KASPERSKY lab

Attacks with Exploits: From Everyday Threats to Targeted Campaigns

www.kaspersky.com
#truecybersecurity

GREAT Global Research & Analysis Team

Contents

Introduction and Key Findings

An 'exploit' is a computer program created to take advantage of a security vulnerability in another software program. Exploits provide malicious actors with a way of installing additional malware on a system. They are an integral part of the cyberthreat landscape because the vulnerabilities they prey on are a fact of life.

Software products comprise many thousands or even more lines of code and there will inevitably be gaps or errors that can be targeted with an exploit. Some vulnerabilities take years to come to light – changing hands for vast sums on the underground market, or hoarded by threat actors who use them to devastating effect. The most prized of these are the unknown and unpatched 'zero-days'. Other vulnerabilities are known, and patched, and yet remain active and destructive for years, integrated into popular exploit kits or able to breach systems that have not been updated.

Attacks conducted with help of exploits are among the most effective as they generally do not require any interaction from the user, and can deliver their dangerous code without the user suspecting anything.

In order to protect a home or corporate network from the most devastating exploit-assisted attacks, it is important that people understand the applications that the attackers (from regular cybercriminals to targeted attackers) are most likely to go after.

This report therefore comprises two sections.

Part I examines the top exploits and the most vulnerable applications affecting users over two 12 month periods, in 2015 and 2016. It also looks at the same landscape from the point of view of Automatic Exploit Prevention technology – a patented Kaspersky Lab technology designed to identify and block unknown exploits such as zero-days, or known but heavily obfuscated exploits.

Part II homes in on the big targeted threat actors and their use of vulnerabilities. For this part we've made an exception and focused on a significantly longer period of time: from 2010 to 2016.

The information sources for this report include, for Part I: depersonalized threat information processed by the Kaspersky Security Network, as well as publicly available information. Part II is based on Kaspersky Lab threat intelligence reports released in the last six years, as well as publically available information.

The aim of this report is two-fold:

1. To raise awareness of the power and endurance of vulnerabilities and their associated exploits – and the corresponding need to implement robust security and software updates.
2. To highlight to customers and corporate users the applications which should be monitored, and about which users should be especially cautious.

Key Findings

Part I – Exploits' Appearance and Attacks 2015 and 2016

- In 2016 the number of attacks with exploits increased 24.54%, to 702,026,084 attempts to launch an exploit.
- 4,347,966 users were attacked with exploits in 2016 which is 20.85% less than in the previous year.
- The number of corporate users who encountered an exploit at least once increased 28.35% to reach 690,557, or 15.76% of the total amount of users attacked with exploits.
- Browsers, Windows, Android and Microsoft Office are the applications exploited most often – 69.8% of users encountered an exploit for one of these applications at least once in 2016.
- In 2016, more than 297,000 users worldwide were attacked by unknown exploits (zero-day and heavily obfuscated known exploits).

Part II – Exploits and the Targeted Attackers, 2010–2016

- Overall, targeted attackers and campaigns reported on by Kaspersky Lab in the years 2010 to 2016 appear to have held, used and re-used more than 80 vulnerabilities. Around two-thirds of the vulnerabilities tracked were used by more than one threat actor.
- Sofacy, also known as APT28 and Fancy Bear seems to have made use of a staggering 25 vulnerabilities, including at least six, if not more zero-days. The Equation Group is not far behind, with approximately 17 vulnerabilities in its arsenal, of which at least eight were zero-days, according to public data and Kaspersky Lab's own intelligence.
- Russian-speaking targeted attack actors take three of the top four places in terms of vulnerability use (the exception being Equation Group in second place), with other English- and Chinese-speaking threat actors further down the list.
- Once made public, a vulnerability can become even more dangerous: grabbed and repurposed by big threat actors within hours.
- Targeted attackers often exploit the same vulnerabilities as general attackers – there are notable similarities between the list of top vulnerabilities used by targeted threat actors in 2010-2016, and those used in all attacks in 2015-2016.

Part 1: General Statistics

In total, in 2016 Kaspersky Lab security solutions blocked 702,026,084 attacks utilizing an exploit against 4,347,966 users globally. In terms of the number of attacks, this is 24.54% higher than in 2015, while the actual number of users attacked with exploits has decreased since 2015, by 20.85%.

Attacks and users/Years	2015	2016	Y2Y change
Number of attacks	563, 888, 454	702, 026, 084	+ 24.54 %
Number of attacked users	5, 493, 568	4, 347, 966	- 20.85%

Fig. 1: Overall number of attacked users and attacks in 2015-2016 y.y.

There could be several reasons for such changes. One of them is a reduction in the number of sources of exploits: 2016 saw several big exploit kits (the Neutrino and Angler exploit kits) leave the underground exploit market, which significantly affected the overall exploit threat landscape – many cybercriminal groups apparently decreased their efforts in spreading the malware. On the other hand, the average number of attempts to infect a user increased from 102 attempts per user in 2015 to 161 in 2016.

Which means that even though the number of unique users encountering exploits decreased, the likelihood that a user would encounter an attack through an exploit increased. In other words, the number of websites infected with exploits and the number of spam messages with malicious attachments keeps growing.

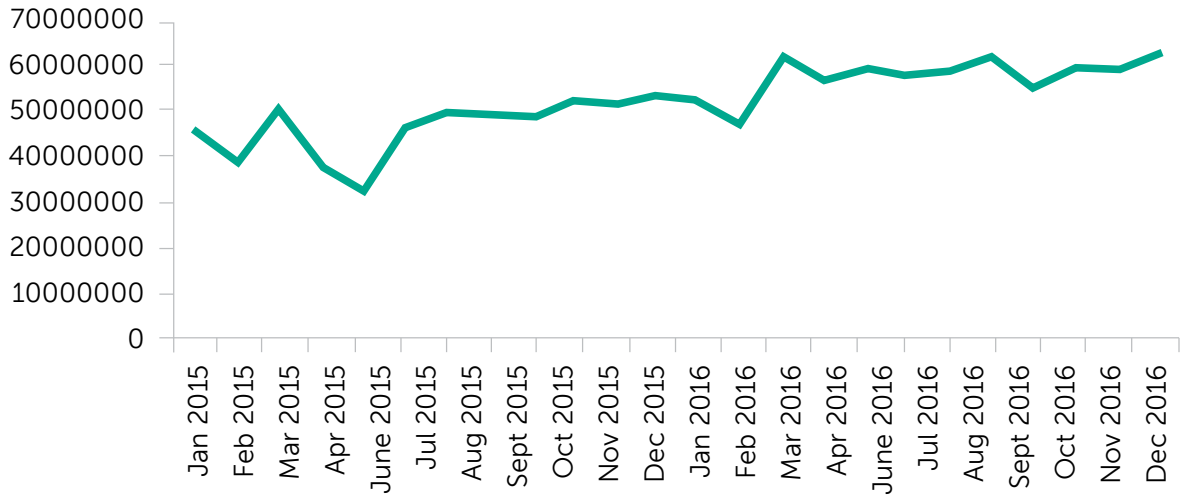

Fig. 2: Overall dynamics of attacks with exploits in 2015-2016.

Interestingly enough, the share of corporate users who encountered an exploit attack increased 6.03 percentage points in 2016.

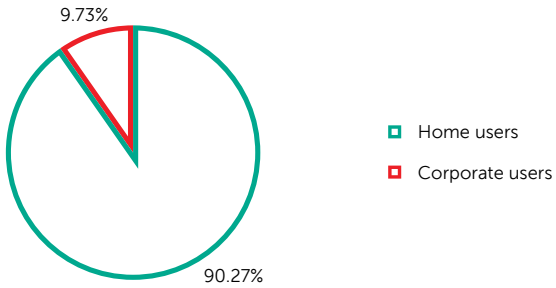

Fig.3: Distribution of users attacked with exploits in 2015 by the type of protection solution they use.

Even though the overall number of users attacked with exploits decreased, this is not the case when it comes to corporate users. Malicious users increasingly use exploits in order to attack companies. In absolute terms, the number of corporate machines that encountered an exploit at least once increased 28.35% in 2016 in comparison to 2015: from 538,037 machines to 690,557 in 2016.

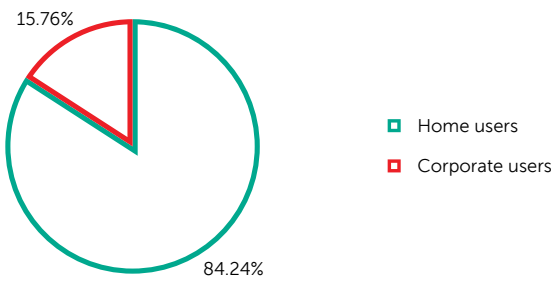

Fig.4: Distribution of users attacked with exploits in 2016 by the type of protection solution they use.

Statistics: the most attacked applications

When looking at the applications whose vulnerabilities were used in real attacks, it can be easily spotted that 2015 was a tough year for internet browsers and Windows components. In 2016 the situation changed significantly. Probably due to the hard work of developers patching newly discovered vulnerabilities, the number of users attacked with browser and Windows exploits decreased by 33.4% and 21.56% respectively. At the same time, the number of users attacked with malware exploiting vulnerabilities in Microsoft Office software, Adobe Flash and Android increased by 102.91%, 23.01% and 11.61% percent respectively. The distribution of users attacked with exploits targeting different applications also changed.

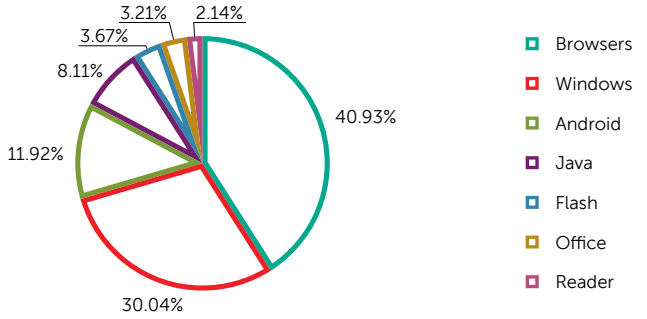

Fig. 5: The distribution of users attacked with exploits targeting different applications in 2015.

The share of browsers declined from 40.93% in 2015 to 26.95% in 2016; Windows – from 30.04% to 23.3%; while the share of users attacked with Android exploits increased from 11.92% in 2015 to 13.15% in 2016.

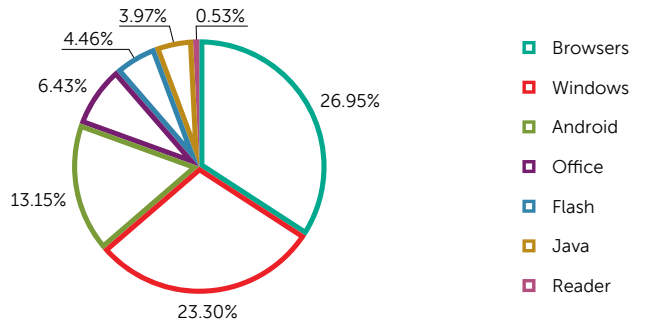

Fig. 6: The distribution of users attacked with exploits targeting different applications in 2016.

Overall, the change in the number of users attacked in 2015 and 2016 looks as follows:

Attacked users	2015	2016	Y2Y change
Browsers	2,310,118	1,538,443	- 33.4%
Windows	1,695,340	1329888	- 21.56%
Android	672,609	750,716	+11.61%
Java	457,824	226,852	- 50.45%
Flash	206,945	254,561	+ 23.01%
Office	180,953	367,167	+102.91%
Reader	120,581	30,431	- 74.76 %

Fig. 7: The change in the number of users attacked with exploits for the most widespread applications and OS in 2015-2016.

Exploits for vulnerabilities in Office software became the absolute champions in terms of the number of attacked users. They increased by almost 103% to reach 367,167 attacked users. On the other hand, exploits to Adobe Reader in 2016 were encountered by 74.76% fewer users than in 2015. Java also dropped significantly – by more than 50%. Exploits for Windows components dropped by 21.56%. The number of users attacked with exploits for Flash and Android in 2016 increased by 23.01% and 11.61% respectively.

As displayed on the timeline below, in terms of the number of attacked users, 2015 was relatively easy for Microsoft Office. However, starting from January 2016, the number began to rise rapidly. These peaks were most likely provoked by the massive distribution of spam emails with exploits targeting the CVE-2015-1641 vulnerability in Microsoft Office.

While for Flash, October 2015 and June and July 2016 were particularly hard – two huge spikes in the number of attacked users were registered in those months. The first peak was provoked by the activity of the Nuclear exploit kit, while the second one resulted from the massive distribution of exploits from the Neutrino exploit kit. In both cases we cannot say for sure which exact exploits were used in the attacks, because of certain technical particularities in how Kaspersky Lab subsystems detect threats.

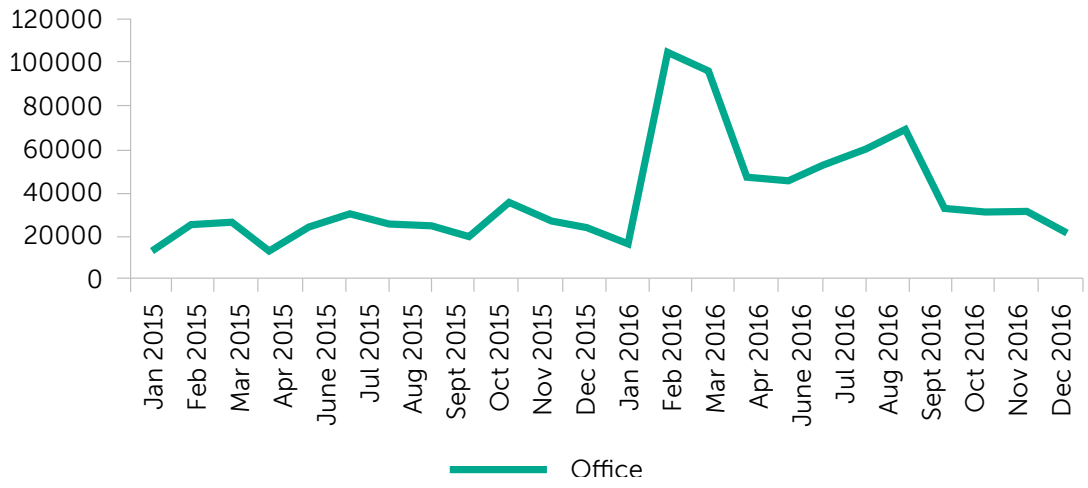

Fig. 8: The change in the number of users attacked with Office exploits in 2015-2016.

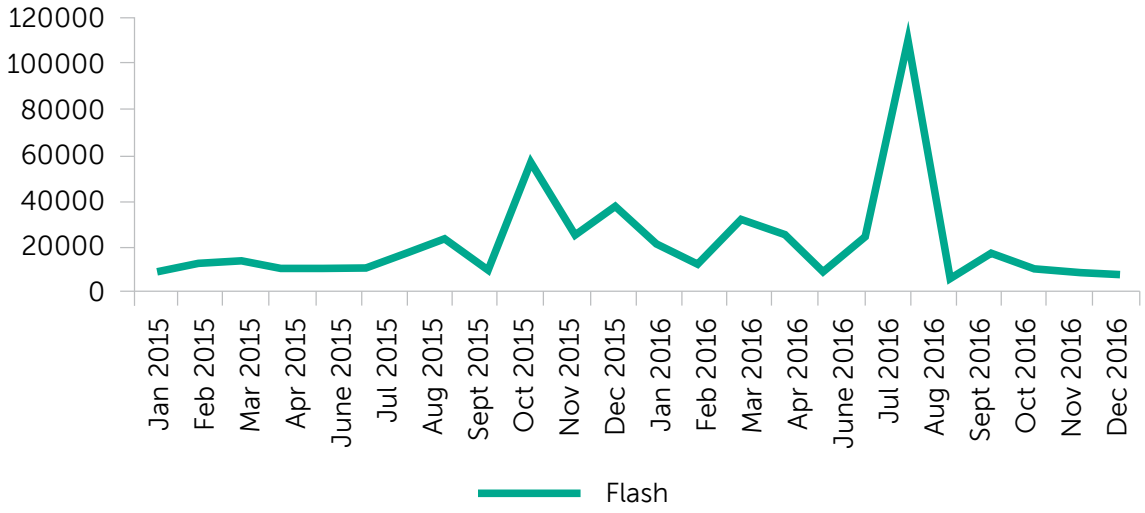

Fig. 9: The change in the number of users attacked with Flash exploits in 2015-2016.

The number of users that encountered exploits for Android grew more or less steadily, with two peaks: in October 2015 and April 2016.

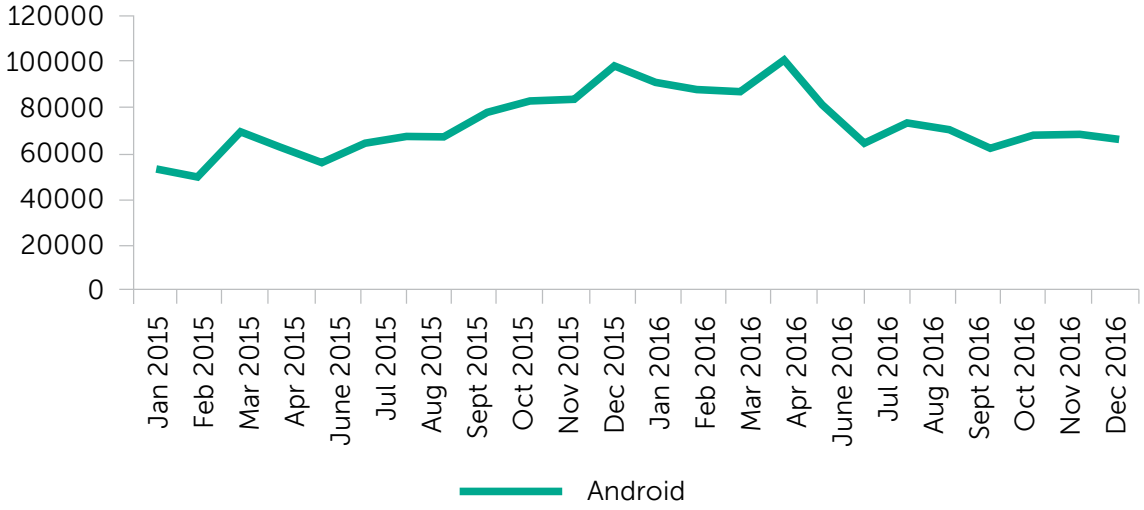

Fig. 10: The change in the number of users attacked with Office exploits in 2015-2016.

It would be too speculative to make any solid conclusions as to the exact reasons for the above changes, but in general we can say that there might be several reasons behind the sudden spikes in the number of users attacked.

First of all, the discovery of new vulnerabilities affects the numbers – the more of them appear, the more attacks happen. Another factor is the presence of working exploits and their availability in exploit kits. Once exploit kit owners start actively distributing exploits to some severe vulnerabilities, the number of attacked users starts growing immediately. One further possible reason is the activity of the malicious actors who utilize exploits in their campaigns. If they implement a massive campaign, it will inevitably provoke a spike in detections.

Perhaps an overview of the number of vulnerabilities discovered can partly answer the question about the reasons behind the increases and decreases in the number of attacked users. For that we've reviewed Kaspersky Lab's own database as well as publicly available information on the vulnerabilities discovered in some of the applications and OSs mentioned above, and looked at how those numbers changed over time. An additional source of information was the CVEdetails.com website, which collects details on the vast majority of vulnerabilities in software. Alongside the general numbers, we looked at how many of the discovered vulnerabilities have a high level of severity (with a score of 9 and higher). In most cases such vulnerabilities allow for the remote hacking and complete compromise of the attacked systems.

2015	Total	High severity	% of severe vulnerabilities
Office	40	37	92.5%
Browsers	624	240	38.46%
JRE	80	26	32.5%
Flash	329	294	89.36%
Android	125	88	70.4%

Fig. 11: The number of vulnerabilities discovered in the most often attacked applications in 2015 (Source: CVEdetails.com and Kaspersky Lab's own database).

In 2016, the number of vulnerabilities discovered in popular browsers (Google Chrome, Mozilla Firefox, Microsoft Edge and Microsoft Internet Explorer) dropped in comparison to 2015 – by 8.81%. And the percentage of severe vulnerabilities, those that would most probably be used by exploit writers, dropped from 38.46% in 2015 to 14.76% in 2016. As was already mentioned above, the number of users attacked with browser exploits also decreased over the same period.

On the other hand, the number of vulnerabilities in Microsoft Office products increased by 20%, and, as we remember, the number of attacked users with Office exploits increased as well.

2016	Total	High severity	% of severe vulnerabilities
Office	48	32	66.67%
Browsers	569	84	14.76%
JRE	37	13	35.14%
Flash	266	224	84.21%
Android	523	254	48.57%

Fig. 12: The number of vulnerabilities discovered in the most often attacked applications in 2016 (Source: CVEdetails.com and Kaspersky Lab's own database).

Android OS faced the most dramatic increase in terms of discovered vulnerabilities: from 125 in 2015 to 523 in 2016. According to Kaspersky Lab's threat statistics, both the percentage and actual number of users who encountered attacks with exploits for vulnerabilities in Android increased during the same period, but at much more modest scale.

The correlation between the number of discovered vulnerabilities and the number of attacks doesn't always work, though. For instance, the percentage and the actual numbers of users attacked with exploits for Flash vulnerabilities increased in 2016 in comparison to 2015, while the number of vulnerabilities discovered during the same period decreased.

Still, the overview of the number of vulnerabilities discovered in particular applications gives a more or less clear understanding on the potential attack surface for each of them. At the same time, it would be interesting to see if there were any widespread exploits for particular vulnerabilities.

The most widespread vulnerabilities used "in the wild"

As we've seen in the previous chapter, when it comes to the number of discovered vulnerabilities, the potential attack surface for malicious users is huge. However, the statistics related to the real use of exploits show that only a few vulnerabilities are actively exploited in the wild. It is important to say here that, in some cases certain technical particularities of Kaspersky Lab's statistics processing systems give only partial visibility on which specific vulnerabilities have been exploited in the wild. That means that some detection names for exploits cover not a single exploit for a single vulnerability, but a whole group of them. Exploits are often grouped on the basis of their presence in popular exploit kits. Another example of a common detection name is when different exploits are part of one exploitation chain or share some exploitation techniques.

Taking into account these particularities, the list of the most widespread exploit threats in 2015 looks as follows.

Exploit threat name	% of users who encountered a particular exploit threat out of all those who encountered any malware categorized as an exploit.
CVE-2010-2568	27%
Exploit.AndroidOS.Lotoor (multiple exploits)	11.02%
Neutrino (multiple exploits)	4.49%
Angler (multiple exploits)	3.14%
CVE-2013-2423	2.02%
CVE-2014-3153	1.57%
CVE-2012-0158	1.25%
CVE-2015-1641	0.31%
MSOffice ASLR bypass (multiple exploits)	0.07%

Fig. 13: The list of the most widespread exploit threats in 2015.

For several years in a row, exploits for the infamous Stuxnet LNK vulnerability CVE-2010-2568 have topped the chart of the most widespread malware of this type. In 2015, 27% of users that encountered any exploit attack during the year at least once, faced exploits to this particular vulnerability. This may be due to the fact that malware that uses these exploits have a self-replicating feature, constantly recreating themselves in the attacked network where vulnerable computers are installed. More about this flaw can be found in the next part of this report.

Second place in the 2015-chart is taken by Exploit.AndroidOS.Lotoor (e.g. CVE-2011-1823, CVE-2012-6422 CVE-2013-2596, CVE-2013-2094 etc.). This is a detection name for a group of exploits used to gain root-access rights on an attacked smartphone or tablet. Of those who encountered an exploit at least once in 2015, one in ten users (11.02%) faced threats from this group.

The third and the fourth place went to the Neutrino (4.49% of attacked users) and Angler (3.14% of attacked users) exploit kits. These are common detection names for group of exploits widely distributed through these exploit kits.

Exploits to the CVE-2013-2423 vulnerability in Java took 5th place with 2.02% of attacked users. It was patched a long time ago, in April 2013, but exploit kit writers still continue to develop malware exploiting the flaw. Most

probably this is due to the fact that, despite a patch being available for years, lots of PCs connected to the Internet haven't been updated.

CVE-2014-3153, which took 6th place in 2015 is a vulnerability in Linux OS kernel, which has been actively used by Android malware to root attacked devices. A patch was released in summer 2014, but exploits continued to be effective, mostly due to the fact that almost any Android-device released before June 2014 remains vulnerable. The support period for many of these devices has ended and but Android smartphones running obsolete versions of the OS continue to be used actively all around the world.

Exploits using CVE-2012-0158 – another very old vulnerability in Microsoft Office - and some other Windows products and components took 7th place with 1.25% of attacked users. Just like the Java exploit mentioned above, this vulnerability was patched in 2012, but continued to be used in real world attacks up to 2015 and beyond.

CVE-2015-1641 (8th place with 0.31% of attacked users) – is another critical vulnerability in Microsoft Office. In 2015 and 2016 Kaspersky Lab researchers observed exploits related to this vulnerability in massive spam campaigns delivering different malicious payloads.

The last place in the 2015 rating (0.07% of attacked users) has been taken by multiple exploits utilizing techniques to bypass the Windows Address space layout randomization memory protection process (ALSR) in Microsoft Office.

In total, during 2015 these nine expoit threats were faced by more than 50% of all users who encountered at least one exploit attack.

The other 50% are distributed between hundreds of less popular exploits. Interestingly enough, in 2016 the list of the most widespread exploit-threats is remarkably shorter. However, the number of users who faced them while surfing the web was fairly the same – a little bit more than 50%.

Exploit threat name	% of users who encountered the exploit threat
CVE-2010-2568	24.68%
Exploit.AndroidOS.Lotoor	15.6%
CVE-2014-3153	3.27%
MSOffice ASLR bypass	3.1%
CVE-2015-1641	2.6%
CVE-2012-0158	2.45%

Fig.14: The list of the most widespread exploit threats in 2016.

In 2016, CVE-2010-2568 again topped the list of the most widespread exploit threats, but at a slightly smaller scale – 24.68% of users were the target of exploits for this vulnerability. The Neutrino and Angler exploit kits disappeared from the top. This was the result of efforts by the security community, including Kaspersky Lab, leading to the complete disruption of the Angler exploit kit and, when it comes to Neutrino, a considerable drop in activity in autumn 2016. That influenced the overall number of users attacked with exploits distributed through the corresponding kits.

The 2nd place in 2016 was again taken by Exploit.AndroidOS. Lotoor – 15.6% of users encountered exploits from this group which is 4.58 percentage points higher than in 2015. It would be fair to assume that this increase was caused by the sudden disappearance of Neutrino and Angler from the top, but this is not the only factor that influenced the rise of Exploit. AndroidOS.Lotoor. In absolute figures, the number of users attacked with this exploit-threat increased in 2016 by 12.12% - from 605,129 in 2015 to 678,451 users in the last year. The amount of users attacked with exploits for CVE-2014-3153 (another Android vulnerability) also increased from 1.57% to 3.27%, along with the ASLR bypassing group of exploits (3.1%), exploits to the CVE-2015-1641 Office vulnerability (2.6%) and exploits to old CVE-2012-0158 (2.45%).

Also not in the top, but very close to it are two vulnerabilities: CVE-2016-0189 in Internet Explorer and CVE-2014-6332 in some Windows components. Both vulnerabilities are very actively used by exploit kit developers and clients, and also by targeted attack actors.

In other words, even though some large sources of exploits, like popular exploit kits, left the threat landscape in 2016, the free space was immediately taken by other exploits. At the same time, it would be fair to mention that the overall number of users attacked with exploits decreased in 2016. To some extent this was the result of the decreased activity of Angler and Neutrino exploit kits.

Another interesting thing about the most widespread exploit-threats described above is that, while the number of newly discovered vulnerabilities in many cases increased significantly, only a relatively small group of them posed a real threat to customers. In fact, we find that most of the vulnerabilities discovered are seldom used in real attacks. Kaspersky Lab has its own vulnerability database that powers the company's Patch Management solution. In 2015 the database listed 3234 vulnerabilities, and, in 2016 – 1710 more. As of April 2017, Kaspersky Lab's vulnerability database lists 5005 unique vulnerabilities. Those are vulnerabilities in applications that are most often used in corporate and home environments. The source of information about these vulnerabilities are the software vendors and security community, including Kaspersky Lab's research team itself.

All the above reviewed information is related to known exploits targeting known vulnerabilities. Meanwhile there are a lot of attacks with unknown vulnerabilities. Sometimes such exploits, called 'zero-day' exploits because the vulnerability such exploits are targeting is not yet known to the software vendor and to the public. Based on what we discovered during our overview of exploit-threats, it is not that hard to encounter such an exploit in the wild.

Statistics on attacks with the help of unknown exploits

The vast majority of exploits are blocked by a standard set of signature and behavior-based anti-malware technologies. However, single percentages of exploits are sophisticated enough to bypass such obstacles and break through all defenses. These are exploits targeting zero-day vulnerabilities or complex, heavily-obfuscated exploits that may use a number of tricks to overcome standard protection technologies. On computers protected by Kaspersky Lab products these exploits would face the Automatic Exploit Prevention (AEP), a technology that specifically targets malware that uses software vulnerabilities. Automatic Exploit Prevention eliminates the most complex or previously unknown exploits and pays particular attention to the most frequently targeted programs such as Java, Adobe Reader, Flash, Internet Explorer, Microsoft Office, and etc.

Any attempts by these programs to launch suspicious executable files or code results in extra security checks. Even though they may be legitimate (for example, if Adobe Reader launches an executable file to check for updates), certain characteristics of the file, as well as actions that took place prior to the attempted launch, can be an indicator of malware. AEP technology discovers the source of the attempt to launch the code - it may originate from the software itself or because of the actions of an exploit. Data on the most typical exploit behavior helps to detect such threats, even in the case of a zero-day vulnerability.

Certain exploits, especially those used in drive-by downloads (when they are launched as a result of visiting a malicious web page) fetch the payload from a certain website before executing it. Automatic Exploit Prevention tracks the origin of files, identifies the browser that initiated the download and the remote web address for the files. In addition, Automatic Exploit Prevention can distinguish between files created with the consent of the user and unauthorized new files. When there is an attempt to launch suspicious code, this information helps to determine the actions of exploits and block it.

Besides protecting users from sophisticated exploit threats, Kaspersky Lab's AEP allows for the statistical analysis of attacks with unknown or heavily obfuscated exploits.

Based on these statistics we've learned that the number of attempts to infect computers in 2016 increased by 96.75% in comparison to 2015, to exceed 21.4 million blocked infection attempts. At the same time, the number of users protected with these technologies increased by 6.79% and reached 297,000+ users.

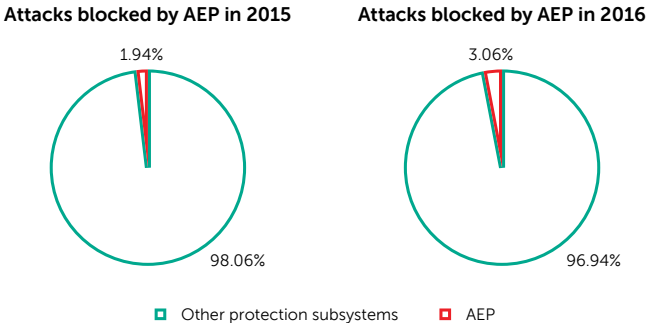

Fig. 15: The change in the percentage of attacks blocked by AEP in 2015-2016.

Certain technical particularities of the technology do not allow for the exact identification of the exploits which provoked such an increase in the number of attacks; however in the last two years we have frequently seen massive malicious campaigns which used exploit kits to distribute malware – ransomware in particular. Neutrino and Angler, mentioned earlier in this report, were two leading ones. Their owners invested lots of resources into the development of the new exploits, flooding the underground market with many high quality malicious tools. These tools were actively used by multiple groups involved in malware distribution. That could, potentially, be one of the key reasons behind the attack anomaly.

As a result, the percentage of attacks blocked by AEP in 2016 increased by 1.12 percentage points. And the percentage of users who encountered unknown exploits increased by 1.78 p.p.

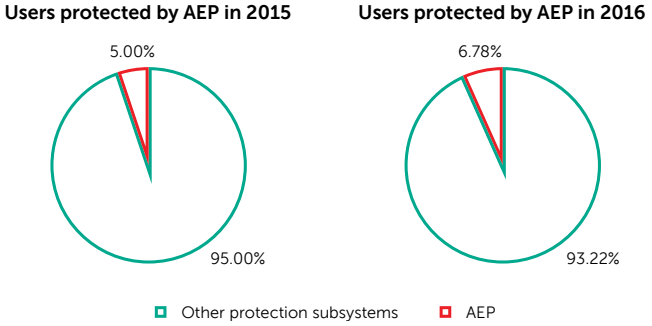

Fig. 16: The change in the percentage of users attacked with unknown exploits and protected by AEP in 2015-2016.

In general, the relatively low use of unknown exploits revealed by the statistics is good news: as it means that in most cases malicious users have no access to advanced exploit development. This increases the probability of detecting an attack through a vulnerability in a popular application. Therefore, if an ordinary user or an organization utilizes a protection solution equipped with exploit prevention technologies, they are reliably protected. But what about those actors that actually have access to advanced vulnerability exploitation capabilities?

Part 2: Exploits and the Targeted Threat Actors

Alongside the groups that create the exploit kits so many attackers rely on, targeted threat actors are among the most enthusiastic users of vulnerabilities and generally have both the funds and the skills to exploit them. Their main goals tend to be cyberespionage, cybersabotage and the theft of data and money. Targeted attackers use vulnerabilities in popular applications to help them breach defences, drop malicious tools, and take control of computers, among other things.

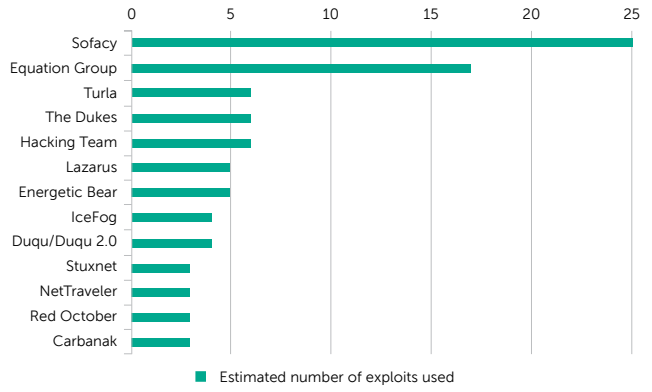

Fig. 17: The approximate number of exploits used by different cyberespionage, cybersabotage and sophisticated cybercriminal groups from 2010 to 2016.

Most of the vulnerabilities exploited by threat actors come from Microsoft (Windows or Office), Adobe Flash and Java.

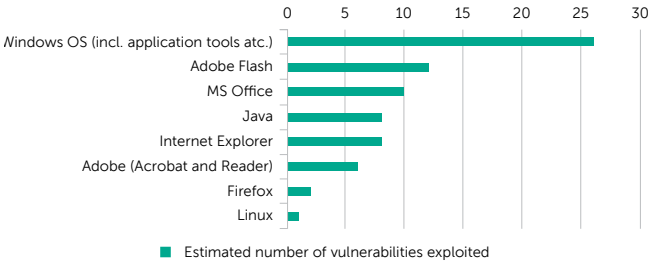

Fig. 18: Applications most often exploited by targeted attack groups.

The threat actors' favorite bugs

The much-loved CVE-2012-0158

The most popular vulnerability used by targeted attack groups reported on by Kaspersky Lab is CVE-2012-0158. A Microsoft Office Rich Text Format (RTF) vulnerability, it was discovered and patched way back in 2012, but is still being used successfully by APTs four years later. Its enduring appeal is largely down to its integration in widely available Office exploit kits. However, the number of computers that can still be breached with this vulnerability is declining – down to just 15% in Europe and North America. Even so, half of the machines in Asia and Russia/Ukraine remain exposed and CVE-2012-0158 continues to be effective for highly targeted attacks in these markets. Big threat actors focused on these territories have used it widely in spear-phishing documents designed to launch cyberespionage operations, often against very sensitive targets such as government, diplomatic and military entities.

Such threat actors include Red October, NetTraveler, and the cyber-mercenary group IceFog (in 2011-2013), Cloud Atlas in 2014, and Carbanak - the first criminal APT - Sofacy, SpringDragon and Dropping Elephant in the years leading up to 2016. More on these later.

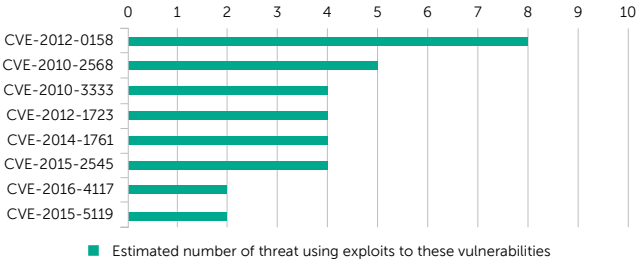

Fig. 19: The top vulnerabilities exploited by targeted attack groups 2010 - 2016.

The infamous Stuxnet worm: CVE-2010-2568

In 2010 a zero-day security vulnerability in the way Microsoft Windows processed shortcut links (LNK) was discovered - being used along with three other zero-days by the infamous Stuxnet worm to attack nuclear systems in Iran through USB sticks. Despite being quickly patched by Microsoft, the vulnerability was used by the Chinese-speaking threat actor Naikon (2009 onwards) to mount cyberespionage attacks against business and geopolitical entities in the Far East, and by Gauss (2011) a nation state sponsored banking Trojan/cyber-surveillance APT which targeted specific individuals in the Lebanon, Syria, Israel and Palestine.

In fact, Stuxnet was not the first to use this LNK vulnerability: Equation Group, a huge complex English-speaking cyberespionage threat actor, active since 2001, was found to have been using it back in 2008.

During their analysis of Stuxnet, Kaspersky Lab researchers found a "Zlob" worm executable that was named "fanny.bmp". A few years later, while they were investigating the Equation Group, they encountered Fanny again, a worm created in 2008 that used the Stuxnet LNK exploit to replicate. The researchers found that Fanny used two zero-day exploits, which were later added to Stuxnet, in June 2009 and March 2010. This means that Equation had access to these zero-days (and others) years before the Stuxnet group did.

This is not the whole story for CVE-2010-2568. In 2012, a curious email was sent to security researchers, containing details of malicious code that could be traced back to Hacking Team, a controversial 'offensive security' organization that distributes spyware to governments. The code formed part of Hacking Team's primary product offering: Remote Control Systems (RCS). Kaspersky Lab analysis revealed that CVE-2010-2568 was integrated into RCS to enable self-replication via a USB drive.

Microsoft finally fixed the last of the CVE's vulnerable code path in March 2015.

The second RTF vulnerability: CVE-2010-3333

Another enduring vulnerability is CVE-2010-3333, a Microsoft Office RTF stack-buffer-overflow vulnerability. Despite the release of a patch in November 2010, it continued to be exploited by targeted attackers and there are signs that was still being abused in 2016.

Hacking Team used it to install RCS on victim computers. Red October, a large scale cyber-espionage network targeting diplomatic, governmental and scientific research organizations in Eastern Europe, the former USSR and Central Asia, used the vulnerability from 2012 onwards. Other targeted attackers to exploit this vulnerability include NetTraveler, a Chinese-speaking cyberespionage threat actor operational from 2004 and targeting mainly Tibetan/ Uyghur activities and scientific entities in regions including Russia and India, as well as Sofacy (also known as APT28 and Fancy Bear).

Over the years, Sofacy, a Russian-speaking threat actor targeting mainly NATO countries, has significantly increased its activity, becoming one of the most prolific, agile and dynamic threat actors in the arena. Since its first appearance in 2008, Sofacy appears to have deployed no less than 25 vulnerabilities and there is little sign of it slowing down.

Coffee to go: CVE-2012-1723

After Microsoft – including Office and the Windows platform – and Adobe, Java is the most vulnerable application when it comes to exploitable bugs for targeted threat actors. The CVE-2012-1723 vulnerability allows malware to evade the JRE (Java Runtime Environment) sandbox so that it can load additional Java classes designed to perform malicious actions. It was integrated into the Blackhole Exploit Kit in 2012 and is often used in watering hole attacks, trapping victims through compromised websites.

Big threat actors that have made use of this vulnerability include IceFog and Equation Group, as well as Energetic Bear/Crouching Yeti, an APT targeting the industrial machinery sector, among others, in the US, Europe and China since 2010; and Turla, a massive Russian-speaking cyberespionage operation targeting sensitive government and research entities in more than 40 countries.

More cracks in rich text: CVE-2014-1761

CVE-2014-1761 is a Word vulnerability uncovered as a zero-day in the wild in March 2014. It allows for remote code execution if a user opens a specially crafted RTF file using an affected version of Microsoft Word, or a specially crafted RTF email message in Microsoft Outlook while using Microsoft Word as the email viewer.

Targeted attackers who have made use of this vulnerability include Energetic Bear/Crouching Yeti, Carbanak, Sofacy and the Dukes, a complex web of disparate yet related, Russian-speaking threat actors that often operate concurrently, targeting government organizations and commercial entities in the US, Germany, South Korea and Uzbekistan and even, allegedly, the White House and the US Department of State.

A contender for 0158's crown: CVE-2015-2545

CVE-2015-2545 is a Microsoft office vulnerability discovered – and patched - in 2015. It enables an attacker to execute arbitrary code using a specially crafted EPS image file.

The exploit was discovered in the wild in August 2015, when it was used in a targeted attack by the Platinum group, presumably against targets in India. In the months that followed there was significant growth in the number of threat actors using the vulnerability to breach victim defences, with nearly all the attackers and their main targets located in South-East and Central Asia and the Far East.

Timeline of atacks using exploits to the CVE-2015-2545 vulnerability

In recent months a wave of cyberespionage attacks have been conducted by different groups across Asia-Pasific (APAC) and the Far East.
All of them share one common feature: in order to infect their with malware, the attackers use an exploit for the CVE-2015-2545 vulnerability.
This vulnerability was patched in November 2015, but exploits to it are still widely used due to a low level of patch-adoption.

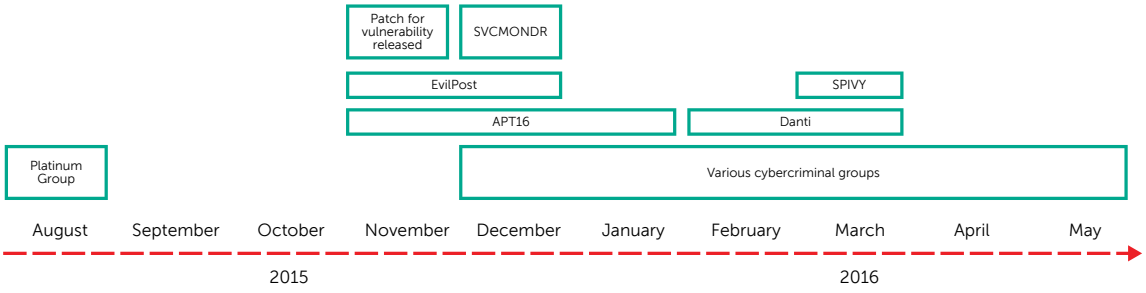

Fig. 9: The change in the number of users attacked with Flash exploits in 2015-2016.

For example, after Platinum, a modified exploit for the vulnerability was used by APT16, a threat actor targeting news agencies and believed to be of Chinese origin. Then in December 2015, Kaspersky Lab uncovered EvilPost targeting the Japanese defense sector with the vulnerability. In spring 2016 it was the turn of SPIVY, which used the vulnerability in spear-phishing attacks against targets in Hong Kong.

Two further groups using the vulnerability are worth mentioning. One is Danti, a previously unknown group, probably related to NetTraveler, which used the vulnerability in early 2016 in targeted attacks against Indian diplomatic organisations, among others, and SVCMONDR, which used the vulnerability in late 2015 to target a Taiwanese security software reseller.

One Flash zero day: CVE-2016-4117

This top-ranking Adobe Flash zero-day was uncovered in the wild in May 2016. It has been used in watering hole attacks by a threat actor known as Scarcruft, a relatively new targeted attack group with victims in Russia, Nepal, South Korea, China, India, Kuwait and Romania, and also by Sofacy.

Followed by another: CVE-2015-5119

The next Flash zero-day, CVE-2015-5119 was leaked in the 2015 Hacking Team breach. It had been used by Hacking Team to penetrate systems for cyber-surveillance and Adobe warned users that it could cause a crash and potentially allow an attacker to take control of the affected system. Not surprisingly, attackers set about exploiting the new vulnerability within hours of the online leak. One of these was BlueTermite, a threat actor targeting a wide range of industry sectors and government organizations in Japan. Active since 2013, its main infection vector was spear-phishing emails, but by August 2015 it was using a drive-by-download exploiting CVE-2015-5119.

Sofacy also exploited this vulnerability. During 2015, the threat actor dropped six zero-days in a period of just four months, five of them were built in-house by Sofacy, while the sixth was a re-written CVE-2015-5119 put into use just 24 hours after it was leaked.

The exception: the Lazarus Group

Of the big targeted attack groups in our list of top exploit users, only one name remains: that of the Lazarus Group, a particularly malicious threat actor responsible for destructive wiper attacks as well as cyber-espionage. Active since 2009, the Lazarus Group targets mainly North and South America and the Middle- and Far-East, and is believed to behind the infamous attack on Sony Pictures Entertainment in 2014 as well as more recent attacks on financial services. The group has deployed multiple tools over the years, including spear-phishing attacks using CVE-2015-6585, a zero-day vulnerability exploiting Hangul WP, a South Korean word processing application.

The group has also made use of a number of new Adobe Flash vulnerabilities, including CVE-2016-4117 (also exploited by Sofacy), CVE-2015-8651 (integrated into the widely used Angler Exploit Kit), and CVE-2016-1019 (integrated into the Magnitude Exploit Kit), as well as the mysterious Microsoft Silverlight zero day CVE-2016-0034.

Overall, at least 35 targeted attack actors and campaigns reported on by Kaspersky Lab in the years 2010 to 2016 appear to have held, used and re-used over 80 vulnerabilities between them. Some were zero-days, while others had been around for years, and around two-thirds were used by more than one threat actor.

Conclusions and advice

As this overview shows, exploits in popular applications and operating systems are a very serious security problem, posing a real threat to millions of home and corporate users around the world. Exploits are an effective delivery tool for malicious payloads and this means they are in high demand among malicious users, whether they are cybercriminal groups, or targeted cyberespionage and cybersabotage actors. The other part of the problem is that, even though developers of popular software invest huge resources into finding and eliminating bugs in their products and exploit mitigation techniques, for at least the foreseeable future the challenge of vulnerabilities will remain.

In order to protect your personal or business data from attacks via software exploits, Kaspersky Lab experts advise the following:

- Keep the software installed on your PC up to date, and enable the auto-update feature if it is available.
- Wherever possible, choose a software vendor which demonstrates a responsible approach to a vulnerability problem. Check if the software vendor has its own bug bounty program.
- If you are managing a network of PCs, use patch management solutions that allow for the centralized updating of software on all endpoints under your control.
- Conduct regular security assessments of the organization's IT infrastructure.
- Educate your personnel on social engineering as this method is often used to make a victim open a document or a link infected with an exploit.
- Use security solutions equipped with specific exploit prevention mechanisms or at least behavior-based detection technologies
- Give preference to vendors which implement a multilayered approach to protection against cyberthreats, including exploits.

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com