

Threat Report

Endpoint Exploitation Trends 2015

Bromium Labs Research Brief



Table of Contents

Executive Summary	3
Exploits for Sale	3
Malvertising Continues Unabated	4
Vulnerabilities and Exploitation Trends	4
Exploit Kit Trends	7
Macro-Malware via E-Mail Spam	8
Crypto-Ransomware	9
Summary	10
References	11
About Bromium	12

Executive Summary

With the conclusion of 2015, we have the opportunity to review one of the busiest years for cyber security in recent memory. IT security teams were on guard, working hard to defend against various attacks, from the [Hacking Team's data trove of zero-days and surveillance Trojans](#) to an explosive surge in ransomware attacks and malvertising.

Here are some of the key trends that we observed:

- Active underground zero-day exploitation 'for hire' came under public scrutiny with the Hacking Team data exfiltration.
- Adobe Flash was one of the most exploited user-initiated applications on the endpoint.
- Exploit kits continue to thrive as the most sought after means to deploy malware—now built with more capabilities to bypass traditional detection-based technologies.
- Macro-based malware embedded in Word documents sent through phishing e-mails is on the rise.
- The lucrative underground crypto-ransomware business demonstrated significant sophistication and continuous growth.
- Malicious ads provide a great ROI for attackers and are difficult to block.

Exploits for Sale

The Internet underground market has long been suspected of the clandestine selling of zero-days and mass surveillance Trojans for launching attacks. This suspicion was confirmed when Hacking Team, a company specializing in selling exploits, was itself hacked and all of its [exploits were made public](#). The Hacking Team data exposed included a range of sophisticated exploits, Trojans, application zero-day exploits for IE, Safari, Flash, Office and more. Even mobile and kernel exploits to escape sandboxes were part of their wares.

This leak proves beyond a doubt that Internet hacking is available to anyone willing to pay—even government organizations and corporations. The leak was also a treasure trove for malware authors, who quickly launched malware campaigns leveraging exploits that were publicly available. With this noteworthy event, it should come as no surprise if similar campaigns leveraging similar services come to light.

Malvertising Continues Unabated

Attackers had an obvious choice for launching wide-spread attacks in 2015—malvertisements. In the past couple of years, abusing the massive ad networks has become the sweet spot for attackers. Malware via ads provides great ROI for the attackers and are difficult to be reliably blocked at the ad launch. We saw a broad spectrum of malicious ads coming via popular websites targeting popular categories of websites.

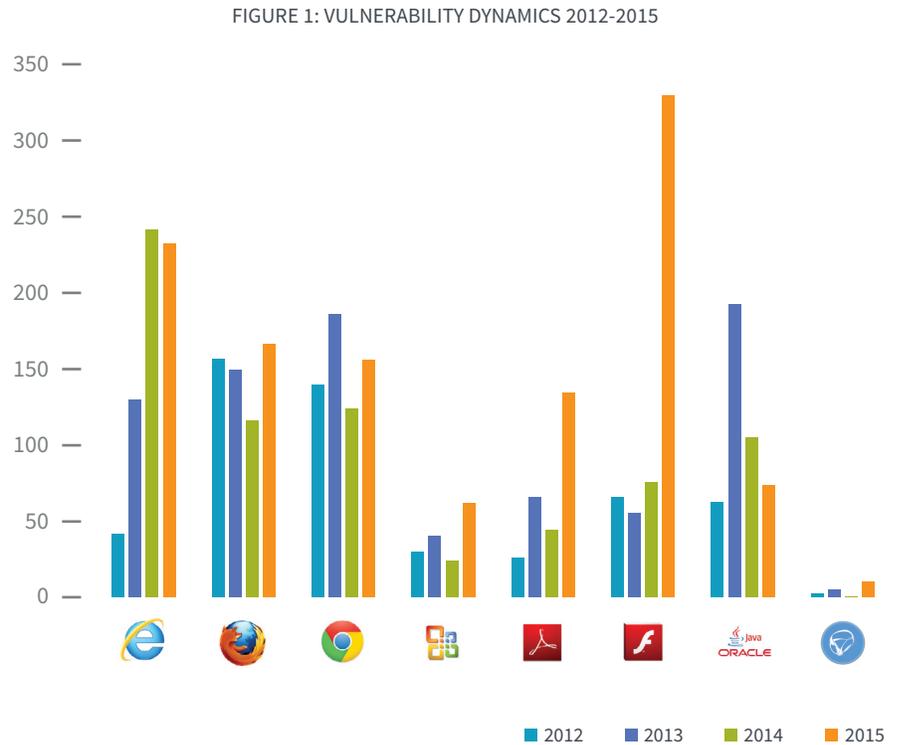
While in our [1H 2015 report](#) we first reported news and entertainment sites to be the lucrative targets for attackers, this trend continues to grow unabated. Based on our threat sensors over the year, we found that at least 27 percent of the [Alexa 1000 websites](#) were delivering malware via malicious advertisements. Until the advertising industry takes more proactive steps to curb these attacks, expect this trend to continue.

Vulnerabilities and Exploitation Trends

Drive-by-download attacks continued to be a favored approach of attackers. The usual high-value targets are typically:

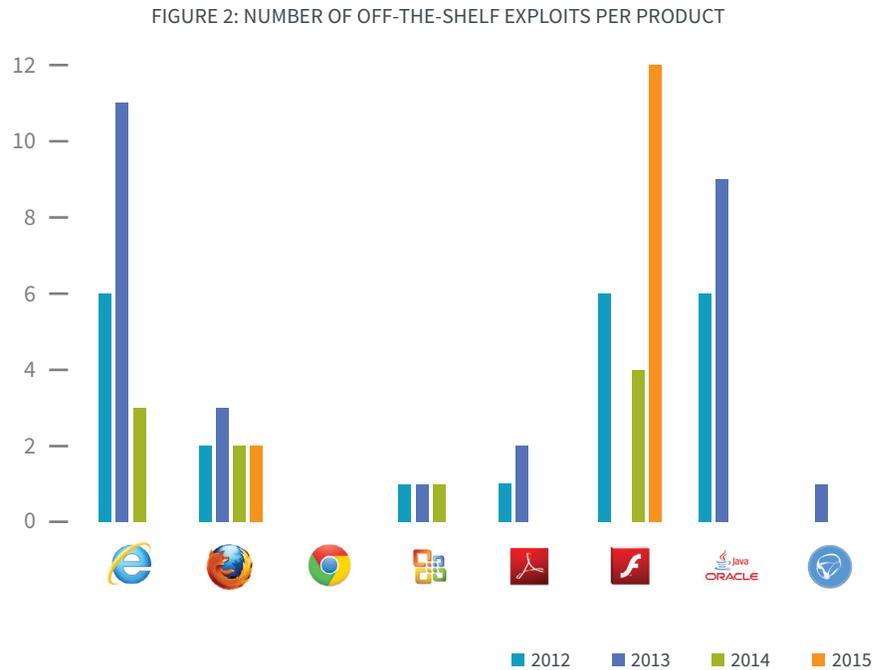
- **Web browsers:** Microsoft Internet Explorer, Mozilla Firefox, Google Chrome
- **Browser plug-ins:** Adobe Flash, Microsoft Silverlight, Oracle Java RE
- **Office productivity software:** Microsoft Office, Adobe Reader

Vulnerability and exploit dynamics for these applications for the period 2012 to 2015 are depicted in Figure 1.



The bar chart shows the number of discovered vulnerabilities [1], which seems to be growing rapidly, an overall increase of 60 percent since 2014. This could be explained by different factors, such as better security testing, shorter release cycles and the development of new analysis approaches. Adobe Flash contributed significantly to the spike in the vulnerability count for 2015, increasing by 333 percent. On the other hand, Oracle Java vulnerabilities were on a decline, a trend consistent with 2014.

Figure 2 illustrates the number of off-the-shelf exploits available in the Metasploit Framework for each product by year. This is a reasonable approximation for the actual threat landscape since Metasploit exploits can be modified to evade anti-malware solutions and incorporated into exploit kits.



2015 was particularly busy for Adobe Flash security. Adobe Flash exploits increased 200 percent. Security researchers seem to have found a sweet spot and keep finding new bugs. The architecture of Adobe’s AVM has multiple flaws allowing attackers to craft reliable exploitation techniques like ROP shellcode on the fly, thus bypassing ASLR, DEP and other protections. Although [some vendors dropped their support of Flash](#), completely eliminating the plug-in will be difficult, given its continued use in Web media, entertainment and advertising applications. The drop-off in Internet Explorer exploits can likely be explained by the addition of new product security measures such as sandboxing, isolated heap and Control Flow Guard. As always, it is only a matter of time before attackers innovate around such measures.

Exploit Kit Trends

Drive-by-download attacks remain a serious issue for Internet users. They have been on the decline due to improved exploitation mitigation techniques, but are far from gone. Case in point, we noted earlier in this report the volume of Web-based infections triggered by malicious advertising.

Just like in 2014, exploit kit writers kept their exploits up to date for new vulnerabilities. From 2010 through 2012 most of the incorporated exploits were at least one year old [2]. In 2013, this trend changed with a focus on Java exploits.

For the last two years exploit kits have been known to include almost entirely new and up-to-date exploits.

FIGURE 3: ESTIMATED DISTRIBUTION OF MOST ATTACKED PRODUCTS IN EXPLOIT KITS

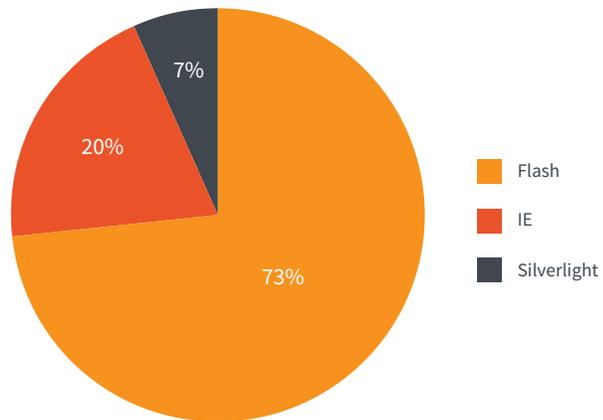


Figure 3 shows the distribution of popular exploited software in exploit kits during 2015. Thanks to the outburst of the Flash vulnerabilities, this year was particularly profitable for the malware underground. New exploits mean better infection rates and more sales on the black market.

Aside from Flash, several Internet Explorer vulnerabilities were actively used by exploit kits (lately it has only been CVE-2015-2419) as well as a Silverlight vulnerability earlier this year (CVE-2015-1671). Exploit kits continue to infect their victims with similar payloads. However, the developers of Web malware also seem to adopt new technologies, such as the use of Diffie-Hellman [3] to establish a secure communication for payload delivery. Although the research community criticized the implementation, it was good marketing for the malware sellers and it potentially may evolve into an effective protection for exploit delivery. Traditional banking Trojans and backdoors such as Dridex and Fareit remain among the most popular malware payload delivered by exploit kits, despite the huge spread of crypto-ransomware.

Angler remains the most active exploit kit used in the majority of incidents we observed through 2015. It also is usually the fastest to adapt to the changes in the vulnerability landscape. As browsers started blocking Flash, the Angler developers added an IE exploit (CVE-2015-2419) to compensate for the declining infection rates. Other notable exploit kits include Fiesta, Magnitude, Neutrino, Nuclear, Sweet Orange and Rig.

Macro-Malware via E-Mail Spam

Companies keep getting hit by socially engineered phishing e-mails containing malicious Microsoft Word documents and Excel spreadsheets. These files contain malicious macros, which download and execute malware from the attacker's server. Office does not allow running macros by default so the tricky part for an attacker is to convince a user to enable them.

One way to do this is to pretend to be a legitimate document with a legitimate macro. The file names such as "invoice_details," "resume" or "order quotations" may seem benign to a user, enticing them to click it, especially when they know it has passed antivirus and network filters. Evading these protections seems to be what malware writers are most concerned about.

A popular approach to evading detection is to copy large repositories of Visual Basic code to obfuscate malicious macros. The actual malicious code is negligibly small compared to these large repositories, making it difficult

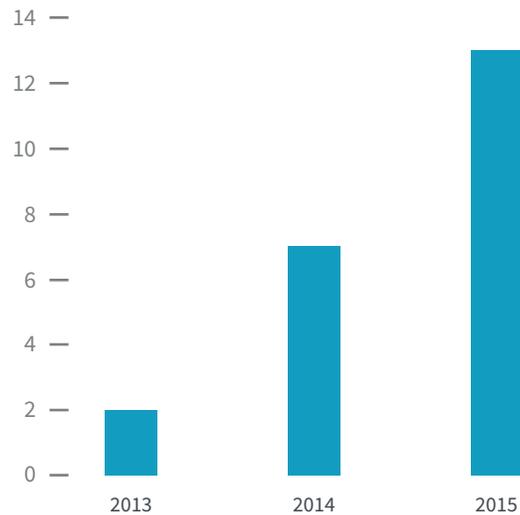
for malware scanners and analysts to detect the attack. The code is usually obfuscated to evade signature scanners. Due to the large amount of noise, it may even break statistical learning algorithms [4].

High volumes of macro malware can be attributed to a reaction to increasing product security measures (isolated heap, Control Flow Guard). As shown in Figure 2, until 2014 the number of working exploits for drive-by-download related software was in decline. In response, cybercriminals started revisiting old techniques to spread new malware.

Crypto-Ransomware

As Figure 4 shows, the number of crypto-ransomware releases is growing, with high diversity of malware families apparently developed by different malware groups. In 2015, about 10 different ransomware families were active. At the same time, we can see two evident market leaders: Cryptowall and TeslaCrypt. Cryptowall has reached its fourth release and has now gained the ability to encrypt file names. The TeslaCrypt team seems to be maintaining cosmetic changes, such as encrypted file name extensions.

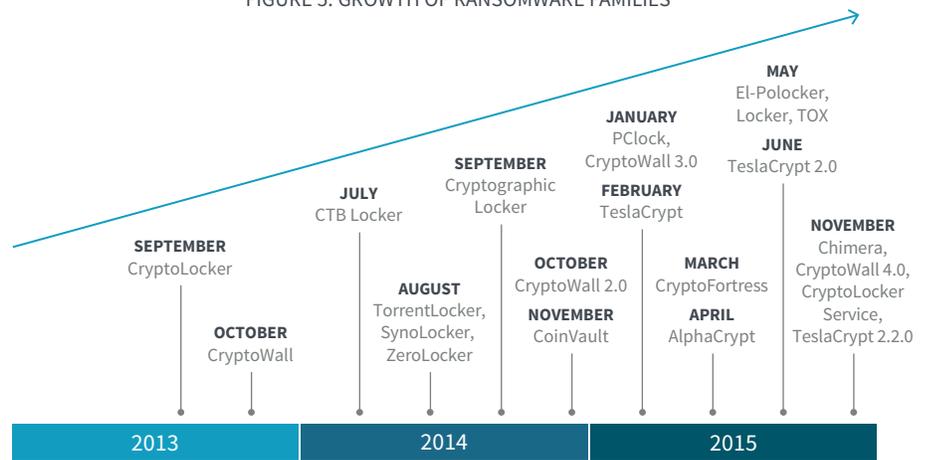
FIGURE 4: RANSOMWARE RELEASES BY YEAR



Two other crypto-ransomware families, TOX and Crypto Locker Service (CLS), turned to a slightly different distribution strategy. TOX is distributed for free, but takes 20-30 percent of the ransom. CLS costs \$50 and takes 90 percent of the ransom. In both cases, delivery of the malware and infection of the victim machines is up to the user. However, the share of TOX or CLS in the ransomware attacks observed by Bromium is minimal.

All the crypto-ransomware we encountered in 2015 was distributed either by drive-by-download attacks or by macro malware in spam e-mails.

FIGURE 5: GROWTH OF RANSOMWARE FAMILIES



Summary

2015 was yet another banner year from a cyber attacker’s perspective, particularly in terms of attack dissemination, using techniques new and old. Our report illustrated several trends that security practitioners—as well as network and endpoint defenders—should understand in order to best deploy resources and to minimize security risk. These trends include:

- The continued rise in vulnerabilities and exploits—we saw a huge spike of vulnerabilities and exploits targeting popular software, including Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Adobe Flash, Oracle Java and Microsoft Office.

- The prevalence of malvertising on the most popular websites. Bromium threat sensors identified malvertising attacks on 27 percent of the Alexa 1000.
- The resurgence of filter-resistant macro malware—macro malware, which masquerades as a legitimate Microsoft Office document, coupled with social engineering techniques, seemed to lay waste to gateway-based anti-malware defenses. We saw a rise in cleverly crafted examples designed to both fly under the radar of perimeter defense and trick users to open the file, enabling the attack to succeed.
- The robust market for ransomware—ransomware was also a key theme throughout this past year as attackers continued to exploit a business model where a user’s data is held for ransom by malware often leveraging encryption algorithms. We noted a 600 percent increase in the number of ransomware families, demonstrating an ongoing trend of innovation in the distribution.

The attacks in 2015 clearly demonstrate the attacker’s ability to bypass detection-based technologies—a trend that will continue in 2016.

For more information

To learn more about Bromium endpoint security solutions, contact your Bromium sales representative or channel partner. Visit us at www.bromium.com.

References

- [1] [Source: National Vulnerability Database nvd.nist.gov/](http://nvd.nist.gov/)
- [2] http://link.springer.com/chapter/10.1007/978-3-642-36563-8_13
- [3] https://www.fireeye.com/blog/threat-research/2015/08/cve-2015-2419_inte.html/
- [4] <http://labs.bromium.com/2015/12/03/a-micro-view-of-macro-malware/>

ABOUT BROMIUM

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks and prevent breaches. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching and remediation—transforming the traditional security life cycle.



Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information go to www.bromium.com
or contact sales@bromium.com

Copyright ©2016 Bromium, Inc. All rights reserved.
RPT.TR2015.US-EN.1601