2017

State of Malware Report

Malwarebytes LABS

TABLE OF CONTENTS

Executive summary

In 2016, we finally saw the headlines catch up with the hype. Cyberattacks and cybersecurity, or a lack thereof, grabbed media attention on both the corporate and consumer sides, even becoming a key issue in the US presidential election. In this respect, you could say that everyone, even those who have never logged on, was affected by cyberattacks and hacking in 2016.

Methodology

We examined data using these:

- Almost one billion malware detections/incidences
- June-November 2016 period unless otherwise noted
- Nearly 100 million Windows and Android devices
- Over 200 countries
- From both the corporate and consumer environments
- Concentrating on six threat categories: Ransomware, ad fraud malware, Android malware, botnets, banking Trojans, and adware

In addition, we used data obtained from our own internal honeypots and collection efforts to identify malware distribution, and not only infection.

Three key takeaways

1. Ransomware grabbed headlines and became the favorite attack methodology used against businesses.
2. Ad fraud malware, led by Kovter malware, exceeded ransomware detections at times and poses a substantial threat to consumers and businesses.
3. Botnets infected and recruited Internet of Things (IoT) devices to launch massive DDoS attacks.

Ransomware rises to the top, targets businesses

In 2016, ransomware grabbed headlines, and for good reason. While traditional malware such as banking Trojans, spyware, and keyloggers requires the cybercriminal to oversee multiple steps before revenue is delivered to their bank account, ransomware makes it a seamless, automated process. Script kiddies (hackers with little or no coding skills) can even buy turnkey ransomware kits known as “Ransomware as a Service” (RaaS) that take all the hassle out of digital thievery. In the fourth quarter of 2016 alone, we cataloged nearly 400 variants of ransomware, the majority of which were created simply by a new criminal group trying to get a piece of the pie.

The trend of ransomware is not new, however, as we’ve watched distribution grow over the last two years and have observed specific families rise to the top of the cybercrime market.

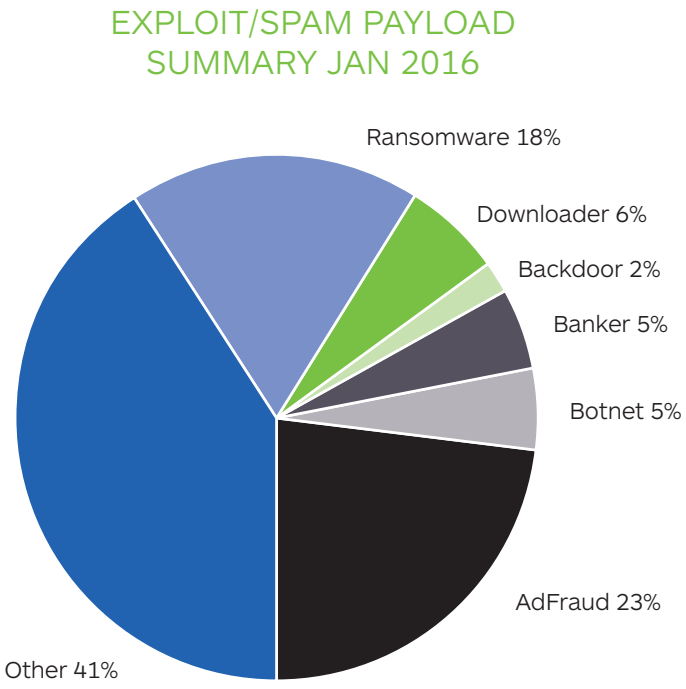


Figure 1. January 2016 payloads.

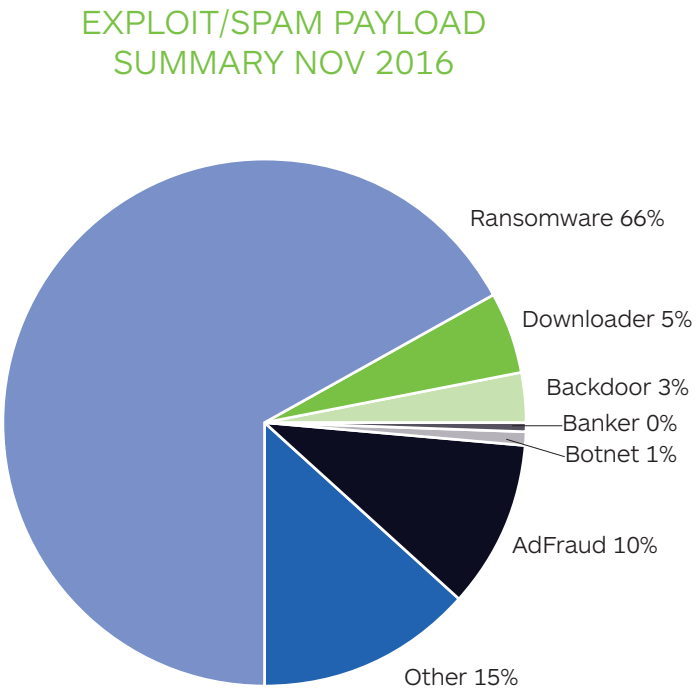


Figure 2. November 2016 payloads.

Ransomware distribution between January 2016 and November 2016 increased by 267 percent. This is an unprecedented domination of the threat landscape—like nothing we've seen before.

Top 10 countries for ransomware detections

1. United States
2. Germany
3. Italy
4. United Kingdom
5. France
6. Australia
7. Canada
8. Spain
9. India
10. Austria

It shouldn't be a surprise that the United States is the country with the most ransomware detections. Many groups from Eastern Europe, as well as across the world, target Americans not only because of the populace's wide accessibility to technology, but also their means to pay the ransom and, possibly, their ideological views.

A country that seems to be missing from this list is Russia. This isn't because Russian citizens have a firm grasp on computer security. Rather, it's an indicator that Russian ransomware developers might shy away from targeting their own.

Ransomware detections by continent

1.	Europe	49.26%
2.	North America	32.51%
3.	Asia	9.84%
4.	Oceania	3.72%
5.	South America	3.67%
6.	Africa	1.00%
7.	Antarctica	0.00%

Top ransomware families in 2016

In 2016, there were three main players in the ransomware game. One of those players dropped out of the race, and the other two continue to compete for dominance.

Top three ransomware families detected

- TeslaCrypt
- Locky
- Cerber

In the chart below, you can see some of the other prominent ransomware families of 2016.

RANSOMWARE FAMILY TRENDS 2016

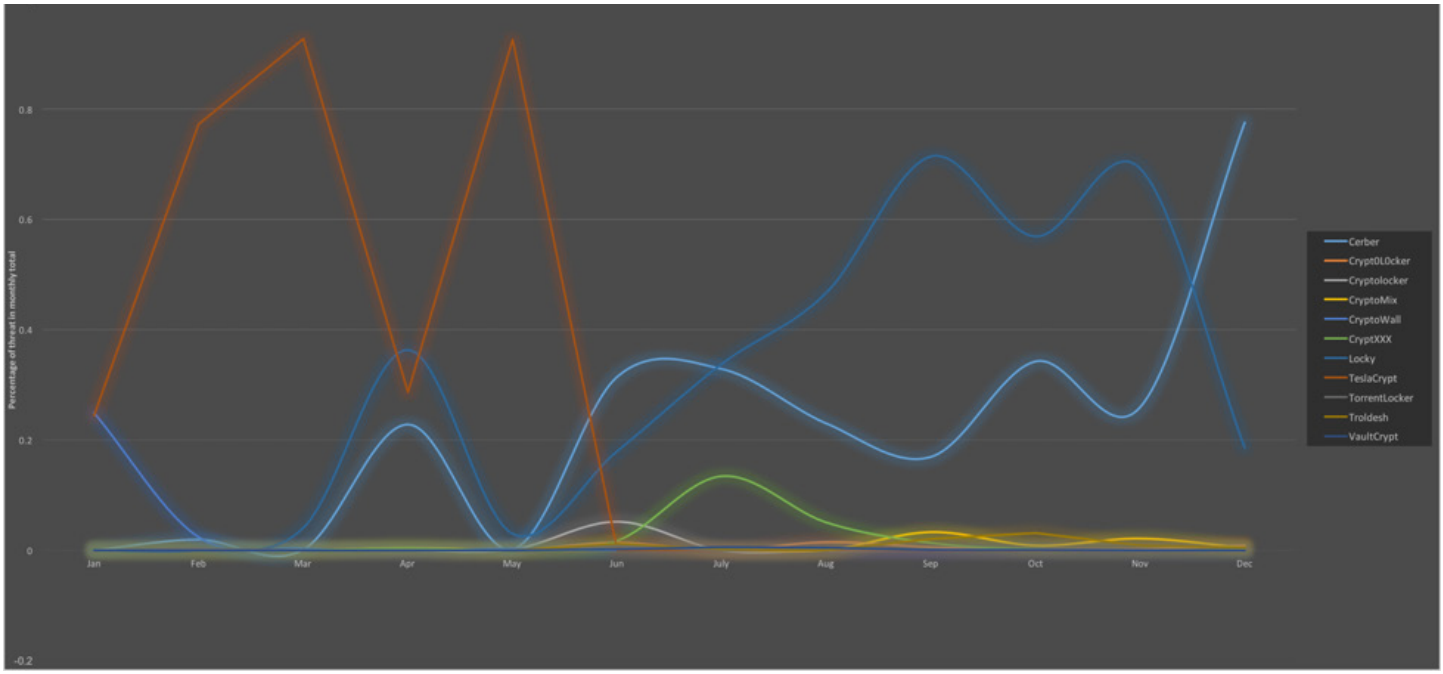
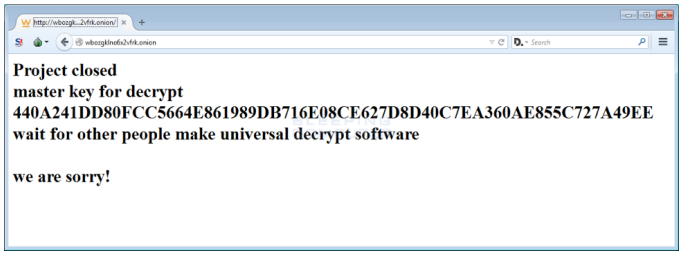


Figure 3. Ransomware family trends 2016.

The beginning of the year showed a huge spike in the use of TeslaCrypt. However, in May TeslaCrypt closed its doors and released the master decryption key for all its victims.


Project closed
master key for decrypt
440A241DD80FCC5664E861989DB716E08CE627D8D40C7EA360AE855C727A49EE
wait for other people make universal decrypt software

we are sorry!

Figure 4. TeslaCrypt closes down. Courtesy of Bleeping Computer

When TeslaCrypt shut down, it created a vacuum that was quickly occupied by two other rising families: Locky and Cerber. It took most of 2016 Q3 and Q4, but these families have managed to make it to the same level of distribution TeslaCrypt had in March and May.

Ransomware detections differ, even in high-incident rate regions, by target

- Eighty-one percent of ransomware detected in corporate environments occurred in North America.
- Fifty-one percent of ransomware detected in home/consumer environments occurred in Europe.

Ransomware cybercriminals concentrated their efforts on businesses, particularly North American enterprises, no doubt realizing that these companies had the most to lose and the resources to pay. Globally, 12.3 percent of enterprise business detections, among the six categories of malware tracked for this report, were ransomware, compared to only 1.8 percent on the consumer side.

Ad fraud malware hits US especially hard

While ransomware has been the dominant malware of 2016, ad fraud malware has also figured prominently. In fact, ad fraud detections, specifically Kovter malware, rivaled ransomware detections during the summer months.

Top 10 countries for ad fraud detections

1.	United States	68.85%
2.	Canada	3.39%
3.	France	3.02%
4.	Germany	2.72%
5.	Italy	2.26%
6.	Spain	2.10%
7.	United Kingdom	1.60%
8.	Australia	0.96%
9.	India	0.90%
10.	Poland	0.84%

Ad fraud malware Kovter, a closer look

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

While Kovter itself is not new, first appearing in 2015, it has historically been used as a downloader for other malware families, a tool to steal personal information, and a backdoor for attackers to gain access to a system.

However, in 2016 we observed it primarily being used as ad fraud malware, which is malware that hijacks the system and uses it to visit websites and click on advertisements in order to create more clicks/hits for an ad campaign (known as click-jacking) run by either the criminals behind the Kovter deployment or their clients. In addition to the novel use of the malware, Kovter distribution also changed in 2016. While Kovter was previously spread primarily through drive-by exploits and exploit kits, we saw a massive surge in malicious phishing emails being used as well.
This change in distribution, combined with the fact that the US population was a preferred target for Kovter distributors, made Kovter one of the biggest threats of 2016 for Americans more than anyone else.

Distribution of Kovter detections by country (top five)

1.	United States	68.64%
2.	Germany	2.58%
3.	Canada	1.65%
4.	France	1.34%
5.	Italy	1.30%

Kovter's change in methodology and distribution is significant because it mirrors the trends we're seeing with surges in ransomware: Kovter and ransomware both provide a source of direct profit for the attackers. Rather than selling password dumps, credit card information, and social media accounts to other criminals, these attacks demand payment from victims directly to retrieve their important files or use the victims to defraud the advertising industry, resulting in more profit for less effort.

Botnets leverage IoT devices to wreak havoc

Botnets (a network of private computers infected with malicious software and used to send spam) have been one of the most commonly developed mechanisms for deploying malware for the past 10 years. This is due to a botnet's small size, ability to hide, and ability to execute an innumerable amount of operations.

This year, we saw a new botnet tactic: compromising, infecting, and recruiting IoT devices, such as Internet-connected thermostats or home security cameras, to become part of the botnet. The most popular IoT-focused botnet of 2016 is known as Mirai, an open-source malware that infects devices and takes commands from a Command and Control operator. In late September, a massive attack used the Mirai botnet to compromise many IoT devices and home routers, with all of the infected devices taking orders

from a single source. Once the army of bots was assembled, the attacker used a Distributed Denial of Service (DDoS) attack to bring down several prominent websites.

A month later, Mirai was used to attack one of the backbones of the Internet, Dyn, and in doing so prevented millions of users from accessing popular sites such as Twitter, Reddit, and Netflix. One of the key features of Mirai was not only scanning the Internet for connected devices but also using an internal database of default username and passwords to gain access to the devices. After gaining access to the device and infecting it, Mirai is able to launch DDoS attacks against any target the operator wants.

Asia and Europe saw an increase in variants developed from popular botnet families. For example, the Kelihos botnet grew 785 percent in July and 960 percent in October, while IRCBot grew 667 percent in August and Qbot grew 261 percent in November.

Distribution of botnet detections by continent

1.	Asia	61.15%
2.	Europe	14.97%
3.	North America	12.49%
4.	South America	6.56%
5.	Africa	4.32%
6.	Oceania	0.51%

Germany dealt with a substantial botnet problem. The country saw a 550 percent increase in the amount of botnet detections from 2015 to 2016.

Cybercriminals change tactics with malware distribution

One of the biggest changes in distribution in 2016 was the use of attached scripts to phishing emails. These scripts usually reside inside of a ZIP file and, once opened and launched, reach out to a remote server to download and install malicious software on the system.

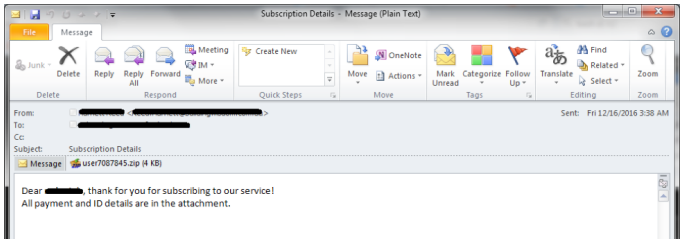


Figure 7. Malicious phishing email with ZIP file attached.

Another method that became popular again in 2016 included the use of macro scripts inside of Microsoft Office documents (.docx, .xlsx, etc.), which would execute once the user opened the document and enabled macros. Using social engineering tactics, the attackers coaxed the user into enabling these features, which would also download and execute malware on the system. Building on top of this preexisting method of infection, attackers have added sophistication by sending protected ZIP files and Office documents, including the password in the phishing email. This gives an increased sense of legitimacy to the attack, as well as being an effective method of defeating automatic analysis of the attack email by malware research tools, including honeypots and sandboxes.

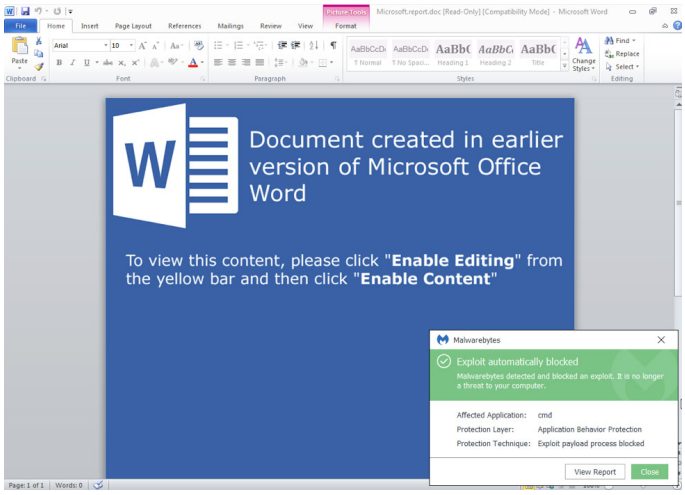


Figure 8. Malicious Word document using social engineering to get the user to enable macros.

There was a huge increase in the use of macro scripts over exploit kits in June. This was because Angler, one of the major exploit kits of 2015 and early 2016, shut down its operations. However, RIG exploit kit is rapidly taking the place of Angler, and we are likely to see more of it in 2017.

Android malware gets smarter

Over the last few years, the mobile threat landscape hasn't changed much. Android malware creators are primarily still playing catch up to the malicious functionality found in modern Windows desktop malware, which can be difficult when it comes to the Android operating system.

However, a notable trend in 2016 was the increased use of randomization used by malware authors in an attempt to evade detection from mobile security engines. This has resulted in an increase in the amount of Android malware being detected.

Figure 9. Android ransomware.

Distribution of Android malware detections by country

1.	United States	12.74%
2.	Brazil	9.95%
3.	Indonesia	6.54%
4.	India	5.04%
5.	Spain	4.60%
6.	Philippines	4.25%
7.	France	4.24%
8.	Mexico	3.87%
9.	United Kingdom	3.59%
10.	Italy	2.79%

Interestingly, Brazil, Indonesia, the Philippines, and Mexico made the top 10 countries for Android malware detections. The high prevalence of Android malware detections in developing countries can be attributed to the extensive use of relatively unsecured third-party app stores in those countries.

Malware attacks vary by nation and geography

Our data showed regional differences in attack methodology and malware used. Unsurprisingly, US- and Europe-targeted attacks were highly differentiated. The United States recorded the most malware detections and leads all countries in the detections of every category charted, except for banking Trojans, where Turkey leads.

Among the malware categories examined in this report, Europe is the most malware-ridden continent and saw 20 percent more infections than North America and 17 times more than Oceania.

- Europe leads all continents in ransomware: 49 percent of ransomware detections were from Europe-based devices.
- Europe leads all continents in Android malware: 31 percent of Android malware detections were from Europe-based devices.
- Europe leads all continents in adware: 37 percent of adware detections were from Europe-based devices.

European malware sets its sights on France, the United Kingdom, and Spain

The countries hit hardest by malware in Europe are France, the United Kingdom, and Spain—although the Vatican City saw the steepest rise, with a 1,200 percent increase in all malware variants during this time period.

The United Kingdom was the second-most targeted country in Europe for all types of malware behind France. In the six-month period of our study, the United Kingdom saw almost twice as many incidents as Russia. Germany is the second-most impacted country by ransomware, following the US, supporting the theory that malware authors use Germany as a testing ground for their wares before wider distribution. Meanwhile, Russia was disproportionately under-impacted by ransomware but remains a popular target for banking Trojans.

2017 predictions

Ransomware

It is possible that, with the major ransomware players taking the main stage at the end of the year, we are unlikely to see many, if any, new advanced ransomware families enter the market with the sophistication and mass penetration of Cerber and Locky. Many of them will be quickly developed just to take advantage of ransomware's popularity amongst cybercriminals.

This is a continuation of a trend started in 2016. Nearly 60 percent of the ransomware variants detected in the last six months of 2016 were less than one year old, further driving home the fact that most ransomware in existence today is developed by newcomers to the ransomware industry.

We may see more variants that modify the infected computer's Master Boot Record (MBR), which is a key part of a system's ability to boot into its operating system. Once modified, the system will boot into a lock screen set up by the malware, demanding payment not only to decrypt files but also to restore access to the main operating system. The addition of this functionality reduces the options for a victim to two: either pay the ransom or have the system wiped completely.

Malware distribution

Over the years, we have observed only one stable truth of malware development: distribution through email. Phishing attacks, including malicious attachments, had a big comeback in the second half of the year. However, we predict that exploit kits (RIG specifically) are likely to become the standard for malware distribution again in the very near future.

We will not see malicious phishing attacks disappear. Due to the new developments in the download and installation of malware originating from phishing emails, as well as the use of macro scripts in Microsoft Office documents, this method of attack will continue at steady levels throughout the rest of the year, likely with increased sophistication.

Internet of Things (IoT)

The surge of new cyberattacks leveraging IoT devices, coupled with a lack of concern for security on the part of the IoT industry, has resulted in botnets like Mirai being able to take down the backbone of the Internet. Despite what the IoT industry decides to do—batten down the hatches or ignore security altogether—the doors have been opened by malware like Mirai for new IoT attack strategies in 2017.

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

 corporate-sales@malwarebytes.com

 1.800.520.2796