



# Cybercrime tactics and techniques

## Q2 2017

# TABLE OF CONTENTS

## 01 Executive summary

## 02 Windows malware

- 03 Cerber joins forces with friends
- 03 Locky won't die
- 04 Jaff ransomware: the new kid on the block
- 05 WannaCry
- 06 Petya, NotPetya
- 06 Windows predictions

## 07 Mac malware

- 07 Proton RAT via Handbrake
- 07 Dok malware
- 07 Mac predictions

## 08 Mobile malware

- 08 Mobile predictions

## 09 Potentially Unwanted Programs (PUPs)

- 09 Fireball
- 09 WDFLoad
- 10 PUPs predictions

## 11 Exploits

- 11 SMBv1 troubles
- 12 Exploit kits
- 12 Domain shadowing and IP-literals
- 13 Private kits
- 13 Social engineering variations
- 14 Malvertising distribution campaigns
- 14 Exploit predictions

## 15 Tech support scams

- 15 Tech support scam predictions

## 16 Breaches

- 16 Personally identifiable information
- 17 Financial information
- 18 Breaches in Q2

## 19 Researcher spotlight: Jean-Philippe Taggart

## 21 Conclusion

## 21 Contributors

# Introduction

The second quarter of 2017 left the security world wondering, “What the hell happened?” With leaks of government-created exploits being deployed against users in the wild, a continued sea of ransomware constantly threatening our ability to work online, and the lines between malware and potentially unwanted programs continuing to blur, every new incident was a wakeup call.

In this report, we are going to discuss some of the most important trends, tactics, and attacks of Q2 2017, including an update on ransomware, what is going on with all these exploits, and a special look at all the breaches that happened this quarter.

## Executive summary

If ransomware weren't big enough news already, it went global in Q2 with the WannaCry outbreak that rapidly spread around the world. Although not as sophisticated as its ransomware counterparts, it had an unusual distribution method. WannaCry didn't come via spam or drive-by downloads as one would expect, but instead was propagated via vulnerability in the SMBv1 protocol for which exploits had recently been leaked.

However, WannaCry wasn't the only piece of malware to take advantage of the SMB flaw. Indeed, several other threat actors had already been busy loading Remote Administration Tools and other digital currency miners onto unpatched machines.

In the meantime, the usual suspects such as Cerber were joined by some newcomers in the already bulging ransomware scene. Incidentally, a large Jaff ransomware wave came via spam the day before the WannaCry outbreak, and although it did not gain as much publicity, it continued for multiple days, no doubt impacting many users.

Mac users were kept busy dealing with more malware in Q2 than they had seen in all of 2016. Meanwhile, Android users had their hands full with the continued rise in ad

fraud, where many alluring free apps come bundled with more than what is advertised. This is something already familiar to Windows users dealing with Potentially Unwanted Programs (PUPs) that abuse digital certificates and attempt to disable security applications and are especially hard to remove.

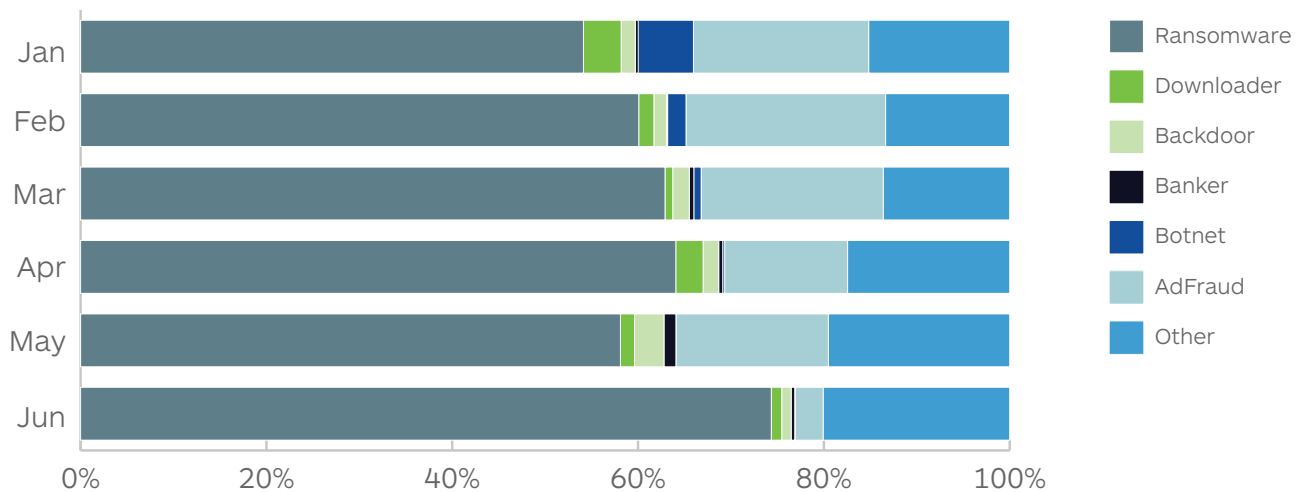
The exploit kit landscape remained fairly quiet but for a few interesting developments. Popular kit RIG EK was disrupted in its use of domain shadowing, resorting to plain IP addresses and relying increasingly on malvertising campaigns for its distribution. Compromised websites were less and less of a factor in EK traffic and strangely even redirected to tech support scams at one point.

Social engineering and scams are still what threat actors rely upon the most. Nevertheless, defenders have been reminded the hard way that exploits can inflict tremendous damage when put in the wrong hands. Just like with data breaches, we can now expect regular leaks of ready-to-use exploits from mysterious groups less interested in cashing in on their trove than watching the aftermath from their release.

# Windows malware

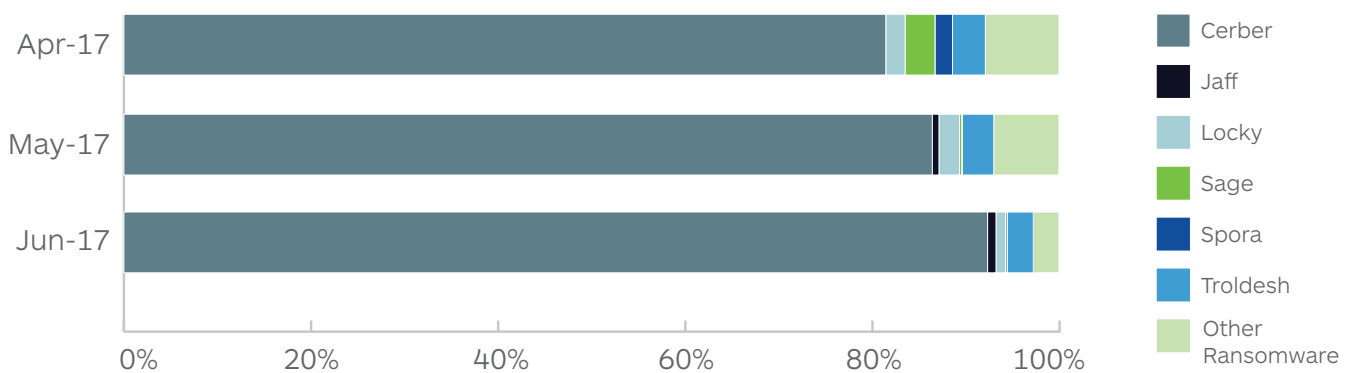
Windows malware has had an interesting quarter. While the majority of threats continued to consist of Cerber ransomware and the Kovter ad fraud Trojan, we also got a look at some interesting ransomware families being distributed in non-traditional ways, for which we can thank the NSA, ShadowBrokers, and some overly ambitious cybercriminals.

Clearly, ransomware continues to dominate the Windows malware scene. Here's a look at the types of malware being dropped by exploits and malspam in the first half of the year.



**Figure 1.** Exploit & malspam drops in 2017 (so far)

With some slight variation month to month, we've been on the same path all year, with ransomware increasingly being used as the go-to malware.



**Figure 2.** Second quarter 2017 ransomware family trends

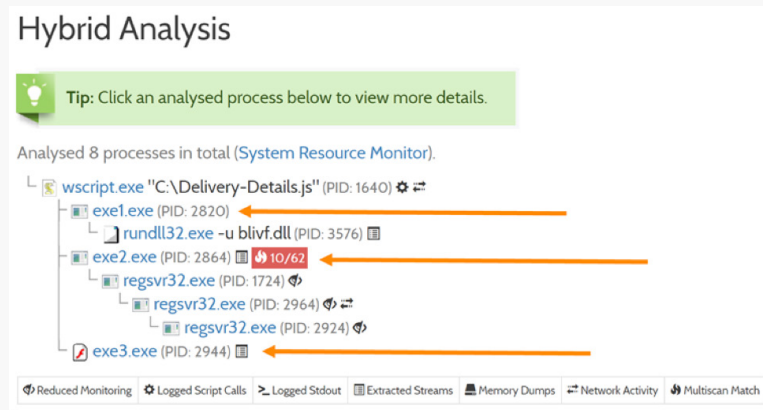
Focusing on ransomware families, Cerber tops the list for the quarter with a massive lead over the next contender, Troldeh (a.k.a. Shade). In third place is Locky, who can't seem to stay dead.

Since we covered Cerber's dominance in the previous two reports, we aren't going to spend much time on it here. Take a look at the Cybercrime Tactics and Techniques 2016 and Q1 2017 reports, as well as the Labs blog for more information.

## CERBER JOINS FORCES WITH FRIENDS

Other than continuing to dominate the threat landscape as the most heavily distributed ransomware since December 2016, it seems that the top dog in malware payloads is joining forces with the second most distributed malware, the ad fraud Trojan, Kovter.

In March 2017, Malwarebytes detected variants of Cerber being distributed along with Kovter, which seemed like a serious threat to users. Not long after, criminals added a third and fourth wheel to the party: Boaxxee (Info Stealer) and Nymaim (Downloader), both Trojans that create backdoors on the system.



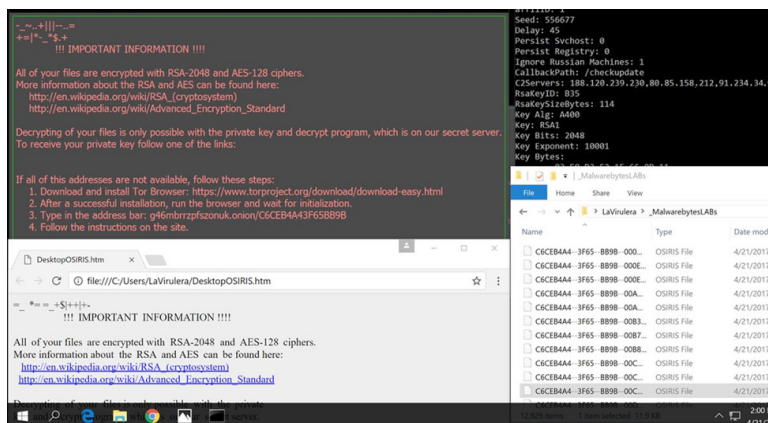
**Figure 3.** Sandbox report of one malicious script dropping three different malware families

During an attack using this method, the victim receives malicious spam with an attachment, probably a Word document. The document is opened and a Macro script is activated, downloading and executing Nymaim, which then identifies whether the victim system is a user or a security researcher, and installs two of the other malware families.

[With all three combined](#), the attack becomes three times as deadly, where users could lose both personal files and login credentials. To top it off, when trying to navigate to a security solution, the browser keeps getting redirected to an ad.

## LOCKY WON'T DIE

One of our predictions for Q1 2017 was that Locky was going to be a huge contender in the ransomware marketplace for a long time. Shortly after, Locky died...or so we thought. Over the last few months, Locky has severely decreased its distribution, failed to be distributed at all, popped back up again, vanished, and popped up again.



**Figure 4.** Locky ransomware seems to return with new C2

Turns out that instead of being abandoned by its creators, Locky simply went dark to continue development. On April 21, 2017, [we observed Locky back at it again](#), this time being pushed through the Necurs spam botnet.

This time, Locky was not nearly as heavily distributed as it was last year. By April 23, we observed Necurs pushing Jaff ransomware instead of Locky. Once again, we assumed Locky was dead, only to be proven wrong again in late June when Locky made another appearance using a new file extension (.loptr) to encrypt files. Turns out this extension has been in use by Locky (with less distribution) since May.

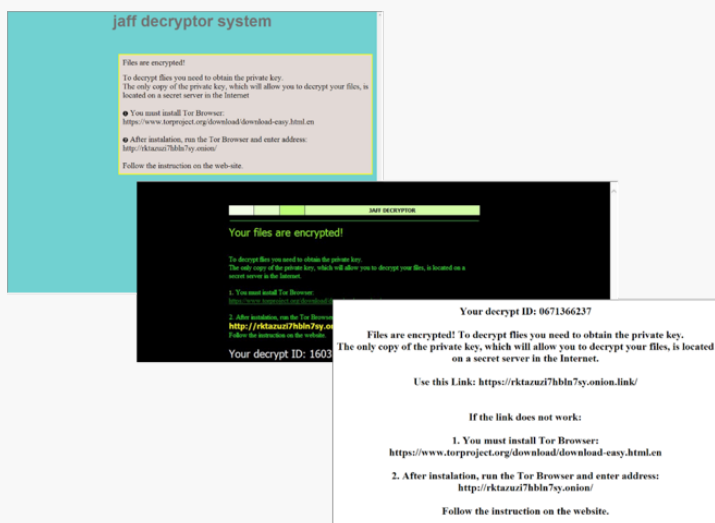
.locky	Feb 2016
.zepto	Jun 2016
.odin	Sep 2016
.shit	Oct 2016
.thor	Oct 2016
.aesir	Nov 2016
.zzzzz	Nov 2016
.osiris	Dec 2016
.loptr	May 2017

**Figure 5. Locky extension history**

One thing we can be sure about with Locky is that its distribution has been severely decreased. What the future holds for this malware is anyone's guess.

## JAFF RANSOMWARE: THE NEW KID ON THE BLOCK

Since its debut in early May 2017, Jaff has had at least three evolutions. Its campaign timing was so perfect (right before WannaCry) and its distribution so heavy that it caused confusion in the security community. Analysts of [Forcepoint Security Lab](#) reported that a malicious campaign to spread Jaff ransomware started on May 11, 2017. Necurs immediately started sending out about 5 million malicious emails per hour. In June 2017, Kaspersky researchers identified a vulnerability in the Jaff code, which made it possible to create a decryptor. However, it's unlikely this will work with future versions of Jaff.



**Figure 6. Jaff ransomware lock screens**

Jaff ransomware looks like Locky. It has the [same distribution via the Necurs botnet](#). It uses the same PDF that opens a Word document with a macro. It even has a similar payment page. Make no mistake, though, Jaff is its own ransomware. And with the backing of the Necurs botnet, it's a very real threat to users and businesses alike.

Jaff is still a threat, and we expect to see more of it in the coming months. However, many security researchers' first exposure to Jaff was as a red herring in the investigation of WannaCry.

ATTRIBUTE	VALUE
Encryption	AES
Ransom \$	2 BTC (nearly \$5,000 as of this writing)
# of extensions attacked	423
Offline encryption	Yes
Encrypted extension	.Jaff
Interesting indicator of compromise	HKCU\Control Panel\Desktop\Wallpaper "C:\ProgramData\userWallpaperR.bmp"
Distribution method	Malspam with blank body and subject including "Payment" or "Receipt"

**Figure 7. Jaff properties**

## WANNACRY

By far one of the more captivating events of the quarter—if not the last 5 years—was the months-long spectacle created by ShadowBrokers and the release of a purported NSA hacking toolkit. The group had the entire security industry on its toes with a barrage of cryptic messages, auctions, and [various releases containing documentation, code](#), and exploits targeting popular versions of Windows and Linux operating systems.

While most of the released exploits had long been patched, one dubbed EternalBlue managed to cause havoc and widespread pandemonium in ways not seen since the Conficker or MyDoom worms.

Similar to other released exploits, Microsoft had issued a patch for EternalBlue (CVE-2017-0144) prior to attackers weaponizing the code, but many IT admins apparently didn't get the memo.

On Friday, May 12, computers across the globe were hit with the WannaCry/WanaCrypt0r ransomware, which used the EternalBlue exploit to cripple machines, leaving companies such as the NHS and FedEx paralyzed in the wake of its destruction.



Figure 8. WannaCry GUI

The malicious actors behind the world's most profound ransomware outbreak failed to capitalize on the opportunity, making critical mistakes that allowed security researchers to shut down the attack before it had a chance to cause what would have inevitably been much greater damage. And while the ransomware made all the headlines, the real story was the underlying SMB vulnerability that allowed it all to happen.

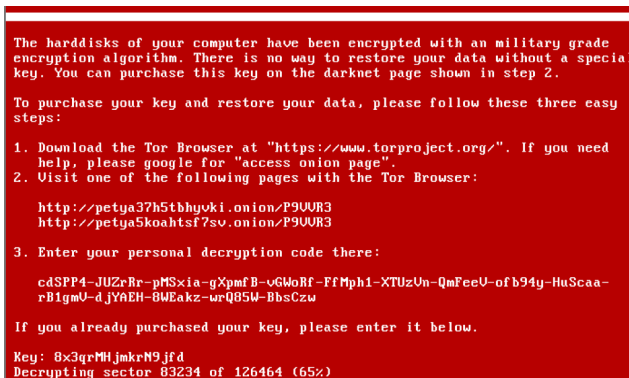
Before the original infection vector of Internet-facing SMB ports being exploited by the ransomware/worm was identified, a lot of folks claimed it was spreading through a malicious spam campaign.

Security researchers spent hours digging through honeypots, inboxes, and forums trying to find the “original infection email” but to no avail. Many thought they had found the WannaCry email when, in reality, the world was under attack by a 5 million mph (mails per hour) malspam campaign from Necurs pushing Jaff ransomware.

## PETYA, NOTPETYA

Just when we thought the Internet was safe from NSA exploits being used by public-facing ransomware, on June 27, new malware that appeared to be inspired by the year-old Petya ransomware showed up on systems all over the world. The malware was spread in large scale, using a mix of different distribution methods that included EternalBlue.

[Petya was a ransomware](#) family that showed up in April 2016. Its main claim to fame was the ability to modify and encrypt the Master Boot Record (MBR) and Master File Table (MFT). In effect, it would redirect the user to a ransom note instead of a normal operating system when the computer was rebooted. This same functionality was duplicated in the [GoldenEye family](#), which we discussed in the [Cybercrime Tactics and Techniques 2016 report](#).



```
The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

http://petya37h5tbhyvki.onion/P9UUR3
http://petya5koahstf7sv.onion/P9UUR3

3. Enter your personal decryption code there:

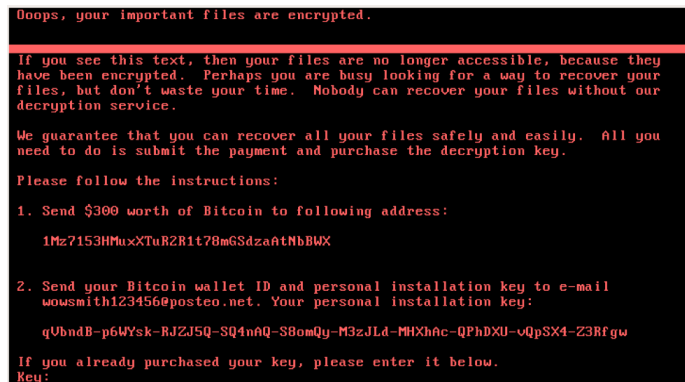
cdSPP4-JUZrBr-pMSxia-gXpmfB-vGwofF-FfMphI-XTUzUn-QmFeeU-ofb94y-HuScaarB1gmU-d_jYAEH-8WEakz-urQ85W-BbsCzw

If you already purchased your key, please enter it below.

Key: 8x3qrMHjmkR9jfd
Decrypting sector 83234 of 126464 (65%)
```

Figure 9. Petya April 2016 ransom screen

The [malware that spread throughout the world](#) on June 27 had a lot of similarities with Petya, including modifications to the MBR and MFT, however there were enough differences to classify it as a completely new family. Kaspersky labeled it “NotPetya,” while a few other names were introduced by different security vendors, continuing the trend of non-standard naming conventions in the computer security world.



```
Dooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaftNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

qUbndB-p6Wysk-RJZJ5Q-SQ4nAQ-S8omQy-M3zJLd-MHXhAc-QPhDXU-oQpSX4-Z3Rfgw

If you already purchased your key, please enter it below.

Key:
```

Figure 10. EternalPetya / NotPetya ransom screen

This malware attack was another instance of the EternalBlue exploit being used in the wild instead of for state-sponsored government espionage missions, which was likely its original intent. (Although as of this writing, the true actors behind the malware and its purpose remain a mystery.) In addition to this malware, we've observed cryptocurrency miners and botnets also infecting systems using the same door that WannaCry opened.

As analysis continues on this malware and the attack, we will continue to keep our users updated through our blog. You can expect a more detailed look at NotPetya in next quarter's report.

## WINDOWS PREDICTIONS

Looking into Q3 2017, we can make a few predictions.

- Cerber will continue to dominate the landscape.
- Jaff is going to make a bigger splash in the ransomware market share.
- We will see at least one more massive attack that leverages leaked NSA exploits against systems in the wild.

We're especially sure of our last prediction because, as of this writing, there are still over a million unpatched, unsecured Windows systems with outward-facing SMB ports online. Unless system and network administrators start updating their systems or at least adding security to block external attacks, we are going to keep seeing the same attack throughout the year.



# Mac malware

In the Mac world, instances of malware are steadily increasing. More new malware families have appeared so far this year than in any other previous year in all the history of Mac OS X, and the year's only half over.

## PROTON RAT VIA HANDBRAKE

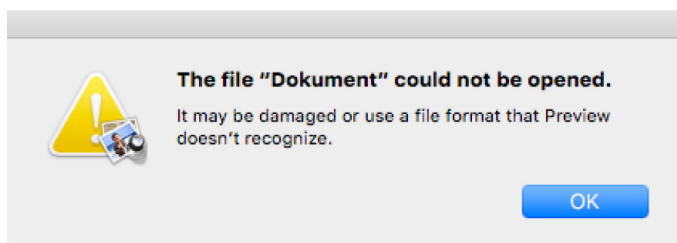
Of the new malware this year, none has been more notable than the infamous Handbrake hack. A mirror server for distributing the Handbrake application—a popular open-source DVD ripping program—was hacked, and on May 2, it began serving up a modified copy of Handbrake. This continued until May 6, when the issue was discovered, but during that time, half of all Handbrake downloads were infected with malware.

The modified version of Handbrake installed a variant of [Proton, a RAT that had been found for sale on cybercrime forums earlier in the year](#). This variant of Proton was focused on exfiltrating password data from a variety of sources, including the macOS keychain, 1Password vaults, and browser auto-fill data.

The most frightening aspect of this event was how many experienced, security-minded people were either infected or nearly infected. This was an apt lesson for Mac users, who are often told that they are safe if they're careful about what they download. If experts can be fooled, behaving cautiously should not be considered the sole necessary security measure in a Mac user's arsenal.

## DOK MALWARE

Another interesting piece of malware was Dok, so named because it masquerades as a Microsoft Word file named "Dokument." In actuality, it is a malicious application and not a Word file at all.



**Figure 11.** Trying to open a Word Dokument

What is most notable about the Dok malware is that it is primarily distributed via email, which is not something that previous Mac malware has used as a primary infection vector. It also comes in many different variants

distributed over a relatively short period of time, each with slightly varying behaviors, which is also unusual in Mac malware.

The Dok malware modifies the system in non-trivial ways: modifying the sudoers file, installing a new certificate as a trusted system root certificate, and routing all web traffic through a malicious proxy server.

This year has also seen the emergence of two different ransomware Trojans: Findzip and MacRansom. Neither was particularly sophisticated or widespread, and neither included any means for saving or transmitting the encryption key. This means that if you were affected and paid the ransom, you would get nothing in return. The hackers behind the ransomware had no way to decrypt your files, reinforcing the importance of never paying the ransom.

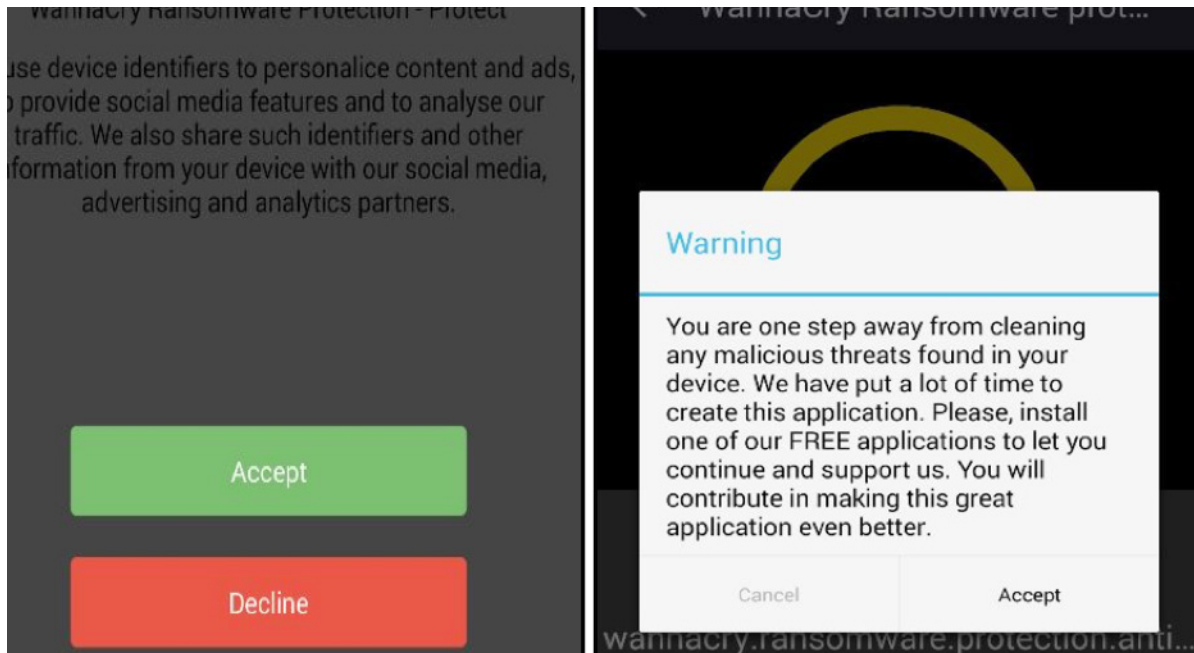
## MAC PREDICTIONS

Every quarter, we see more and more malware created for and targeting Apple operating systems. This quarter was no different and we can expect the same moving through the rest of year.

# Mobile malware

WannaCry made big news this quarter and many wanted to jump on the train, including Android developers. Although, neither the EternalBlue exploit nor the WannaCry ransomware was a threat to Android devices, there were some who wanted to take advantage of the situation.

With the paranoia from Windows users in full effect, it was understandable that users would wonder if WannaCry affected other platforms, too. The creators of one app wanted to make sure you were protected on Android with “WannaCry ransomware protection,” which turned out to be nothing but an app that pushes ads and app installs.



**Figure 12.** Fake Wannacry protection app

For what it's worth, the app does do a rudimentary scan of installed apps, checking permissions and flagging those with “risky” permissions—including itself. What it doesn't do is tell you if you are protected against WannaCry.

## MOBILE PREDICTIONS

This upcoming quarter we expect to see a continued rise in ad fraud. This form of malware uses a victim's device to generate ad traffic resulting in revenue for the app developer. The ad traffic is generated by going behind the scenes without the user's knowledge. Besides being used as a bot, the victim could expect to see increased amount of data usage.

# Potentially Unwanted Programs (PUPs)

Every quarter we observe more obvious malicious behavior coming from the creators of Potentially Unwanted Programs (PUPs). However, some PUP creators have cleaned up their acts, leaving only the truly malicious developers the primary focus of companies that fight against PUPs, like Malwarebytes.

## FIREBALL

A widespread PUP of Chinese origin that made a notable impact was FireBall. This is a typical example of the “malware overkill” which seems to be a trademark of the Adware.Elex family. They have made a name for themselves by using RATs, rootkits, and other serious threats to get clicks for their advertisements. As of this writing, [FireBall is in use as a browser-and-search-hijacker](#), being spread by bundlers. But it deploys the added possibility to use tracking pixels to keep track of the browsing habits of their users.

The bad news is that FireBall has a backdoor capability to download and run additional software on the affected computers. This means that the issuing company (Rafotech) has the option to drop any software they want on the 250 million infected systems. Imagine what would happen if they used that number to perform DDOS attacks or even to infect the machines with some ransomware.

The chances of these scenarios are highly unlikely, because attribution would be easy and the effect on the company would be disastrous. But what if some clever cybercriminal finds a way to take control? The damage could still be done and every finger would point to Rafotech. Either way, it must pay well at an estimated 30 billion fraudulent impressions per minute!

## WDFLoad

[WDFLoad has been an active infection for a while now](#), and especially the last few weeks of the quarter. It is classified as an adware Trojan and injects advertisements into search results and other websites. At least some variants have been found with bitcoin miners wrapped in bundlers such as InstallCube, InstallCore, and possibly Amonetize.

Cryptocurrency miners hijack your computer resources, which in turn uses your electricity, and they profit from it because the infected machine is mining coins for the malware creator.

We have observed potentially unwanted programs like toolbars and bundlers install miners before, but what WDFLoad does takes it out of the realm of shady business practices into criminal action.

Basically, the software does the following to the system:

- Schedules a task that launches a DLL component, which in turn launches a coin miner
- Acts as “clicker” malware, encouraging the user to click on the ads it pushes
- Uses aggressive techniques to block anti-malware’s ability to remove
- It does this by inserting “disallowed signatures” for applications like Malwarebytes and several other AV companies so Windows will not allow them to run.

By using the “disallowed certificates” list, Windows User Access Control (UAC) may pop up a warning informing the user that the program was blocked or the user may get a warning from security software stating it cannot connect to its service.

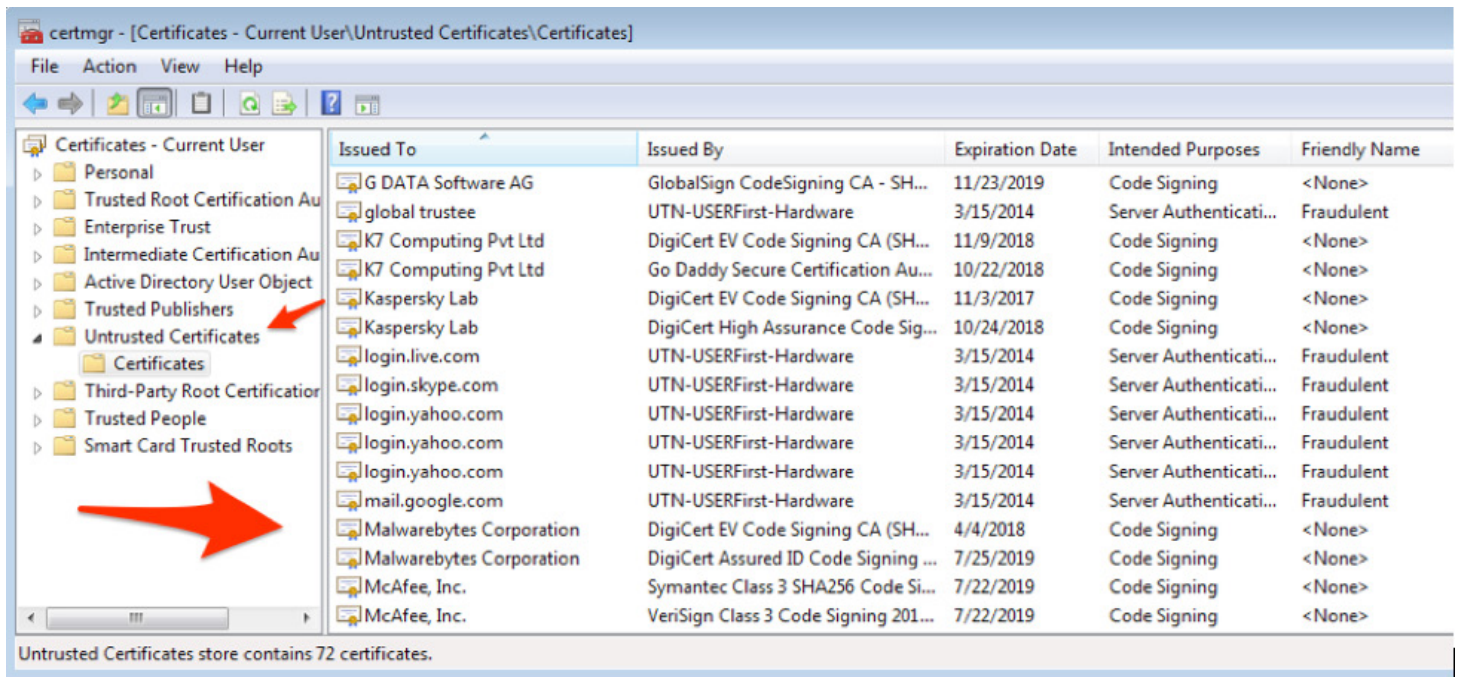


Figure 13. Untrusted certificates created by WDFLoad

Because security solutions cannot launch, the adware cannot be removed. They want to do this because the more clicks they get, the more money they make.

## POTENTIALLY UNWANTED PROGRAMS PREDICTIONS

While legitimate browser developers like Firefox and Chrome are making efforts to tighten security, the adware industry is creating its own custom browsers without any built-in security features and bundling them along with adware applications. They will shamelessly replace your own browser as the default browser and expose you to the greater risks of using such a browser.

We expect to see even closer ties between the potentially unwanted system optimizers and tech support scammers. Given the whack-a-mole game most system optimizers are playing now, they will be looking for a bigger return on investment.

The growing budget in advertising will undoubtedly result in numerous and more advanced developments of adware and ad fraud malware. As some of these companies apparently have the budget and the resources to do so, we may see them use the latest ShadowBroker releases and other vulnerabilities without consequence. We are already seeing the use of rootkits and the manipulation of certificates to block security software, which we also expect to get worse.

What an interesting quarter for exploits! While in general, exploit activity has been shadowed by the use of malicious spam for malware distribution, the leaks made by the ShadowBrokers group allowed criminals to use targeted exploit attacks against vulnerable victims.

## SMBv1 TROUBLES

EternalBlue was part of the collection of tools released by the ShadowBrokers group in mid-April. The dump contained several exploits with ornate names such as EternalRomance, DoublePulsar, ExplodingCan, and EternalChampion—all affecting various Windows protocols and systems.

A number of the disclosed tools were capable of exploiting vulnerabilities in SMBv1 to allow propagation of the malicious code. SMB, also known as Server Message Block, allows applications on a computer to read and write files and to request services from server programs in a computer network. This ability allows for applications to access files or other resources and to read, create, and update files on a remote computer. Furthermore, SMB can also communicate with any server program that is configured to receive an SMB request.

This ability to communicate with any server that is configured to receive an SMB request allows for infected machines to beacon out to other computers on a connected network in attempts to spread the malicious code by exploiting the vulnerabilities in the SMB protocol.

Protocol	Length	Info
SMB	191	Negotiate Protocol Request
SMB	187	Negotiate Protocol Response
SMB	194	Session Setup AndX Request, User: anonymous
SMB	259	Session Setup AndX Response
SMB	150	Tree Connect AndX Request, Path: \\192.168.56.20\IPC\$
SMB	114	Tree Connect AndX Response
SMB	136	Trans2 Request, SESSION_SETUP
SMB	93	Trans2 Response<unknown>, Error: STATUS_NOT_IMPLEMENTED

**Figure 14.** *EternalBlue SMBv1 exploit traffic capture*

The DoublePulsar exploit, also released by ShadowBrokers, played a pivotal role in the spread of the WannaCry ransomware. DoublePulsar is what's called a malware loader and was used to install WannaCry in an elevated state to compromised machines.

DoublePulsar is a Windows kernel Ring-0 exploit. This means that the exploit code runs with the highest privileges possible and can facilitate any modification or addition to the system with ease.

Once executed, DoublePulsar uses an APC (Asynchronous Procedure Call) to inject a DLL into the user mode process of lsass.exe. The code establishes a high-level connection, allowing an attacker to exfiltrate information and/or install additional software to the system.

The combination of these powerful attack mechanisms, along with a well-crafted plan to seek out and identify vulnerable machines, allowed for one of the most vicious and dangerous ransomware strains ever seen to spread across the globe like wildfire.

The quick weaponization of the EternalBlue exploit sparked a national debate regarding the stockpiling of vulnerabilities for use by nation states, and even caused Microsoft President Brad Smith to call for a set of [Geneva Convention-like rules](#) in cyberspace as a means to prevent similar outbreaks. While the likelihood of this remains to be seen, what is for certain is that we haven't seen the end of ShadowBrokers or their release of dangerous code capable of inflicting damage on unprecedented scales.

## EXPLOIT KITS

There has been increased scrutiny on the RIG exploit kit from the security community and several takedown actions in the past quarter. We also continue to observe private kits such as Magnitude EK and Neutrino EK with limited targeting.

One interesting aspect is the trend towards social engineering, which has expanded beyond focusing solely on Chrome users as part of a notable website infection campaign. One surprising case we wrote about was the [numeric tech support scam](#) campaign, which for a while was pushed onto Internet Explorer users instead of trying to infect them via exploits.

## DOMAIN SHADOWING AND IP-LITERALS

RIG is one of the most well-documented exploit kits due in part to the fact that it is the most widespread and easiest to catch. The EK operators have gone through a few URL patterns variations and added a gate to pre-filter against bots.

There was also a concentrated [takedown operation](#) of some of RIG's infrastructure initiated by RSA Research, going after the use of domain shadowing, a technique that has been in use for years and continues to work well.

RIG EK, like other exploit kits, operates on a constantly moving infrastructure, where subdomains—hence the name “domain shadowing”—act as reverse proxies. Threat actors rotate through subdomains to avoid detection by maintaining a large pool of stolen hosting credentials.

While RIG still relies on domain shadowing post takedown, it has been heavily using IP-literal hostnames in Q2.

Host	URL	Body	Comments
185.159.129.240	/?ct=tuesday70w&yus=95rtuesday.70qm105.406x1r6b8&q=wX...	118,642	RIG_EK_URL (Landing Page)
185.159.129.240	/?ct=navigation100u&yus=111mnavigation.97f110.406e6g4i9&...	16,484	RIG_EK_URL (Flash Exploit)
185.159.129.240	/?q=z37QMvXcJwDQDoTEMvrESLtEMU_OFUkk2OH_783VCZv9JH...	375,806	RIG_EK_URL (Malware Payload)

Figure 15. RIG EK traffic

We also see [Terror EK](#) with the same domain-less URI pattern:

Host	URL	Body	Comments
138.197.138.41	/e71cac9dd645d92189c49e2b30ec627a/a0fe71502d686132824...	5,806	Terror_EK_URL (Landing Page)
138.197.138.41	/a0fe71502d6861328241425e4670b712/80673/5932972dc3937	21,796	Terror_EK_URL (IE Exploit)
138.197.138.41	/uploads/ufj.swf	18,074	Terror_EK_URL (Flash Exploit)
46.101.74.81	/d/a0fe71502d6861328241425e4670b712/?q=r4&r=d6a879c9d...	97,904	Terror_EK_URL (Malware Payload)

Figure 16. Terror EK traffic

## PRIVATE KITS

Magnitude EK is, as usual, targeting certain Asian countries and delivering the Cerber ransomware.

Host	URL	Body	Comments
afsc17b5c641.sadlong.com	/1033YQnN0yM963YQnN96yM960YQnN96yM2172YQ...	1,474	Magnigate_Campaign_URL
c4476fz1ez2p6c.ifroute.racing	/	19,078	Magnitude_EK_URL (Landing Page)
c4476fz1ez2p6c.ifroute.racing	/037162088fbp	37,568	Magnitude_EK_URL (Flash Exploit)
c4476fz1ez2p6c.ifroute.racing	/037162088fbp	0	Magnitude_EK_URL
c4476fz1ez2p6c.ifroute.racing	/5a42dce6d2f4c24b8945efbcfa48b3f7.sct	1,218	Magnitude_EK_URL
c4476fz1ez2p6c.ifroute.racing	/037162088fbp	880	Magnitude_EK_URL
46.105.248.150	/c9e682138951a97ae57c420228f234db	65,088	Magnitude_EK_URL
46.105.248.150	/eecd5f99bcc2eda5b781ce1a0827a6f3	334,336	Magnitude_EK_URL (Malware Payload)

Figure 17. Magnitude EK traffic

Neutrino EK is seen here and now, but remains quite elusive in general. It boasts better exploits than most of its counterparts, except for the even stealthier Astrum EK which have seen only a few rare occasions.

Host	URL	Body	Comments
goewpad.ecarefulme.top	/autumn/loose-33053722	882	Neutrino_EK_URL (Landing Page)
goewpad.ecarefulme.top	/2005/05/15/monsieur/associate/friendship/fault-brown-clumsy-jail-blue-se...	95,882	Neutrino_EK_URL (Flash Exploit)
goewpad.ecarefulme.top	/2009/11/21/tumble/control/ball-planet-meanwhile-pursue-concern-daw.html	19,408	Neutrino_EK_URL

Figure 18. Neutrino EK traffic

## SOCIAL ENGINEERING VARIATIONS

The [EITest](#) campaign (which is comprised of hacked but legitimate websites) has been redirecting to several different kinds of exploit kits over the years. However, in this quarter we saw some rather unusual activity. Indeed, in addition to the [HoeflerText](#) social engineering scheme, it also redirected users to tech support scams.

This was a rather puzzling move considering those redirections happened if a visitor was running Internet Explorer, even if outdated and exploitable. This is symptomatic of an exploit kit landscape in search of itself.

The image shows a browser window with a red box highlighting a "Tech support scam pop up" containing the following text:

This virus is well known for complete identity and credit card theft. Further action through this computer or any computer on the network will reveal private information and involve serious risks. Call Microsoft Technical Department: (877) 593-4297 (Toll Free)

Below the browser window, a Fiddler screenshot shows the request headers for a GET / HTTP/1.1 request. The User-Agent is identified as Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko, which is linked to OS: Windows 8.1, Browser: Internet Explorer 11, and Engine: Trident 7.0.

The page content shows a JavaScript injection labeled "EITest injection" that triggers a "Tech support scam URL" pop-up. The injected code includes a function to check for a cookie named "popundr" and, if present, to open a window to a specific URL: http://334565980512304890156510490.win/?a=10013208&offer\_key=...

Figure 19. EITest campaign pushing tech support scams

## MALVERTISING DISTRIBUTION CAMPAIGNS

Exploit kit activity stemmed from various malvertising campaigns while redirections from compromised websites are fewer in between. This is a sign that malvertising remains a top threat especially as it leverages techniques promoted by certain ad networks to bypass ad-blockers, including [RoughTed](#).

Malvertising feeds into specific malware distribution channels that are quite different from each other. However, most tend to do IP filtering for geolocation and blacklisting of known security researchers or crawlers. Some of those campaigns have been around for a long time and evolved, while others are much newer. Figure 20 shows the most common malvertising chains we have been running into for Q2 2017, leading to RIG EK.

Host	URL	Body
<b>Caramella</b>		
ganzerri.me	/click.php?post=indurooups&websiteid=1&quality=10&categoryid=...	0
caramella.fun	/	1
mail.eggperience.com	?q=znzQMvXcJwDQDoTGMvrESLTEMUJQA0KK2OH_76eyEoH9JHT1vrTUSkrttgWC&oq=el-...	118,748
mail.eggperience.com	?q=w3fQMvXcJxvQFYbGMvvrDSKNbNk_WHVIPxomG9MildZuqZGX_k7DDfF-qoV_cCgWRxf...	16,484
mail.eggperience.com	?yus=99smaps.109xv65.406r8a3w8&ct=maps119l&q=w3bQMvXcJx3QFYbGMvvrDSKNb...	303,104
<b>HookAds</b>		
stadiately.info	/banners/uaps	5,707
185.159.129.240	?ct=tuesday70w&yus=95rtuesday.70qm105.406x1r6b8&q=wXnQMvXcJwDQDIBGMvrE...	118,642
185.159.129.240	?ct=navigation100u&yus=111mnavigation.97f110.406e6g4l9&q=zn_QMvXcJwDQDofG...	16,484
185.159.129.240	?q=z37QMvXcJwDQDoTEMvrESLTEMU_OFUJK2OH_783VCz9JHT1yvHPRAP3tgWCeg&o...	375,806
<b>Fobos</b>		
playeve.info	/	35,125
playeve3.info	/mal/?	550
193.124.117.67	?q=m2C9PF5kbNUaAezjfrdc0mttZV14SoauqjLUwULIMaL_ETcUTp1u9CXUbi&q=wXf...	32,759
193.124.117.67	?q=wX3QMvXcJwDQDIBGMvrESLTEMUQA0KK2ir2_dqyEoH9eWnhNzJUSkr6682aCm2&oq...	16,484
193.124.117.67	?q=7QofcsJbYFOVGz3EzSlgRnyYtZUjwwR86msj0mBnR7NidT_yWITygpH_qLIVL14&ct=fr...	103,424
<b>Seamless</b>		
193.124.89.196	/signup4.php	0
185.159.130.85	?yus=108ykill.110jx107.406n8l5a5&oq=hpyYvLLEEbAbliReJfVfizokIB1hH96CrjEcdzRKYh...	118,660
185.159.130.85	?oq=-KLNTaQuwiEHScgxnyIOPB1NG9f2uh0LYyECYhJWG_kSIMAwX9qKWELU92jFJLJTJg&...	16,484
185.159.130.85	?ct=split113d&oq=-LLEEbAbliReJfVfizosIB1hH96CvjEcdzRKYhJTT-ETfaAt19pudfbcg90VT...	156,672
<b>Rulan</b>		
www.ecoredirect.ru	/lan	607
185.159.130.85	?yus=114dfreezy.80xb73.406y1r8m9&q=wH_QMvXcJwDLFYbGMvrESaNBnNkQA0-PxpH...	118,687
185.159.130.85	?ct=split95i&yus=119gsplit.115ko95.406m5d4g6&oq=X8vEsk7tWPwXl2BbRegNpyIkJU1...	16,484
185.159.130.85	?q=znvQMvXcJwDQDoPGMvrESLTEMUzQA0KK2OH_76qyEoH9JHT1vrPUSkrttgWCel3X8&...	217,088
<b>AdultTracker</b>		
tracker.adstrack.host	/c_01skr02s950s093_adult?source=...&ad_campaign_id=...	0
31.41.44.225	?Tech&bahr_fl=4713&session=SwBgmY1fUJ14S_6r8j0SGnxLII2LW-BDfNq4XrJaTHLI-0V6k...	34,162
31.41.44.225	?Mon&help=3887&travel=99oapril.94oj76.406o3o3s1&separamaters=xHvQMxYbRvFFY...	16,308
31.41.44.225	?vel&help=1385&session=gmyPflJ18S_6z8j0WGNxPTIIZPW-BDfNqXrJGTHLU-0vmkyrIVL...	353,792

Figure 20. Q2 2017 Malvertising chains

## EXPLOIT PREDICTIONS

It has been just over a year since the Angler exploit kit vanished, following a series of arrests tied to the Lurk gang. With it gone, we witnessed a decrease in quality exploits and techniques, followed by an overall stagnation.

The cost to acquire new exploits, especially zero-days, seems out of reach for current threat actors evolving in this space. Most of them have actually been reusing code and stealing from each other. However, exploit dumps and leaks are a new reality because of ShadowBrokers, and there is no doubt EK authors are paying close attention to any public release of proof-of-concept code that would help them rejuvenate their arsenal.

It is possible that a critical flaw in a popular browser (not just a plugin) will be leaked and weaponized very rapidly. The exact extent of future exploits has yet to be determined, but if the ShadowBrokers yet-to-be released exploits are of the scale and caliber as we have seen with previous releases, then rest assured we haven't seen the end of this show just yet.



# Tech support scams

In late May, a wave of spoofed Amazon emails hit consumers, claiming to be about a cancelled order. This is a relatively common pitch that has traditionally led to malware. This wave was notable for leading to a tech support scam. Upon clicking the order number, the user was redirected to a compromised site.

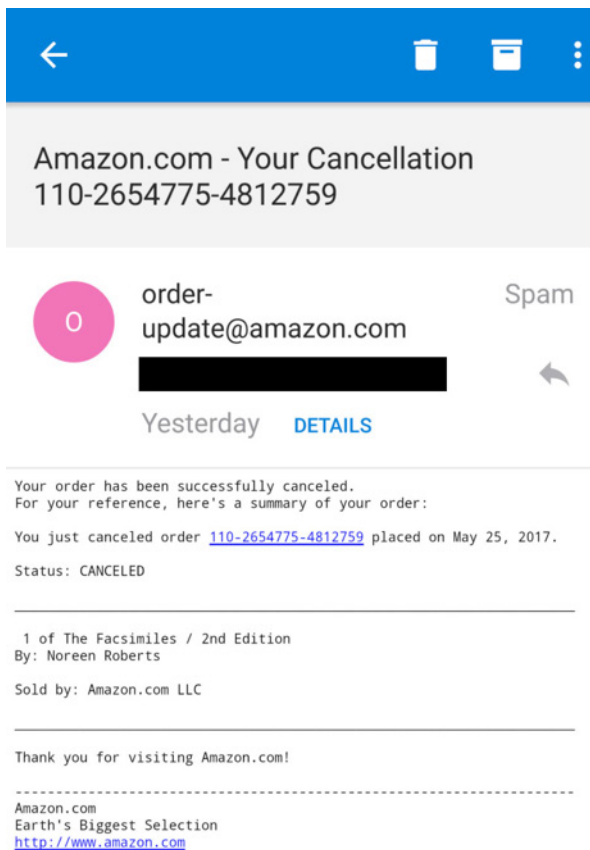


Figure 21. Tech support scammer email phish

The second redirect lands on a (now down) tech support scam site. A look at the infrastructure for the initial hacked site shows a new batch of redirects pushing mostly pharmaceutical spam that coincides with a second wave of fake Amazon emails in early June.

Hostname	First	Last
<a href="#">diet4forweight-loss.com</a>	2017-06-13	2017-06-21
<a href="#">weight-0lospremium.world</a>	2017-06-11	2017-06-21
<a href="#">mygenericsoutlet.ru</a>	2017-05-24	2017-06-21
<a href="#">goodherbvalue.ru</a>	2017-06-20	2017-06-20
<a href="#">clean-diet4you.world</a>	2017-06-13	2017-06-20
<a href="#">diet4forlost.world</a>	2017-06-11	2017-06-20
<a href="#">loss0weight-fast.world</a>	2017-06-11	2017-06-19
<a href="#">fitness-4weight-lossess.world</a>	2017-06-13	2017-06-19

Figure 22. Domains used by tech support scammers

The TTPs on display here are a little unusual, and most likely indicative of a third party renting infrastructure for tech support scammers to use. The general lack of technical sophistication on the part of scammers has been well known for years, and it's unsurprising that other criminals would see this as a business opportunity. We assess the current scam market as having potential to expand into new tactics like these, sold by more technically proficient third parties.

## TECH SUPPORT SCAM PREDICTIONS

We predict that, considering the payment processing crunch outlined in last quarter's report, the more successful scammers will continue to migrate away from outbound calls for lead generation, and towards social media, email, and malvertising. Tech Industry practices make meaningful defense against these vectors almost impossible, so moving scam infrastructure to use them would be a logical progression.

Tech support scams will continue to have a long tail at the bottom of the sophistication scale, almost exclusively due to prominent bargain hosting companies' unwillingness to consider these scams abuse of their services. Twitter will continue to play a significant role in the perpetuation of these scams as well, given their historic inability to deal meaningfully with IP fraud and abuse of link shortening services to serve malicious sites.

Database breaches make up a significant component of the threat ecosystem. Malicious actors search out vulnerable systems using a large number of methodologies and then compromise those systems for the purpose of data exfiltration or ransom. Once systems have become compromised, user databases are collected and then released to the Internet.

Some malicious actors simply do this as a form of entertainment while others have a financial incentive or personal vendetta. Regardless of the motive, the confidential information of companies, purchasers, voters, employees, and applicants are available for the world to see—if you know where to look.

Unfortunately, these leaks occur on almost a daily basis and affect businesses large and small. No database is immune to attack from a curious or dedicated attacker and no one's information is safe from release. Most of us

have probably already had our personal information leaked to the Internet and we don't even know it.

This past quarter was no exception. Databases of organizations large and small were compromised and released to the Internet or offered for sale. The list of compromised organizations is exhaustive, and we could write an entire quarterly report discussing the various attacks and leaks. Instead, we will focus on database leaks affecting (or suspected of affecting) more than 1M individuals, or affecting more than 200 locations.

This report will also exclude the various database vulnerabilities reported by security researchers encompassing potentially hundreds of millions of personal records, yet have not been proven to have been compromised by malicious actors. This includes the Republican voter database reportedly containing 198 million records.

## PERSONALLY IDENTIFIABLE INFORMATION

The personal information of potentially hundreds of millions of individuals has been compromised over the past quarter. This includes names, email addresses, phone numbers, and student records.

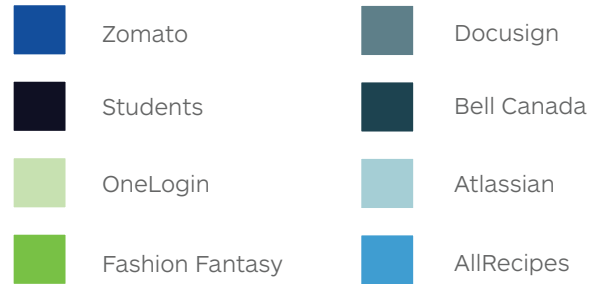
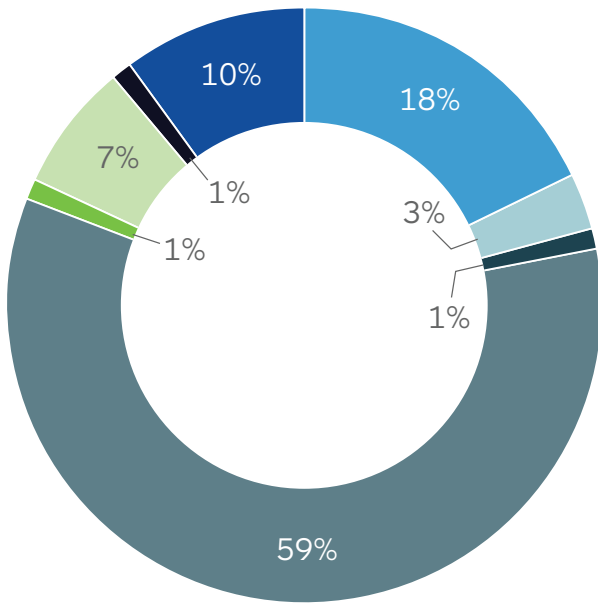
On April 19, [AllRecipes](#), the self-described “food-focused social network” notified users who registered since June 2013 that their email address and password may have been stolen. While AllRecipes has yet to confirm the number of affected users, the site boasts membership totals of more than 30 million.

[Atlassian](#), the makers of the instant messaging service Hipchat, began resetting passwords on April 24 after a possible breach of their systems. While the number of affected users has not been released, the company IPO filing indicates 5 million users.

By far the largest of the compromised databases is [DocuSign](#), with potentially 100 million email addresses being used for spam campaigns. On May 9, the company announced that a malicious third party had hacked a non-core system the company uses to send out service announcement emails.

[Zomato](#) is India's largest online restaurant guide. On May 17, the company announced that user records containing email addresses and hashed passwords were stolen from internal systems. 17 million accounts may have been affected by the breach.

To round out the top 5, on May 31, password management firm [OneLogin](#) reported that an unauthorized individual had gained access to a database containing various stored records. Way back in 2013, the company had 700 business customers and 12 million licensed users. The current number of affected users has not yet been reported.



**Figure 23.** Chart shows percentage of known records over 1M released in Q2

This excludes a number of reports impacting smaller organizations or companies that have yet to release the number of compromised users. This includes [TripAdvisor](#), [BankGiro Lottery](#), and a number of [medical facilities](#). If you think your email might have been compromised, check out <https://haveibeenpwned.com> to find out.

## FINANCIAL INFORMATION

Organizations dealing with financial information and transactions are highly sought-after targets for attackers. Notable attacks this past quarter targeted several large retailers including Kmart, Saber Corporation, and Chipotle.

On April 4th, clothing retailer [Brooks Brothers](#) acknowledged in a Breach Filing to the State of California that systems were compromised and credit card information was possibly stolen. While the company has yet to release total figures, the company operates 220 locations.

Gaming retailer [GameStop](#) acknowledged to Brian Krebs on April 7th that they were investigating a serious breach of compromised credit card information. While the company has yet to release what information may have been compromised or the number of locations affected, the company operates a total of 6,614 stores.

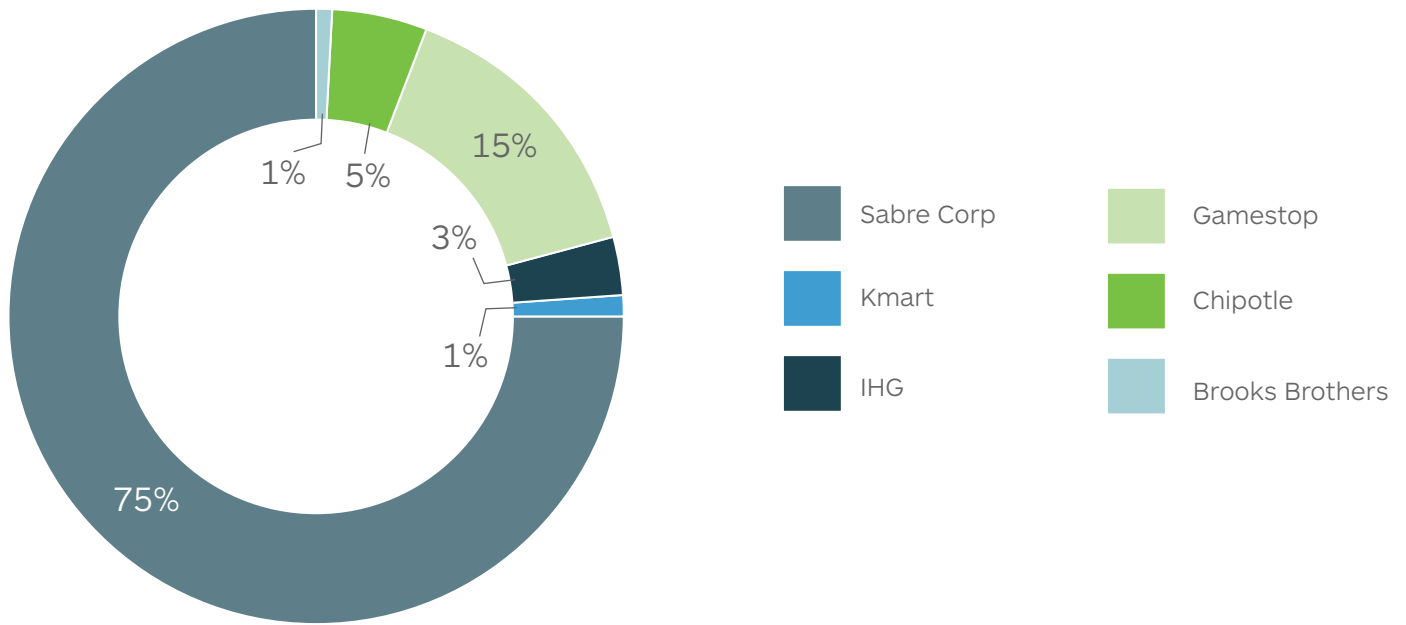
On April 14th, [IHG-branded](#) franchise locations including Holiday Inn and Holiday Inn Express, alerted customers

to a credit card data breach affecting some Point of Sale systems. This attack affects potentially 1,175 locations.

May 1st, travel giant [Sabre Corporation](#) disclosed a significant breach of the payment and customer data systems tied to bookings and reservations. The system serves more than 32,000 hotels and lodging establishments – making this the largest breach of a payment system in Q2.

[Chipotle](#) released notice on May 30th that the credit card information of 2,250 locations may have been compromised in a breach.

And just one day later, [Kmart](#) announced they had found a security breach involving ‘unauthorized’ credit card activity following the some customer purchases. While the company has not yet released total figures, 624 of their famous red and blue are still scattered across the country.



**Figure 24.** Chart showing percentage of financial information released in Q2

This graph also excludes a number of reports affecting smaller organizations. This includes [FAFSA](#), [Scottrade](#), [Full House Lottery](#), [Shoney's](#), and a large number of [car washes](#).

Attacks against infrastructure are a continual battle that enterprises must face, and there is no indication that the attacks are slowing down. Rather, services such as [Shodan](#) make it easier than ever to find vulnerable machines and services, and with the ever-increasing sophistication of attacks, we expect to continue to see these types of breaches released to the wild.

## BREACHES IN Q2

**Figure 25.** Breaches in Q2 2017 with links to relevant articles

<a href="#">OneLogin</a>	<a href="#">TripAdvisor</a>	<a href="#">Waterworks</a>
<a href="#">Atlassian</a>	<a href="#">DocuSign</a>	<a href="#">Brooks Brothers</a>
<a href="#">Concordia</a>	<a href="#">IHG</a>	<a href="#">Full House Lottery</a>
<a href="#">AllRecipes</a>	<a href="#">GameStop</a>	<a href="#">Free Application for Federal</a>
<a href="#">Zomato</a>	<a href="#">Chipotle</a>	<a href="#">Student Aid (FAFSA)</a>
<a href="#">MacKeeper</a>	<a href="#">Kmart</a>	<a href="#">Bowlmor AMF Bowling Centers</a>
<a href="#">Spotify</a>	<a href="#">Shoney's</a>	<a href="#">Sabre Corp</a>
<a href="#">Prairie Mountain Health</a>	<a href="#">Carwashes</a>	



**JEAN-PHILIPPE  
TAGGART**

Senior Security Researcher  
at Malwarebytes Labs

**Q.** Tell us three things about yourself.

**JT:** I like hardware. I like building boxes. I used to be a computer repair technician in a past life and I always liked building bespoke systems. I was deathly afraid of virtualization when that came on the scene. I learned to embrace it eventually, as you need to build pretty beefy underlying hardware to run all these VM's. That being said, I still love wiring switches, running color-coded cables from one system to another. I like the physical aspect of a network.

My battle station is epic. I'm surrounded by monitors and I'm convinced lights dim in my neighborhood when I turn everything on. I find the soft glow of LEDs, the blinking lights of switches, and the low whirr of cooling fans strangely soothing. I love that I have at my disposal tools and environments that would only really make sense to own and deploy if you were a business.

I'm operating system agnostic. Too many people get evangelic about what they use. Linux, MacOS, Windows...it's all just different flavors of the same things. It's challenging to maintain them all, but there are some programs or tasks that just work better in specific environments.

**Q.** What do you like to work on?

**JT:** I like designing environments that are hardened and "safe" to detonate malware. Being able to see exactly what is taking place, what files are modified by the malware, what network traffic is generated, where the malware is trying to reach out to. All these things are fascinating to me. This is a challenging thing to deploy. The bad guys never rest and they're continually innovating. Being able to poke and probe at samples and most of all successfully fooling a tricky piece of malware that actively tries to prevent analysis is an exhilarating feeling.

**Q.** What cool or interesting things have you written about/researched/ discovered?

**JT:** I once successfully deployed a memory acquisition environment on a live system using a firewire card and laptop. The laptop masqueraded as an external drive to have DMA access to the internal memory of the victim system. I thought this was pretty cool, as memory acquisition gives a unique perspective in malware analysis. For a bonus, this was done with pretty much junk hardware I had lying around. Other commercial solutions are super expensive or simply not made available to the general public.

**Q.** What's the biggest security failure you've seen?

**JT:** Witnessing a small business owner having to pay for a ransomware decryption key. This particular individual had no disaster recovery plan and would have had to put the key under the door and close the business as critical data was encrypted. Never in my life was buying bitcoins and acquiring the decryption key a more depressing event. This is the worst-case scenario and the worst possible outcome. Not only did such an event demonstrate the viability of a ransomware attacks to criminals, it is something I never want to have to do again. Needless to say, this particular victim now has multiple backup solutions, as well as a strictly enforced work-only machine policy. I was profoundly uneasy in providing assistance with this ransomware infection, as I am a strong advocate in never paying, but in this case they saw no other solution. Despite successfully recovering most of the data, it felt like a defeat.

**Q.** Advice for newcomers to the field?

**JT:** Air gap. Roll out a completely separate environment to play in. Computers have never been cheaper. Dedicate some boxes to analysis and keep them separate from your personal stuff. It takes discipline, and it adds a cost to deploying a malware lab, but it's worth it. Also, make bare metal backups and test them! If you go in with the knowledge that is a when and not an if, it will make rebuilding from scratch that much less painful. Accept that these are disposable machines that should go from your lab to the bin once their usefulness has been expanded. Be prepared to deal with an outbreak in your lab. No one is perfect, and it is hubris to think you'll never make a mistake.

**Q.** Who are some of your heroes in the industry?

**JT:** It's going to sound super cheesy, but Marcin is my infosec hero. Here is someone who has achieved more in the battle against malware than most, and at such an early age. He has put together an amazing team, who made an amazing anti-malware solution, and I feel very proud to be part of it..

**Q.** What could we do better?

**JT:** Petition our governments to stop hoarding zero-days. The "nobody but us" doctrine has been proven wrong time and time again. Allowing these vulnerabilities to exist unpatched and not notifying the software or hardware vendors for long periods of time only means that they will be independently discovered by others or escape their control. This weakens everyone's security posture and results in widespread infections, such as the recent Wannacry incident.

**Q.** Name your favorite security events and why.

**JT:** Defcon without a doubt. It's an ever-expanding mosaic of everything security related. A melding pot of security professionals, law enforcement, and sometimes also less savory characters! Defcon is a conference that rewards participation. You get what you put in. It's an opportunity to meet amazing people and it never fails to surprise me, even with the recent rapid growth it has experienced. I have walked into talks I would never have thought about attending because the ones I wished to attend were full and discovered passionate presenters and fresh new ideas.

**Q.** Nastiest/cleverest infection you've seen?

**JT:** There are so many to choose from. I would pick the virtualization aware threats as whole family. Any piece of malware that actively checks what environment it is in before detonating presents interesting challenges. Malware authors can do these check in a variety of ways, and it is a fascinating game of cat and mouse.

# Conclusion

What a quarter this was! Two massive global attacks using ransomware combined with leaked NSA exploits, tech support scams all over the place, and more malware than ever before. To a computer security specialist, these are interesting times, however to a regular user, it's likely quite scary.

To calm nerves, it helps to remember that the best way to combat the threats you see online are to use a combination of technological security solutions (antivirus, anti-malware, etc.) and awareness of threats and how to avoid them.

## KEY TAKEAWAYS

- Cerber continued to dominate the ransomware market share for the third quarter in a row
- WannaCry and Petya attacks using the EternalBlue exploit have forever shaken the computer security world
- Jaff ransomware joined the fray, being heavily pushed by the Necurs botnet in early May
- Locky ransomware still managed to make a small dent in the ransomware market share, however it has yet to return to its former glory
- Mac users are dealing with more malware than in all of 2016 and can expect that to continue throughout the year
- The WDFLoad potentially unwanted program modifies trusted certificates on infected systems, disabling antivirus/antimalware software
- The popular RIG exploit kit was disrupted heavily by security researchers following poor practices
- Tech support scams are being pushed through malvertising attacks, bundlers, and toolbars
- Q2 2017 saw a massive amount of breaches, meaning lots of user information is in the hands of the bad guys

## KEY PREDICTIONS FOR Q3 2017

- Cerber will continue to dominate the landscape
- Jaff is going to make bigger splashes in the ransomware market share
- We will see at least one more massive attack that leverages one or more leaked NSA exploits against systems in the wild for malware spreading, distribution, and scams
- More Apple product malware is going to be developed; the end of this year is going to look very different than the beginning if you are a Mac user
- More ad fraud malware will be developed for mobile devices
- Custom adware browsers are going to try and replace legitimate browsers, likely used to push users to tech support scams as well as advertisements
- We expect to see a greater effort to push users to tech support scams using malicious means, such as malvertising

## CONTRIBUTORS

Adam Kujawa – Editor-in-Chief

Wendy Zamora – Editor

Phoebe Tai – Designer

Jérôme Segura – Exploits, Windows malware, Editor

Marcelo Rivero – Windows malware

Thomas Reed – Mac malware

Armando Orozco – Android malware

Nathan Collier – Android malware

Adam McNeil – Breaches, Windows malware

William Tsing – Tech support scams


Tammy Stewart – Potentially unwanted programs


Pieter Arntz – Potentially unwanted programs

Jean-Philippe Taggart – Researcher profile

# ABOUT MALWAREBYTES

Malwarebytes is the next-gen cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against dangerous threats such as malware, ransomware, and exploits that escape detection by traditional antivirus solutions. The company's flagship product combines advanced heuristic threat detection with signature-less technologies to detect and stop a cyberattack before damage occurs. More than 10,000 businesses worldwide use, trust, and recommend Malwarebytes. Founded in 2008, the company is headquartered in California, with offices in Europe and Asia, and a global team of threat researchers and security experts.

 [malwarebytes.com](https://malwarebytes.com)

 [corporate-sales@malwarebytes.com](mailto:corporate-sales@malwarebytes.com)

 1.800.520.2796

 Santa Clara, CA