Cybercrime tactics and techniques: 2017 state of malware

Provided by

Malwarebytes LABS

Table of contents

Executive summary

2017 was a tumultuous year in politics, media, gender, race—and cybersecurity didn't beat the rap. Last year was full of twists and turns in the cybercrime world, with major outbreaks, new infection methods, and the evolution of the cryptocurrency crime industry keeping researchers not so much on our toes as flipped upside down on our heads.

In aiming to make sense of the madness, we gathered information from our data science, research, and intel teams throughout the year, checking in on trends, the rise and fall of malware families, distribution methods, and more. To create this report, we analyzed telemetry gathered from our products from January to November 2016 and January to November 2017. In addition, we combined data collected from our own threat-facing honeypots in 2017 with the observations and analysis of Malwarebytes' researchers. What we came up with was a more complete picture of the 2017 threat landscape that showed us just how much can change in a year.

This special end-of-year report will look at the tactics of infection, attack methods, and changing development and distribution techniques used by cybercriminals over the last 12 months. We'll dive into the exponential increase of malware volume and severity year-over-year, (and which malware types are experiencing decreases), as well as trends in high-impact threats, such as ransomware and cryptomining. What we'll ultimately show is an evolution in cybercrime that's sure to lead to even bigger bad business in 2018.

Key takeaways for businesses and consumers

Ransomware volume was up in 2017, but is trending downward.

The last year made it clear that, for attacking businesses anyway, ransomware was the tool of choice. Our telemetry shows that in 2017, ransomware detections increased by 90 percent for business customers, climbing the charts from last year to become our fifth-most detected threat. Ransomware saw a banner year among consumers as well, with detection rates up 93 percent over 2016.

Despite such a high-profile year of high-volume outbreaks, development of new ransomware families grew stale. Closer to the end of the year, there was a significant change in distribution, with many avenues known for ransomware drops diversifying their payloads with banker Trojans and cryptocurrency miners instead.

What they can't hold for ransom, criminals will steal instead.

With ransomware slowly going out of favor, criminals pivoted to banking Trojans, spyware, and hijackers in 2017 to attack companies instead. These types of malware are used to steal data, login credentials, contact lists, credit card data, distribute more malware, and spy on a victim for information about the business or how to dig deeper into the network. We saw an increase of 40 percent in hijackers and 30 percent in spyware detections in 2017. The second half of the year also marked an average of 102 percent increase in banking Trojan detections.

Top 10 business detections		
2016	vs.	2017
Fraud Tool	1	Hijacker
Adware	2	Adware
Hijacker	3	Riskware Tool
Riskware Tool	4	Backdoor
Backdoor	5	Ransomware
Hack Tool	6	Spyware
Worm	7	Worm
Crack Tool	8	Hack Tool
Banking Trojan	9	Fraud Tool
Ransomware	10	Banking Trojan

Figure 1. Top 10 business threats of 2016 and 2017

Consumer threats are on the rise.

From a consumer view, malware is growing to be a more severe problem every single year. In 2017, overall threat detections for consumers rose 12 percent. This aligns with the observation that malware development and distribution methods have evolved over 2017, allowing for more threats to quickly be created and distributed to victims.

Adware volume is up, but there are fewer players in the game.

Detections of adware in 2017 showed immense distribution volume, up 132 percent year-over-year. It rises from our second most common consumer threat in 2016 to number one on our list for 2017. Adware now represents almost 40 percent of our consumer threat detections, up from less than 20 percent in 2016. However, due to more security companies detecting potentially unwanted programs, there are fewer players creating new adware. Despite this, the developers still around are utilizing malware-like tactics to stay undetected and persistent.

Cryptomining is out of control.

Alongside a sudden cryptocurrency craze, bad actors have started utilizing cryptomining tools for their own profit, using victim system resources in the process. This includes compromised websites serving drive-by mining code, a significant increase of miners through malicious spam and exploit kit drops, and adware bundlers pushing miners instead of toolbars. By the end of 2017, basically anyone doing any kind of cybercrime was also likely dabbling in cryptomining.

Top 10 consumer detections		
2016	vs.	2017
Fraud Tool	1	Adware
Adware	2	Fraud Tool
Riskware Tool	3	Riskware Tool
Backdoor	4	Backdoor
Hack Tool	5	Hack Tool
Hijacker	6	Worm
Crack Tool	7	Hijacker
Worm	8	Crack Tool
Banking Trojan	9	Ransomware
Rootkit	10	Spyware

Figure 2. Top 10 consumer threats of 2016 and 2017

Cybercriminals got creative with their delivery methods in 2017.

2017 should be known as the year of interesting infection vectors, as we observed leaked government exploits, such as EternalBlue used in the WannaCry ransomware outbreak, compromised update processes, and increased geo-targeting being used by attackers in the wild. Likely, these are tactic adopted to evade traditional detection methods that are watching for the most common infection avenues.

Exploit kits took a dive while malspam was unleashed.

In an interesting turn, 2017 showed little development for exploit kits, as no new zero-day exploits were used by any of the remaining exploit kits still in the wild. This is a significant change from previous years, where exploits were the primary method of infection. Instead, intense development of malicious spam detection evasion tactics, as well as the inclusion of multiple exploits for Microsoft Office documents, caused a surge of malware delivery through these vectors.

Scammers shifted away from traditional browser locks to other tactics.

Scams in 2017 were notable for a shift in tactics away from the traditional browser locker to phishing emails and malvertising. In addition, at the back end of the year we saw an upswing in Bitcoin-related content, where TSS turned to impersonating popular exchanges as their next pretext.

2018 predictions

As Mark Twain once said in *Following the Equator*, "Prophecy is a good line of business, but it is full of risks." We acknowledge that making predictions about cybercrime is a bit more art than science, but when we look back over years of patterns and data and experience, we can make some educated guesses about where we think this is all going.

Our predictions for 2018 cover a lot of ground, including the future of cryptocurrency mining, possible IoT attacks, and Mac malware. Cybercriminals showed immense effort in 2017 to expand the capabilities of existing threats and utilize them in ways never seen. This trend is likely going to continue through 2018, however, we do expect to see new malware families and new infection techniques continuing to be introduced. In the meantime, we can learn the lessons of the previous year and not only deploy solutions to protect our systems from the next big threat, but make our users aware of what to watch out for and how to avoid it.

Malware

Ransomware

If you've been following our 2017 quarterly reports, you know that we've already covered the danger and scale of the ransomware threat this year. This includes large-scale outbreaks of ransom-worm malware, dominant ransomware families that were distributed through most of the year, and the consolidation of power to a few notable groups.

However, when we look at the entire year, we can see that, statistically, this was a banner year for ransomware. According to telemetry gathered from Malwarebytes products, business and consumer ransomware detections have increased 90 and 93 percent, respectively, in 2017. This is largely because of families like WannaCry, Locky, Cerber, and GlobeImposter. In fact, the monthly rate of ransomware attacks against businesses increased up to 10 times the rate of 2016.

A strong start

While we primarily saw Locky and Cerber at the beginning of the year, the summer months brought in a flood of ransomware infections from a couple of new players, such as GlobeImposter and Jaff. Between July and September 2017, there was a 700 percent increase in ransomware (according to Malwarebytes' telemetry)—with just two families making up most of that statistic:

- GlobeImposter increased 341 percent from July to August 2017.
- WannaCry surged 375 percent from August to September 2017.

In addition, nearly seven percent of all attacks against businesses in September 2017 involved ransomware, compared to the average rate of ransomware attacks in 2016, which totaled 1.11 percent.

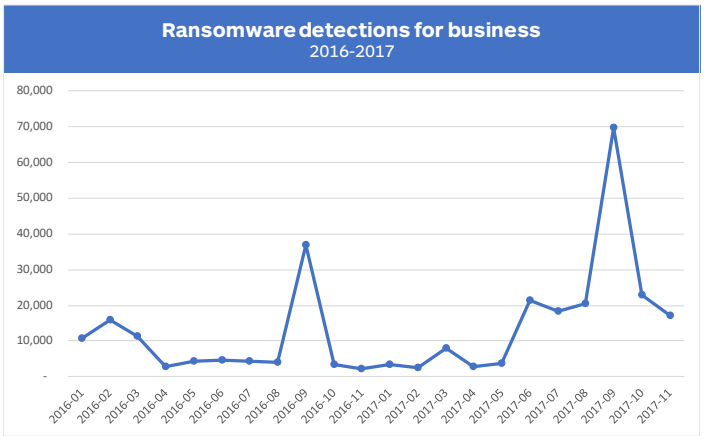


Figure 3. Ransomware detections among businesses 2016–2017

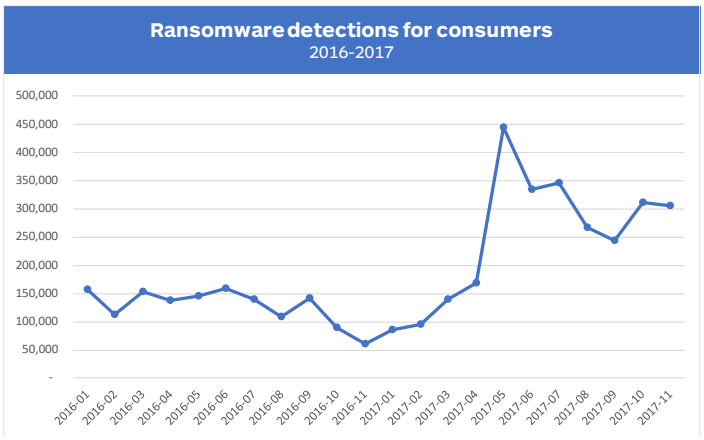


Figure 4. Ransomware detections among consumers 2016–2017

Stale development

Despite numerous high-profile attacks, as well as the shockingly high volume of ransomware shown above, new ransomware development has been a bit stale. The primary pushers of ransomware are made up of a few families that hold most of the market share, either due to a better overall product to sell on the darknet or a special relationship with the holders and herders of malicious spam botnets and exploit kits (the primary methods of distributing malware).

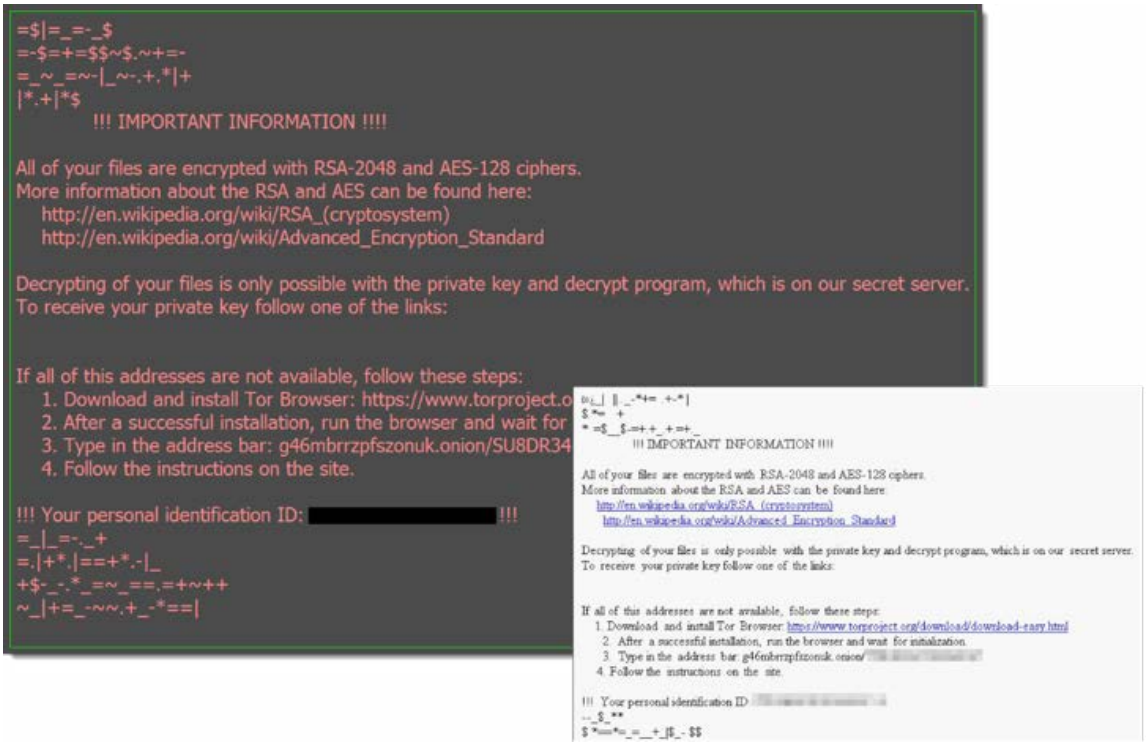


Figure 5. Locky screen and ransom note

The exception to this dry patch of innovation is the inclusion of worm functionality found in ransomware families like WannaCry and NotPetya, which we'll discuss in greater detail in our section on EternalBlue.

Ransomware out of style

At the beginning of the year, the domination that ransomware had over the primary infection vectors made it seem like dealing with ransom malware would be the new norm moving forward. However, trends over the last few months have shown a shift away from ransomware. In fact, many mechanisms for distributing malware have either gone back to the old favorites, like banking Trojans and spyware, or moved onto the newer trend of delivering cryptocurrency miners.

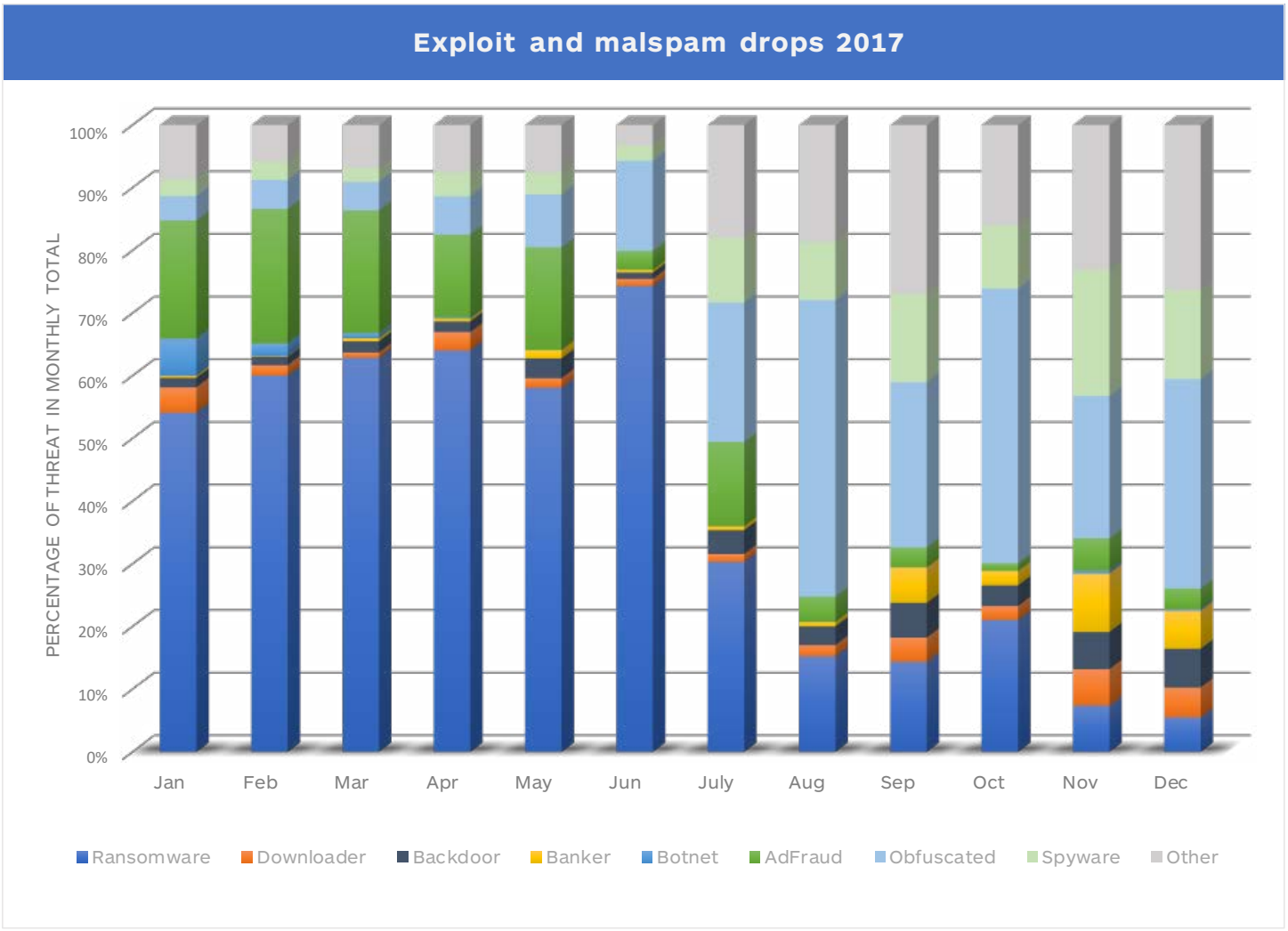


Figure 6. Malspam and exploit drops 2017

The likely motivation behind this move involves a lower return on investment for the groups behind larger ransomware families. The adoption and use of anti-ransomware technology, backup precautions, and a greater general knowledge of threats and protection methods has resulted in fewer cases where the ransom is paid. Therefore, today, it is more economical for criminals to utilize cryptominers, ad fraud malware, and good old-fashioned credential stealing over ransomware.

Spyware

Spyware made its biggest impact for both businesses and consumers during the last half of 2017. This is likely due to ransomware attacks having less success for cybercriminals.

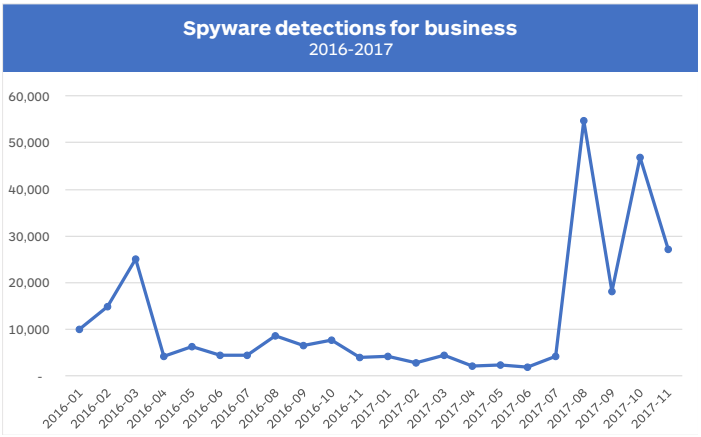


Figure 7. Spyware detections for business 2016-2017

Spyware, as the name conveys, is a category of malicious software with the intention of spying on the user. This can be done through numerous methods, including capturing data through screenshots, webcam captures, keylogging, or stealing form data from the websites the user visits.

The chart above focuses on spyware detections for business customers in both 2016 and 2017. The upturn near the end of the 2017 matches with the jump and drop of ransomware detections during the same period. This is indicative of criminals diversifying their attack strategy to increase attack success by using different malware types.

The business impact of a heavy spyware attack campaign could result in the theft of intellectual property, however it could also be used to "scout" the corporate network, identifying the best possible attack points to launch more dangerous forms of malware.

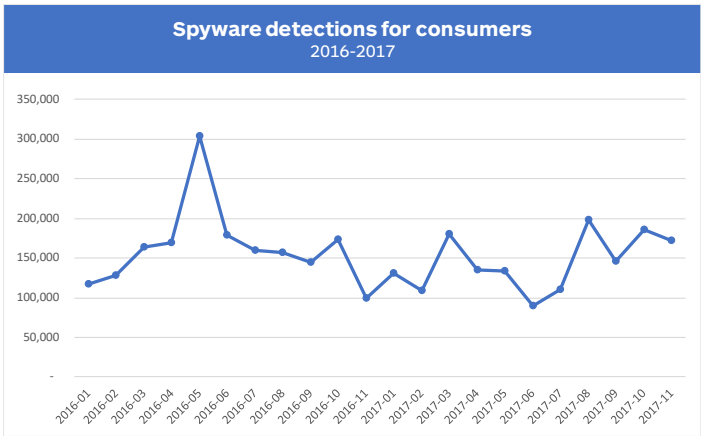


Figure 8. Spyware detections for consumers 2016-2017

The chart above illustrates detections for spyware against consumers over the last two years. From a consumer standpoint, spyware has stayed a constant threat, finishing off the second half of 2017 stronger than the first. This generally steady trend makes sense when you consider that spyware against a regular consumer is far more entertaining and likely rewarding than a business victim.

We expect to see a continued steady stream of spyware for consumers and more big spikes against businesses in 2018.

Hijackers

Trends in hijackers moved in two sharply contrasting directions this year, with businesses seeing a sharp increase in hijacker detections while consumers experienced a dramatic drop.

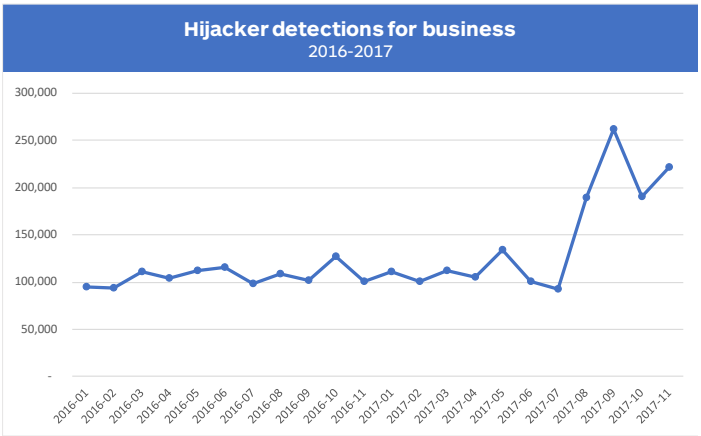


Figure 9. Hijacker detections for business 2016-2017

August 2017 had the greatest amount of hijacker malware detections for business than ever before. This is an interesting trend considering the primary method of infection for hijacker malware is through installation of untrusted potentially unwanted program bundles.

Hijacker malware interacts and modifies victim browser operations to push advertisements, redirecting the browser to third-party search engines or shopping sites. Depending on the family of hijacker, it may also install additional malware or steal personal information.

From a business impact, hijackers primarily cause work down-time, however they could also lead to additional infection or worse. Therefore, it is highly recommended to keep an eye out for these annoying, but deceptively dangerous malware types.

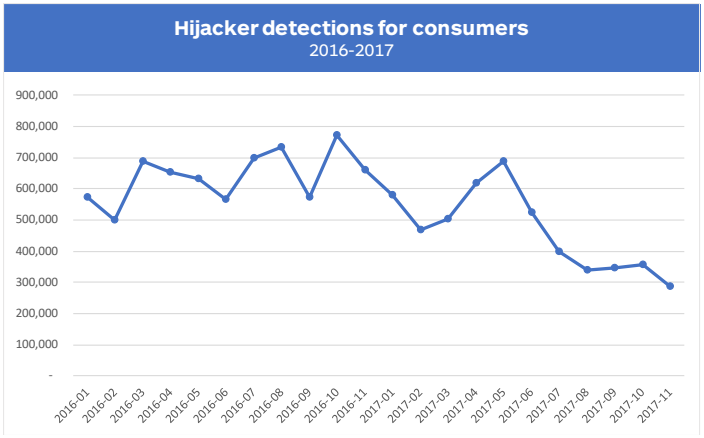


Figure 10. Hijacker detections for consumers 2016-2017

Consumers had the opposite problem, as hijacker malware detections were on the decline for the second half of the year. This matches up with observations earlier in the year of fewer active developers for bundled scam software, since bundlers are the primary method of spreading hijacker malware.

With this kind of steady drop in detections for hijackers, it is unlikely that we will see a large increase in 2018, at least not to the levels of 2016.

Banking Trojans

Prior to 2016, banking Trojans were everywhere you looked. Some of the most advanced features used by malware were by families whose goal was to steal bank and financial information. As the years went on, it became less and less common, likely due to increased security measures by banks against fraud, as well as improved recovery measures. For example, if you get your card stolen you can freeze it, get a new one sent to you, and have the charges reversed with minimal effort.

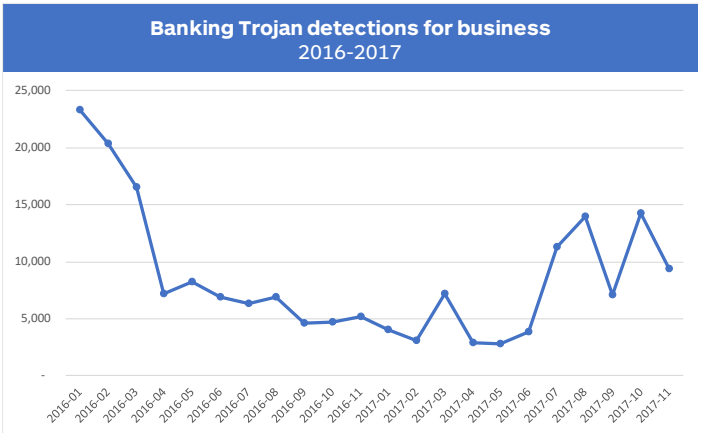


Figure 11. Banking Trojan detections for business 2016-2017

Despite a slow trend for the last two years of fewer and fewer banking Trojan detections for businesses, the end of the year saw a great increase in attacks pushing this form of malware. Looking at Figure 11, you can see a rise starting in July 2017 followed by a big dip in September. This matches up almost perfectly with our statistics for spyware detections by business customers, likely meaning that the same campaign that was pushing the banking Trojans was also pushing spyware. Another theory is that one malware type was installing the other, which is not uncommon.

The greatest business impact this type of threat could have includes personal and corporate financial information being stolen by criminals and either used to try and steal actual money or to be sold on the black market. The use of this type of malware against businesses during the end of the year is indicative of a declining ransomware return on investment and cybercriminals leaning on tried and true attack methods.

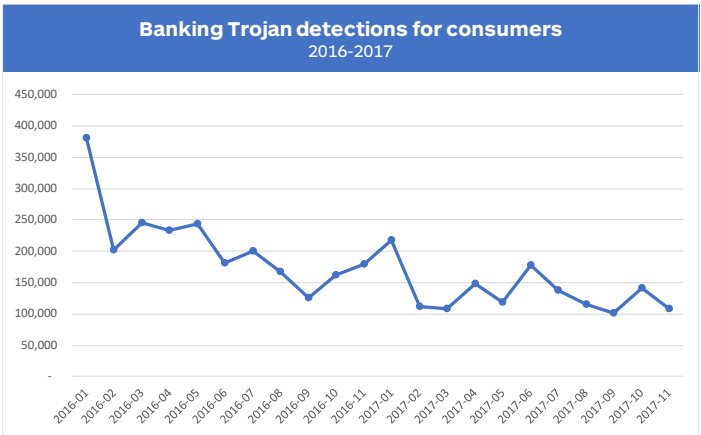


Figure 12. Banking Trojan detections for consumers 2016-2017

The story is the same on the consumer side, except with a different ending. The decline in banking Trojan detections throughout the year illustrates a dying attack method that is unlikely going to make it through 2018 on a strong note. The advancements in bank and financial security against fraud and theft have been phenomenal; likely they are the biggest contributing factor of banking Trojans' decline. However, we still have a long way to go in preventing personal information being used to open bank accounts and credit cards in victims' names.

Adware

The volume of adware continues to increase year over year. Adware makes up 40 percent of our consumer threat detections, up 132 percent over last year. It's now our most detected threat. However, like ransomware, there are fewer families in the mix. Most of the work is being done by a handful of active adware developers for Windows, macOS, and Android.

Why are the numbers of adware makers dwindling? The tech industry has become much more aggressive about adblocking. Google, Mozilla, and Microsoft have all made moves to introduce more sophisticated ad blocking tools into their respective browsers. Other adware-blocking plugins have become ubiquitous. Adware creators with fewer resources and less adaptability were thus rendered extinct by technical Darwinism.

What that means is that if threat actors wanted to deliver adware, they had to step up their game to avoid being blocked. To do that, their formerly grey tactics turned to black. Survival of the fittest and all.

Windows adware

A prime example of this more aggressive adware trend is a Windows software program called Smart Service. Smart Service is bundled with adware and PUPs to act as protection against their removal. It uses two methods to achieve this goal.

First, Smart Service hooks into the Windows CreateProcess function so it can inspect new processes before they are allowed to run. In order to prevent the adware from being removed from the affected system, it blocks security software from running or even being installed. It does this based on the security certificate and process name. The user will get an error message stating, "The requested resource is in use."

Second, the program protects certain processes from being terminated, and stops the user from removing critical files and registry keys. The user will get an error message that says "Unable to delete" when attempting to perform this action.

Smart Service includes an adfraud component capable of earning money for threat creators. The bundlers are happy to include the package, as it prevents victims from being able to remove the unwanted software.

So, it's a win/win for the bad guys.

Being able to fight this infection is an ongoing battle, as the creators of Smart Service actively monitor what the research community is doing in order to develop countermeasures as soon as new defenses are published. Smart Service is detected and blocked by Malwarebytes' real-time malware scanner; however, it's quite difficult to remove once an infection has already occurred.

Android adware

Over the last six months, there's been a lot of clickers and bundled adware getting into the Google Play Store. Those getting through are aggressive, using creative new tactics to obfuscate their true purpose.

In fall of 2017, a new mobile malware variant was found in Google Play known as Android/Trojan.AsiaHitGroup. The malware installs under a generic app name, Download Manager, which is different from the name provided in Google Play. Once installed, the app creates a shortcut icon, but that icon is quickly deleted after the first time you open the app.

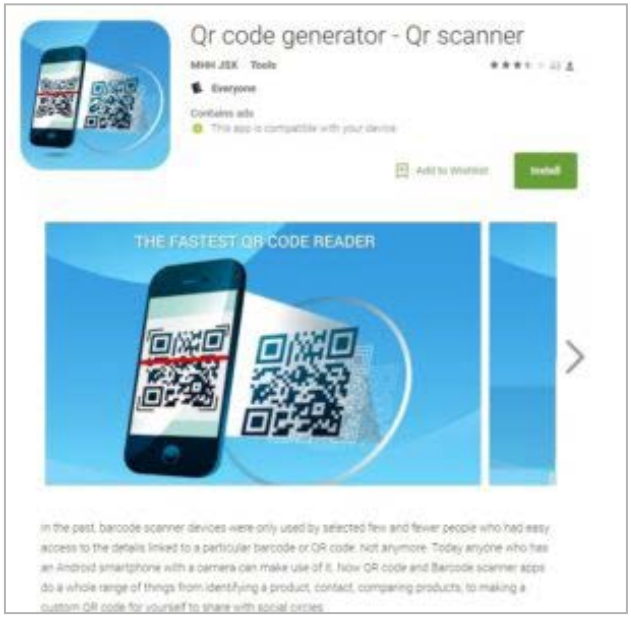


Figure 13. Trojan.AsiaHitGroup

The malicious app proceeds to check the mobile device's location via a geolocation website that uses the device's IP address. If the location is within certain perimeters, it continues to download and install a Trojan SMS. This Trojan SMS is used to propagate the malware even further. Additionally, the malicious app contains hidden adware, which runs regardless of location. Ultimately, we believe that the end goal of this malware is to run this hidden piece of adware to collect revenue.

The advanced approach of hiding adware is a rising trend among mobile malware. The approach is to use legitimate ad SDKs that pay a small amount of revenue for each ad shown. The malware deceptively runs these ads to collect revenue quickly.

Mac adware

On the Mac, we saw an interesting technique in use by the VSearch (aka Pirrit) adware. The vast majority of adware (and malware) on macOS uses the most popular and recommended methods of persistence; namely, launch agents/daemons and login items. Those are easy to implement and fully supported by Apple, but it also makes for easy detection.

Some variants of VSearch were spotted using older technology, most likely in hopes of going unnoticed. Specifically, they used the old cron process, a Unix program for scheduling recurring tasks. Since Apple has been recommending the use of launch agents/daemons over the simpler cron tasks for a long time, few people today ever think about cron, much less check to see what it's doing. Since cron still exists in a functional state in the latest versions of macOS, this makes it a good target for adware or malware trying to stay persistent, but under the radar.

```
$ sudo crontab -l
50 * * * * /Library/stateliness.hu/stateliness.hu cr
```

Figure 14. VSearch adware

Botnets

The last year showed a steady decline in detections for botnet malware, a huge shift from what we saw in 2016. This aligns for both business and consumer customer telemetry. Declines are likely due to a shift in focus away from the desktop, aiming at IoT devices such as routers or smart appliances instead. Cybercriminals often shift platforms in order to capitalize on the easier infection, and IoT devices are much more vulnerable to this type of attack.

Botnets are basically groups of "dumb" malware, infecting numerous systems. The "dumb" part, or the bot, consists of a lightweight and sometimes quiet application that runs in the background of a victim system, waiting for instructions from the attacker.

Botnets are used for launching distributed denial of service (DDoS) attacks, spreading malicious emails, and installing more malware. Although, depending on the family of bot, capabilities can also include the use of more traditional spyware methods, such as keylogging or screen capturing.

The biggest threat to business when it comes to botnets are primarily the families of botnet malware that perform more intrusive, data theft operations. However, the infection of company endpoints by bot malware can lead to those systems being used in a DDoS attack against someone else, which not only hurts other legitimate users but also eats up resources in the source network.

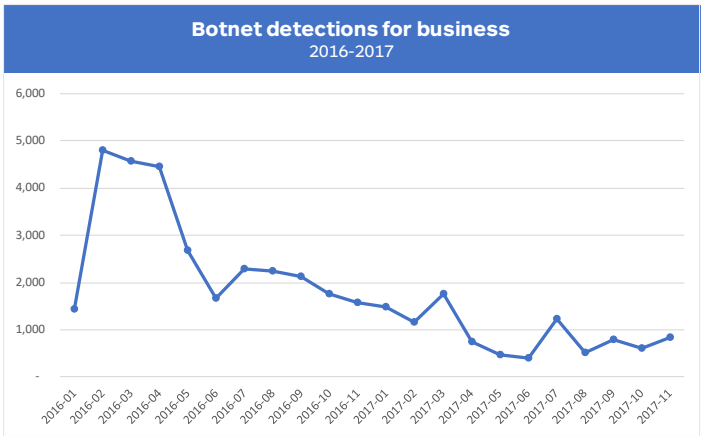


Figure 15. Botnet detections for business 2016-2017

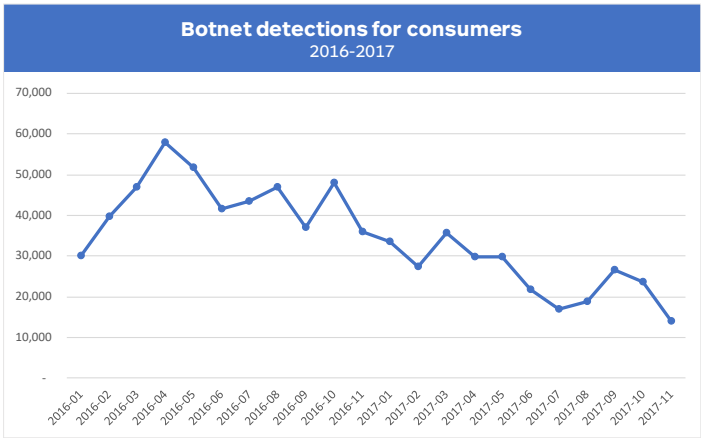


Figure 16. Botnet detections for consumers 2016-2017

Cryptocurrency miners

Cryptocurrency…so hot right now. In 2017, cryptocurrency miners experienced a surge in evolution, paired with an increase in distribution across multiple channels.

Due to the growing popularity and market value of cryptocurrencies, we have seen an increase in not only the number of malicious attacks using cryptominers, but also the methods used for attack. We define the malicious use of cryptominers to include any method that uses the system resources of an unsuspecting victim in order to mine cryptocurrency. We call this drive-by mining.

The most popular currency for drive-by mining in 2017 is Monero, likely due to:

- The higher speed with which transactions are processed, even small amounts.
- The anonymity automatically incorporated into the Monero blockchain.
- The mining algorithm that does not favor specialized chips.

Drive-by mining

In the fall of 2017, a new venture called Coinhive revived an old and failed concept of browser-based mining using JavaScript. Trying to capitalize on the popularity of cryptocurrencies, Coinhive provided a simple API for webmasters to add to their website, which would turn any visitor into a miner for the Monero digital currency.

Unfortunately, this technology was immediately abused by webmasters that ran it silently, therefore exploiting their visitor's CPU for their own gain. Eventually, criminals also took note and started compromising websites with cryptomining code.

During that time period, Malwarebytes blocked an average of 8 million drive-by mining attempts from websites and visitors all over the world. Coinhive is now one of many new copycats that are boasting about being able to run without being discovered by ad blockers or antivirus.

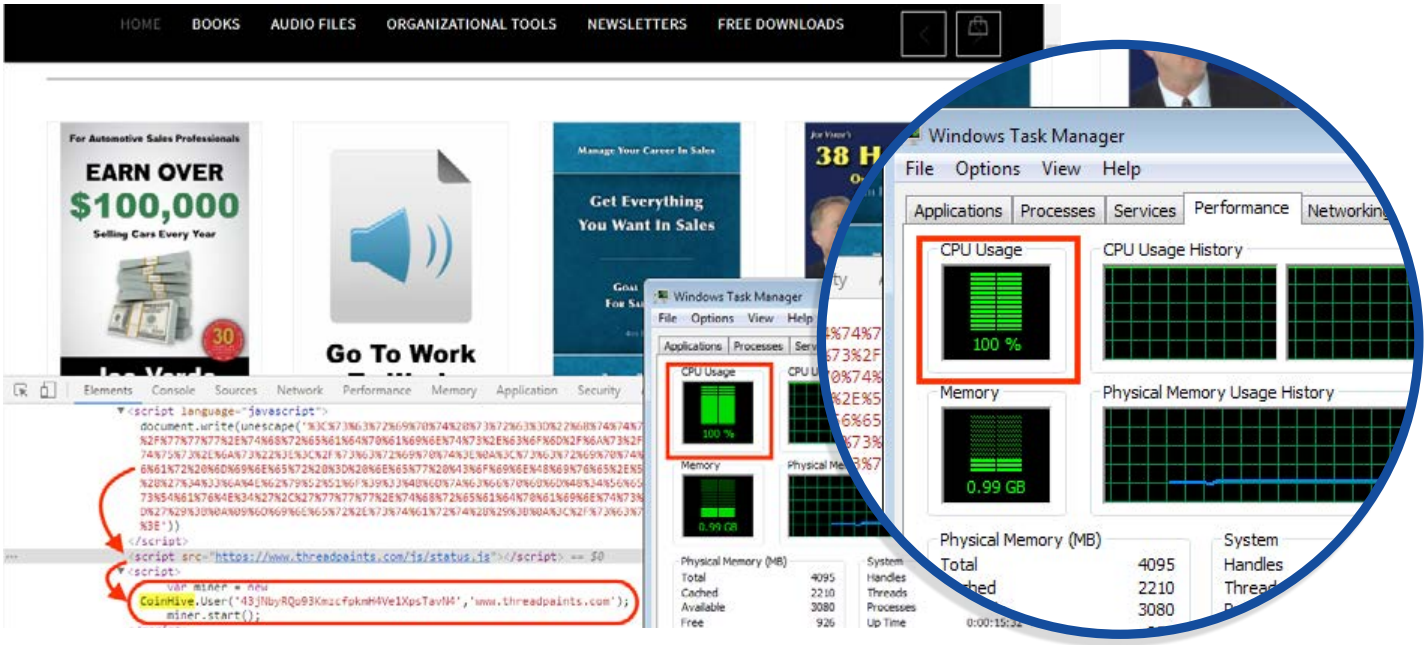


Figure 17. An example of script-based mining being abused

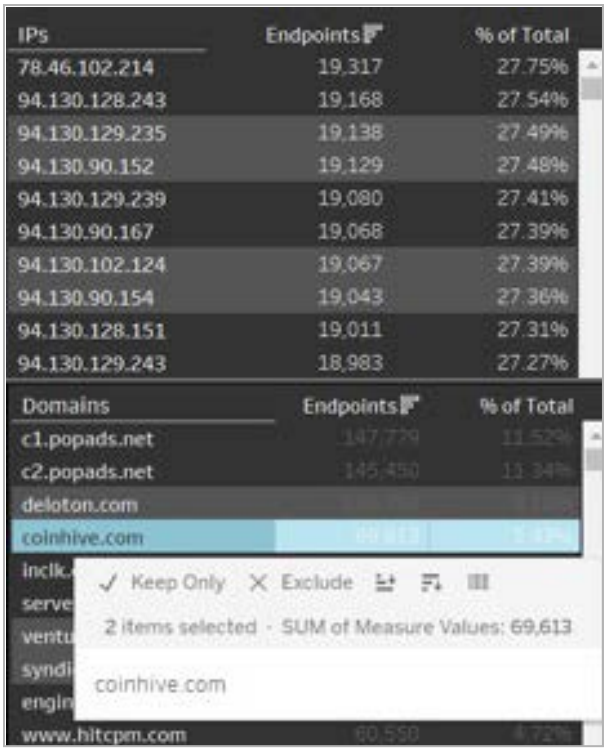


Figure 18. The number of coinhive.com blocks by Malwarebytes in five days

The statistics above show five days' worth of blocking coinhive.com. The activity on this domain alone accounts for over 5 percent of our total blocked domains, and equals over 27 percent of the blocked IPs. Adding related domains like coin-hive.com, authedmine.com, and cnhv.co brought us to over 100 million blocks per month.

Methods of drive-by mining attacks

PUP wrappers

Several bundlers and PUP wrappers have been found to install miners, and it seems they are replacing adware as a payment method. IStartSurf, a PUP well known for its browser hijackers, has started to include miners to its silent installs. InstallMonster, a more general-use bundler, has been doing the same.

Exploit kits and malvertising

The payload of RIG exploit kit now includes cryptominers in 2017. The same is true for Terror EK, but to a lesser extent. More about that in our section about exploit kits.

Even the EternalBlue exploit, of WannaCry fame, was used to spread a miner detected as Trojan.BitcoinMiner that used Windows Management Instrumentation for a fileless, persistent infection.

In addition, crooks mixed malvertising and ad fraud techniques to make the cryptomining process persistent, even after users closed their browser window. What could have been an alternative business model to online advertising turned into a big dumpster fire.

Malicious spam

Spammers are having a field day with cryptocurrencies. Not only have they used the Ethereum testnet to run a spam campaign, but they are also using Bitcoin value fluctuations as a means for phishing—while, of course, sending out cryptominers or installers for these miners as malspam.

Figure 19. Bitcoin malspam

Social engineering

Social engineering is another attack vector in use for drive-by mining. The so-called Roboto campaign used social engineering to let users believe they needed to install a new font when, in fact, they were served a cryptominer.

Figure 20. Social engineering used to install miner

And we have seen some miners (e.g. Cloud Packager) that were offered as cracked versions of popular software.

Bankers going for Bitcoin wallet theft

Banker Trojans have also expanded their working field into stealing cryptocurrencies right out of people's virtual wallets. Coinbase is a cryptowallet that trades in several cryptocurrencies, including Bitcoin. A Trickbot variant was spotted that includes the Coinbase exchange to steal credentials from the sites it monitors. Other Trojans have been spotted that steal cryptocurrencies on the fly, including CryptoShuffler, a Trojan that monitors the clipboard, the temporary storage area for cut/paste operations. As soon as it spots the address of a cryptocurrency wallet on the clipboard, it replaces the address with that of the threat actor. Sneaky. Tricksy. False.

Delivery techniques

In this next section, we'll dive deeper into noteworthy delivery techniques criminals used to drop their payloads in 2017. From the creative use of leaked NSA exploits to Trojanized CCleaner files to ransomware written specifically for South Korea, threat actors wasted no time in 2017 coming up with innovative ways to evade detection and keep researchers up at night.

Perhaps the creative inspiration for these hijinks comes from the fact that exploit kits and botnet attacks are on the decline, making way for good ole mainstays like malspam and tech support scams.

SMB exploit / EternalBlue

One of the most surprising and powerful attacks of 2017 was made possible due to a leaked NSA exploit known as EternalBlue. Both WannaCry and NotPetya ransomware utilized the this exploit during two campaigns in the middle of the year.

The exploit

EternalBlue (CVE-2017-0144) exploits a vulnerability found in numerous Windows operating systems, specifically a bug in how the Server Message Block (SMB) is handled. An attacker can use this exploit to execute code on a target system by sending specially-crafted network packets to a system with a vulnerable version of SMB version 1 installed.

Figure 21. MS17-010, the security bulletin that announced a patch for EternalBlue

The vulnerability was reported to Microsoft months before the first public attack in May; an emergency bulletin (MS17-010) was released by Microsoft on March 14, 2017. Patches were rolled out to every version of Windows still supported. Despite having a two-month head start, hundreds of thousands of systems were still not updated, and thus vulnerable to the EternalBlue exploit when it was spotted in the wild with WannaCry.

In the wild

WannaCry

WannaCry is classified as ransomware with worm functionality, or ransomworm. In the May outbreak, it used EternalBlue to infect Internet-facing systems all over the world. After infection, WannaCry would use EternalBlue, along with other leaked NSA exploits, to quickly traverse through the network connected to the victim system, encrypting files and demanding payment.

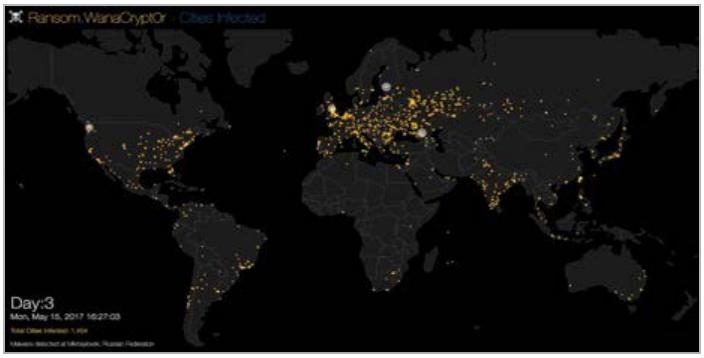


Figure 22. Map of WannaCry infection

The initial version of WannaCry included a "killswitch" in the form of a network traffic beacon. The malware would reach out to a hard-coded domain, expecting no response. If a response was received, however, the malware would not encrypt any files. When this domain was registered by a security researcher, the original version of WannaCry became benign.

NotPetya

The arrival of NotPetya in June—just one month after WannaCry—may have seemed like a bad joke, but no one was laughing.

NotPetya appeared to be heavily influenced by Petya and WannaCry. Similar to ransomware strains before it, NotPetya was able to spread by exploiting two Server Message Block (SMB) vulnerabilities: EternalBlue (CVE-2017-0144) and EternalRomance (CVE-2017-0145). It also attacked low-level structures of affected systems by encrypting their MFTs (Master File Table) and the MBRs (Master Boot Record).

Unlike previous ransomware strains, NotPetya had additional means to propagate, such as credential theft and impersonation using network file-shares and WMI (Windows Management Instrumentation) or PSEXEC.

Evidence collected by multiple security researchers and law enforcement point to Intellect Service, a small software company in Ukraine, as the outbreak's "patient zero," or where the malware originated.

Furthermore, our friends at ESET revealed that threat actors had illegally tainted at least three update files of the firm's popular tax accounting software, M.E.Doc, by incorporating a backdoor in it.

Further evidence suggested that NotPetya was not really ransomware but a destructive malware. Why?

The ransomware was essentially ineffective at collecting its ransom. Users affected by NotPetya were advised not to bother paying, as the email service that hosted the address where victims were instructed to send payments to was closed. As such, recovering files via payment was no longer possible. Other security researchers advised using a vaccine to recover the affected system. Lastly, all users of M.E.Doc were advised to change all passwords for proxies and email accounts.

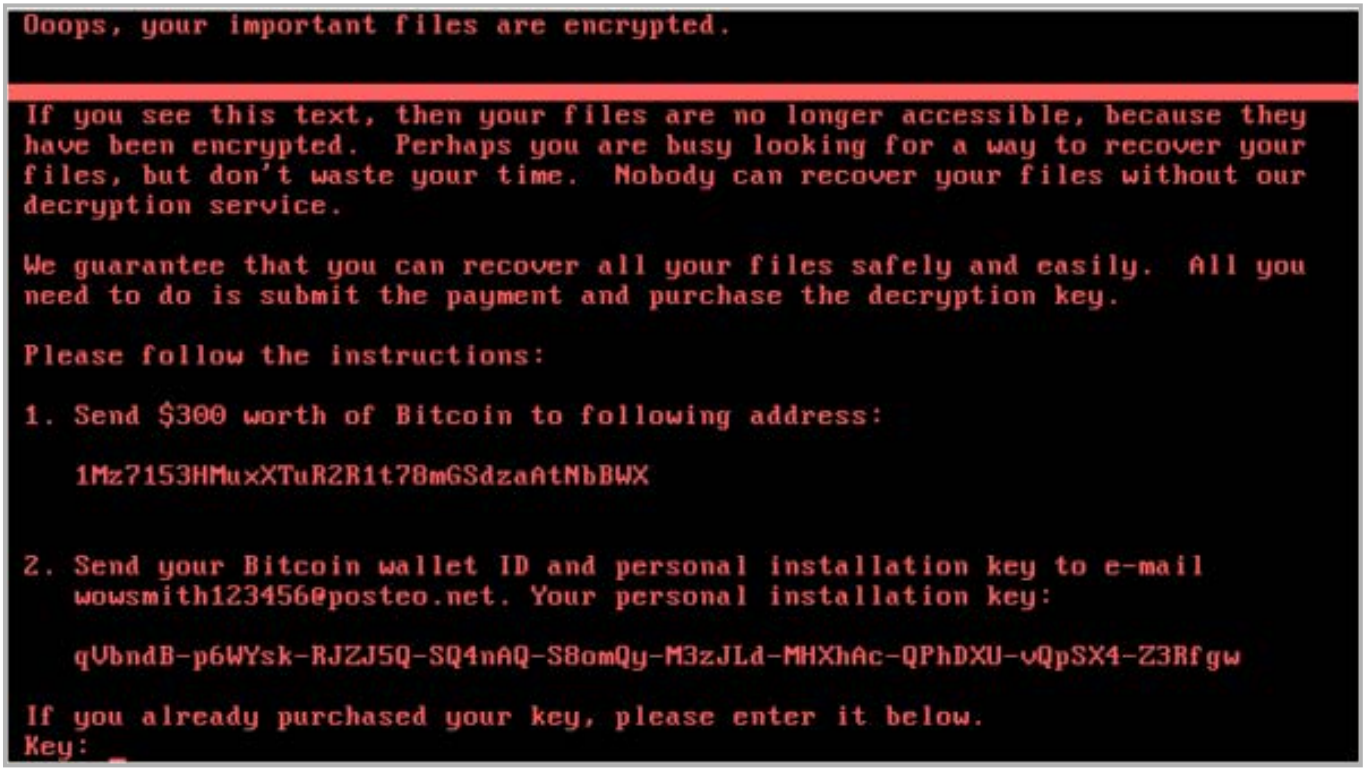


Figure 23. NotPetya's ransom note

Others

While WannaCry and NotPetya made headlines and sent the security community into a frenzy, there were, and still are, other forms of malware that have used EternalBlue and other leaked exploits to their advantage. For example:

- Adylkuzz is a family of BitCoin miners that not only used the EternalBlue exploit to infect systems weeks before WannaCry did, but also patched the victim systems so no additional malware could be installed!
- CoinMiner is another mining family that uses EternalBlue to breach a network, however, instead of installing a malware executable, it executes in the running memory of the system. This tactic is known as a fileless infection and has proven to be an effective method at defeating detection by security solutions in the past. CoinMiner has the unique distinction of being the first fileless BitCoin miner.
- Retefe (not Covfefe) is a family of banking Trojan malware with a geographic focus on Austria, Sweden, Switzerland, and Japan. It adopted the EternalBlue exploit into newer variants of the malware to traverse through networks after initial infection by malicious code embedded in a Word document and attached to a spam email.

Supply chain attacks

As if keeping a business' physical supply chain secured isn't challenging and complicated enough, the threat of cybersecurity risks targeting it just adds to the problem. Cybercriminals homing in on the most vulnerable part of an organization's supply chain is not new; however, this tactic has become more popular in the last quarter of 2017 compared to previous quarters of the year.

Here, we summarize some notable supply chain attacks of 2017, focusing on how they began and the motivations behind them.

Trojanized CCleaner file

CCleaner has been around for more than a decade. With over 2 billion downloads under its belt, it has been a household name when it comes to free clean-up and maintenance tools for the PC.

In mid-September, CCleaner version 5.33.6162 and CCleaner Cloud version 1.07.3191 were found to contain a backdoor payload that allowed it to profile machines it was installed on aggressively, phone the information back to its command-and-control (C&C) server, and, if predefined requirements were met, fetch a secondary payload.

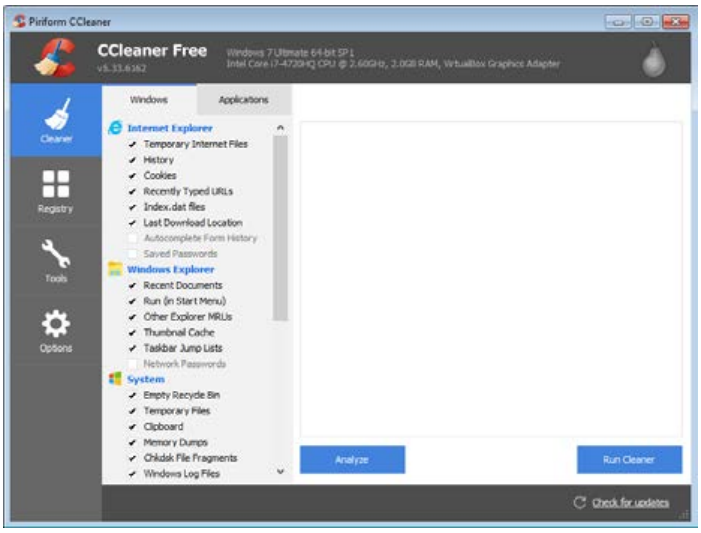


Figure 24. The affected version of CCleaner for the PC

The threat actors behind this attack clearly demonstrated meticulous planning and a high level of sophistication, from the point they illegally modified the CCleaner update file during its build process to their targeted end-result, which was the eventual infiltration of certain high-profile organizations, including Samsung, Sony, and Microsoft. This suggests that they were after invaluable intellectual property.

As of this writing, investigations are still ongoing, and the threat actors remain unknown and quite possibly at large.

Trojanized Elmedia Player file

The Mac malware OSX.Proton used supply chain attacks to infect users twice in 2017. The first time was in May, when a mirror server that distributes the popular DVD-ripping software, HandBrake, began pushing out a malicious copy of said application. Then in October, the Eltima Software website was compromised, and two of its applications, Elmedia Player and Folx, were maliciously modified.

The specially-crafted Elmedia Player program appeared completely legitimate, even when opened. This is because the Trojanized software was a wrapper that contained the legitimate app. So once executed, the player ran in the foreground, appearing normal to unsuspecting users, while the malicious code ran in the background.

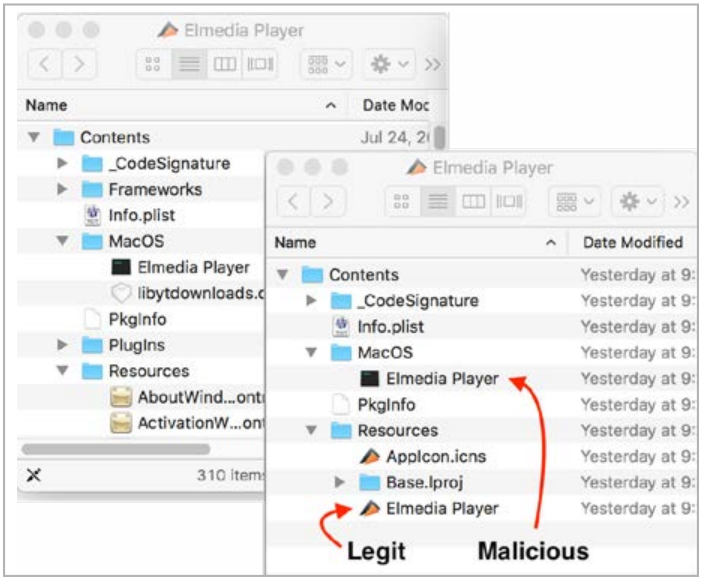


Figure 25. A comparison: the legitimate Elmedia Player and the malicious wrapper

The Proton variant that tainted the Elmedia Player was capable of surreptitiously extracting system keychains, 1Password vaults that contain user passwords, and other sensitive information, such as stored login credentials for those who use browser functionality to remember their passwords. It also went after cryptocurrency wallets, suggesting that it can steal digital currencies like Bitcoin and other data that criminals can use to connect to potentially sensitive resources of the affected user.

Because the primary goal of the Proton malware is to steal credentials of any kind, it is likely these attacks will continue to be perpetrated through compromised accounts. These attacks are extremely easy for people to fall for—including experts.

Geo-targeting

Geo-targeted attacks—where hacker groups or nation states select one location of interest then do everything they can to disrupt, destabilize, or compromise data—continue to be a popular method of aggressively dismantling an opponent.

Over the past few months, we've seen many clinical, methodical pieces of threat execution resulting in chaos for governments, organizations, journalists, and even consumers trying to tune up their PCs.

Magniber (South Korea)

In October, Magniber ransomware became the new payload of choice for the previously dormant Magnitude exploit kit, targeting only systems using Korean language packs, but also factoring in IP address and geolocation to ensure the spread would be as closely confined to the South Korean region as possible.

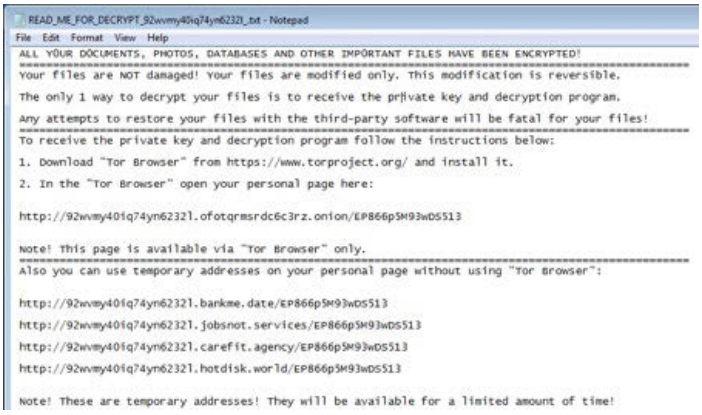


Figure 26. Magniber ransomware

Distributed via malvertising sites owned by the hackers behind the attack, the ransomware tried to encrypt a long list of files including documents, source code, and more. If the file decided the victim was outside South Korea, it would self-delete harmlessly, which is interesting—one would assume hackers would relish the chance for some accidental extra profit, but it seems they weren't interested. This attack was pinpointed on South Korea with a laser-like focus.

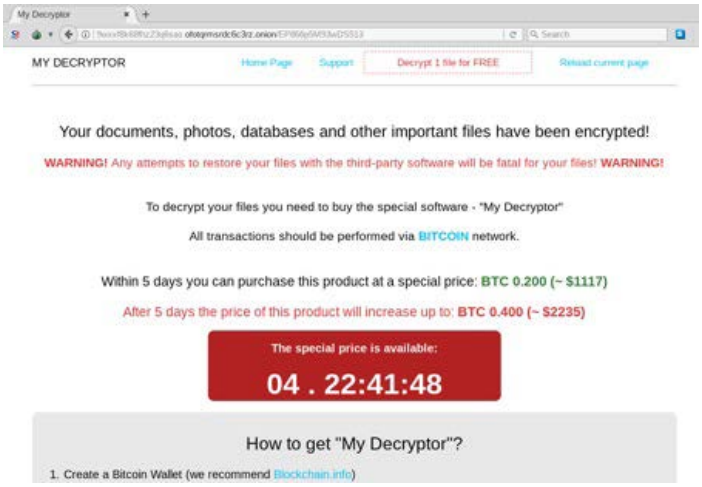


Figure 27. Decryptor for Magniber

Magnitude has had an Asia-centric spread over the last few years, after previously having had more of a worldwide approach to infections. But coming back to life with such a one-track attack is noteworthy, and we wonder who, exactly, had it in for South Korea to such a degree that they would resurrect a dormant exploit kit in such a fashion.

Finfisher (Middle East)

Elsewhere in October 2017, a hacking group with a reputation for espionage, BlackOasis, was found to be targeting organizations and individuals with strong connections to politics in the Middle East, including those in news correspondence, activists, and even members of the United Nations.

BlackOasis lured victims into an exploit trap with email bait that resembled politically-themed office documents. The documents included embedded ActiveX objects, which triggered a Flash exploit and set the trap into motion.

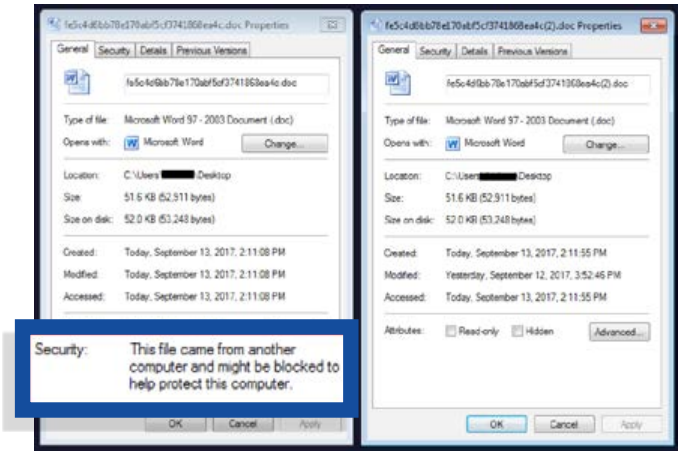


Figure 28. Infected Microsoft Word document

The final payload of the attack was the FinSpy malware, which is typically sold to law enforcement or nation states for the purposes of lawful surveillance. Said files are created by the so-called Gamma Group, though it's not known if BlackOasis has been buying spyware and exploits in bulk from Gamma, or obtaining everything from a variety of different sources.

Much of the end-game for these attacks seems to have been related to oil, and the regions affected all had ties to Saudi Arabia—itself an alleged purchaser of spyware—which muddies the waters still further.

French tech support scams

Multilingual tech support scams have been around for some time, with scammers diversifying into Spanish, German, Japanese, and more in their quest to generate revenue. In 2017, we saw a targeted campaign against French speakers, with operations based in both Quebec and Mauritius.

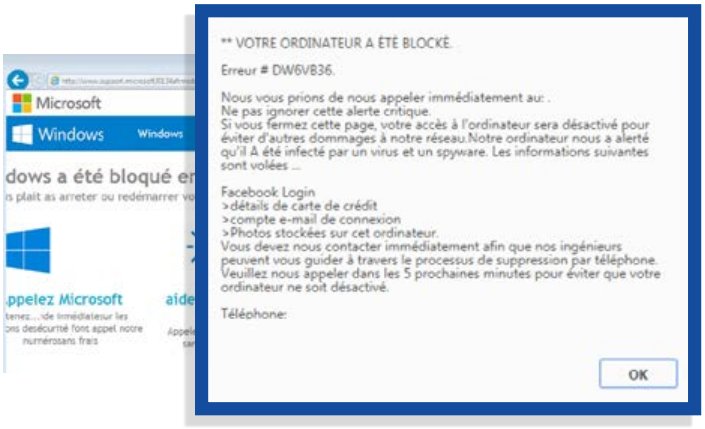


Figure 29. A French tech support scam

As with most popular scams now, the tactics used to steer victims to payment screens involved malvertising and custom-built fake pages leading to operators who spoke fluent French (albeit with a slight accent). Scams along these lines will sometimes give away clues about where they're located—for example, a city name in the URL—but in most other respects, they've done their homework to remain anonymous. Chinese web registrars, hard-to-track toll-free numbers purchased in bulk, and registration information hidden behind proxies are not an uncommon sight.

BadRabbit and NotPetya (Ukraine)

Transport systems including airports and underground railways were severely affected by an outbreak of BadRabbit ransomware in Ukraine in October, demanding £220 for access to be restored to compromised systems. Spread via so-called watering hole attacks (where frequently-visited sites by an organization are compromised and then used to distribute malware), fake Flash installers would install the ransomware when activated.

This relatively simple approach resulted in an encrypted master boot record and a ransom request once rebooted. From there, BadRabbit would spread across networks and cause even more misery for admins, even attempting to brute force its way into any administrative shares it happened to come across.

BadRabbit itself bore a striking resemblance to NotPetya, so called because it's designed to look like the malware actually known as Petya.

NotPetya was infamous for causing chaos across the Ukraine in June, affecting major shipping companies and power outfits, and it's also claimed it contributed to taking down a power grid. Some analysts believe either one or both attacks were launched by Russia, which Russia fervently denies.

The potential for targeted attacks against one region, or individuals working on important resources or intel tied to said region, is huge, and a constant source of exploitation for hackers, nation states, and professional criminal groups.

Exploit kits

Drive-by attacks

The drive-by threat landscape has changed a lot during the past couple of years. 2017 saw further retreat of exploit kit activity, while new schemes emerged among an overall increase in social engineering-based attacks. There are many reasons for these transformations but perhaps the biggest factor is tied to the browser market share and the development of (or lack of) web exploits.

Downfall of exploit kits continues

Exploit kits have lost their appeal for some time. Only a handful were still active in 2017 and used in malvertising chains. Relying on old Internet Explorer and Flash vulnerabilities simply does not provide an efficient way to infect users on a mass scale any longer.

RIG EK remains the most visible and stable exploit kit we have tracked all year long. Following a takedown operation of its domain-shadowing infrastructure, its distributors have made no attempt to revert to using hacked hosting accounts and subdomains as a way to evade blacklisting. It is one of the few (perhaps only) to use IP literal URIs, which makes it easier to spot and block.

Protocol	Host	URL	Body	Content-Type
HTTP	free.joshualanglais.com	/?q=wXbQMvXcJwDQCYbGMvrESLtANknQA0KK2Ir2_dqyEo...	118,619	text/html;charset=UTF-8
HTTP	free.joshualanglais.com	/?yus=souls.87od69.406e1l6n2&oq=vQ9acsfuBQbwrliUKC...	16,433	application/x-shockwave-flash
HTTP	free.joshualanglais.com	/?ct=mart&fix=mart.128ub69.406f4a1f3&q=wXrQMvXcJw...	409,502	application/x-msdownload
		Domain shadowing to IP literals		
HTTP	81.177.140.59	/?q=z37QMvXcJwDQDoTBMvrESLtEMU_OGUKK2OH_783VC...	32,962	text/html;charset=UTF-8
HTTP	81.177.140.59	/?yus=sound.89sc65.406y2q6s3&ct=sound&biw=sound.1...	14,854	application/x-shockwave-flash
HTTP	81.177.140.59	/?biw=april.106al62.406u2n0h2&q=wH_QMvXcJwDPFYbG...	288,768	application/x-msdownload

Figure 30. IP literal URIs

Perhaps because of its prominent place among exploit kits, RIG has been distributing a variety of payloads, including ransomware, which surprisingly is not the most popular payload exploit kits have been dropping throughout the year. (That would be cryptominers.)

One exploit kit that has shown quite a bit of activity is Terror EK. Although its distribution scale is a lot more limited than RIG's, its operators have been tweaking their code consistently and testing out certain features, such as SSL.

EKFiddle v.0.5.3 (Fiddler)

File Edit Rules Tools View Help Links

QuickSave VPN Import SAZ/PCAP View/Edit Regexes Run Regexes Clear Markings Advanced UI on/off WinConfig Replay

Server IP	Protocol	Host	URL	Body	Comments
188.226.179.53	HTTPS	yakset.accountant	/spex.php?[redacted]	413	Terror_EK (Decoy Page)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/picture.gif?dongdong=4934311698	114,990	Terror_EK (IE exploits)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/serve.ebbnhf.popads.net/tihv.doc	4,614	Terror_EK (Flash calls)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/serve.ebbnhf.popads.net/ipha.jng	1	Terror_EK (empty Flash)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/serve.ebbnhf.popads.net/oxey.jng	44,392	Terror_EK (Flash Exploit)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/serve.ebbnhf.popads.net/bzti.jng	18,997	Terror_EK (Flash Exploit)
188.226.180.230	HTTPS	dimplethan.stream	/serve.mfaif.popads.net/vqzn-makei.gif	120,006	Terror_EK (Malware Payload)

Figure 31. Terror EK using SSL

Ad fraud and the mighty Kovter

Ad fraud continues to be a huge problem for advertisers that see much of their ad spending go to waste because of botnets that mimic real users. The gang behind Kovter is notorious for its involvement in this big business, making use of both high profile malvertising campaigns and fileless malware to evade detection.

One such campaign ran on the Yahoo! Ad network and enticed users to download a fake patch for the Firefox browser. The downloaded file was actually JavaScript, which would retrieve Kovter and make it persistent with the Windows registry, leaving few traces behind.

The Kovter group has evolved over time and is well aware of the most effective distribution methods. While it once used exploit kits driven by malvertising, it has devised its own social engineering tricks backed by multiple evasion techniques to infect millions—and yet stay under the radar.

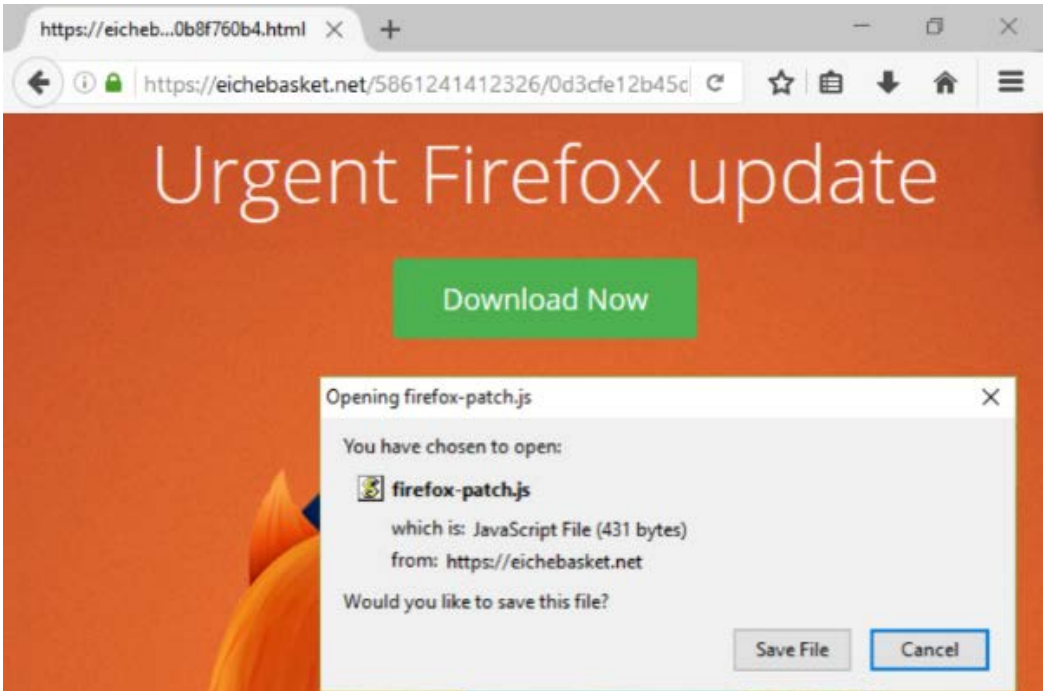


Figure 32. Fake Firefox update

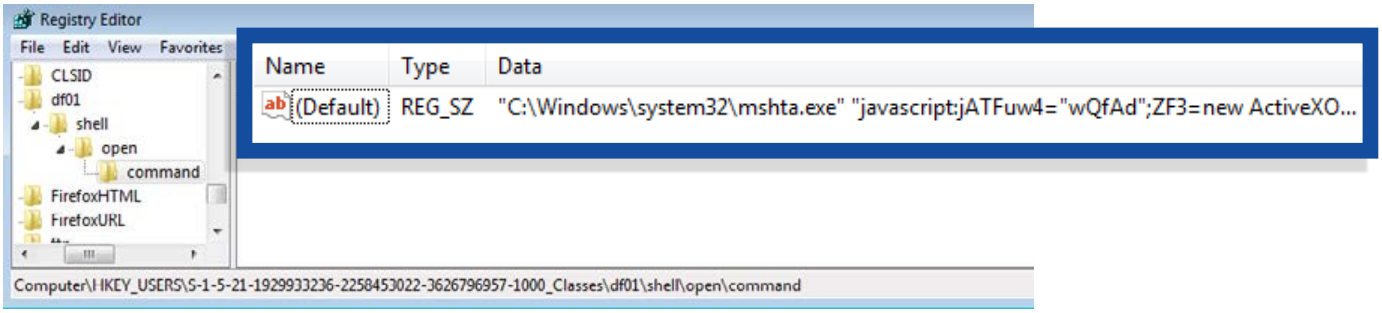


Figure 33. Kovter registry

Social engineering attacks

Perhaps correlated with the slow-down in exploit kit activity, the number of hacked websites redirecting to drive-by download attacks has also diminished. There are still plenty of ways that criminals continue to leverage compromised sites though, and one of them relies on social engineering.

This long-running campaign, which we first coined EITest back in 2014, is not only geolocation aware but also browser-based, serving fake font updates or tech support scams.

By cleverly altering the text on the page and replacing it with bogus characters, crooks give visitors the illusion that they are missing a font to properly display the site's content. Of course, that font installer is not what it's supposed to be, and in many cases turns out to be ransomware, such as Spora.

It's worth noting that hacked websites often distribute more than one payload, and while they may push a browser locker, they could easily be used to host malware, phishing templates, or pharma spam.

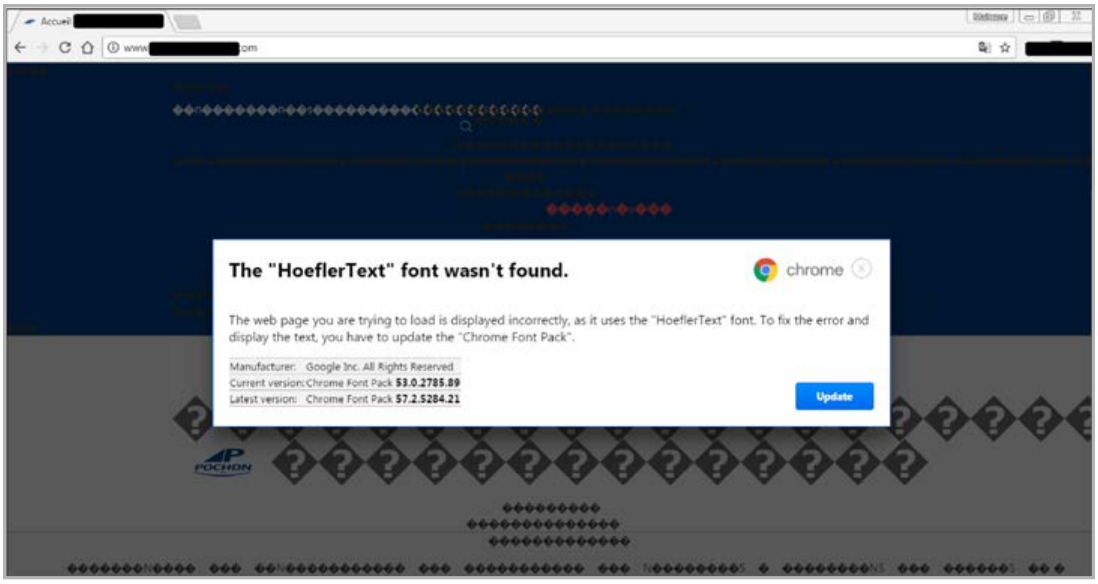


Figure 34. EITest's "missing font" message

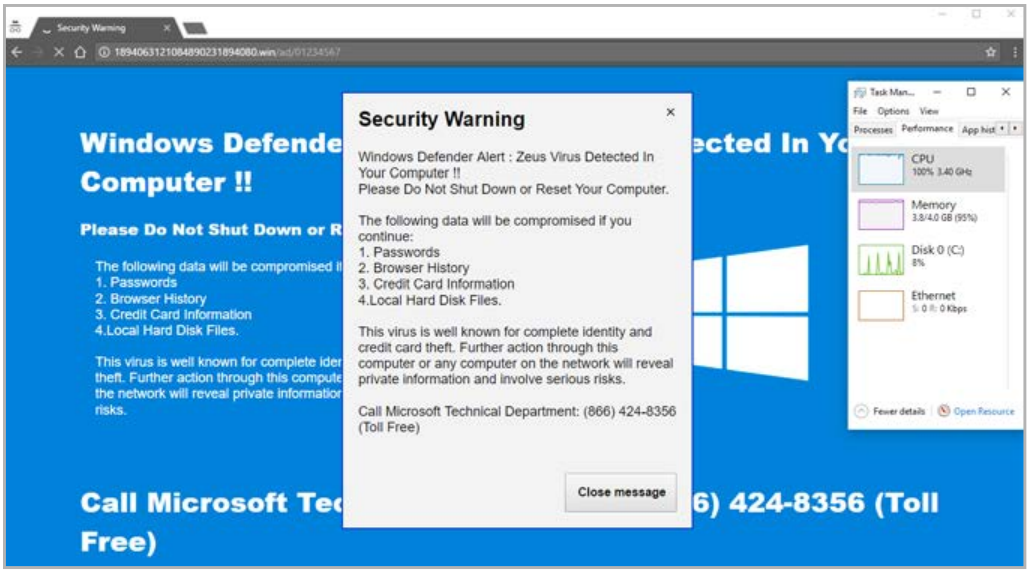


Figure 35. EITest tech support scam

Malspam

Despite a slow start to the year, with a decrease in the number of malware-laced emails due to the unexpected hibernation of the Necurs botnet, 2017 went out with a malspam bang. Attackers were rewarded with a steady stream of usable exploits throughout 2017, and many leveraged email as a vector to launch attacks by the millions.

This year, we also saw an increase in tech support email fraud targeting multiple languages and locales. In addition, we took a trip down memory lane with the large-scale reemergence of an old compression type.

Email delivers malicious documents

While 2016 saw massive attacks using zero-day vulnerabilities that were being used in malvertising attacks and exploit kits, 2017 instead gave us a comparable number of exploitable methods favoring email distribution and targeting Microsoft products.

There has been no shortage of Microsoft Office vulnerabilities allowing for arbitrary code injection of malicious payloads, and attackers wasted no time in leveraging the proven strengths of email to help facilitate the delivery of malicious documents through craftily-worded emails.

Of particular note has been the adoption of vulnerabilities CVE-2017-0199 and CVE-2017-8759 by malware authors to facilitate installation of malicious payloads, with little to no interaction required.

CVE-2017-0199 is a vulnerability targeting a flaw in the olelink object of Microsoft Office, which can cause an http request to be made, and the resulting .hta code executed in response. Malware authors quickly jumped on the vulnerability to send specially-crafted emails containing a variety of payloads. We took an in-depth look at one such example in our Labs blog titled Fake IRS notice delivers customized spying tool.

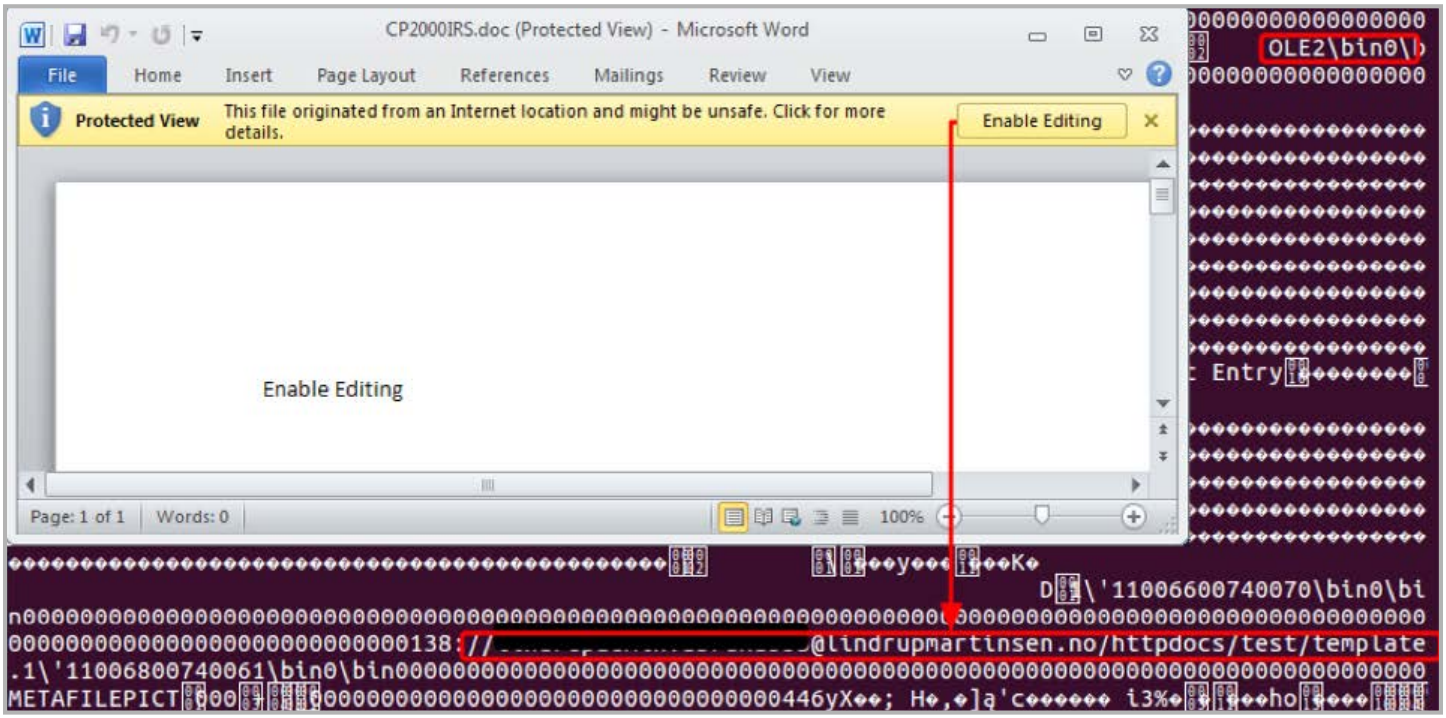


Figure 36. Example of document using CVE-2017-0199

CVE-2017-8759 also caught the attention of attackers with the methodology it uses to automatically download and execute malicious code. This .NET vulnerability allows attackers to take advantage of a flaw in the protection mechanisms of the Web Services Description Language engine. This flaw allows attackers to send well-worded documents that, once opened on a vulnerable machine, can automatically download and install malicious content. We've already seen this exploit deliver the infamous FinSpy malware, and Malwarebytes has a detailed analysis of the attack in our post, Decoy Microsoft Word document delivers malware through a RAT.

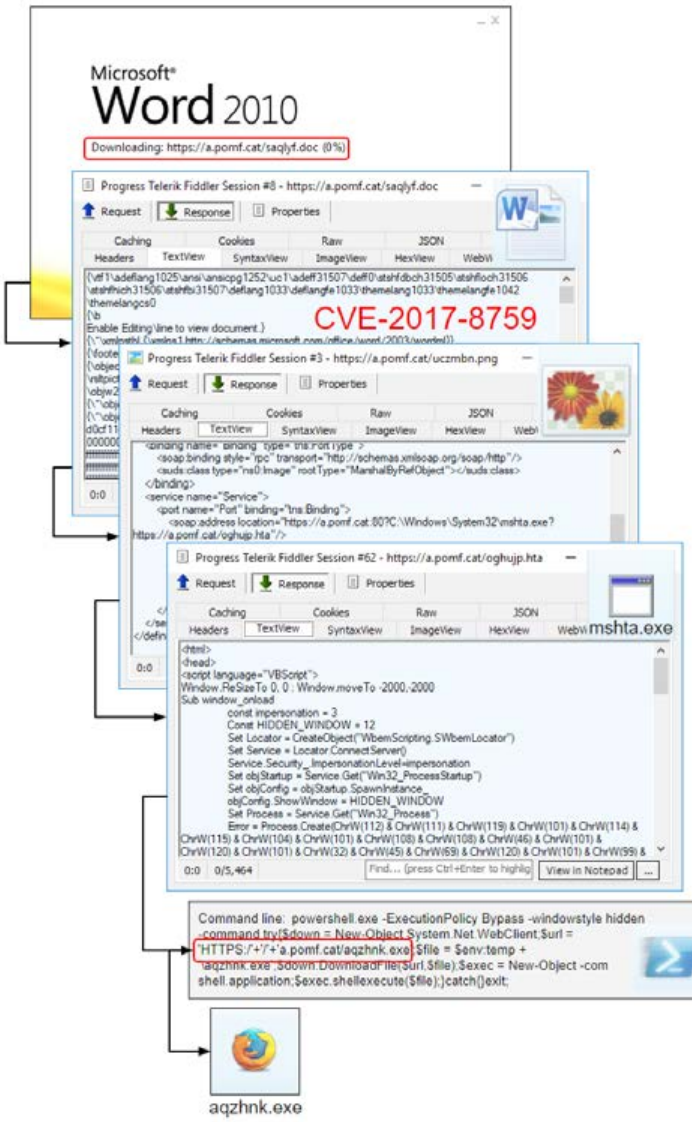


Figure 37. CVE-2017-8759 flow

.ace format makes a comeback

Throughout 2017, spam has been a dominant driving force behind the distribution of malware. Attackers will utilize every known mechanism to facilitate installation of malicious payloads. While this usually includes new and flashy exploits that target vulnerable machines, other times attackers may use old and dated technologies in the hopes of thwarting automated systems and spam detection utilities.

One such mechanism we saw an increase of in 2017 was the use of the .ace archive utility to compress malware payloads into email-friendly formats. While indeed the .ace format has been around for quite some time, the compression format fell from widespread use as more common and easily accessible solutions became available.

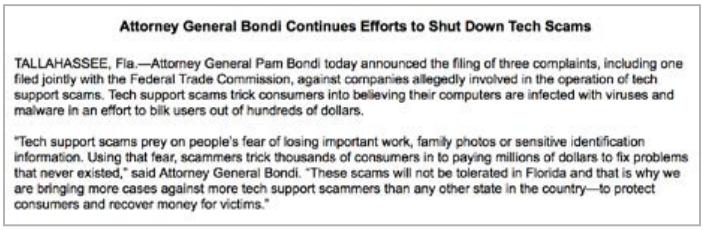
Tools that exist, yet have a low adoption rates, can often be used by attackers to help thwart automation and detection systems, as such systems may not natively support those formats. An oversight in development such as this may be exactly what a malware author needs for successful deployment; so attackers add the methodology to their arsenal.

Scam trends

Scams in 2017 were notable for some moderate successes in enforcement activity, a shift in tactics away from the traditional browser locker, and an upswing in Bitcoin-related content. Overall, as defenders have improved collaborative efforts against scammers, focusing on identifying and eliminating the infrastructure supporting them, scammers have adapted by either shifting tactics toward targeted outbound calling, or developing alternative revenue by standing up infrastructure for other scam groups.

Defender successes

Increased communication between state and federal law enforcement and private industry have resulted in some impressive judgements against scam groups, including at least partial compensation for thousands of victims. Most notably, in August, the FTC obtained $10 million from scam company Advanced Tech Support and created a fund for victims to seek restitution. In addition, state attorney generals have achieved more local successes, helping to create a generally less hospitable climate for these scammers. As a result, US-based scam groups and payment processors serving off-shore tech support have seen a steady decline over 2017. Scam groups have, in some instances, been reduced to relying on physical checks from victims.



Attorney General Bondi Continues Efforts to Shut Down Tech Scams

TALLAHASSEE, Fla.—Attorney General Pam Bondi today announced the filing of three complaints, including one filed jointly with the Federal Trade Commission, against companies allegedly involved in the operation of tech support scams. Tech support scams trick consumers into believing their computers are infected with viruses and malware in an effort to bilk users out of hundreds of dollars.

"Tech support scams prey on people's fear of losing important work, family photos or sensitive identification information. Using that fear, scammers trick thousands of consumers in to paying millions of dollars to fix problems that never existed," said Attorney General Bondi. "These scams will not be tolerated in Florida and that is why we are bringing more cases against more tech support scammers than any other state in the country—to protect consumers and recover money for victims."

Figure 38. Florida attorney general brings more cases against tech support scams

Decline of the browser locker

As consumer sophistication and browser-based defenses make browser lockers less tenable, scammers shifted to new vectors toward the end of 2017, like malicious email and malvertising. Malvertising has been particularly effective over the year due to difficulty in reproducing the attack for analysis, and an unwillingness or inability of the major advertising companies to police the issue. As implementing meaningful security in ad vetting and sales would cause significant revenue decline across the board, we expect malvertising to be a strong vector for delivering TSS into 2018.

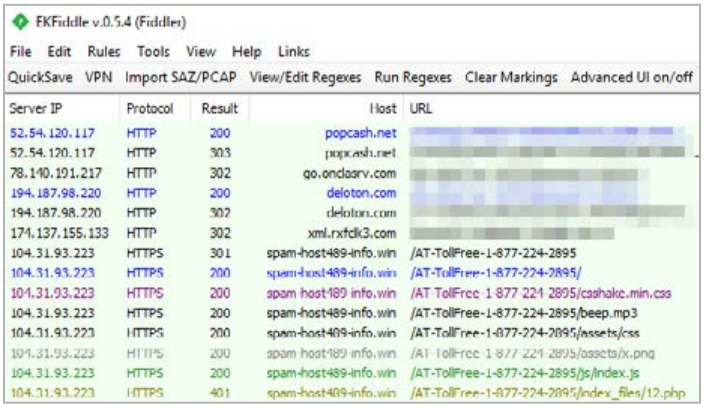


Figure 39. Fiddler EK serves scams

Phishing for TSS

The flood of successful attacks malware authors launched via email has also attracted those in the tech support scam business. 2017 marked an increase in the number of scams originating by email.

Scammers are known to utilize an ever-changing selection of ruses to persuade victims into clicking malicious links. Throughout the year, we have seen email attacks leveraging brand names such as Amazon, Walmart, Walgreens, USPS, UPS, and more.

While the content of the email may change, the purpose remains the same: to entice victims to click the link. Regardless of the method being implemented, users should always avoid contacting businesses that advertise this way.

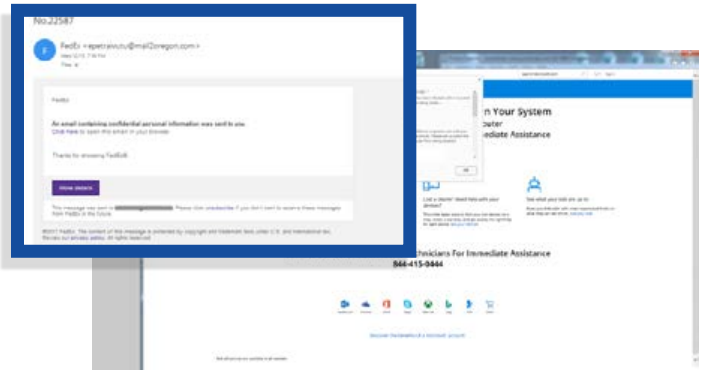


Figure 40. Example of an email containing a notice from FedEx, but leading to a TSS once clicked

Bitcoin: a new challenger enters

As Bitcoin valuations spiked towards the end of the year, tech support scams have turned to impersonating popular exchanges as a next pretext. A scam group targeting Coinbase has been particularly successful, reportedly stealing up to five figures from victims. Using a combination of social engineering and phishing for personal data, scammers have been able to leave customers with much fewer protections and recourses than from losses in traditional investment vehicles.

Figure 41. Bitcoin scam

2018 predictions

The last year has thrown us a few curveballs, with massive ransomware attacks, changes in malware distribution, and the unexpected interest in cryptocurrency miners. Attempting to completely predict the entire year in front of us has never been more difficult. But we figured...what the heck. Here are our predictions for 2018.

Cryptocurrency mining fever will give birth to dangerous new threats.

Our first prediction comes during a period of cryptocurrency fever, where drive-by mining and skyrocketing values are driving interest from both users and criminals alike. If this craze continues, we are likely going to keep seeing an evolution of drive-by mining tools, new mining platforms (such as Android and IoT devices), and new forms of malware designed to mine and/or steal cryptocurrency.

A "slow" year for Internet of Things threats means more attacks in 2018.

In October 2016, we witnessed what could happen when harnessing the power of the Internet of Things with the Mirai botnet. While there was a lack of massive IoT attacks in 2017, attackers have been spending their time focused on developing new tools to take advantage of IoT with cryptocurrency mining, spam-spreading botnets, and likely more DDoS attacks.

It is not farfetched to think we may see DDoS attacks against large organizations, like airline companies and power utilities, demanding a ransom payment to call off an army of botnet-infected IoT devices. Based on the observed decline in ransomware infections toward the end of 2017, likely due to a decreasing return on investment, criminals could continue to utilize the ransom approach, but rather than encrypting files, their attacks will disrupt businesses and their operations until payment has been made.

A continued series of supply chain attacks will lead to new methods of malware infection.

This past year experienced two notable supply chain attacks: the spread of NotPetya through the MeDoc accounting software update process and the compromise of CCleaner software. This will continue to be an avenue that cybercriminals take as long as they can break through the defenses of software development company networks. This may lead to infection through update/upgrade, replacement of legitimate downloads with malware, drive-by exploits, and even database updates for security software.

Malware on Mac systems will take many different forms.

Threats for the Mac have increased drastically over the last few years. The use of script-based malware, supply chain attacks, and an increase in PUP development in 2017 exposed what we are certainly going to see more of in 2018. At the same time, as Mac threats become a more mainstream issue, fake scanners and cleaners will become more commonplace.

Government and private business leaks will lead to more weaponized zero-day vulnerabilities.

The WannaCry attack in May confused many security professionals, primarily due to the unexpected infection method: the utilization of leaked exploit code. Two years prior, leaked exploits from a private security firm made their way into popular exploit kits in the wild. Unless governments and businesses disclose discovered vulnerabilities quickly and publicly, we will continue to unknowingly live in houses made of Swiss cheese.

Conclusion

That's it, folks. The biggest observations, takeaways, and predictions coming from 2017. The cybercrime industry is going through a growth spurt, where many actors are consolidating efforts to create more dangerous threats. However, along with the continued evolution of malware, more and more users are learning how to protect themselves by using software, reading articles and reports, and deploying common security tactics on every system they use. Criminals are unable to profit from their efforts without victims. If we can reduce how many possible victims there are through knowledge and software development, then 2018 might just turn out alright.

Contributors:

- Adam Kujawa, Director of Malwarebytes Labs: Ransomware / SMB exploits / 2018 predictions
- Wendy Zamora, Head of Content, Malwarebytes Labs: Editor-in-chief / Executive summary / adware
- Jérôme Segura, Head of Investigations, Malwarebytes Labs: Exploits / Drive-by mining
- William Tsing, Head of Operations, Malwarebytes Labs: Scam trends
- Adam McNeil, Senior Malware Intelligence Analyst: Malicious spam
- Pieter Artnz, Malware Intelligence Analyst: Cryptocurrency miners / PUPs
- Chris Boyd, Senior Malware Intelligence Analyst: Geo-targeting
- Jovi Umawing, Malware Intelligence Analyst: Supply chain
- Nathan Collier, Senior Mobile Research Engineer: Android
- Thomas Reed, Director of Mac and Mobile: Mac
- Marcelo Rivero, Malware Intelligence Analyst: Ransomware