attacks, where attackers co-opt victims' mobile devices to send paid text messages and collect the revenue, or adware, where attackers collect attribution for ad impressions and app downloads, either by forcing the user to view web pages or download content. Infostealers allowed attackers to harvest personal data from mobile phones which could then be traded in underground markets.

In recent years, attackers have turned to ransomware on mobile phones where profits are made by locking devices or by encrypting personal data and extorting a ransom payment from the victim to allow them to regain access. In 2017, a number of mobile apps emerged that allowed attackers to generate their own ransomware in an automated fashion, lowering the barrier to entry for cyber criminals. Another innovation was the use of voice-enabled ransomware. Rather than having the user key in an unlock code, this ransomware contains a speech recognition module which allows the victim to say the unlock code. The payment methods have also evolved, with some ransomware variants accepting payment from barcodes from social media apps.

> **"Notably, with 99.9 percent, the clear majority of discovered mobile malware was hosted on third-party app stores."**

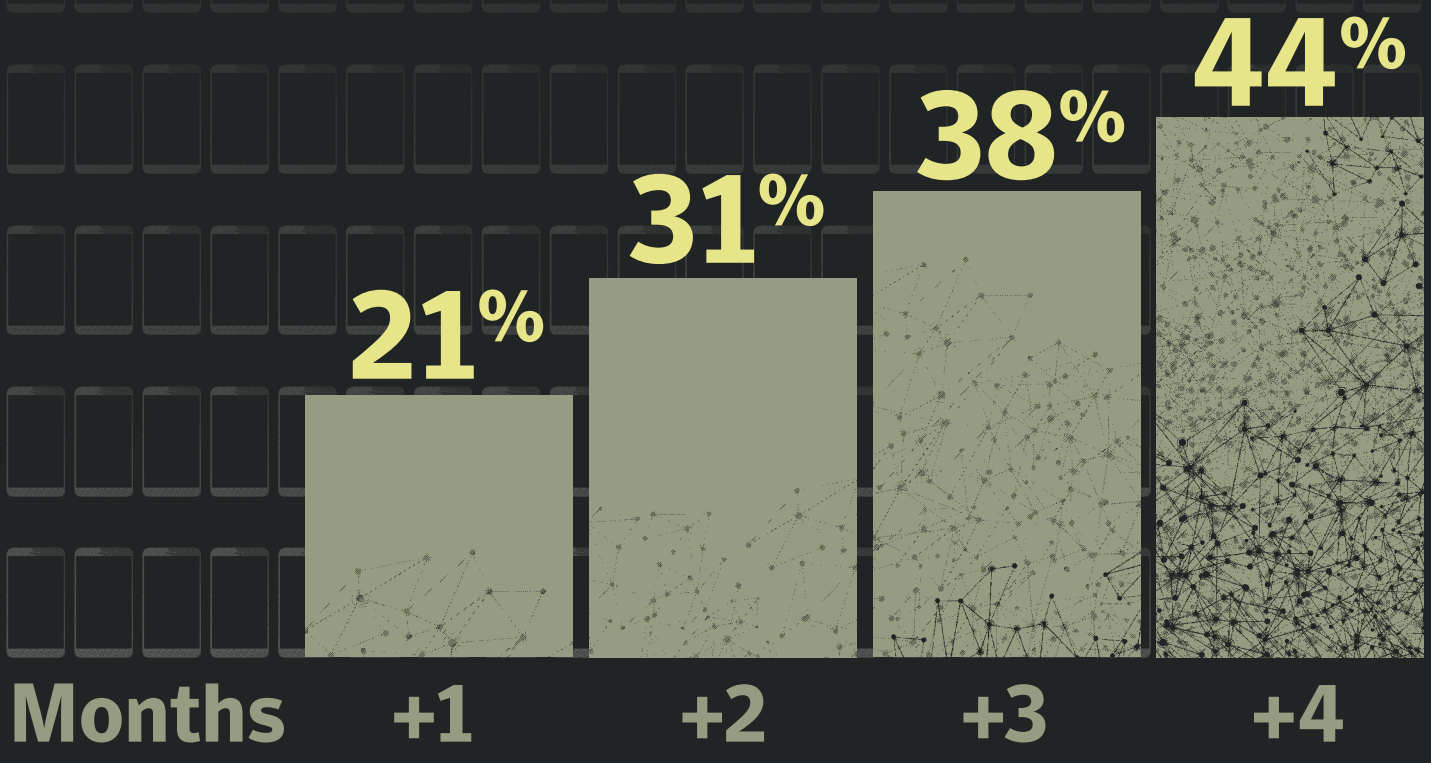
Mobile devices also weren't immune from the cryptocurrency coin-mining explosion of 2017. While mining Bitcoin isn't profitable on mobile devices, Monero provides a lighter alternative means of coin mining and we identified a number of fake apps in 2017 packaged with functionality for mining Monero.

User behavior and security profiling

Keeping up-to-date

Analysis of Android mobile devices that are on the latest major version, e.g. 7.x or 8.x for 2017, reveals that 20 percent of devices are on the latest major release, and only 2.3 percent are on the latest minor release. Although only 1 in 5 Android mobile devices are kept up-to-date with the latest major release, this is an increase compared with only 15 percent (1 in 7) for 2016. It is a difficult gap to close however, since many older devices will never be powerful enough to run the latest version and currently 80 percent of Android devices are lagging the latest major release.

Cumulative exposure to network threats



Percentage of Android devices running newest version of OS

	2016	2017
Android Devices on Newest Major Version	15.0%	20.0%
Android Devices on Newest Minor Version	11.8%	2.3%

Percentage of iOS devices running newest version of OS

	2016	2017
iOS Devices on Newest Major Version	79.4%	77.3%
iOS Devices on Newest Minor Version	24.0%	26.5%

The story is a little different for iOS™, as we see approximately 77.3 percent of iOS devices using the latest version, and 26.5 percent using the latest minor version. iOS updates are rolled out much more quickly as they are not dependent on a carrier making the updates available for their devices on their network, often with bespoke changes required before doing so. Interestingly, although this figure is higher on iOS than for Android, the number is in decline since 2016, when 79.4 percent of iOS devices were patched to the latest major version, and 24 percent were at the latest minor release.

Cumulative exposure to network threats over time

We analyzed the scale of the potential threat from devices being exposed to insecure networks over a longer period. As can be seen, the effect becomes cumulative over a longer period. For example, typically 21.2 percent of new devices were exposed to network threats in their first month of use. This figure rises to 43.7 percent after four months. In this model, a network threat may be something such as a malicious man-in-the-middle (MitM) style attack.

Such an attack may be used to intercept and decrypt SSL traffic, or to manipulate content in transit to or from the device. Sometimes this can be down to a misconfigured router that can expose certain data. Regardless of intent, individuals and organizations would be wise to avoid any network that does not accurately and securely perform the connection services originally requested by the user and the device.

Jailbroken and rooted devices

The act of "rooting" an Android device, or "jailbreaking" an iOS device, is a means by which the user can gain greater control over the device and bypass certain security controls enabling access to more personalization options and functions which are otherwise blocked by the operating system. This activity has decreased in recent years as newer versions of operating systems now provide increased functionality. However, because of the power it can offer an attacker, jailbreaking or rooting a compromised device is still a goal, and monitoring for such activity can often reveal it as an indicator of compromise.

Ratio of devices that are jailbroken or rooted, by year and by operating system

	2016		2017	
	iOS	Android	iOS	Android
Enterprise	1 in 10,839	1 in 254	1 in 14,351	1 in 1,589
Individual or Consumer	1 in 694	1 in 92	1 in 1,658	1 in 281

Additionally, in 2017, 1 in 107 devices were identified as high-risk, including rooted or jailbroken devices and devices considered to have high certainty of malware apps installed, compared with 1 in 65 for 2016.

Percentage of devices that have passcode protection enabled by operating system

In 2017, approximately 1 in 20 enterprise devices were not protected with a passcode, and this number rises to 1 in 10 for consumers.

	2016	2017
Enterprise	84.1%	95.2%
Individual or Consumer	70.0%	90.5%

> **"Regardless of intent, individuals and organizations would be wise to avoid any network that does not accurately and securely perform the connection services originally requested by the user and the device."**

Percentage of devices that have encryption enabled by operating system

In relation to encryption, we can see the proportion of Android devices not being encrypted is falling, but it is still at a considerably high level.

Android Only	2016	2017
Enterprise	57.8%	43.1%
Individual or Consumer	57.7%	45.5%

iOS provides encryption by default, as has Android in recent years. However, it is still a potential risk for older versions of operating systems, if they are still in use and remain unencrypted. Encryption is key to ensuring data on a device is not exposed if it becomes lost or stolen.

Recommendations

Since user behavior is such a huge factor in mobile security, user education is one of the most important things an organization can do to minimize the threat posed by mobile devices. Users should know to only install apps from the primary app stores, and don't click on untrusted links or approve device permissions and accesses without good reason.

Facts and Figures

Section

03

03 Facts and Figures

FACTS AND FIGURES CONTENTS

Symantec

Malware

Key findings

- Coin mining was the biggest growth area in cyber crime in 2017, with antivirus detections up 8,500 percent.
- Ransomware infections are up 40 percent in 2017, driven primarily by WannaCry (Ransom.Wannacry).
- The number of ransomware variants is up 46 percent, despite fewer new families emerging, indicating intensifying activity by established groups.
- Emotet (Trojan.Emotet), a new player in banking threats, remerged in late 2017; detections increased 2,000 percent in the final quarter.
- Script and macro downloaders increased by 92 percent, as they continue to be aggressively propagated in order to install ransomware and banking threats.
- Overall malware variants are up by 88 percent; however, these numbers are inflated by a single threat type.

New malware variants

The growth in malware variants was largely owing to the Kotver Trojan (Trojan.Kotver), which accounted for 78 percent of the new variants in 2017.

Year	New Variants	Percent Change
2015	355,419,881	-
2016	357,019,453	0.5
2017	669,947,865	87.7

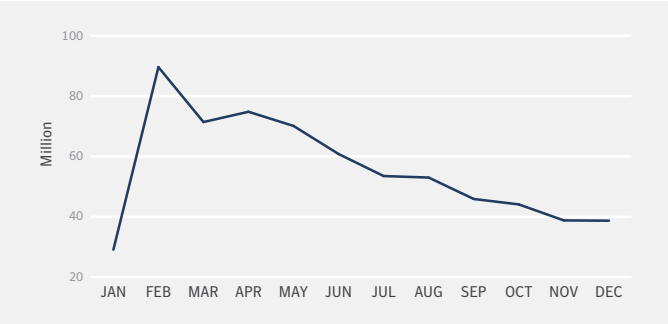
New malware variants on Mac

The number of Mac malware variants was dominated by JS.Webcoinminer variants, which accounted for 60 percent of this number in 2017.

Year	New Variants	Percent Change
2016	772,018	-
2017	1,390,261	80.1

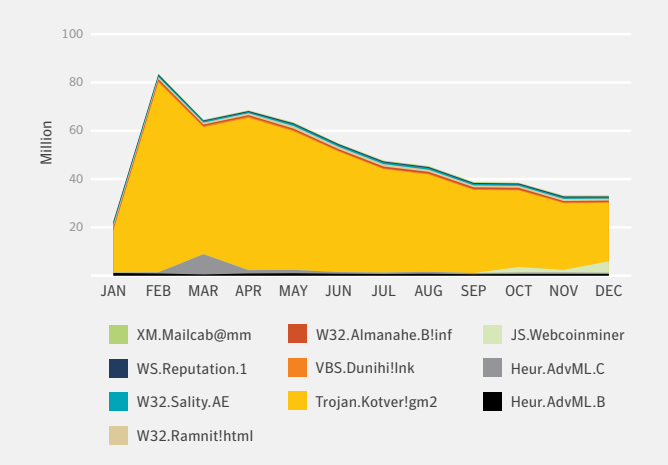
New malware variants per month

Early 2017 was dominated by a large number of new variants related to the Kotver Trojan.



Top new malware variants per month

Variants of the Kotver Trojan accounted for the majority of new malware variants in 2017.



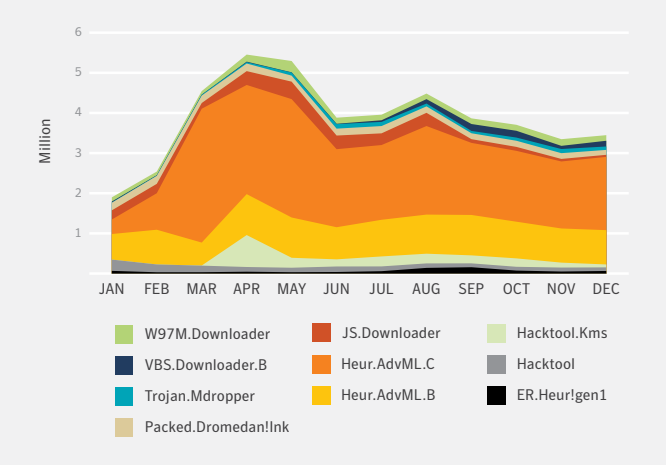
Top 10 malware detections

Advanced machine learning heuristics and JavaScript downloaders accounted for the top three in this list, and are often used to drop other forms of malicious code, malware, and ransomware.

Rank	Malware	Attacks Blocked	Percent
1	Heur.AdvML.C	23,335,068	27.5
2	Heur.AdvML.B	10,408,782	12.3
3	JS.Downloader	2,645,965	3.1
4	Hacktool.Kms	2,318,729	2.7
5	Packed.Dromedan!Ink	1,995,429	2.4
6	W97M.Downloader	1,763,143	2.1
7	Hacktool	1,615,555	1.9
8	ER.Heur!gen1	799,479	0.9
9	VBS.Downloader.B	772,080	0.9
10	Trojan.Mdropper	763,328	0.9

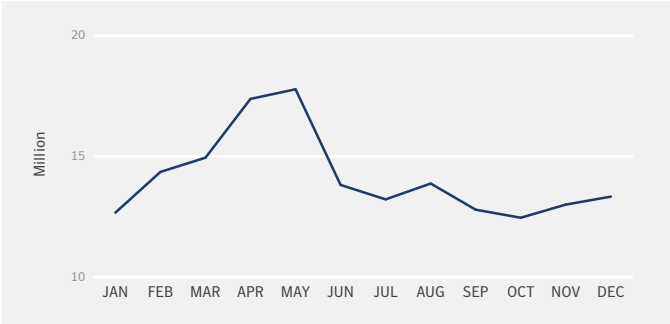
Top 10 malware detections by month

The top 10 list was dominated by advanced machine learning heuristics used to detect new forms of generic malware.



Malware detections by month

The increase in April and May was related to a growth in generic malware and downloaders.



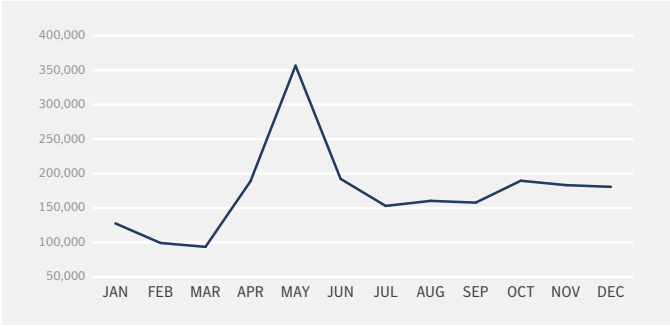
Downloader detections

The number of downloaders increased by 91.7 percent in 2017.

Year	Attacks Blocked
2015	399,386
2016	1,602,335
2017	3,072,126

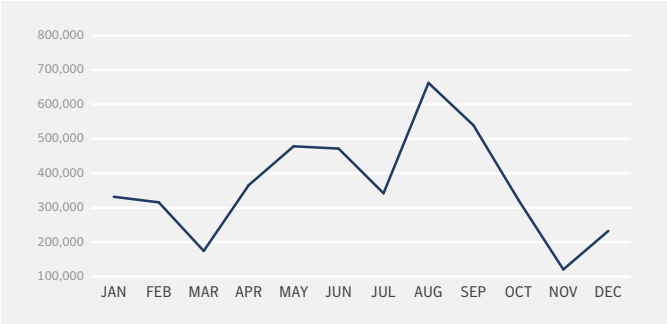
Office® macro downloader detections per month

W97M.Downloader - A sharp increase was observed in April and May, stabilizing at higher levels than previously seen.



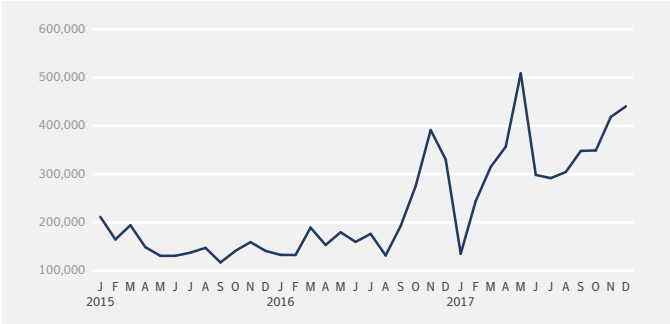
JavaScript downloader detections per month

JS.Downloader - A notable spike was observed in August. The frequency of JS.Downloader detections is higher than for W97M.Downloader.



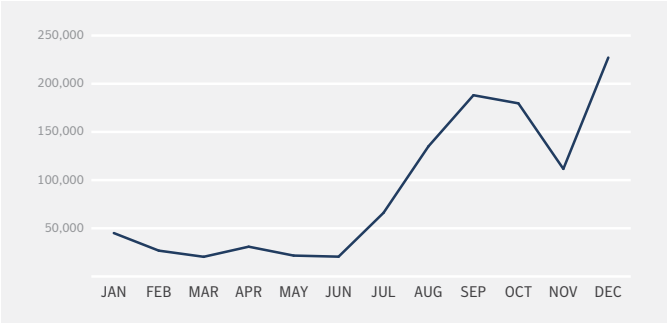
Mac malware distribution per month

There was a notable increase in attacks against Macs that began at the end of 2016 and accelerated during 2017.



VBScript downloader detections per month

VBS.Downloader - A significant increase began in September and continued through October and for the duration of the year, peaking in December.



New malware variants on Mac endpoints by month

Attacks on Macs were dominated by the growth in JS.Webcoinminer variants during the final quarter of the year.

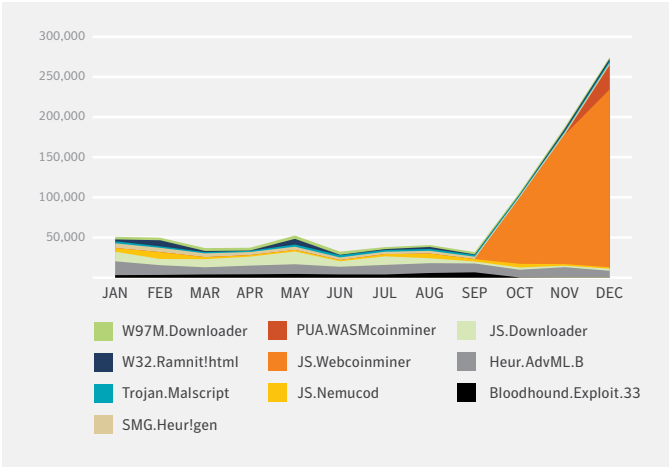
Malware distribution by operating system

Mac malware attacks rose by 64 percent in 2017, driven by JS.Webcoinminer. Windows malware attacks grew by 2.5 percent.

Year	Mac	Windows
2015	1,824,685	300,966,231
2016	2,445,414	161,707,491
2017	4,011,252	165,638,707

Top new malware variants on Mac endpoints by month

JS.Webcoinminer variants on Mac surged in September and continued to grow.



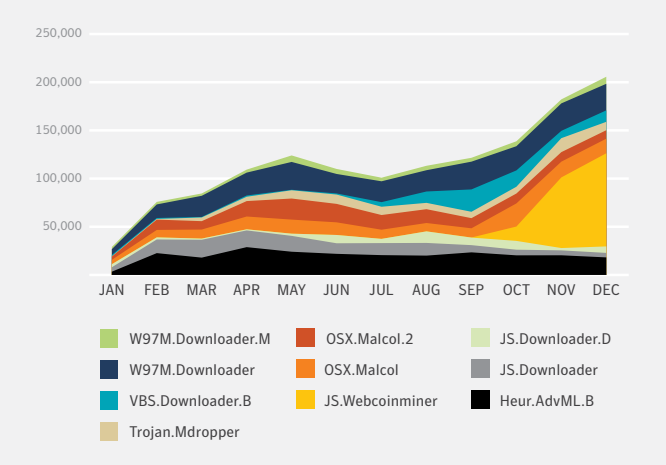
Top malware blocked on Mac endpoints

Although JS.Webcoinminer activity was only significant during the final quarter of the year, it was still enough to secure third place in the top 10 ranking for the entire year.

Rank	Malware	Attacks Blocked	Percent
1	W97M.Downloader	268,497	6.7
2	Heur.AdvML.B	241,832	6.0
3	JS.Webcoinminer	184,944	4.6
4	OSX.Malcol.2	148,872	3.7
5	OSX.Malcol	145,886	3.6
6	JS.Downloader	130,854	3.3
7	Trojan.Mdropper	79,438	2.0
8	VBS.Downloader.B	82,216	2.0
9	JS.Downloader.D	61,149	1.5
10	W97M.Downloader.M	51,432	1.3

Top malware blocked on Mac endpoints by month

W97M.Downloader and JS.Webcoinminer activity overshadowed the Mac threat landscape in 2017.



Percentage of malware that uses SSL

Malware that used SSL to encrypt its communications increased from 2.8 percent to 4.5 percent in 2017.

Year	Percent
2016	2.8
2017	4.5

Ransomware

New ransomware variants

The number of new ransomware variants increased by 45 percent in 2017.

Year	New Variants
2016	241,021
2017	350,496

Ransomware detections by year

The number of ransomware attacks blocked in 2017 grew by 41 percent.

Year	Attacks Blocked
2016	482,833
2017	678,497

Enterprise vs. consumer ransomware detections

59 percent of ransomware attacks were against businesses in 2017. This was largely because the WannaCry (Ransom.Wannacry) attacks affected mainly enterprises than consumers.

Year	Consumer	Enterprise
2017	281,325	396,764

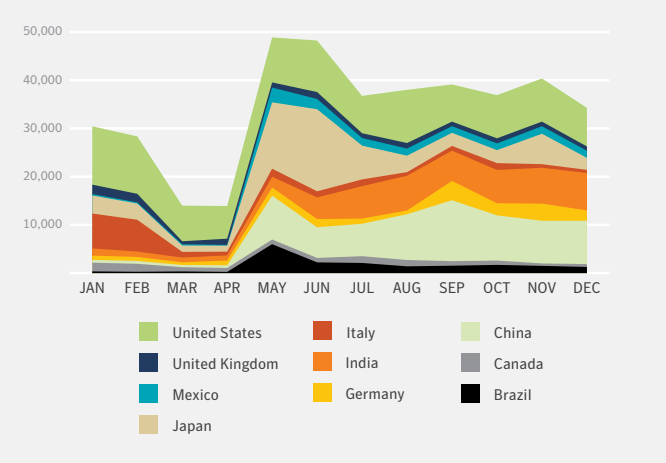
Ransomware detections by country

Typically, ransomware has been more dominant in countries with higher numbers of internet-connected populations.

Rank	Country	Percent
1	United States	18.2
2	China	12.2
3	Japan	10.7
4	India	8.9
5	Italy	4.1
6	Germany	3.4
7	Brazil	3.1
8	Mexico	2.5
9	United Kingdom	2.3
10	Canada	2.1

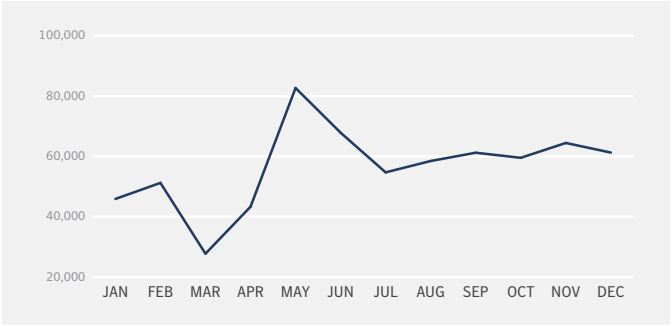
Ransomware detections by country per month

Ransomware attacks against Japan spiked between May and June, while attacks in China grew during the same period, but remained higher for the remainder of the year.



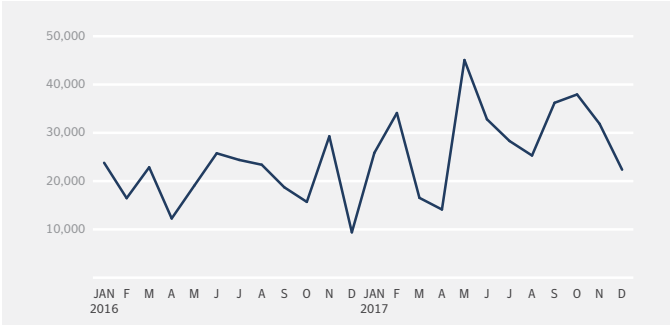
Ransomware detections by month

Following the spike in May, ransomware attacks continued to increase at a steady rate during the remainder of the year.



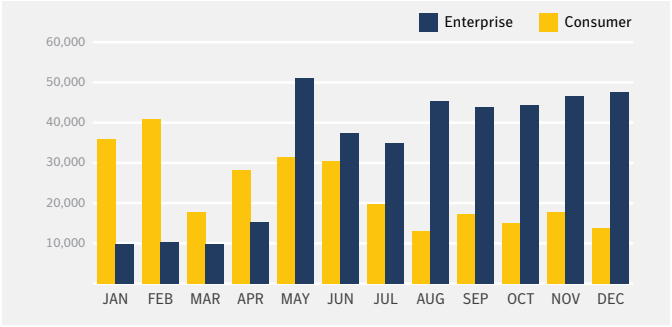
New ransomware variants by month

The general trend for the number of ransomware variants discovered each month indicates an overall increase as the year progressed.



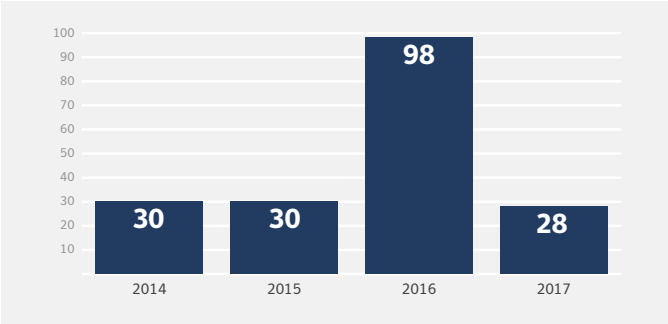
Enterprise vs. consumer ransomware detections by month

Although ransomware attacks against consumers dominated in the early part of 2017, attacks against enterprises dominated following the WannaCry outbreak in May.



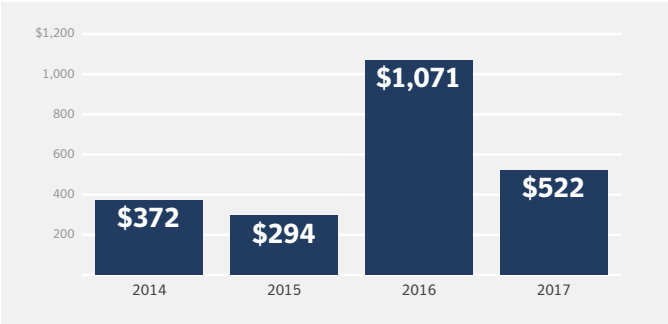
New ransomware families

The number of new ransomware families returned to previous levels, following a very active year in 2016.



Average ransom demand

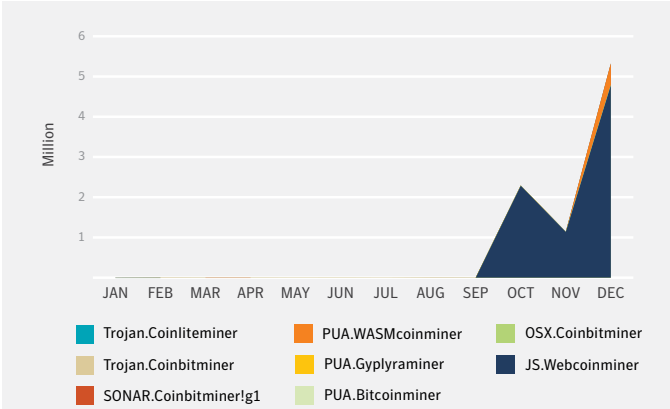
The average value of a ransomware demand fell to $522 in 2017, following a peak of $1,071 in 2016. In part this may be affected by the volatility in cryptocurrency values towards the end of 2017. Ransomware demands were often advertised in U.S. dollars, with payment requested in the equivalent value in Bitcoin or Monero, for example.



Coinminers

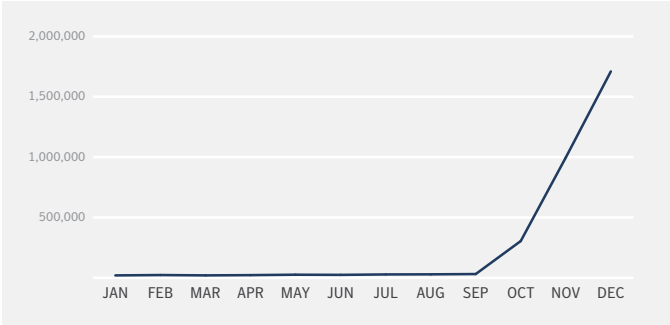
New coinminer variants

JS.Webcoinminer produced the greatest number of coin-mining malware variants in this list, towards the end of the year.



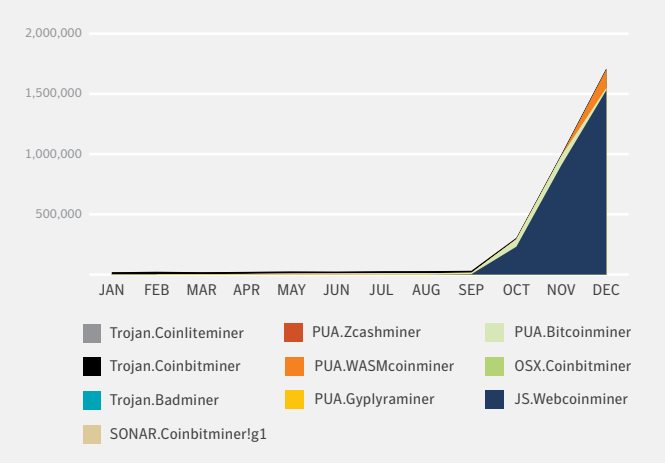
Coinminer detections by month

Before the surge that began in September, cryptocurrency mining malware was not particularly notable, with detections numbering in the tens of thousands, quickly rising to hundreds of thousands, and peaking at 1.6 million in December.



Top coin miner detections by month

JS.Webcoinminer accounted for the greatest number of coin-mining malware detections in 2017, particularly after September.



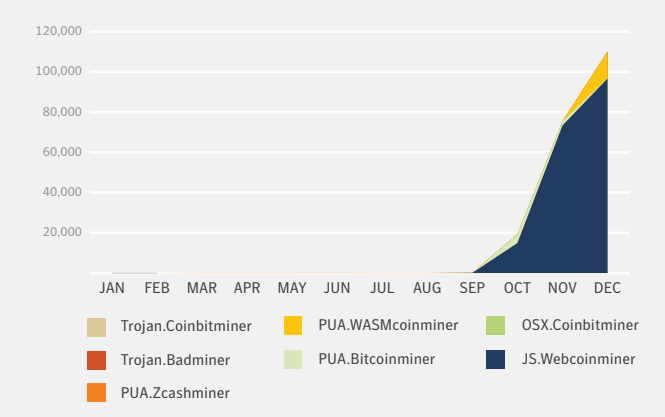
Top coinminer detections

JS.Webcoinminer was the most frequently blocked coin-mining malware in 2017.

Rank	Coin mining Malware	Percent
1	JS.Webcoinminer	82.6
2	PUA.Bitcoinminer	6.9
3	Trojan.Coinbitminer	5.7
4	PUA.WASMcoinminer	4.6
5	PUA.Gyplyraminer	0.2

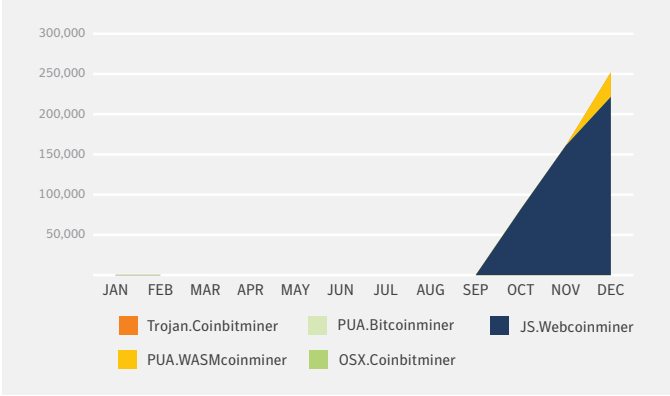
Top coinminer detections on Mac by month

JS.Webcoinminer also dominated on the Mac platform, after September.



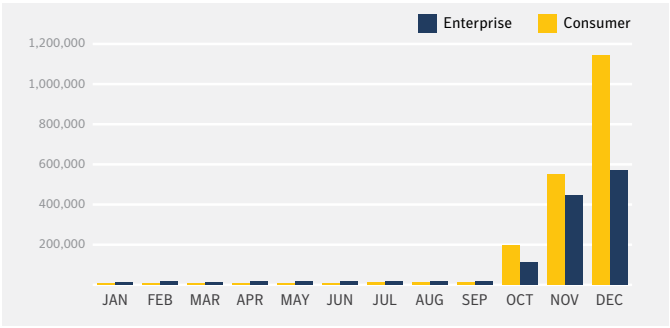
Coinminer variants on Mac by month

The rapid growth in the number of variants of JS.Webcoinminer was also observed on Mac, most notably towards the end of the year.



Enterprise vs. consumer coinminer detections by month

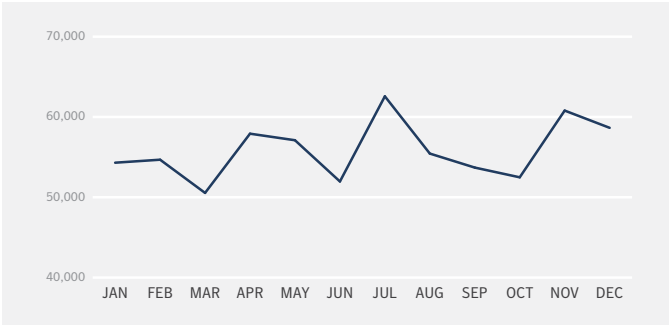
Coin-mining malware attacks on Mac were more frequently identified on consumer hardware, especially related to JS.Webcoinminer.



Financial Trojans

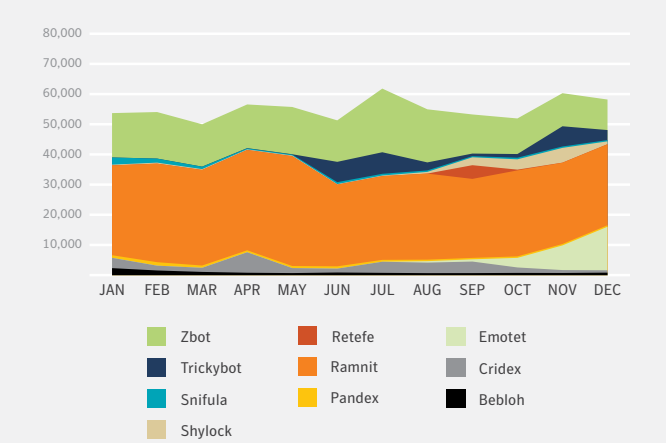
Financial Trojans by month

A new Emotet variant emerged in November, making use of certain Windows API features seeking to evade detection and anti-sandboxing techniques.



Top financial Trojans by month

Ramnit (W32.Ramnit) and Zbot (Trojan.Zbot) were the most prevalent financial malware in 2017.



Top financial Trojans

Although it only appeared in November, Emotet was quick to secure fifth place in the top malware list for all of 2017.

Rank	Threat Names	Percent
1	Ramnit	53.0
2	Zbot	25.8
3	Cridex	4.6
4	Trickybot	4.3
5	Emotet	4.0
6	Shylock	2.1
7	Bebloh	1.7
8	Snifula	1.3
9	Pandex	1.2
10	Retefe	0.7

Web threats

Key findings

- 1 in 13 URLs analyzed at the gateway were found to be malicious. In 2016 this number was 1 in 20.
- There was a 62 percent increase in overall botnet activity identified at the gateway.
- As the year progressed, web attacks blocked at the endpoint trended upwards driven by coin-mining activity.
- There was a 448 percent increase in exploit kit activity blocked at the endpoint.

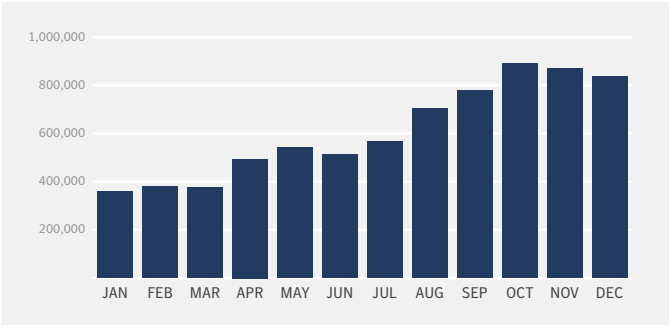
Web attacks blocked

This shows the total number of web attacks blocked in 2017, and corresponding average number per day.

Year	Total Web Attacks Blocked	Average Web Attacks Blocked per Day
2017	223,066,372	611,141

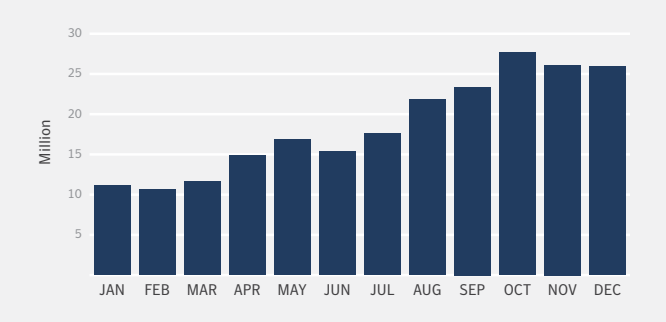
Web attacks blocked per day

As the year ended, the number of web attacks blocked each day was more than double the number at the start of the year.



Web attacks blocked per month

The peak level of malicious activity took place in October, when more than 27.7 million web attacks were blocked.



Classification of most frequently exploited websites

The "Malware" classification identifies websites that are known for harboring malware, and accounted for 15.9 percent of web-based malware blocked. The "Dynamic" classification relates to domains that use dynamic DNS services, and accounted for 13.2 percent of malicious websites in 2017.

Rank	Domain Categories	2016 (%)	2017 (%)	Percentage Point Difference
1	Malware	1.4	15.9	14.5
2	Dynamic	< 0.1	13.2	13.2
3	Technology	20.7	11.5	-9.2
4	Business	11.3	7.5	-3.7
5	Hosting	7.2	6.9	-0.3
6	Gambling	2.8	6.7	3.9
7	Health	5.7	4.8	-0.9
8	Shopping	4.2	3.8	-0.3
9	Educational	4.1	3.1	-1.0
10	Travel	3.6	2.8	-0.8

URLs analyzed per day

Symantec WebPulse URL classification and reputation analysis service scanned 1.07 billion URLs per day in 2017.

Year	Total	Percent Change
2016	1,020,000,000	-
2017	1,076,000,000	5.5

* Out of a total 6 billion web analysis requests. The number used for analysis is sourced from the WebPulse URL Reputation Service and does not include requests from Symantec Web Security Service and other sources

Percentage of malicious traffic in web traffic

In 2017 the number of malicious URLs grew by 2.8 percent, with 7.8 percent (1 in 13) of all URLs identified as malicious.

Year	Total	Percent of Total	Ratio	Percentage Point Change
2016	50,675,406	5	1 in 20	-
2017	83,351,181	7.8	1 in 13	2.8

Percentage of botnet traffic in web traffic

The number of URLs resulting from bot-related traffic, such as that used for command and control, grew by 62.3 percent, accounting for 14.7 percent (1 in 88) of all malicious URLs in 2017.

Year	Per Day	Percent of All URLs/Day	Ratio	Percent of Malicious URLs	Ratio	Percent Change	Percentage Point Change
2016	7,567,271	0.7	1 in 135	14.9	1 in 7	-	-
2017	12,281,279	1.1	1 in 88	14.7	1 in 7	62.3	-0.2

Percentage of phishing URL traffic in web traffic

The number of URLs related to phishing activity rose by 182.6 percent, which accounted for 5.8 percent (1 in 224) of all malicious URLs in 2017.

Year	Per Day	Percent of All URLs/Day	Ratio	Percent of Malicious URLs	Ratio	Percent Change	Percentage Point Change
2016	1,699,214	0.2	1 in 600	3.4	1 in 30	-	-
2017	4,802,409	0.5	1 in 224	5.8	1 in 17	182.6	2.4

Email threats

Key findings

- The disappearance of Necurs (Backdoor.Necurs) in the first quarter of the year led to a decline in email malware from 1 in 131 in 2016 to 1 in 412 in 2017.
- The Necurs botnet sent out almost 15 million malicious emails in 2017, 82.5 percent of which were sent in the second half of the year.
- 7,710 organizations are hit by a BEC scam every month.

Email malware

Overall email malware rate

In 2017, the rate for email-borne malware fell to 1 in 412 (0.2 percent), from 1 in 131 (0.8 percent) in 2016.

Year	1 in
2015	220
2016	131
2017	412

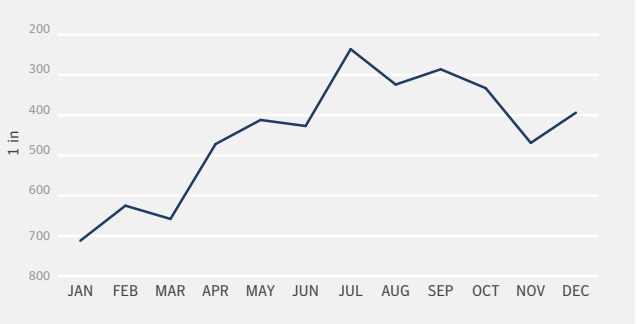
URL malware rate

In 2017, the proportion of email-borne malware that comprised a malicious URL, rather than an attachment, grew by 10.7 percentage points to 12.3 percent.

Year	Percent of Email Malware
2016	1.6
2017	12.3

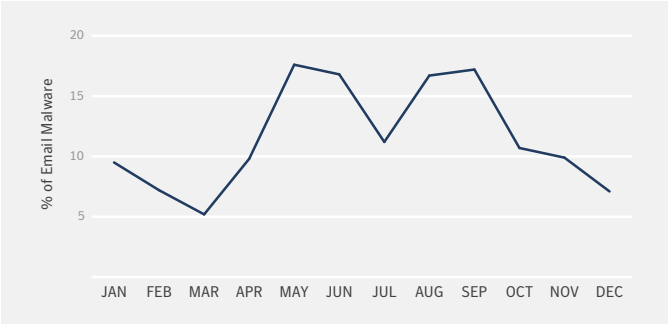
Monthly email malware rate

This chart shows the gradual decline in email-borne malware through 2017.



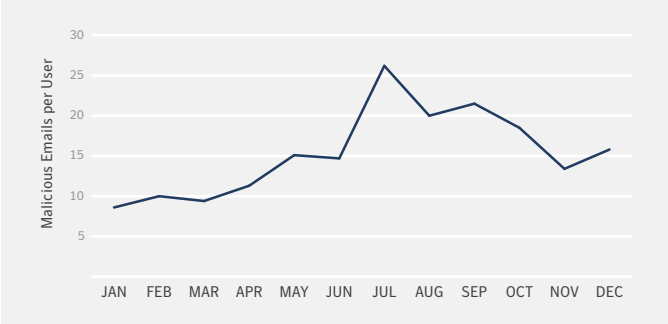
Monthly URL malware rate

This chart shows the proportion of email-borne malware using a malicious link rather than an attachment.



Malicious emails per user

Although the overall rate fell slightly in 2017, the number of malicious emails sent to the average user each month increased from 9 in January, to 16 by the end of the year.



Email malware rate by industry

The highest rate of email-borne malware was for the organizations in the Public Administration sector. Many organizations potentially suffered much higher rates than the global annual average.

Rank	Industry	1 in
1	Public Administration	120
2	Agriculture, Forestry, & Fishing	211
3	Mining	273
4	Wholesale Trade	364
5	Manufacturing	384
6	Services	400
7	Nonclassifiable Establishments	437
8	Construction	472
9	Transportation & Public Utilities	486
10	Retail Trade	489
11	Finance, Insurance, & Real Estate	612

URL malware rate by industry

Malware destined for organizations in the Construction industry had the highest rate of malware in links vs. attachments, with 27.2 percent of malware comprising a link instead of an attachment.

Rank	Industry	Percent of Email Malware
1	Construction	27.2
2	Agriculture, Forestry, & Fishing	21.5
3	Retail Trade	19.4
4	Finance, Insurance, & Real Estate	16.6
5	Mining	13.3
6	Public Administration	11.6
7	Transportation & Public Utilities	11.5
8	Services	10.6
9	Manufacturing	9.5
10	Nonclassifiable Establishments	9.5
11	Wholesale Trade	9.1

Email malware per user by industry

During 2017, approximately 53 email viruses were sent to the average user in the Public Administration sector.

Rank	Industry	Email Malware per User
1	Public Administration	53.1
2	Wholesale Trade	34.4
3	Mining	30.0
4	Agriculture, Forestry, & Fishing	26.5
5	Manufacturing	25.5
6	Nonclassifiable Establishments	21.8
7	Retail Trade	19.9
8	Construction	18.1
9	Services	12.1
10	Finance, Insurance, & Real Estate	9.1
11	Transportation & Public Utilities	8.7

Email malware rate by company size

Some of the lowest email malware rates were for organizations in the large enterprise category (2,500+ employees).

Company Size	1 in
1-250	376
251-500	306
501-1000	425
1001-1500	244
1501-2500	355
2501+	512

URL malware rate by company size

Large enterprises and small businesses were affected equally by the proportion of email-borne malware that comprised a malicious link.

Company Size	Percent of Email Malware
1-250	12.8
251-500	8.1
501-1000	15.0
1001-1500	11.4
1501-2500	10.9
2501+	12.9

Email malware per user by company size

The average user both in large enterprises and small businesses was targeted by a similar number of viruses during 2017 (10 and 9 respectively).

Company Size	1 in
1-250	9
251-500	6
501-1000	5
1001-1500	3
1501-2500	4
2501+	10

Email malware rate by country

Austria was the country that had the highest email malware rate in 2017, with 1 in 102 emails received in the country blocked as malicious.

Rank	Country	1 in
1	Austria	102
2	Hungary	108
3	Indonesia	140
4	Oman	156
5	Saudi Arabia	175
6	Netherlands Antilles	184
7	Malaysia	216
8	Kuwait	217
9	South Africa	233
10	Taiwan	234

URL malware rate by country

Ireland, Australia, and New Zealand had the highest proportion of malicious email-borne links in 2017.

Rank	Country	Percent of Email Malware
1	Ireland	32.4
2	Australia	26.7
3	New Zealand	26.3
4	Brazil	23.1
5	Norway	18.0
6	United Kingdom	16.8
7	Mexico	16.4
8	Sweden	16.1
9	Finland	11.5
10	Canada	11.4

Top malicious email themes

This table shows the most common themes used in email malware subject lines.

Rank	Subject Topic	Percent
1	Bill	15.9
2	Email Delivery Failure	15.3
3	Legal/Law Enforcement	13.2
4	Scanned Document	11.5
5	Package Delivery	3.9

Keywords used in malware spam campaigns

The most frequently used words in malicious emails included, "delivery," "mail," "message," and "sender."

Rank	Words	Percent
1	delivery	12.1
2	mail	11.8
3	message	11.3
4	sender	11.2
5	your	11.2
6	returning	7.6
7	failed:	7.6
8	invoice	6.9
9	images	6.6
10	scanned	6.5

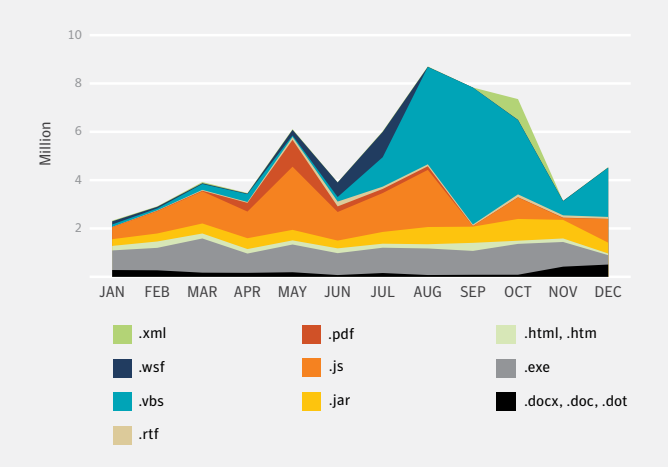
Payloads used in malware spam campaigns

Visual Basic Script and JavaScript were among the most common type of malicious attachments in 2017.

Rank	File Type	Percent
1	.vbs	27.7
2	.js	21.4
3	.exe	18.6
4	.jar	9.8
5	.docx, .doc, .dot	3.9
6	.html, htm	3.5
7	.wsf	3.4
8	.pdf	3.3
9	.xml	1.7
10	.rtf	1.5

Payloads used in malware spam campaigns by month

This chart shows the growth of different malware attachment types over time, and the increased use of VBS-based attacks in the latter half of 2017.



Payload types used in malware spam campaigns

Malicious scripts accounted for 61.4 percent of malicious attachments. Executables are typically easier to block and are often disabled by default for many email applications.

Rank	File Type	Percent
1	Scripts	61.4
2	Executables	29.6
3	Other	7.6

Phishing

Average number of companies targeted by BEC scams

Business email compromise (BEC) scams could have potentially affected 7,700 organizations in 2017 were these attacks not blocked.

Year	Average
2017	7,710

BEC emails received per organization

Each of these targeted organizations was attacked an average of 4.9 times during 2017.

Year	Average
2017	4.9

Top subject lines in BEC scam emails

Analysis of the BEC emails shows that the most frequently occurring words included, "payment," "urgent," "request," and "attention."

Rank	Subject	Percent
1	payment	13.8
2	urgent	9.1
3	request	6.7
4	attention	6.1
5	important	4.8
6	confidential	2.0
7	immediate response	1.9
8	transfer	1.8
9	important update	1.7
10	attn	1.5

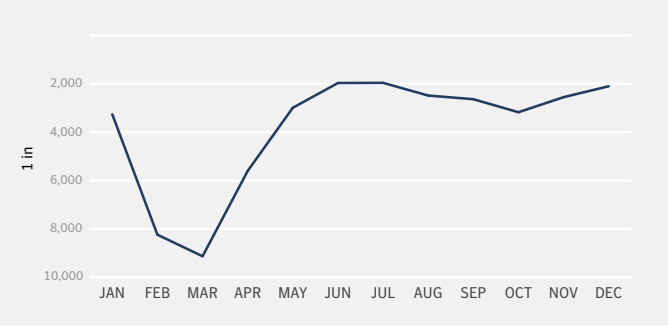
Overall phishing rate

The phishing rate declined from 1 in 2,596 in 2016 to 1 in 2,995 in 2017.

Year	1 in
2015	1,846
2016	2,596
2017	2,995

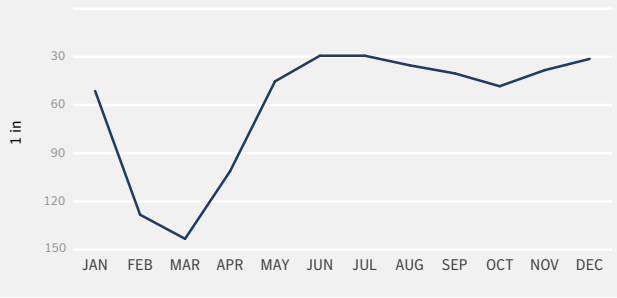
Monthly phishing rate

The phishing rate increased during 2017, recovering from an early dip at the start of the year.



Email users sent phishing attempts per month

As the year progressed, the average number of users per phishing attack increased, following a dip around March. In January, 1 in 53 users were sent a phishing attack, compared with 1 in 33 by the end of the year.



Phishing rate by industry

Many types of industry had phishing rates that were much higher than the global average, with the highest rate for organizations in the Agriculture, Forestry, & Fishing sector.

Rank	Industry	1 in
1	Agriculture, Forestry, & Fishing	2,212
2	Nonclassifiable Establishments	2,240
3	Public Administration	2,418
4	Mining	2,453
5	Services	2,737
6	Finance, Insurance, & Real Estate	3,013
7	Manufacturing	3,998
8	Retail Trade	4,353
9	Wholesale Trade	4,406
10	Construction	4,667
11	Transportation & Public Utilities	5,567

Email users sent phishing attempts by industry

Nonclassifiable Establishments, Mining, and Wholesale Trade had the highest ratio of users per phishing attack in 2017.

Rank	Industry	1 in
1	Nonclassifiable Establishments	24
2	Mining	30
3	Wholesale Trade	35
4	Public Administration	38
5	Agriculture, Forestry, & Fishing	39
6	Manufacturing	41
7	Retail Trade	45
8	Finance, Insurance, & Real Estate	54
9	Construction	55
10	Services	57
11	Transportation & Public Utilities	131

Phishing rate by company size

For organizations that could be classified by size, the phishing rate appeared to be much lower than the global average.

Company Size	1 in
1-250	3,111
251-500	3,539
501-1000	3,844
1001-1500	7,173
1501-2500	3,854
2501+	3,019

Email users sent phishing attempts by company size

The ratio of users per phishing attack was highest in 501-1,000, and 1,500-2,500 sized organizations, where 1 in 41 and 1 in 42 email users was targeted, respectively.

Company Size	1 in
1-250	72
251-500	64
501-1000	41
1001-1500	75
1501-2500	42
2501+	58

Phishing rate by country

The phishing rate in South Africa was the highest in world ranking for 2017, where 1 in 785 emails was a phishing attack.

Rank	Country	1 in
1	South Africa	785
2	Netherlands	1,298
3	Malaysia	1,359
4	Hungary	1,569
5	Portugal	1,671
6	Austria	1,675
7	Taiwan	1,906
8	Brazil	2,117
9	Indonesia	2,380
10	Singapore	2,422

Spam

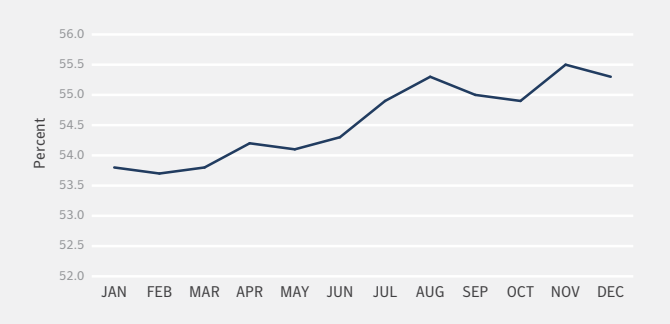
Overall spam rate

The percentage of email determined to be spam increased by 1.2 percentage points in 2017.

Year	Percent
2015	52.7
2016	53.4
2017	54.6

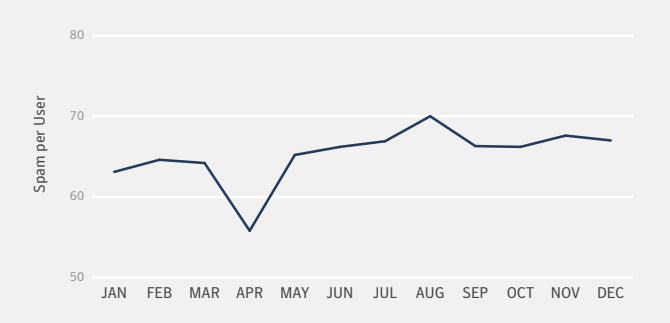
Monthly spam rate

Spam levels were much higher in the latter half of 2017, peaking at 55.5 percent in November.



Amount of spam per user

In 2017, the average number of spam emails per user each month increased from 63 in January to 67 in December.



Spam rate by industry

The Mining industry had the highest spam rate for 2017, with 58.8 percent of emails identified as spam.

Rank	Industry	Percent
1	Mining	58.8
2	Construction	56.9
3	Manufacturing	55.9
4	Finance, Insurance, & Real Estate	55.2
5	Nonclassifiable Establishments	54.6
6	Agriculture, Forestry, & Fishing	54.5
7	Transportation & Public Utilities	53.9
8	Services	53.7
9	Public Administration	53.4
10	Retail Trade	53.3
11	Wholesale Trade	53.1

Amount of spam per user by industry

In contrast, recipients in the Wholesale Trade sector had the highest average number of spam emails per user per month. Similarly, for Manufacturing and Retail, the number of employees that have an active email account in these sectors is comparatively low, with higher numbers of blue-collar workers.

Rank	Industry	Spam per User
1	Wholesale Trade	125.8
2	Manufacturing	103.5
3	Nonclassifiable Establishments	98.2
4	Retail Trade	98.1
5	Construction	91.8
6	Mining	91.0
7	Public Administration	64.2
8	Finance, Insurance, & Real Estate	58.5
9	Agriculture, Forestry, & Fishing	57.9
10	Services	49.1
11	Transportation & Public Utilities	43.3

Spam rate by company size

Many larger organizations had higher spam rates in 2017.

Company Size	Percent
1-250	54.9
251-500	52.8
501-1000	53.9
1001-1500	56.4
1501-2500	52.9
2501+	54.7

Amount of spam per user by company size

Email recipients within small businesses potentially received fewer spam emails than their counterparts working at larger organizations.

Company Size	Spam per User
1-250	45.2
251-500	55.4
501-1000	95.2
1001-1500	101.8
1501-2500	92.2
2501+	54.0

Spam rate by country

This list shows the countries with the highest spam rates in 2017.

Rank	Country	Percent
1	Saudi Arabia	69.9
2	China	68.6
3	Brazil	64.7
4	Sri Lanka	64.6
5	Hungary	60.4
6	Kuwait	59.8
7	Oman	58.9
8	South Africa	57.1
9	Norway	56.9
10	United Arab Emirates	56.3

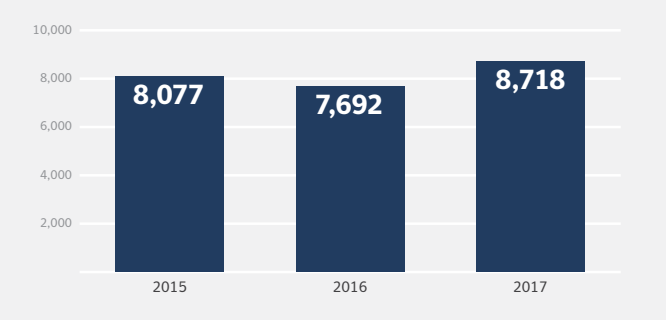
Vulnerabilities

Key findings

- While major vulnerabilities such as EternalBlue, Meltdown, and Spectre made headlines, vulnerability disclosures across the board were up in 2017. This doesn't necessarily translate to a rise in exploits, and may be indicative of the popularity of bug bounty programs.

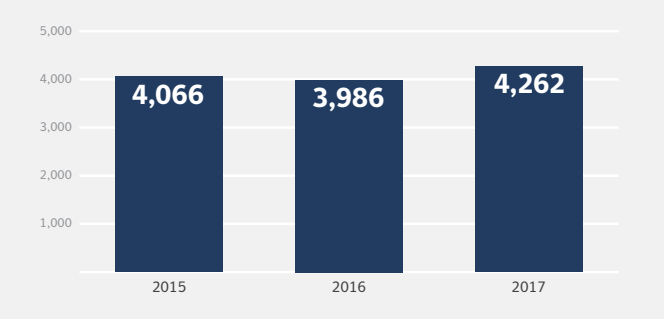
Total number of vulnerabilities

This shows a 13 percent increase in the number of reported vulnerabilities recorded in 2017.



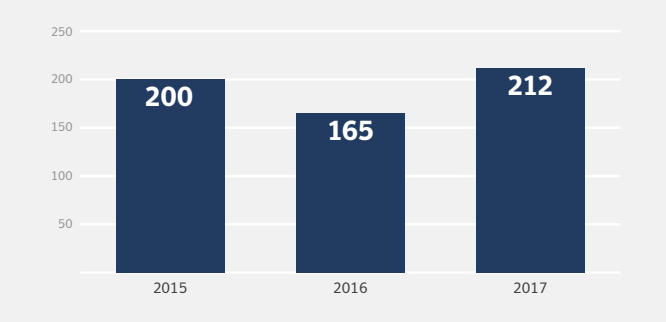
Zero-day vulnerabilities

There was an increase of 7 percent in the number of zero-day vulnerabilities recorded in 2017.



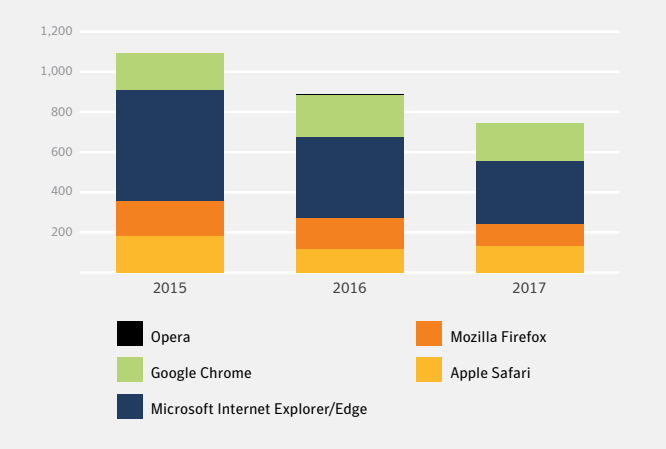
Vulnerabilities disclosed in industrial control systems

There was an increase of 29 percent in the number of recorded vulnerabilities affecting industrial control system (ICS) technology in 2017.



Browser vulnerabilities

The number of recorded vulnerabilities affecting Safari rose by 14 percent in 2017. The number related to Firefox fell by 29 percent. Edge and Internet Explorer vulnerabilities were down by 23 percent, and those affecting Chrome were down by 9 percent.



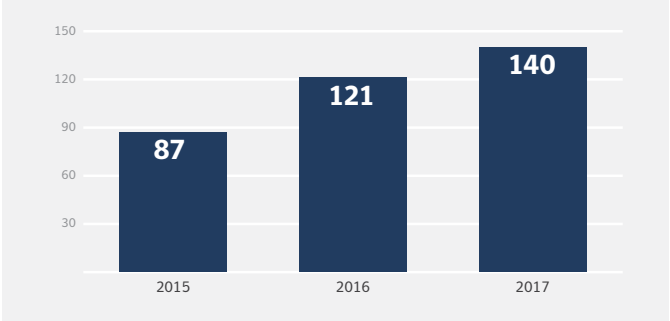
Targeted attacks

Key findings

- 90 percent of targeted attack groups are motivated by intelligence gathering.
- Over the past three years, the most active groups compromised an average of 42 organizations.
- 71 percent of groups use spear-phishing emails as the primary infection vector.
- The U.S. was the most targeted country in the past three years, accounting for 27 percent of all targeted attack activity.
- The number of organizations affected by targeted attacks increase by 10 percent in 2017.

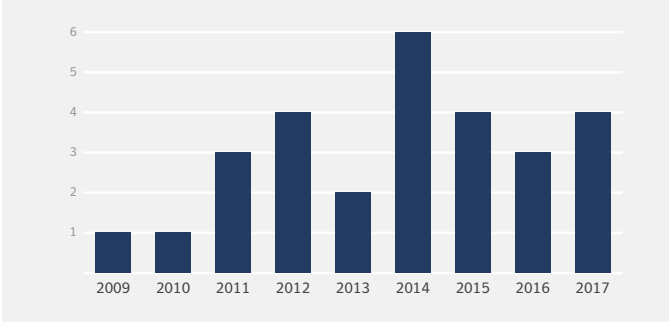
Number of new targeted attack groups discovered by year

140 distinct groups were known to be conducting targeted attacks in 2017, a 15.7 percent increase since 2016.



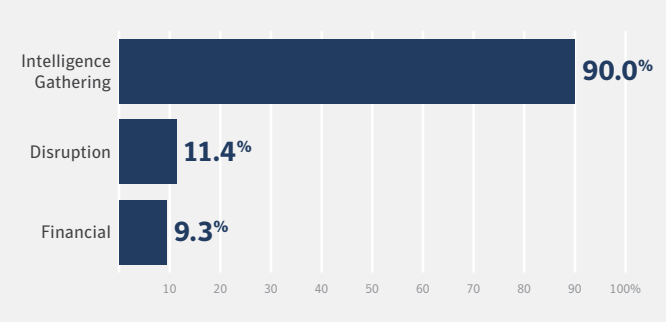
Targeted attack groups exposed by Symantec

Since 2009, a total of 28 different targeted attack groups have been identified by Symantec.



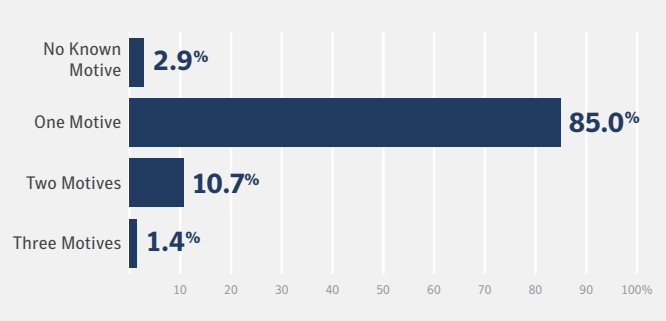
Motives of targeted attack groups

The vast majority of attacks (90 percent) appeared to have been designed to gather intelligence from targeted organizations.



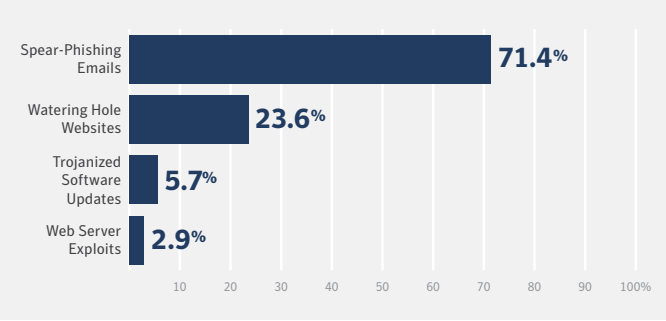
Number of motives per group

Further analysis revealed that for 85 percent of attacks, only one motive was involved.



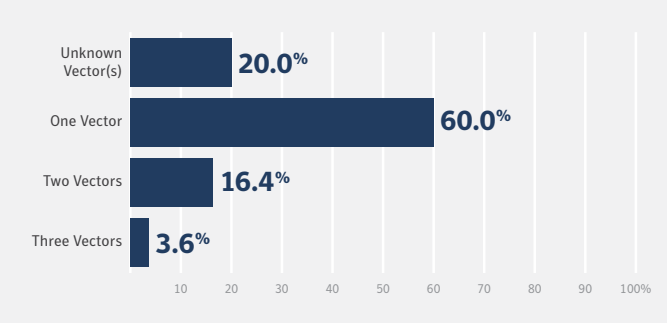
Infection vectors

In 2017, 71.4 percent of targeted attacks involved the use of spear-phishing emails.



Infection vectors used per group

Only one infection vector was used in 60 percent of targeted attacks in 2017.



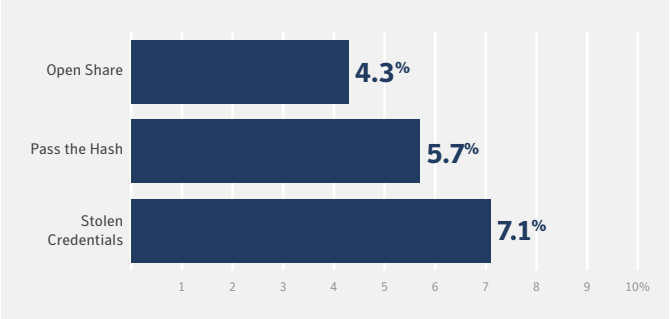
Countries most affected by targeted attack groups

This table shows the geographic locations that were the most frequent focus of targeted attacks in 2017.

Rank	Country	Total
1	U.S.	303
2	India	133
3	Japan	87
4	Taiwan	59
5	Ukraine	49
6	South Korea	45
7	Brunei	34
8	Russia	32
9	Vietnam	29
10	Pakistan	22

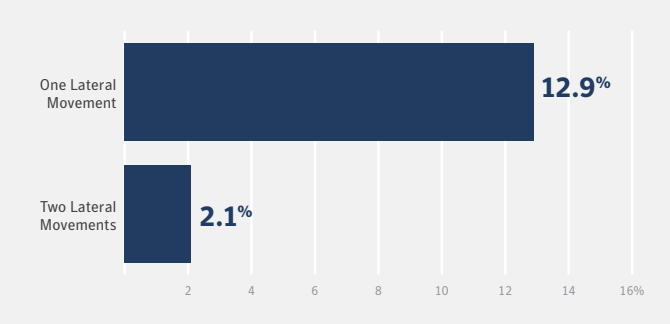
Lateral movement techniques

In 2017, 7.1 percent of targeted attacks used stolen credentials as a lateral movement technique. Lateral movement concerns the techniques used to traverse a compromised network, searching for other exploits and valuable data that can be utilized and stolen.



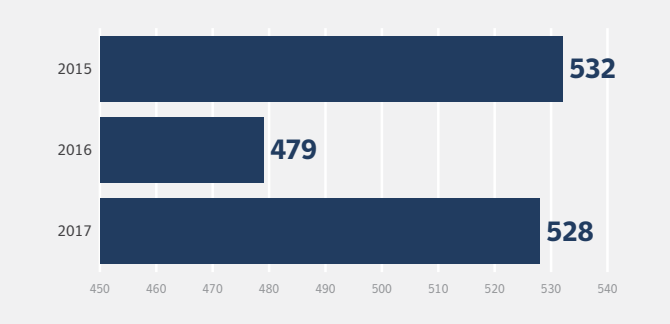
Lateral movement techniques per group

Referring to lateral movement, 12.9 percent of attacks used only one lateral movement technique in 2017.



Number of organizations affected by targeted attacks per year

The number of organizations targeted increased by 11.1 percent in 2017, to 532.



Other attack group numbers

The lowest number of tools used by attack groups was one, in contrast to the highest number, 18, used by the Lazarus group.

Average number of tools used by groups	3.6
Average number of organizations targeted per group (over three years)	42
Average number of individuals targeted per group (over three years)	65
Percentage of groups known to use zero-day vulnerabilities	27%
Percentage of groups known to use destructive malware	6%

Mobile threats

Key findings

- The number of new discovered mobile malware variants grew by 54 percent from 2016 to 2017
- In 2017 an average of 24,000 malicious mobile applications where blocked on devices per day.
- 27 percent of malicious apps were found in the Lifestyle category, followed by Music & Audio with 20 percent.
- 63 percent of the grayware apps in 2017 leaked the phone number and 37 percent reveal the phones physical location.
- 77.3 percent of the iOS devices had the newest major version installed in 2017, a drop of 2.1 percent from 2016. With Android only 20 percent of the devices were running the newest major version, but there was an increase of 5 percent from 2016.

New mobile malware variants

In 2017, the number of new mobile malware variants increased by 54 percent.

Year	New Variants
2016	17,214
2017	26,579

Number of blocked apps

Approximately 23,795 malicious app were blocked each day in 2017.

Year	Blocked Malware per Day
2017	23,795

Most common app categories for malware

27.3 percent of malicious apps were categorized as Lifestyle apps, followed by 19.7 percent categorized as Music & Audio apps.

Rank	Category	Percent Malware
1	Lifestyle	27.3
2	Music & Audio	19.7
3	Books & Reference	9.9
4	Entertainment	6.2
5	Tools	5.5
6	House & Home	4.5
7	Education	3.9
8	Art & Design	3.7
9	Photography	2.7
10	Casual Games	2.2

Sensitive information leaked by apps

63 percent of mobile apps leaked users' phone numbers, and 37 percent revealed devices' physical locations.

Type of Information Leaked	Percent
Phone Number	63.0
Location Info	37.0
Installed App Info	35.0

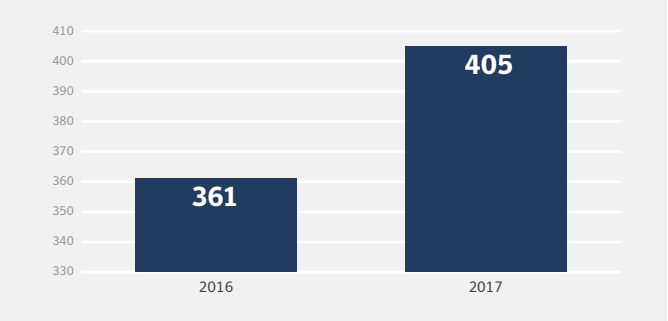
Keeping devices up to date

77.3 percent of iOS devices had the newest major version installed in 2017, a drop of 2.1 percent. With Android, only 20 percent of the devices were running the newest major version, with an increase of 5 percent from 2016.

Year	iOS Devices Using Newest Major Version (Percent)	Android Devices Using Newest Major Version (Percent)
2016	79.4	15.0
2017	77.3	20.0

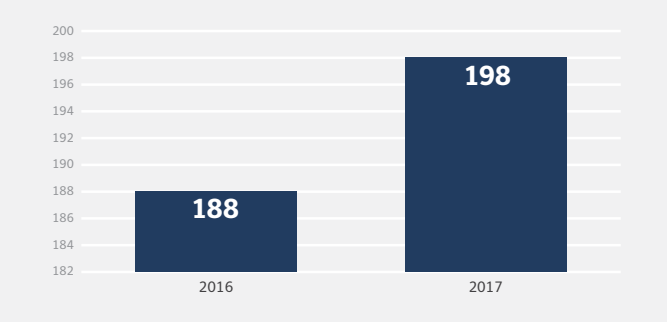
New mobile malware families

The number of new mobile malware families increased by 12.2 percent between 2016 and 2017.



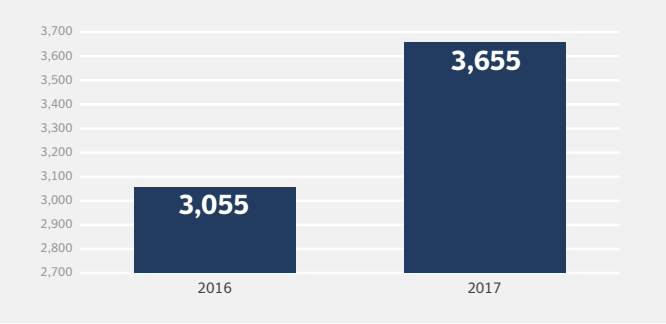
New mobile grayware families

The number of new mobile grayware families grew by 5.3 percent in 2017.



New mobile grayware variants

The number of new mobile grayware variants increased by 19.6 percent 2017.



Mobile ransomware

The number of ransomware apps blocked each month in 2017.

Year	Average Number of Ransomware Blocked per Month
2017	3,510

Biggest source of mobile malware

The vast majority of mobile malware was found in third-party app stores.

Year	Malware Found in Third-Party App Stores (Percent)
2017	99.9

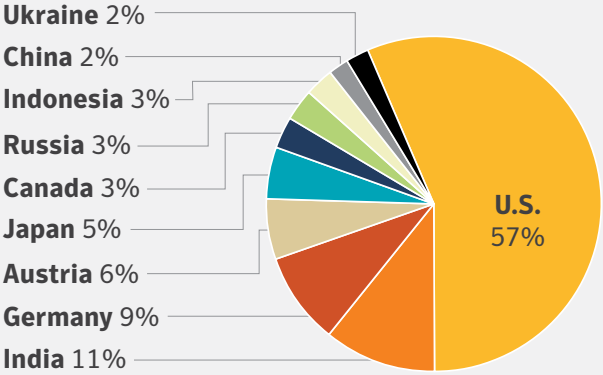
Top Android threats

Top 10 list of most frequently blocked Android malware in 2017.

Rank	Threat Name	Percent
1	Malapp	20.2
2	FakeInst	16.4
3	Premiumtext	11.2
4	MalDownloader	10.0
5	Simplocker	8.8
6	Fakeapp	8.5
7	SmsBlocker	7.1
8	Mobilespy	4.8
9	Smsstealer	2.0
10	Opfake	1.9

Top countries for mobile malware

Top 10 list of countries where mobile malware was most frequently blocked in 2017.



Jailbroken or rooted devices

This shows the proportion of devices that are jailbroken or rooted is gradually diminishing, but remains a key indicator of compromise.

Year	OS	Enterprise	Consumer
2016	iOS	1 in 10,839	1 in 694
	Android	1 in 254	1 in 92
2017	iOS	1 in 14,351	1 in 1,658
	Android	1 in 1,589	1 in 281

Devices protected by passwords

Approximately 5 percent of enterprise devices were not password protected, compared with almost 10 percent of consumer devices.

Year	Enterprise (Percent)	Consumer (Percent)
2016	84.1	70.0
2017	95.2	90.5

Exposure to network threats

This shows the cumulative exposure to network threats over time. In 2017, 1 in 5 devices were exposed to attacks in their first month of use, rising to 3 in 7 after four months.

Devices exposed to network attacks after	1 month	2 months	3 months	4 months
2016	21.6	31.2	38.6	44.3
2017	21.2	30.7	37.7	43.7

Internet of things

Key findings

- There was a 600 percent increase in IoT attacks from 2016 to 2017.
- More than half of the attempted attacks against IoT devices targeted the Telnet service.

IoT attacks by source country

This table shows the country of origin, based on IP address, of the attacking devices.

Rank	Country	2017 Percent	Country	2016 Percent
1	China	21	China	22.2
2	United States	10.6	United States	18.7
3	Brazil	6.9	Vietnam	6
4	Russian Federation	6.4	Russian Federation	5.5
5	India	5.4	Germany	4.2
6	Japan	4.1	Netherlands	3
7	Turkey	4.1	United Kingdom	2.7
8	Argentina	3.7	France	2.6
9	South Korea	3.6	Ukraine	2.6
10	Mexico	3.5	Argentina	2.5

IoT attacks' most used user names

This table shows the most frequently attempted login names for attacks against IoT devices.

Rank	2017 User Name	2017 Percent	2016 User Name	2016 Percent
1	root	40	root	33.5
2	admin	17.3	admin	14.1
3	enable	10.3	DUP root	6
4	shell	10.2	DUP admin	2.1
5	guest	1.5	ubnt	1.3
6	support	1.3	test	1.1
7	user	1.1	oracle	1.1
8	ubnt	0.9	postgres	0.7
9	DUP root	0.6		0.7
10	supervisor	0.5	123321	0.6

IoT attacks' most used passwords

This table shows the most frequently attempted passwords for attacks against IoT devices.

Rank	2017 Password	2017 Percent	2016 Password	2016 Percent
1	system	10.3	admin	9.5
2	sh	10.2	root	5.8
3	123456	9.1	12345	5
4	admin	3.7	123456	3.7
5	1234	3.1	password	3.2
6	password	2.5	1234	2.4
7	12345	2.5	ubnt	1.7
8		2.3	admin123	1
9	root	2.1	abc123	0.9
10	support	1.2	pass	0.7

Top threats detected by IoT honeypot in 2017

This shows the most frequently blocked malware aimed at IoT devices in 2017.

Rank	Threat Name	Percent
1	Linux.Lightaidra	57.5
2	Trojan.Gen.NPE	10.2
3	Linux.Mirai	8.7
4	Trojan.Gen.NPE.2	4
5	Linux.Kaiten	3.6
6	Downloader.Trojan	3
7	Linux.Gafgyt	2.7
8	Trojan.Gen.8!cloud	2.2
9	SecurityRisk.gen1	1.9
10	Trojan.Gen.6	1.7

Top 10 attacked services for IoT honeypot in Q4 2017

Telnet and HTTP were the most frequently targeted IoT services.

Rank	Service	Percent
1	Telnet	50.5
2	HTTP	32.4
3	HTTPS	7.7
4	SMB	5.8
5	SSH	2.1
6	UPnP	0.9
7	FTP	0.2
8	CWMP	0.1
9	SNMP	0.1
10	Modbus	0.1

Top 10 attacked ports for IoT honeypot in Q4 2017

The most frequently targeted IoT ports in network-based attacks in the last quarter of 2017.

Rank	Port	Percent
1	23/tcp (Telnet)	43.1
2	80/tcp (HTTP)	31.6
3	443/tcp (HTTPS)	7.7
4	2323/tcp (Telnet)	7.2
5	445/tcp (SMB)	5.8
6	22/tcp (SSH)	1.9
7	1900/udp (UPnP)	0.9
8	8080/tcp (HTTP)	0.8
9	2222/tcp (SSH)	0.2
10	21/tcp (FTP)	0.2

Top device type performing attacks against IoT honeypot

This table identifies the types of devices involved in the IoT attacks against the Symantec honeypot in 2017, with routers being the most frequently exploited type of device.

Rank	Device Type	Percent
1	Router	33.6
2	DVR (Digital Video Recorder)	23.2
3	Network	9.3
4	Satellite Dish	7.3
5	DSL/Cable Modem	7
6	SOHO Router	4.7
7	NAS (Network Attached Storage)	3.6
8	Camera	3.5
9	PLC (Programmable Logic Controller)	3.4
10	Alarm System	1.9

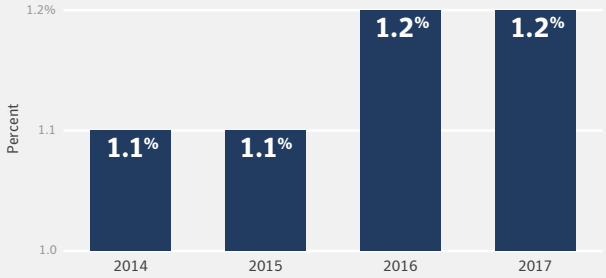
Top reputation of device attacking IoT honeypot

Further analysis of the attacking IP addresses reveals that almost half were not previously blacklisted, or involved with other malicious activity.

Rank	Category	Percent
1	Not Blacklisted	48.9
2	Bot	17
3	Spam	16.1
4	Attacks	9.8
5	Malware	8.1

Fraud attempts

1.2 percent of U.S. credit applications made during 2017 were considered fraudulent.



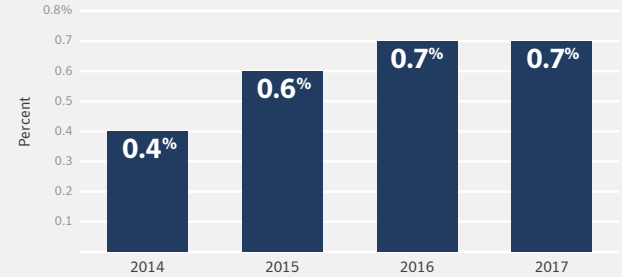
Fraud and the underground economy

Key findings

- Bankcard, retail card, and wireless fraud rates are 1.8 times higher than they were in 2014.
- The price of a premium ransomware toolkit ($450) is currently less than one average ransom ($522).
- Coin-mining toolkits are available on the dark web for as little as $30.

Confirmed fraud rate

The confirmed fraud rates in the bank card, retail card, and wireless industries are 1.8 times higher than they were in 2014.



Pricelist for goods

Although priced in U.S. dollars, payments are often made using cryptocurrencies, such as Bitcoin or Monero, at the daily exchange rate equivalent values.

These prices are taken from publicly accessible underground forums and dark web TOR sites. Closed, private forums tend to have even lower prices. We cannot verify if the goods are genuinely sold for the asked price, some of them might be fake offers.

Credit Cards	
The credit card data prices vary heavily depending on the country they are from (U.S. cards are cheaper as there are more available, EU cards are more expensive), the company (Visa®, Mastercard®, American Express®), the level (gold, platinum, business), and the extra information provided, such as date of birth (DoB), Verified by Visa®, Mastercard SecureCode™, etc. Often, the more you take the cheaper it gets (bulk prices).	
Single credit card	$0.50-25
Single credit card with full details (Fullz)	$1-40
Dump of magnetic strip track1/2 data (e.g. from skimming)	$20-60
500 credit cards already used for fraud in the last week	$1
Malware	
Common banking Trojan toolkit with support	$40-1500
Spyware	$15-50
Android banking Trojan	$2-500
Office macro downloader generator	$5
Cryptocurrency miner & stealer (Monero)	$30-300
Ransomware toolkit	$5-450
DDoS bot software	$1-15

Services	
DDoS service, short duration <1 hour, medium protected targets	$5-20
DDoS service, duration >24 hours, medium and strong protected targets	$10-1000
Hacker for hire	$100+
Credit score repair	$50
Messing up peoples online presence	$500
Airplane ticket and hotel bookings	10% of value
Money Transfer Services	
Cash redirector service for online money platforms (Pay $100 in Bitcoin and get a transfer of $1,000 to your account)	1-20% of value
Cash redirector service for bank accounts	2.5-15% of value
Accounts (User Name and Password)	
Video and sound streaming accounts	$0.10-10
Various services, more than 120+ available (gaming, food, shopping, etc.)	$0.5-10
Online banking accounts	0.5-10% of value
Online money accounts (depending on value and verification)	$10-100
Retail shopping account	$5-50
Cloud accounts	$5-10
Hacked Gmail accounts	$0.1-5
500,000 email accounts with passwords from data breaches	$90
Hotel loyalty/reward program accounts with 100,000 points	$10-20
Shopping loyalty accounts with cash points	$2-7
VPN services	$1-10
Online retailer gift cards	15-50% of face value
Restaurant gift cards	15-40% of face value

Identities	
Identity: Name, SSN, and DOB	$0.1-$1.5
Scanned documents (utility bill etc.)	$1-3
Fake ID, driver license, passport	$10-600
ID/passport scans	$1-25
Anonymous IBAN bank account	$7

Predictions

Section 04

Predictions for 2018

Mid-tier mature cloud providers will likely see the impact of the Meltdown and Spectre vulnerabilities

At the beginning of January 2018, two serious vulnerabilities were discovered which affected nearly all modern processor chips. Known as Meltdown and Spectre the vulnerabilities could permit attackers to gain unauthorized access to a computer's memory.

Meltdown and Spectre can affect all kinds of computers, but the most worrying possible impact is in the cloud, because an attack on a single server could lead to the compromise of multiple virtual machines running on that server.

Chip manufacturers, software vendors, and cloud providers have all been working hard, both before and after the vulnerabilities were disclosed, to ensure patches were in place. While major cloud providers possess the resources to ensure mitigations are in place, smaller and less-prepared cloud companies, such as smaller hosting providers, may struggle to respond, leaving their customers exposed.

WannaCry and Petya/NotPetya may inspire new generation of self-propagating threats

Worms—self-spreading malware—enjoyed their heyday around the turn of the century. For example, in 2003, the Slammer worm managed to infect most of its victims within one hour. Until May 2017, it seemed unlikely that another threat could cause global disruption in the same way.

That all changed with the arrival of WannaCry and Petya/NotPetya. Both threats were capable of self-propagation largely because they used the EternalBlue exploit. Although the vulnerability had been patched several months previously, there was enough unpatched computers online for both threats to cause serious disruption.

Attackers will no doubt have noticed how effective both threats were. EternalBlue's usefulness may be exhausted at this stage since most organizations will have patched, but there are other techniques that can be used. Petya/NotPetya employed other SMB spreading techniques using legitimate tools, such as PsExec and Windows Management Instrumentation Command-line (WMIC), to spread to network shares using stolen credentials. The use of these "living off the land" techniques allow attacks to fly under the radar making them more appealing to attackers. It's likely we'll see an increase in threats self-propagating using these techniques.

IoT attacks will likely diversify as attackers seek new types of devices to add to botnets

During 2016, we heard a lot about IoT attacks as the Mirai botnet appeared and caused serious disruption with large DDoS attacks. While IoT attacks weren't in the headlines as much in 2017, they certainly haven't gone away. In fact, attacks against IoT devices were up by 600 percent last year.

Our current research shows that attackers are still primarily focused on routers and modems, and are using infected devices to power botnets. Attacks are now so frequent that botnet operators are fighting over the same pool of devices and have to configure their malware to identify and remove malware belonging to other botnets.

IoT continues to be plagued by poor security, with default passwords and unpatched vulnerabilities all too common. Some IoT attackers have already started looking beyond routers and have begun to target other connected devices in a serious way.

Coinminer activity will likely continue to grow but will increase focus on organizations

2017 was the year that cyber criminals cashed in on cryptocurrency mining. Detections of coinminers grew by an astonishing 8,500 percent. This is not surprising considering Bitcoin prices began the year at just below $1,000 and finished at over $14,000 towards the end of 2017.

Coin-mining attacks are likely to continue into in 2018 and attackers will spend a lot of time and energy discovering more creative and effective forms of attack. Broadly speaking, their strategies will likely follow three directions:

01 Distributed mining, either through conventional botnets of malware-infected computers and IoT devices or browser-based coinminers, hosted on websites.

02 The second avenue of attack is likely targeting corporate or organizational networks in order to harness the power of servers or supercomputers.

03 Finally, cloud services offer the possibility of high-powered mining. This has a possible financial impact on cloud customers where they pay based on CPU usage.

Although the immediate rewards may ostensibly seem lower, coin mining offers a long-term, passive revenue stream if the miners can remain undiscovered for longer. We believe that coin-mining activity will increase in the mobile space into 2018 and beyond. We saw an uptick at the end of 2017 and if this proves lucrative, it may grow.

All of this is likely dependent on one thing: cryptocurrency values remaining high. Bitcoin prices have begun to slip backwards in recent months. However, this is perhaps seen as more of a market adjustment. Bitcoin is not the only cryptocurrency, and it also depends on how other cryptocurrencies fare, especially Monero. We believe we will see a shift away from Bitcoin as the lingua franca for cyber crime, perhaps with alternatives such as Ethereum, Monero, and Zcash gaining in popularity due to their stronger anonymity. Continued volatility in the Bitcoin market will become a major hindrance, particularly for smaller transactions.

However, if the value of all cryptocurrencies falls back, attackers will likely quickly lose interest in coin mining. At the moment, coin mining is more profitable than ransomware, but if cryptocurrencies lose their value, attackers are likely to move on to something more lucrative.

Attacks on critical infrastructure likely to step up in 2018

Attackers have been exhibiting a growing interest in critical infrastructure in recent years and the scale and persistence of these attacks is now reaching worrying proportions. Our latest research on the Dragonfly group found that it has continued to target the energy sector in Europe and North America. For now, Dragonfly appears to be focusing on gaining access to operational systems and gathering as much intelligence as possible about how these plants operate.

These attacks would likely give Dragonfly the ability to sabotage or gain control of these systems should it decide to do so. However, it seems unlikely that any group would go to these lengths unless it was prepared to launch disruptive attacks. Nonetheless, there is a real risk that at some stage soon, Dragonfly's masters may decide to play this card.

Credits

Team

Gillian Cleary
Mayee Corpin
Orla Cox
Hon Lau
Benjamin Nahorney
Dick O'Brien
Brigid O'Gorman
John-Paul Power
Scott Wallace
Paul Wood
Candid Wueest

Contributors

Shaun Aimoto
Pravin Bange
Albert Cooley
Stephen Doherty
Brian Duckering
James Duff
Daniel Grady
Sara Groves
Kevin Haley
Dermot Harnett
Robert Keith
Sean Kiernan
Anudeep Kumar
Chris Larsen
Carmel Maher
Matt Nagel
Alan Neville
Gavin O'Gorman
Hitesh Patel
Yun Shen
Dennis Tan
Tor Skaar
Parveen Vashishtha
Pierre-Antoine Vervier
William Wright

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.

Further Information

Symantec Managed Security Services: https://www.symantec.com/services/cyber-security-services

DeepSight Intelligence Service: https://www.symantec.com/services/cyber-security-services/deepsight-intelligence

Symantec Messaging Gateway: https://www.symantec.com/products/messaging-gateway

Symantec Email.cloud: https://www.symantec.com/products/email-security-cloud

Symantec's Advanced Threat Protection for Email: https://www.symantec.com/products/advanced-threat-protection-for-email

Symantec Web Security.cloud: https://www.symantec.com/products/cloud-delivered-web-security-services

Symantec On-Premise Secure Web Gateway: https://www.symantec.com/products/secure-web-gateway-proxy-sg-and-asg

Symantec CloudSOC: https://www.symantec.com/products/cloud-application-security-cloudsoc

Symantec Endpoint Protection (SEP): https://www.symantec.com/products/endpoint-protection

SEP Mobile: https://www.symantec.com/products/endpoint-protection-mobile

Norton: https://www.norton.com

ID Analytics: https://www.idanalytics.com/

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.

03/18

ISTR