Bromium®

Bromium Labs Research Brief

Endpoint Exploitation Trends H1 2014

Table of Contents

Executive Brief

The only constant in cyber security is change. Cyber-attacks come in cycles. Hackers always attack the weakest link in the chain and adjust their targets frequently. As a result of high profile attacks and the increasing spotlight on cyber-security, vendors are improving their software development practices, but in reality all software is vulnerable to attack. In the ever-shifting cyber-landscape the attackers' choice of targets is driven by the ease with which a particular product can be attacked, its importance to the intended targets of the attacker and how prevalent the software is in the market.

Security teams tasked with protecting critical enterprise assets need to track the shifting attack landscape to understand key trends in attack methods and targets. It is important to understand the changing dynamics of the battle against attackers because it enables organizations to make the most effective use of security personnel and defend against attacks in a more effective way.

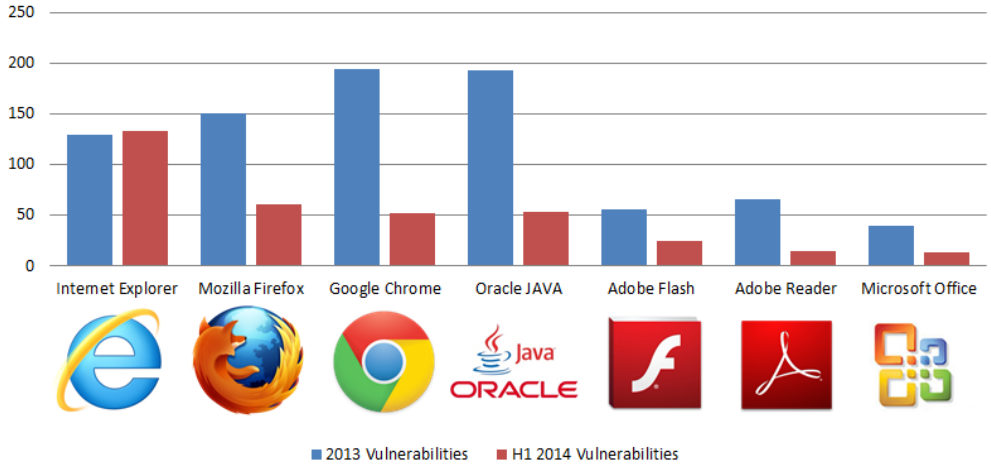
Bromium Labs studies key trends in the cyber-attack landscape on an ongoing basis. These latest trends should be factored into security planning in the months to come:

1. Microsoft® Internet Explorer set a record high for reported vulnerabilities in the first half of 2014.
2. Internet Explorer also leads in publicly reported exploits,
3. Web browser release cycles are becoming more frequent - as are initial security patches.
4. Adobe Flash is the primary browser plugin being targeted by zero day attacks this year.
5. New 'Action Script Spray' techniques targeting Flash have been uncovered in the wild exploiting zero day vulnerabilities.

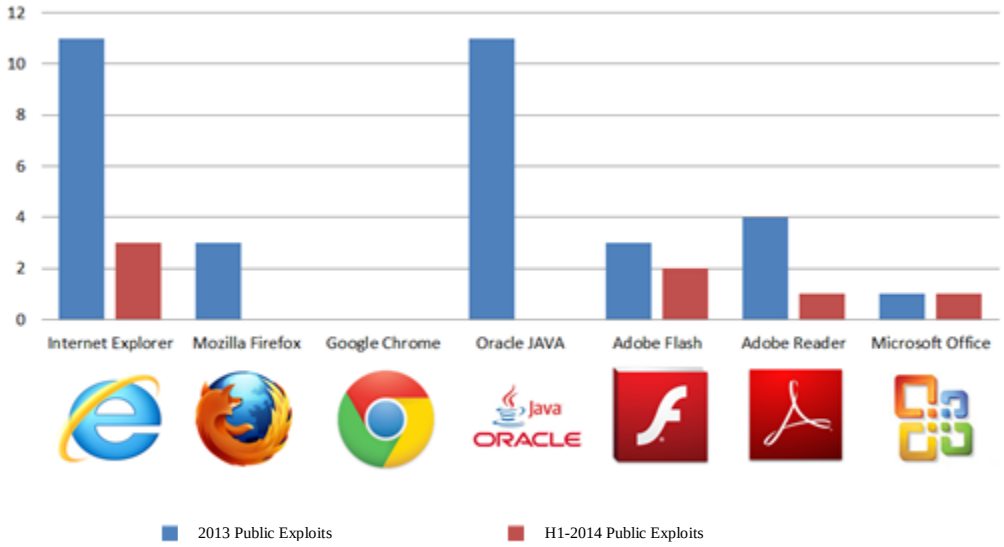
Vulnerability and Exploit Trends H1 2014

Zero day trends

In the first half of 2014, the growth in zero day exploitation continued unabated from 2013. Unsurprisingly, all of the zero day attacks targeted end-user applications such as browsers and productivity applications like Microsoft Office. Typically these attacks are launched leveraging users as bait using classic spear-phishing tactics. The notable aspect for this year thus far in 2014 is that Internet Explorer was the most patched and also one of the most exploited products, surpassing Oracle Java, Adobe Flash and others in the fray. Bromium Labs believes that the browser will likely continue to be the sweet spot for attackers.



Source: NVD



Source: exploit-db.com

It is notable that despite its past notorious reputation, Java had no reported zero day exploitation in the first half of 2014.

Internet Explorer 11 was released late last year and security patches seem to have emerged rather quickly, compared to its predecessors. We did an analysis of timelines for each release of Internet Explorer and when the first Critical patch emerged after it was Generally Available (GA).

Internet Explorer release to patch timeline

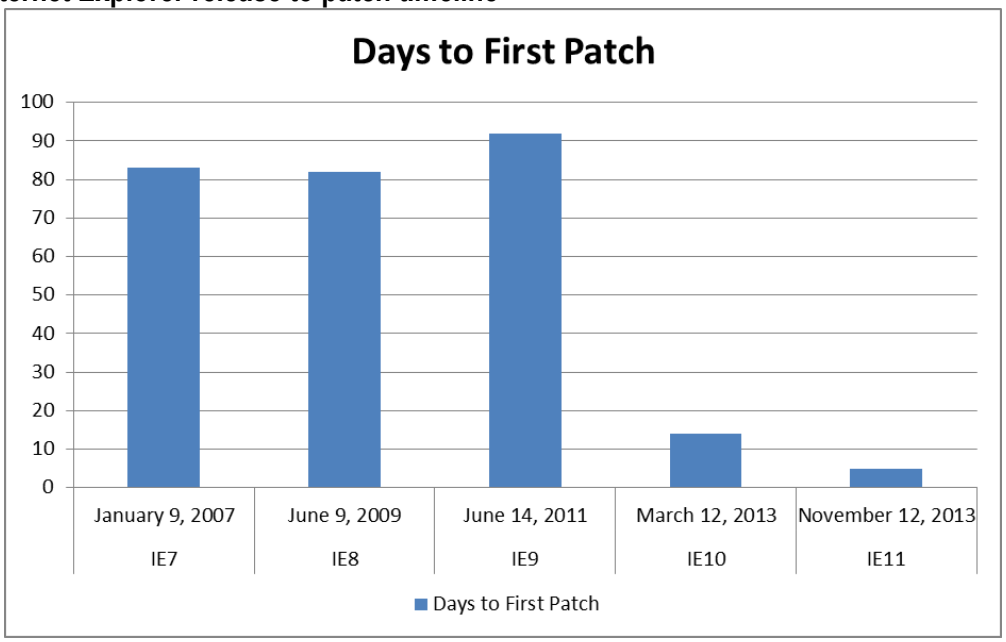


Fig: How long from the GA release of Internet Explorer until the first patch is released?

Notable Zero Day exploitation techniques
We've summarized the key exploitation trends that were observed for these zero days identified

Internet Explorer

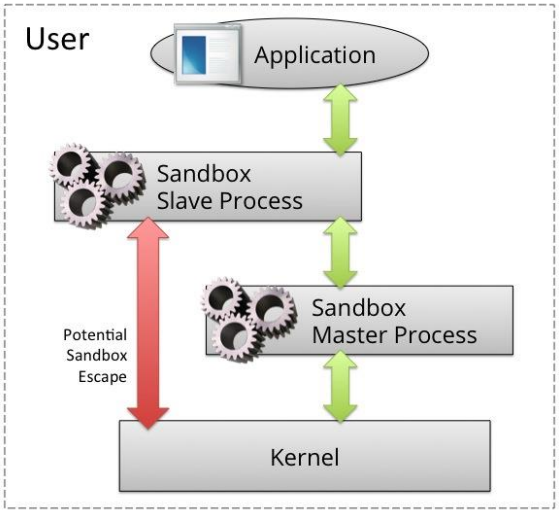
- Almost all Internet Explorer memory corruption exploits now use de facto ROP (Return Oriented Programming) techniques for bypassing the default Operating System security mechanisms (ASLR, DEP).
- Both the IE zero days exploits leveraged 'Action Script Spray' technique to bypass ASLR.

Adobe Flash

- Attackers were quick to leverage Adobe Flash new features released in late 2013 to exploit ActionScript Virtual Machine ASVM implementation flaws using 'Action Script Spray' techniques.
- Non-ASLR libraries continued to be the weakest link leveraged by malware authors to bypass OS protections.

Adobe Reader Sandbox Escape

- This vulnerability was uncovered in the wild late 2013 and finally patched in January 2014.
- Two vulnerabilities were used to bypass the Adobe Reader sandbox.
  - CVE-2013-3346: Use-after-free vulnerability in Adobe Reader
  - CVE-2013-5065: Kernel-mode zero day vulnerability NDProxy.sys



Adobe Flash Player and recent client exploits
2010-2013 were clearly the years of Java exploits. Since then a lot of things have changed: old versions of JRE are blocked in the browser by default, Java applets now require explicit activation from users so this attack vector becomes harder and harder to leverage. In response to ever increasing defenses deployed by security vendors and software developers attackers switched to other popular plugins. In the past 6 months, Adobe Flash Player was seen to be abused leveraging 2 attack vectors:

- Exploiting ASVM vulnerabilities
- Abetting exploitation of IE UAF bugs

Emerging 0-day exploitation techniques

Action Script Virtual Machine attacks

In 2014 there were three severe vulnerabilities that were detected in live attacks. Unlike Java where in most cases malicious code leverages JRE's capabilities, Flash exploits require DEP and ASLR bypass for successful execution. Table below gives a summary of 2014 ASVM attacks.

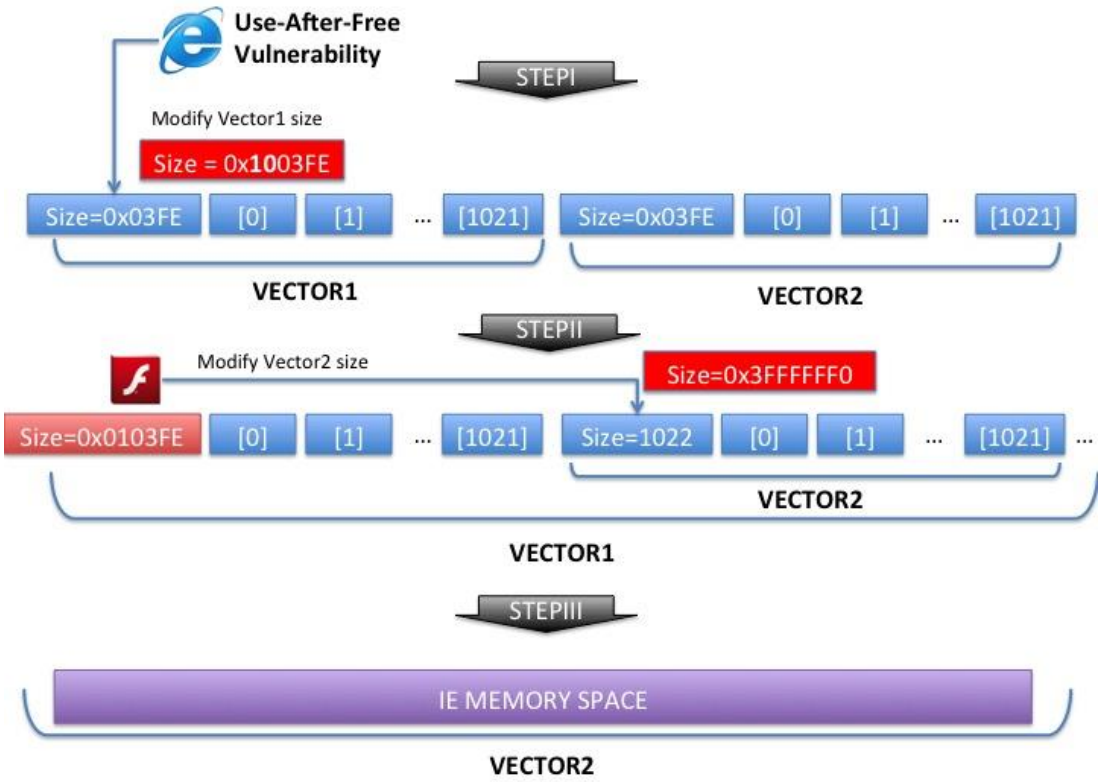
CVE	Vulnerability	Exploitation Technique
2014-0497	N/A	Non-ASLR libraries of Flash Player
2014-0502	Double Free of AS3 Shared Object	Non-ASLR libraries of JRE 1.6 and 1.7 and MS Office 2007 and 2010, ROP-chain is built relative to fixed offset
2014-0515	Heap overflow in compiled Shader	Dynamic ROP generation based on Action Script Spray

Unlike the first two exploits, CVE-2014-0515 used a relatively new technique to bypass ASLR allowing dynamic crafting of ROP chain called Action Script Spray. This technique was also seen in two IE exploits released this year.

ROP bypass using Action Script Spray

Both IE exploits released in 2014 (CVE-2014-1776, CVE-2014-0322) used Flash to build the ROP chain and launch shellcode. This technique leverages the way dense arrays are allocated in memory.

If a vulnerability allows an attacker to control the size of a vector they could make it as big as the whole memory space and then search for the necessary API calls and ROP gadgets. The following picture illustrates an Action Script Spray attack.



If the whole process memory is accessible, an attacker can now craft an ROP chain using ASVM capabilities and modify vtable with a pointer to the shellcode and trigger it.

The attack is more complex than a traditional heap spray, which indicates that cybercriminals are ready to invest more time and resources into development of new techniques in response to ever increasing protection measures. In addition to that, the prevalence of IE+Flash is much higher than IE+Java JRE, so this provides the attackers with a bigger opportunity.

Conclusions

Attackers continue to increase the sophistication of their exploit techniques. Internet Explorer and Adobe Flash are the targets of choice in the first half of 2014.

Action Script Sprays are a new technique to exploit Adobe Flash that has been seen in the wild. We expect to see similar techniques in the months to come. This is further evidence that the world of Web browser plugins presents a weak link that is just waiting for exploitation in the future.

Web browser release cycles are compressing and the interval between the general availability of a new release and the appearance of the first security patches has been decreasing recently. This may represent greater efforts on the part of software manufacturers to secure their products, or it may represent products being released to market with less security testing than earlier versions received. Notably 'Use-After-Free' type vulnerabilities were the favorite of zero day attackers.

Much attention was paid to JAVA exploits in 2013 and countermeasures such as disabling JAVA may have had a role in forcing attackers to switch to new targets this year. Regardless of the causes, zero day exploits in JAVA have experienced a recent lull in activity. Time will tell.

References

http://blogs.mcafee.com/mcafee-labs/flash-zero-day-vulnerability-cve-2014-0497-lasts-84-days

http://nvd.nist.gov/

http://en.wikipedia.org/wiki/Internet_Explorer

https://technet.microsoft.com/en-us/security/bulletin

Appendix

Oracle Java Runtime Environment

Year	National Vulnerability Database	Exploit-DB
2013	193	11
H1-2014	54	0

Adobe Flash Player

Year	National Vulnerability Database	Exploit-DB
2013	56	3
H1-2014	25	2

Microsoft Internet Explorer

Year	National Vulnerability Database	Exploit-DB
2013	130	11
H1-2014	133	3

Microsoft Office

Year	National Vulnerability Database	Exploit-DB
2013	40	1
H1-2014	13	1

Adobe Reader

Year	National Vulnerability Database	Exploit-DB
2013	66	4
H1-2014	15	1

Mozilla Firefox

Year	National Vulnerability Database	Exploit-DB
2013	150	3
H1-2014	61	0

Google Chrome

Year	National Vulnerability Database	Exploit-DB
2013	194	0
H1-2014	52	0

Exploited CVEs (2013 and H1-2014)

JRE 2013

1. CVE-2013-0422
2. CVE-2013-0431
3. CVE-2013-1488
4. CVE-2013-1493
5. CVE-2013-2416
6. CVE-2013-2419
7. CVE-2013-2423
8. CVE-2013-2460
9. CVE-2013-2465
10. CVE-2013-2470
11. CVE-2013-2472

Oracle JRE2014

N/A

Flash Player 2013

1. CVE-2013-0633
2. CVE-2013-0634
3. CVE-2013-5331

Flash Player 2014

1. CVE-2014-0497
2. CVE-2014-0515

IE 2013

1. CVE-2013-0025
2. CVE-2013-1311
3. CVE-2013-1347
4. CVE-2013-1451
5. CVE-2013-2551
6. CVE-2013-3184
7. CVE-2013-3205
8. CVE-2013-3893
9. CVE-2013-3897

10. CVE-2013-3918
11. CVE-2013-5045

IE 2014

1. CVE-2014-0282
2. CVE-2014-0307
3. CVE-2014-0322

Office 2013

1. CVE-2013-3906

Office 2014

1. CVE-2014-1761

Adobe Reader 2013

1. CVE-2013-0640
2. CVE-2013-2729
3. CVE-2013-2730
4. CVE-2013-3346

Adobe Reader 2014

1. CVE-2014-0514

Mozilla Firefox 2013

1. CVE-2013-0753
2. CVE-2013-1690
3. CVE-2013-1710

Mozilla Firefox 2014

N/A

Google Chrome 2013

Google Chrome 2014

N/A