RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: BR-T07

Exploitation Trends: From Potential Risk to Actual Risk

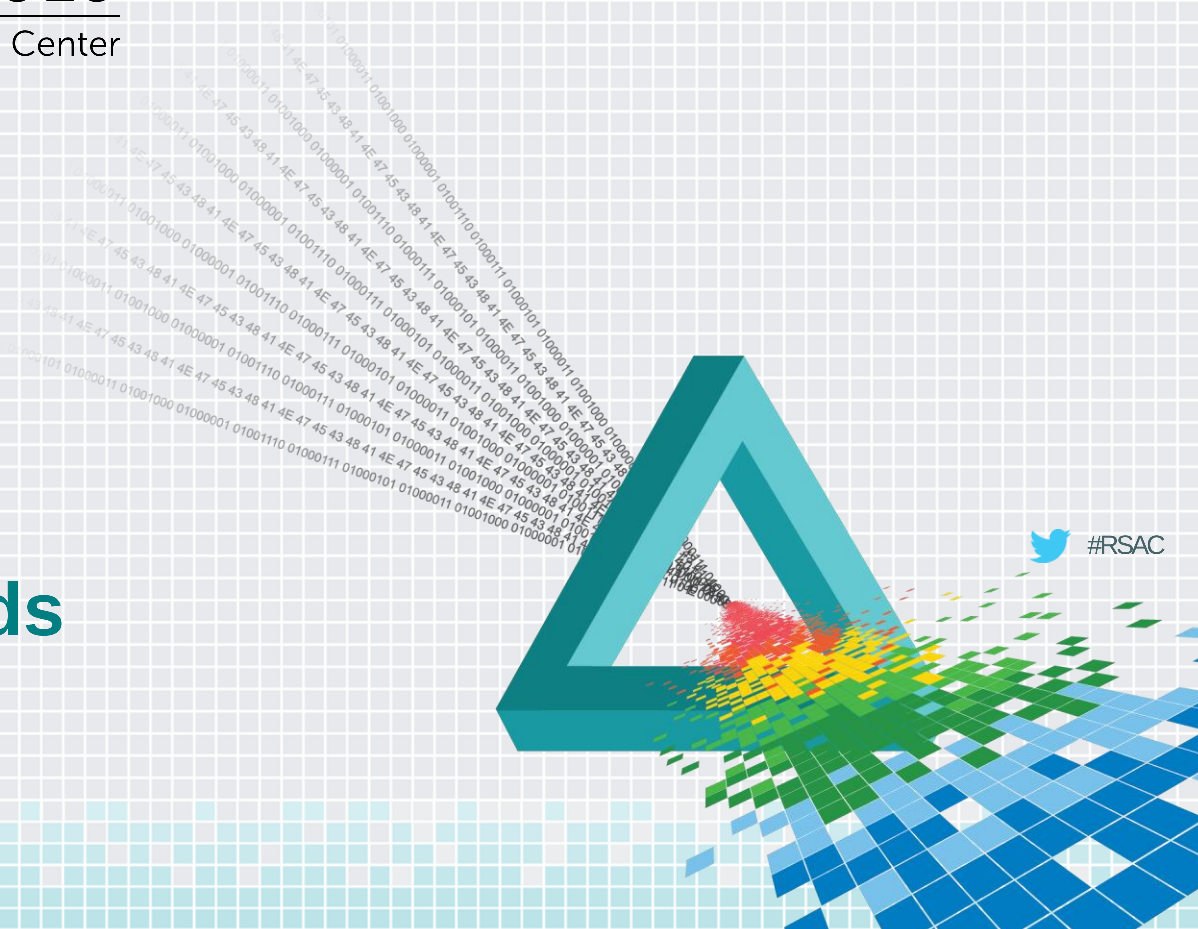
Tim Rains
Chief Security Advisor
WW Cybersecurity & Data Protection
Microsoft

Matt Miller
Principal Security Software Engineer
Microsoft Security Response Center
Microsoft

David Weston
Principal Program Manager
Operating Systems Group
Microsoft

RSAConference2015

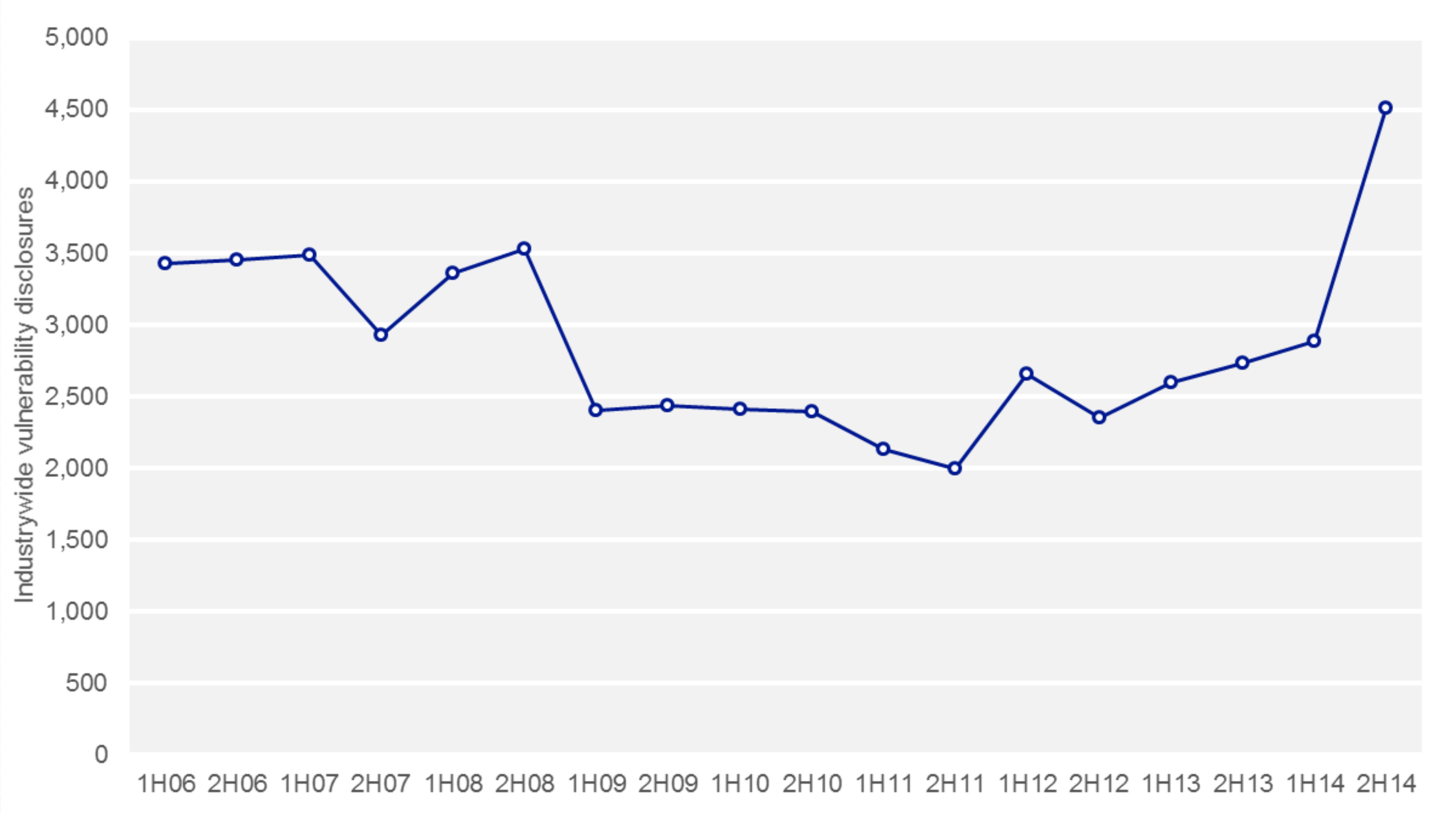
San Francisco | April 20-24 | Moscone Center



#RSAC

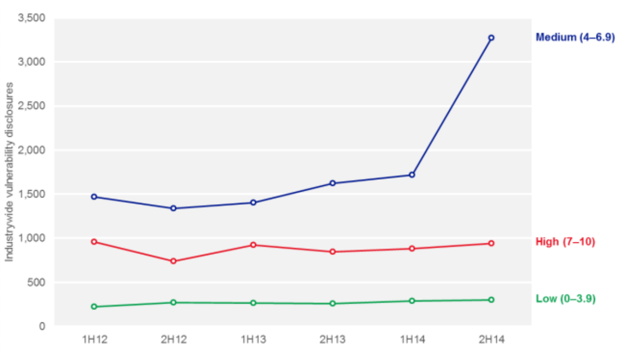
Vulnerability trends

Industry-wide vulnerability disclosures

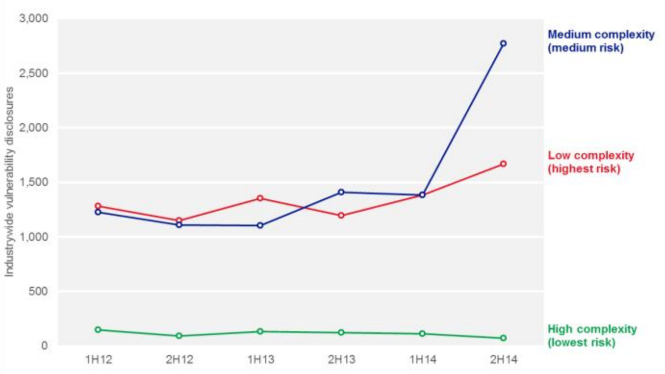


Industry-wide vulnerability disclosures

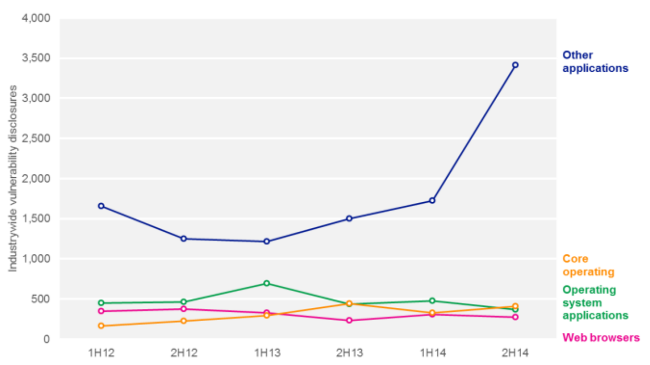
By severity



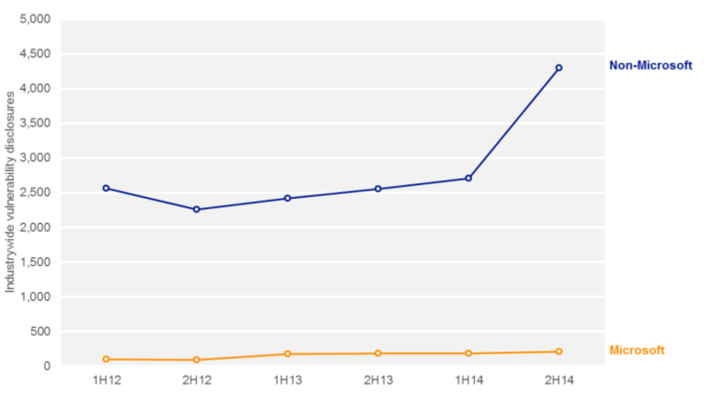
By access complexity



OS, browser, and application vulnerabilities

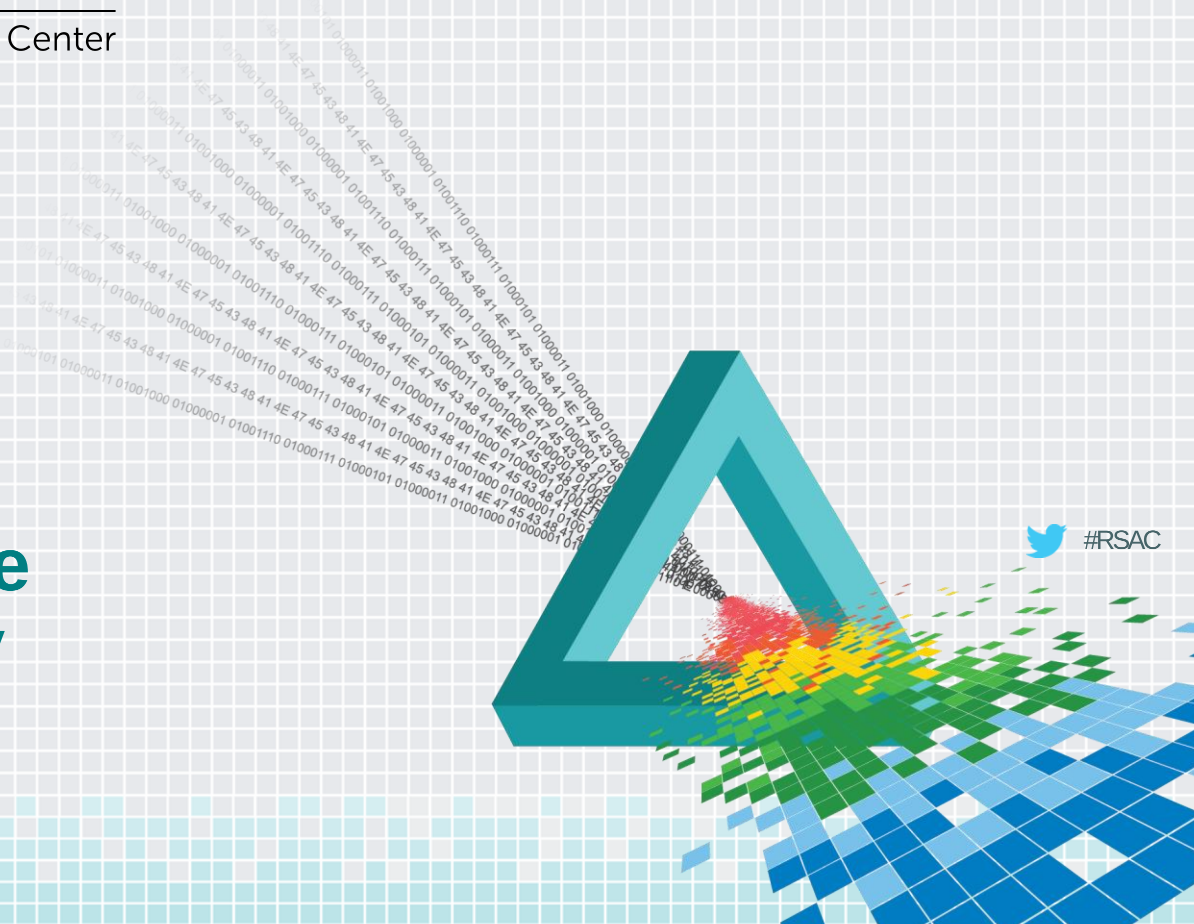


Industry-wide vulnerability disclosures



RSAConference2015

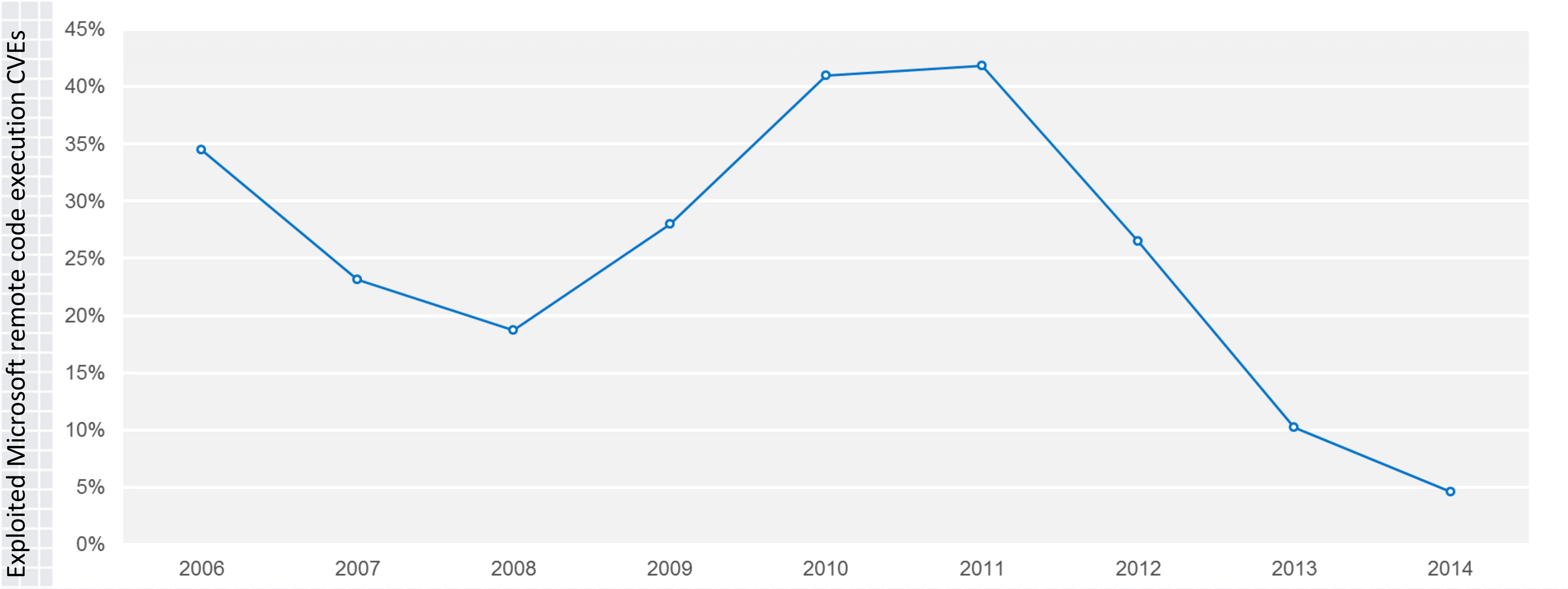
San Francisco | April 20-24 | Moscone Center



#RSAC

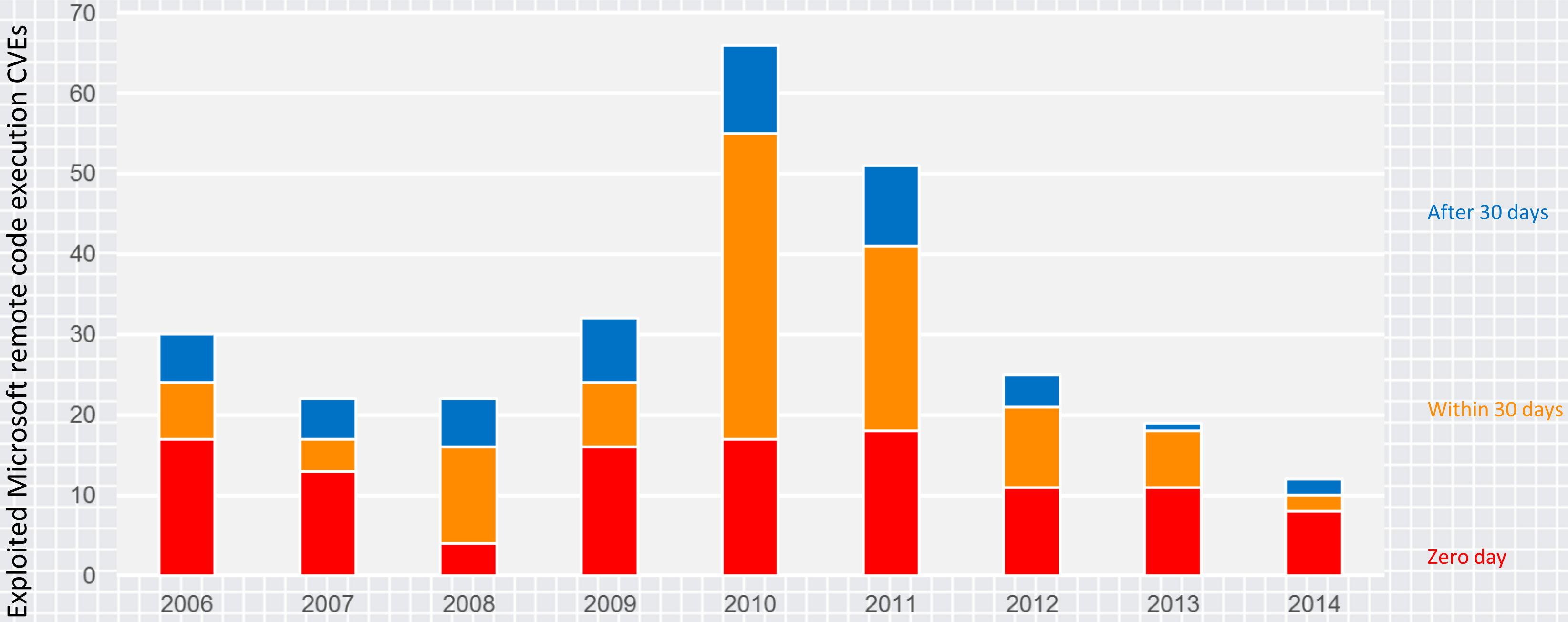
Microsoft software exploitation study

Microsoft remote code execution CVEs, by year



Remote code execution vulnerabilities are exploited in the minority of cases.

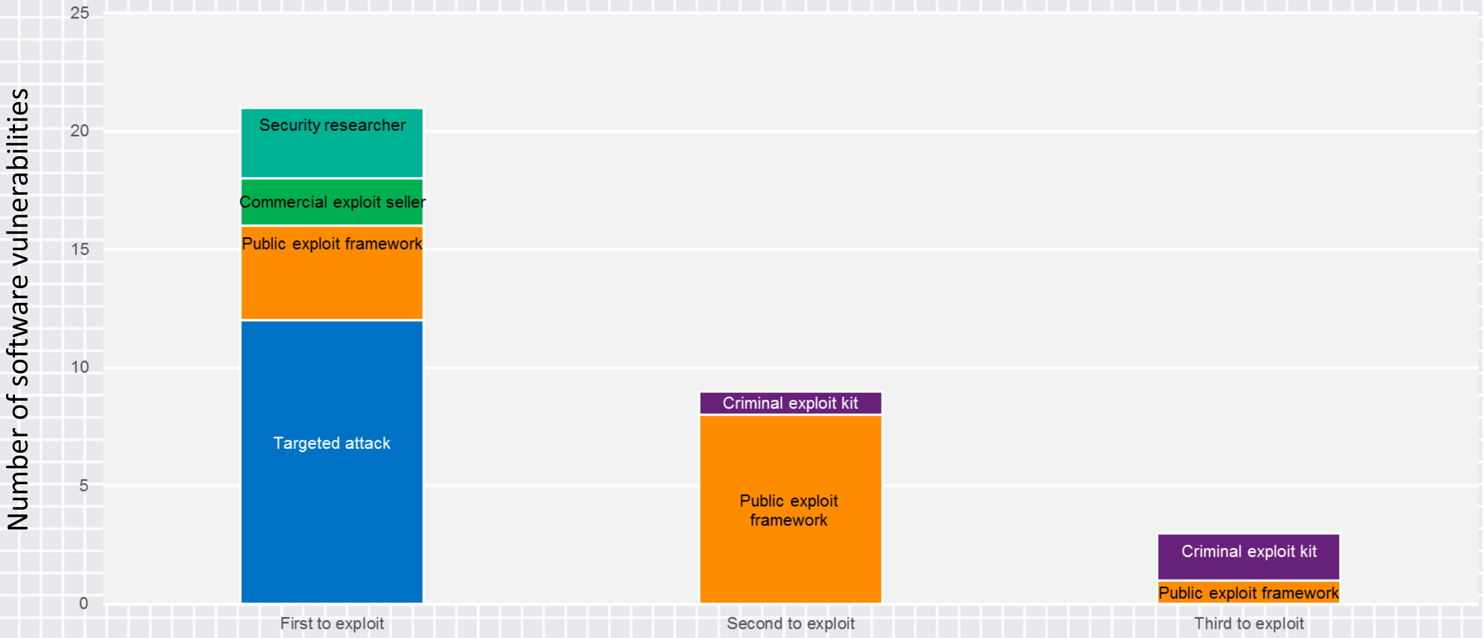
Microsoft RCE CVEs, by timing of first known exploit



Zero-day exploits have accounted for the bulk of Microsoft remote code execution vulnerabilities.

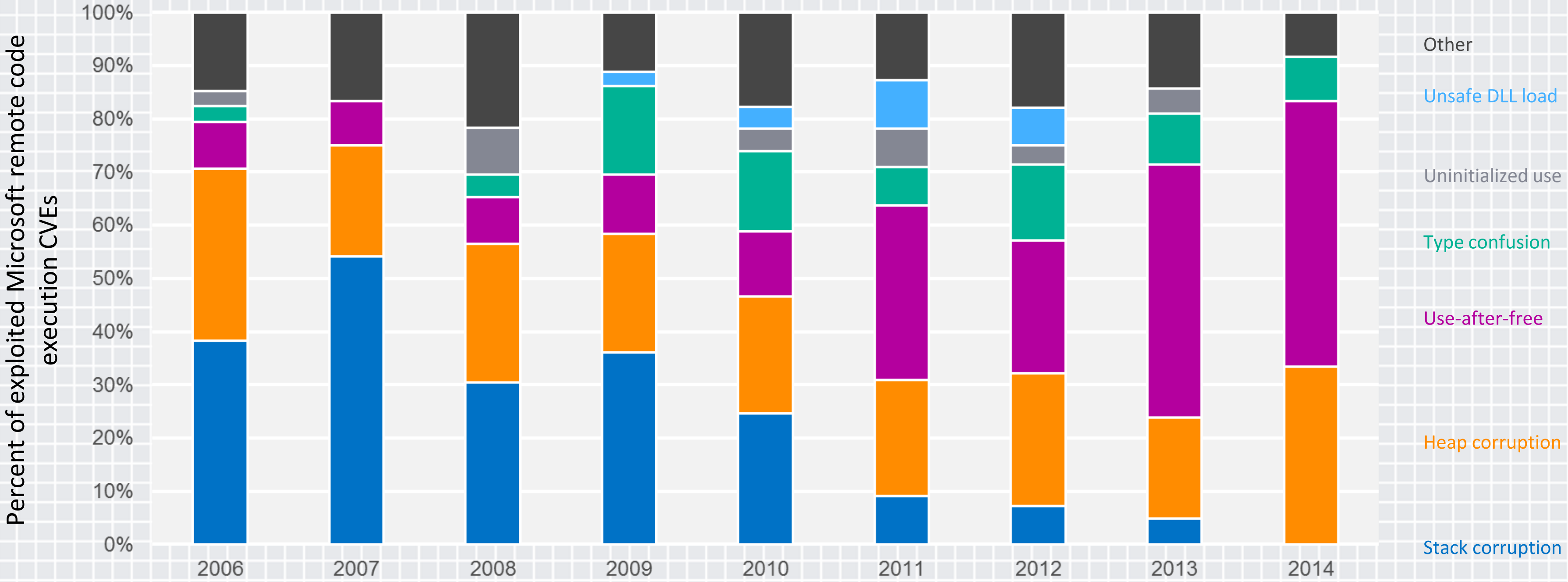
The number of Microsoft remote code execution vulnerabilities that are exploited continues to decline

Parties responsible for known exploits, Jan. 2012–Mar 2015



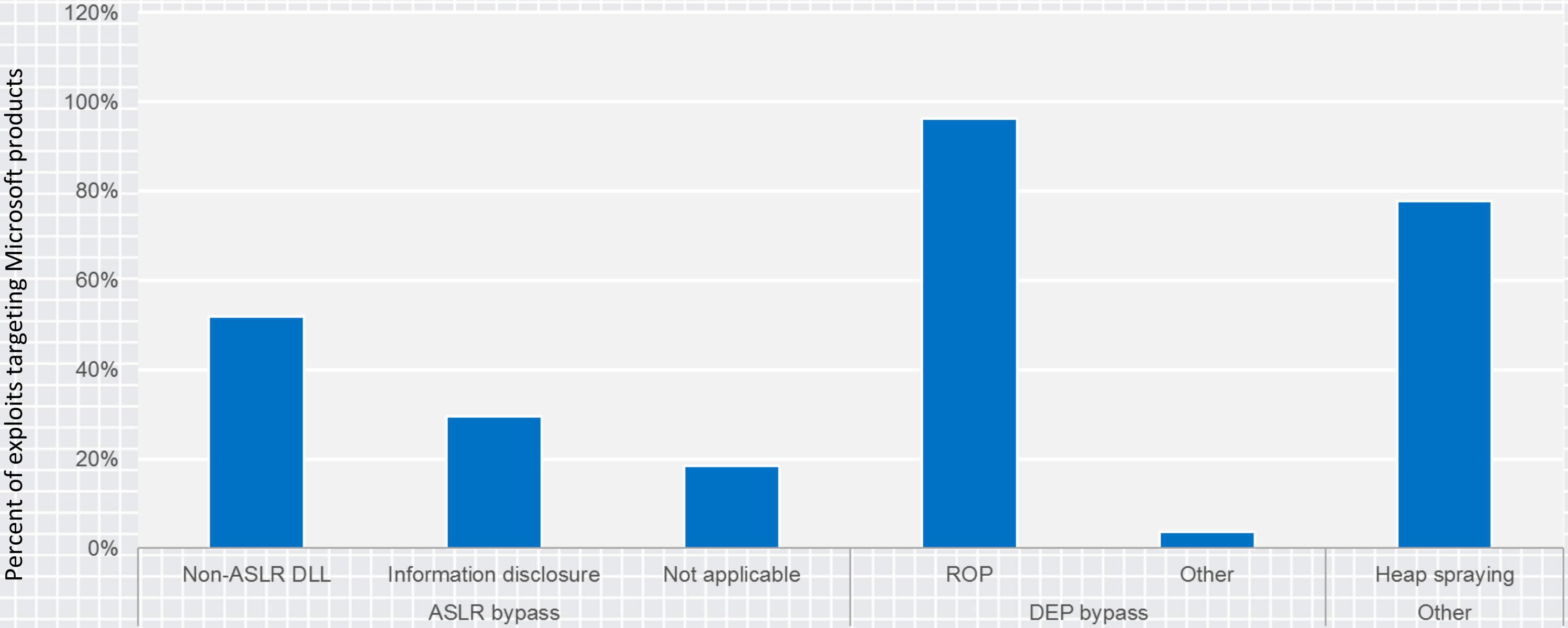
- Vulnerability disclosures originate from a variety of sources, from the dangerous to the beneficial.
- Criminal exploit kits affect a much larger number of people; until recently exploits were typically added to the kits several months after security updates that addressed the vulnerabilities were published and widely distributed.

Microsoft RCE exploitation root causes, by year



- Exploits for stack corruption vulnerabilities have declined – none were observed in 2014.
- Two factors that could be contributing to this decline are mitigations for stack corruption issues and increasing effectiveness of static analysis tools.

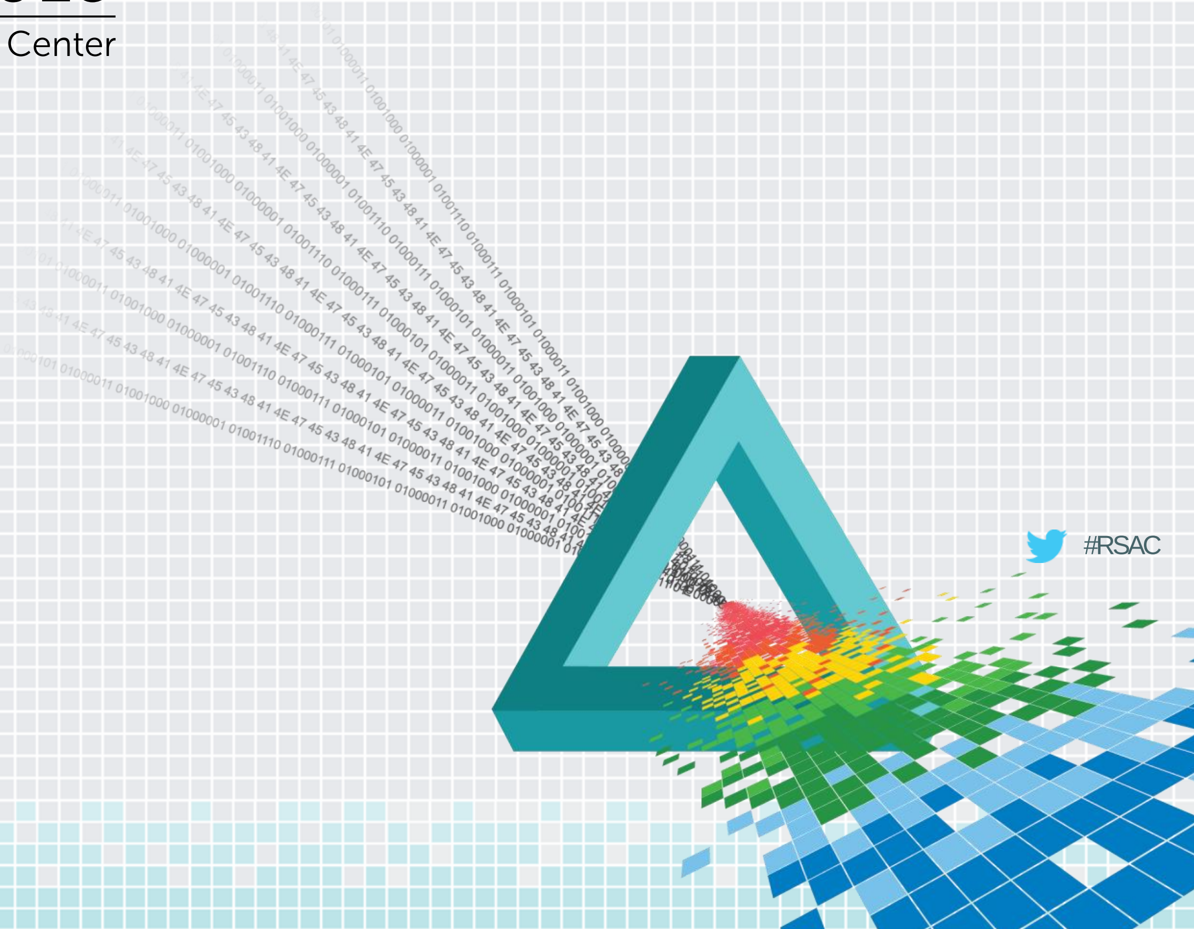
Exploit techniques, Jan. 2012–Mar. 2015



- The increasing prevalence of DEP and ASLR has forced attackers to identify new techniques that can be used to exploit vulnerabilities.
- Almost all exploits discovered in the last two years have used return-oriented programming techniques.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

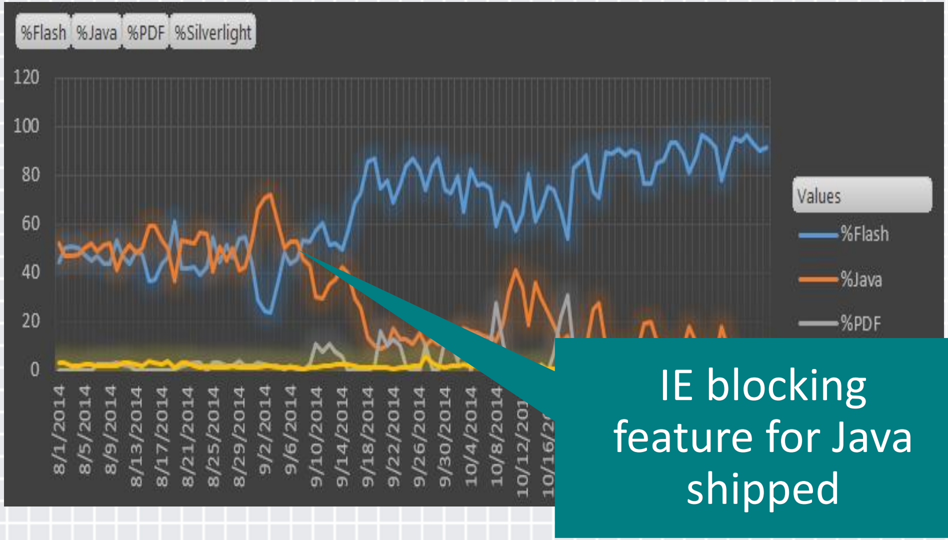


#RSAC

Exploit trends

Exploit Targets are Shifting

Flash Attack Trend Based on IEV Data



IE blocking feature for Java shipped

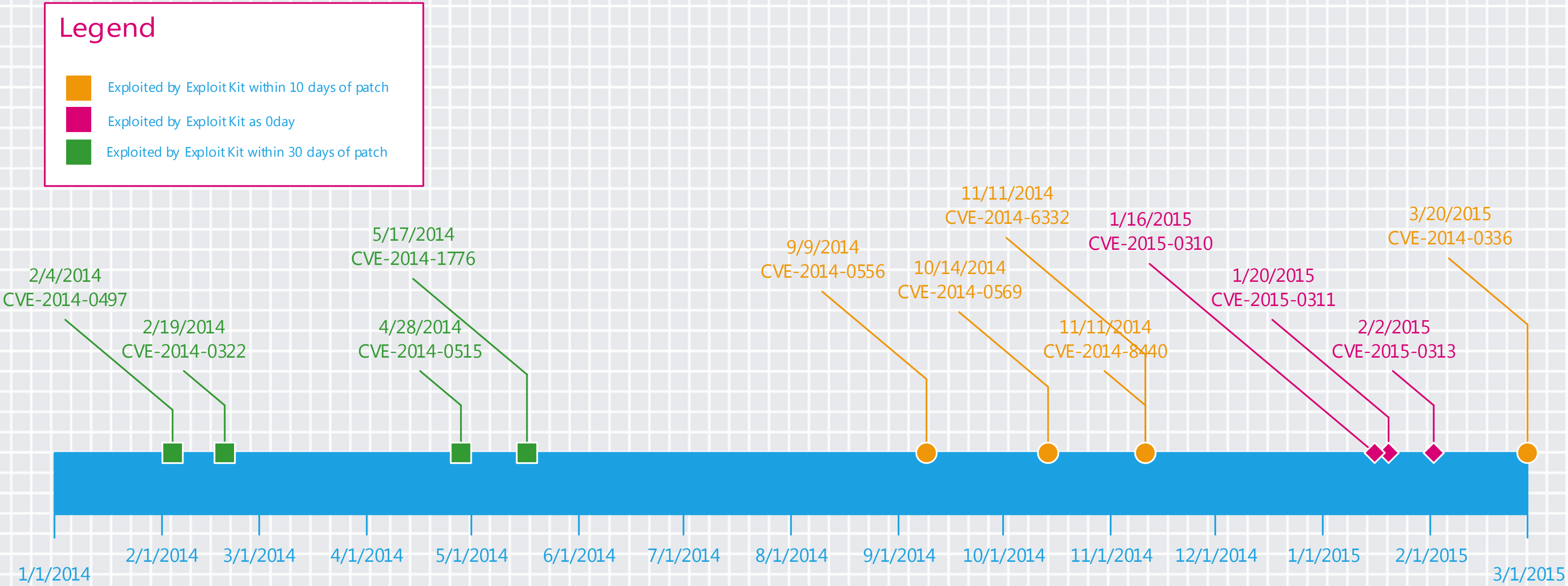
% of Flash user's that are out-of-date

	Win 8.1	Win 8	Win 7 SP1	Win 7 SP0
Total Out-of-Date	1.85%	7.53%	20.98%	23.27%

Exploit	In-the-Wild	Percentage of Users Vulnerable
CVE-2014-9163	Yes	20.98%
CVE-2014-8440	Yes	16.00%
CVE-2014-8439	Yes	16.96%
CVE-2014-0569	Yes	15.32%
CVE-2014-0556	Yes	13.96%
CVE-2014-0515	Yes	11.82%
CVE-2014-0506	Yes	11.56%
CVE-2014-0502	Yes	10.83%
CVE-2014-0497	Yes	10.53%
CVE-2013-5332	Yes	9.70%
CVE-2013-5331	Yes	9.70%

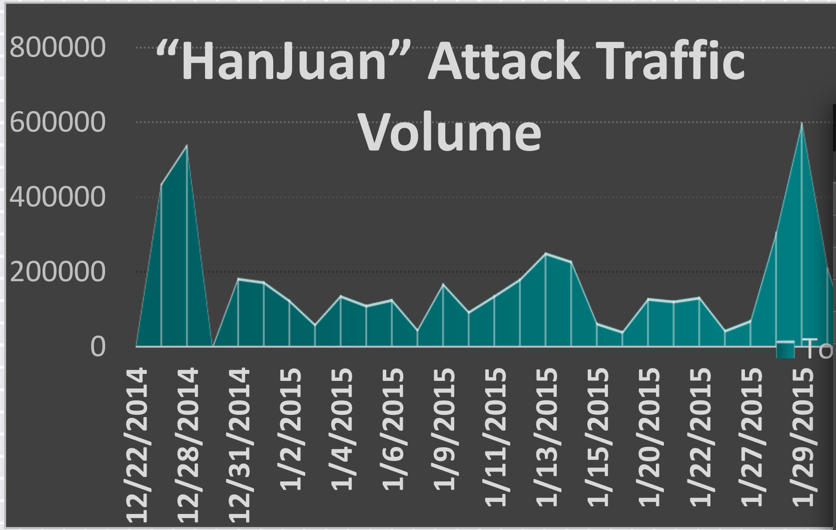
- 2014 saw a shift from a balanced targeting of Java and Flash to **over 90% focus on Flash**
  - The drop in Java exploits corresponds to a new IE feature which blocks the use of out-of-date Java
- New attacks on Flash increased in 2014
  - 5 of 8 new exploits integrated into Exploits kit in 2014 were Flash
  - 3 of 5 Flash exploits were exploited within 10 days of patch release

Time-to-Exploit-Kit is Decreasing



- 2014 saw commercial crimeware exploit kits shorten the timespan between availability of an update and exploit kit integration
- Early 2015 has shown exploit kits begin to integrate zero days with increasing regularity

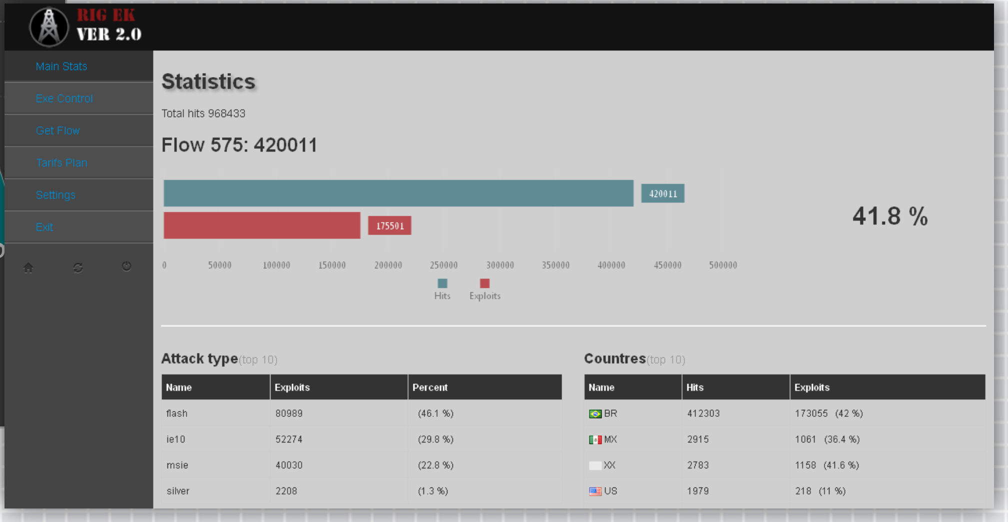
Exploit Impact Remains Large



“HanJuan” Attack Traffic Volume

The “HanJuan” exploit kit leveraged malicious ads to distribute a zero day Flash Exploit (CVE-2015-0311) to over 5 million users. The 0-day was discovered by Microsoft and Reported to Adobe

Image Credit: Spiderlabs



Statistics

Total hits 968433

Flow 575: 420011

41.8 %

Attack type(top 10)

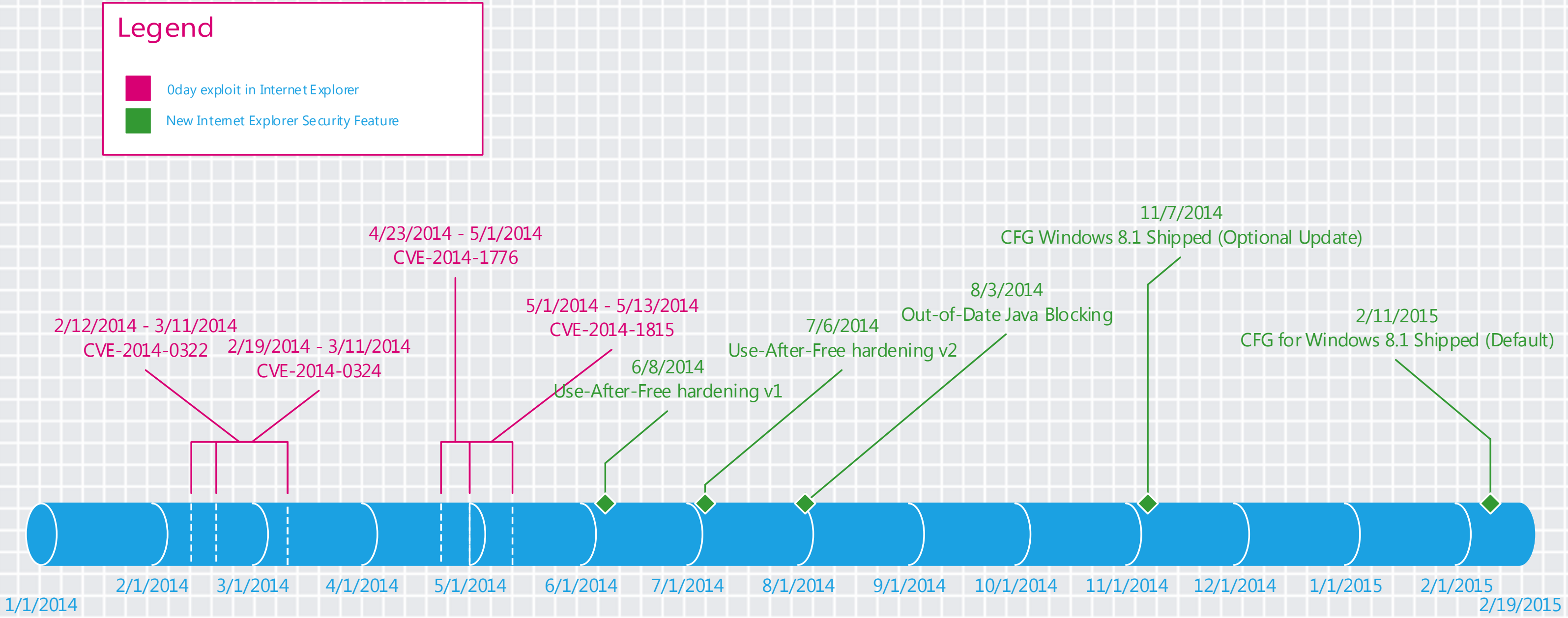
Name	Exploits	Percent
flash	80989	(46.1 %)
ie10	52274	(29.8 %)
msie	40030	(22.8 %)
silver	2208	(1.3 %)

Countres(top 10)

Name	Hits	Exploits
BR	412303	173055 (42 %)
MX	2915	1061 (36.4 %)
XX	2783	1158 (41.6 %)
US	1979	218 (11 %)

Exploit “panels” from the RIG exploit kit show that surprising success rates are still possible with older exploit due to chronic patching problems

IE Mitigations Impact new Exploits



Legend

🟥 0day exploit in Internet Explorer

🟩 New Internet Explorer Security Feature

2/12/2014 - 3/11/2014
CVE-2014-0322

2/19/2014 - 3/11/2014
CVE-2014-0324

4/23/2014 - 5/1/2014
CVE-2014-1776

5/1/2014 - 5/13/2014
CVE-2014-1815

6/8/2014
Use-After-Free hardening v1

7/6/2014
Use-After-Free hardening v2

8/3/2014
Out-of-Date Java Blocking

11/7/2014
CFG Windows 8.1 Shipped (Optional Update)

2/11/2015
CFG for Windows 8.1 Shipped (Default)

- No new remote code execution zero days in IE since shipping new use-after-free mitigations “out-of-band”
- Only **one new exploit in 2014** (CVE-2014-6332) and **one in 2015** (CVE-2014-4130) after shipping new exploit protections

Apply What You Have Learned Today

Next week you should:

Assess your risk based on exploit trends

In the first three months you should:

Get current on **security updates**

Within six months you should:

Use the **newest versions** of applications

Resources

- Microsoft Security Intelligence Report: http://microsoft.com/sir
- Microsoft Cyber Trust blog: http://blogs.microsoft.com/cybertrust/category/cybersecurity/
- Twitter: @MSFTSecurity

Malware Data From Over
600 Million Systems Worldwide

ONE SECURITY REPORT

The Security Intelligence Report (SIR) is an analysis of the current threat landscape based on data from internet services and over 600 million systems worldwide to help you protect your organization, software, and people.

View the Security Intelligence Report at **www.microsoft.com/SIR**

Microsoft | Security Intelligence Report