Exploits: how great is the threat?

By Kaspersky Lab on April 20, 2017. 8:57 am

PUBLICATIONS

INTERNAL THREATS STATISTICS VULNERABILITIES AND EXPLOITS

VULNERABILITIES AND HACKERS VULNERABILITY STATISTICS ZERO-DAY VULNERABILITIES

How serious, really, is the danger presented by exploits? The recent leak of an exploit toolset allegedly used by the infamous Equation Group suggests it's time to revisit that question. Several zero-days, as well as a bunch of merely 'severe' exploits apparently used in-the-wild were disclosed, and it is not yet clear whether this represents the full toolset or whether there's more to come, related to either Equation or another targeted threat actor.

Of course, Equation Group is not the first, and is certainly not the only sophisticated targeted attacker to use stealthy, often zero-day exploits in its activity.

Today we are publishing an overview of the exploit threat landscape. Using our own telemetry data and intelligence reports as well as publically available information, we've looked at the top vulnerabilities and applications exploited by attackers.

We have examined them from two equally important perspectives. The first part of the report summarises the top exploits targeting all users in 2015-2016, and the most vulnerable applications. The second part considers the vulnerabilities exploited between 2010 and 2016 by significant targeted threat actors reported on by Kaspersky Lab: that's 35 actors and campaigns in total.

This report focuses on attacks using client-side exploits and does not include data on attacks using server-side exploits.

Key findings on exploits targeting all users in 2015-2016:

- 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 were 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).

2015-2016 witnessed a number of positive developments in the exploit threat landscape. For example, two very dangerous and effective exploit kits – Angler (XXX) and Neutrino, left the underground market, depriving cybercriminals community of a very comprehensive set of tools created to hack computers remotely.

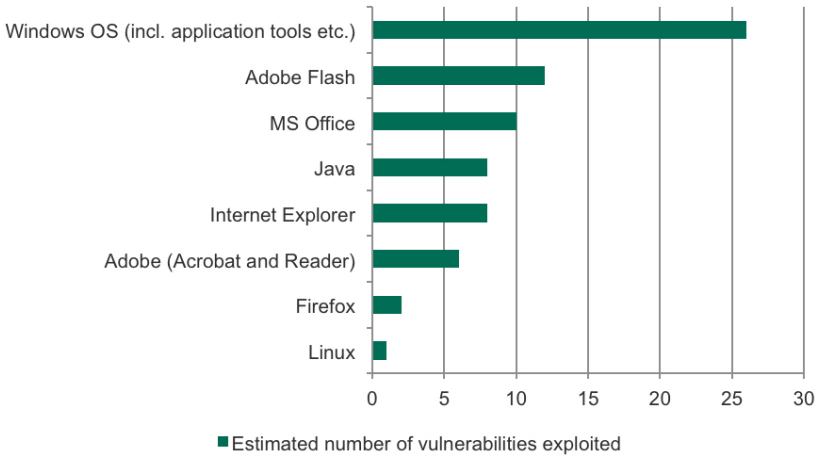
A number of bug bounty initiatives aimed at highlighting dangerous security issues were launched or extended. Together with the ever-increasing efforts of software vendors to fix new vulnerabilities, this significantly increased the cost to cybercriminals of developing new exploits. A clear victory for the infosec community that has resulted in a drop of just over 20% in the number of private users attacked with exploits: from 5.4 million in 2015 to 4.3 million in 2016.

However, alongside this welcome decline, we've registered an increase in the number of corporate users targeted by attacks involving exploits. In 2016, the number of attacks rose by 28.35% to reach more than 690,000, or 15.76% of the total amount of users attacked with exploits. In the same year, more than 297,000 users worldwide were attacked by unknown exploits. These attacks were blocked by our Automatic Exploit Prevention technology, created to detect this type of exploits.

Key findings on exploits used by 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.

When looking more closely at the applications used by targeted threat actors to mount exploit-based attacks, we weren't surprised to discover that Windows, Flash and Office top the list.

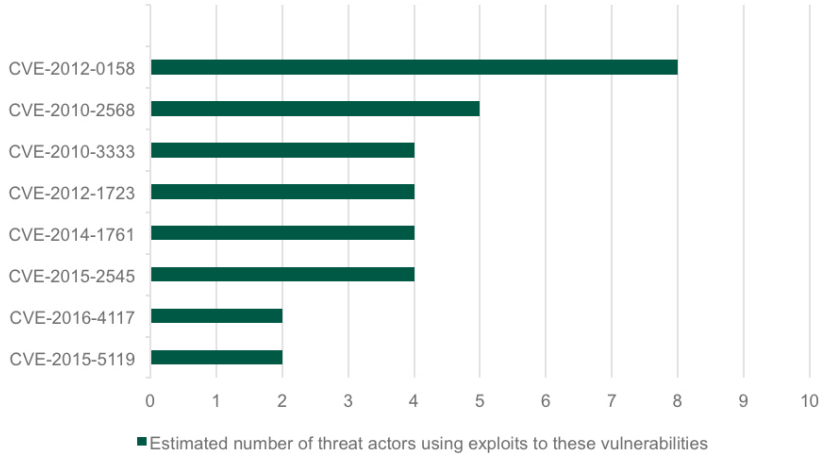


Applications and Operation Systems most often exploited by targeted attack groups.

Moreover, the recent leak of multiple exploits allegedly belonging to the Equation cyberespionage group highlighted another known

but often overlooked truth: the life of an exploit doesn't end with the release of a security patch designed to fix the vulnerability being exploited.

Our research suggests that threat actors are still actively and successfully exploiting vulnerabilities patched almost a decade ago – as can be seen in the chart below:



Everyone loves an exploit

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.

To take just one example, when we looked at our most recent threat statistics we found that exploits to CVE-2010-2568 (used in the notorious Stuxnet campaign) still rank first in terms of the number of users attacked. Almost a quarter of all users who encountered any exploit threat in 2016 were attacked with exploits to this vulnerability.

Conclusion and Advice

The conclusion is a simple one: even if a malicious user doesn't have access to expensive zero-days, the chances are high that they'd succeed with exploits to old vulnerabilities because there are many systems and devices out there that have not yet been updated.

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.

Further details on exploits used in attacks in 2015 and 2016, as well as by the big targeted threat actors over the last six years – and Kaspersky Lab guidance on how to address the threat they present, can be found in the full report.

offers and premium assets like white papers, webcasts, videos, events and other marketing materials and related offers as per Kaspersky Lab's Privacy Policy

Submit

Related Articles

THE SECURITY IS STILL SECURE

UNRAVELING THE LAMBERTS TOOLKIT

KASPERSKY SECURITY BULLETIN 2016. REVIEW OF THE YEAR. OVERALL