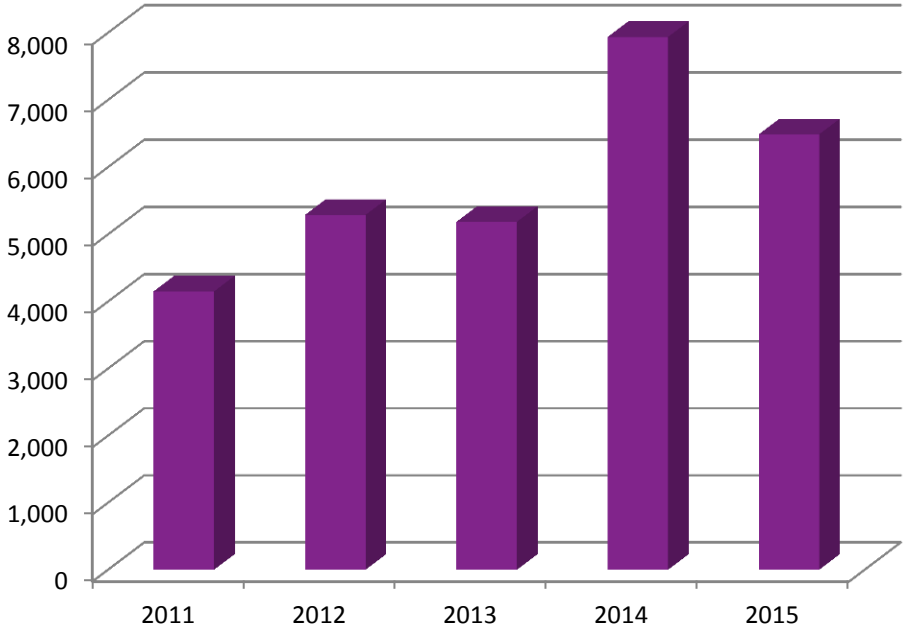
Overwhelmed By Security Vulnerabilities? Learn How to Prioritize Remediation

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

Vulnerabilities



QUALYS®

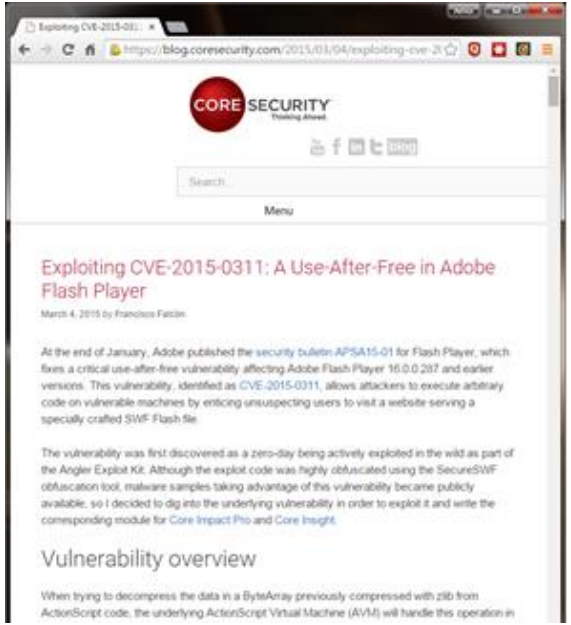
Vulnerability

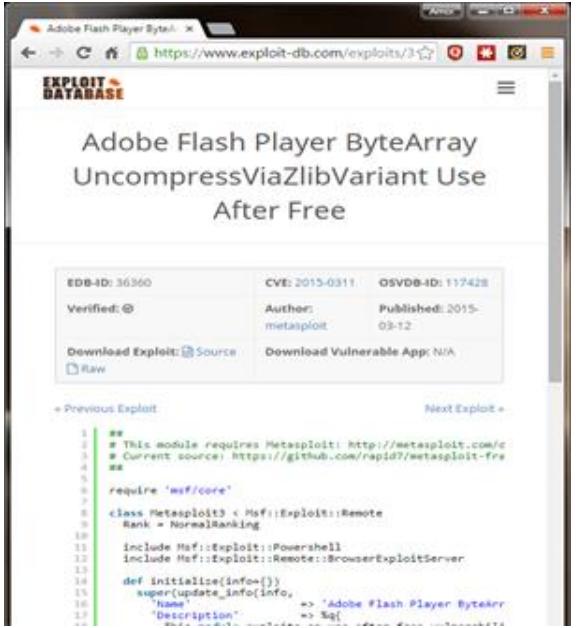
*Vulnerability is a **flaw** in the system that could provide an attacker with a way to bypass the security infrastructure.*

QUALYS®

Exploit

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





Exploit Frameworks Examples

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

QUALYS®

Exploit Kit

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.*

QUALYS®

Exploit Kit

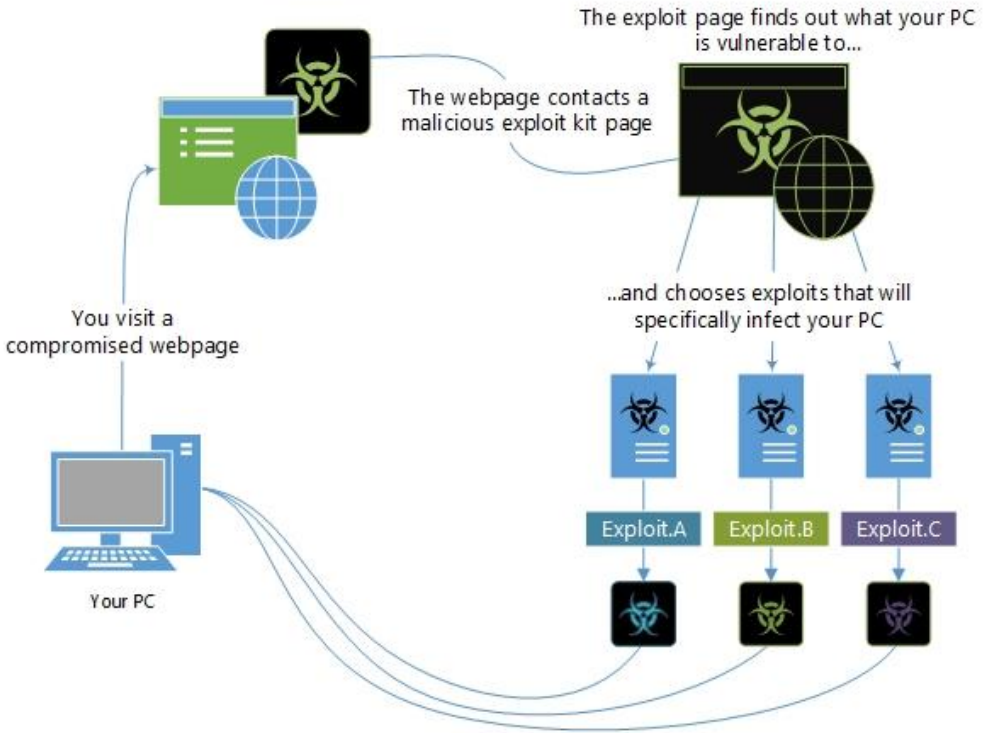
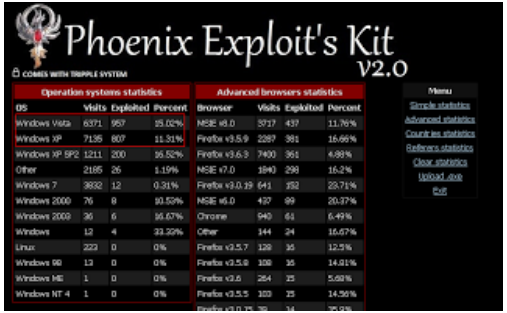


Image: http://www.microsoft.com/security/portal/mmpc/threat/exploits.aspx

Exploit Kit


crimepack


Phoenix Exploit's Kit
v2.0


NB Exploiter 2011 Build 2.0.1
NB EXPLOITER 2011
download/exec
windows/exec
add system user
bing shell
生成
官网
退出


Nuclear Pack v3.0

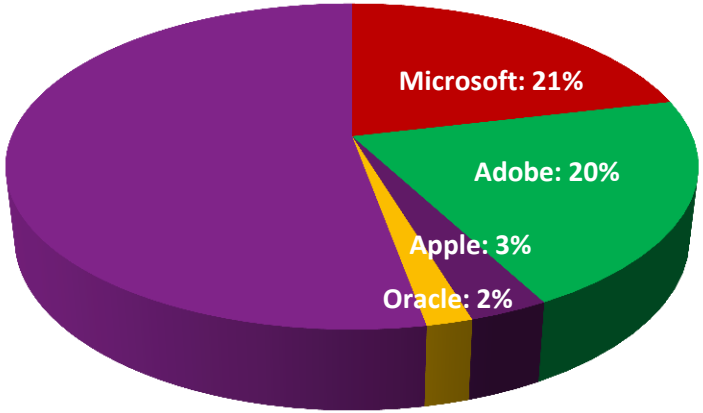
Exploit Kit Examples

QUALYS®

Exploit Trends

and how to use them to our advantage

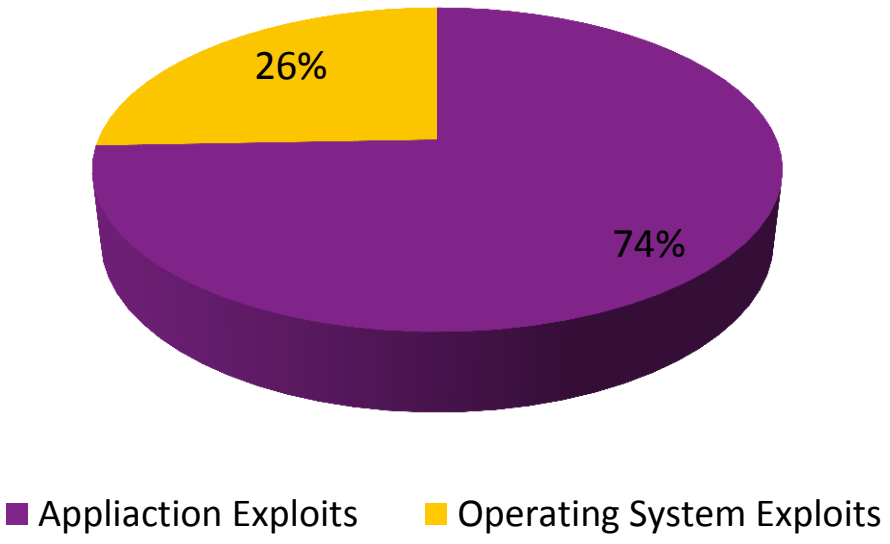
#1. Most affected



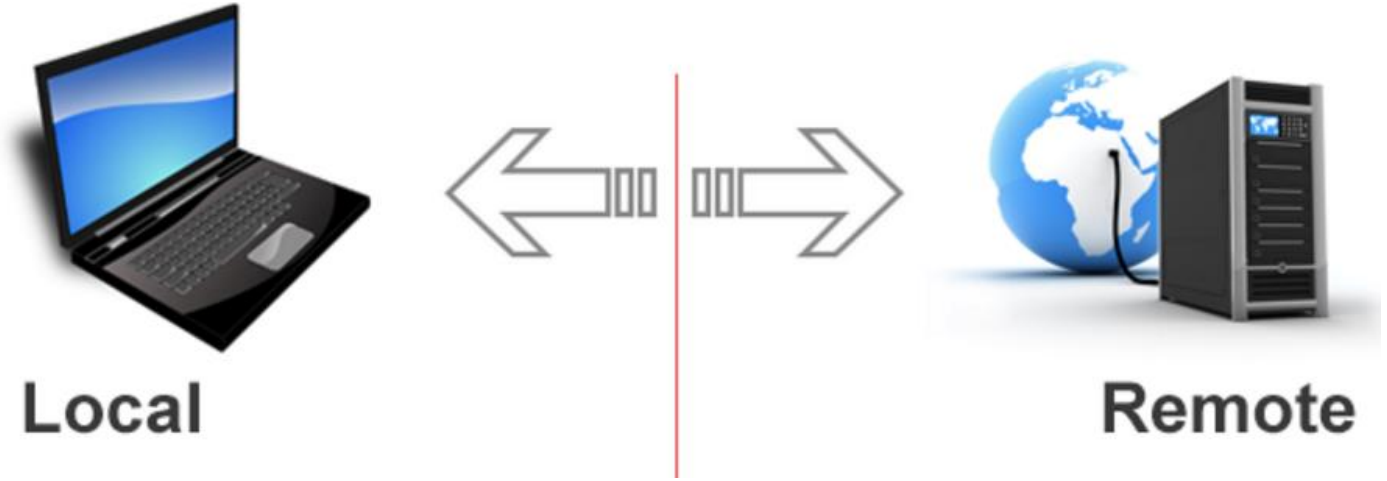
- microsoft
- pixabay_images_project
- foxitsoftware
- apport_project
- f5
- simple_ads_manager_project
- adb
- betster_project
- cups
- ericsson
- insanevisions
- magic_hills
- oxwall
- phpmybackuppro
- qlik
- sysaid
- webgroupmedia
- zend
- adobe
- redhat
- igniterealtime
- apptha
- genixcms
- thecartpress
- 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
- 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
- softsphere
- thycotic
- wotlab
- ferretcms_project
- debian
- novell
- cmsjunkie
- novius-os
- xceedium
- atlassian
- clip-bucket
- ecommercemajor_project
- gsm
- kcodes
- moodle
- persistent_systems
- pragyan_cms_project
- solarwinds
- two_pilots
- wpmembership
- goautodial
- d-link
- symantec
- dell
- refbase
- yuba
- auto-exchanger
- cloudbees
- ektron
- h5ai_project
- libmimedir_project
- npds
- pfsense
- proftpd
- sudo_project
- vboxcomm
- wpsymposium
- google
- elasticsearch
- wpml
- emc
- samsung
- zohocorp
- avinu
- crea8social
- elegant_themes
- horde
- linux
- ntop
- photocati_media
- projectsend
- sympies
- webgate
- xen
- joomla
- fortinet
- ajsquare
- etouch
- sefrengo
- accunetix
- beehive_forum
- cs-cart
- endian_firewall
- hp
- maarch
- nvidia
- php
- qemu
- synametrics
- webgateinc
- yoast

#2. Only 26% Exploits targeted Operating Systems

74% of Exploits Target Applications

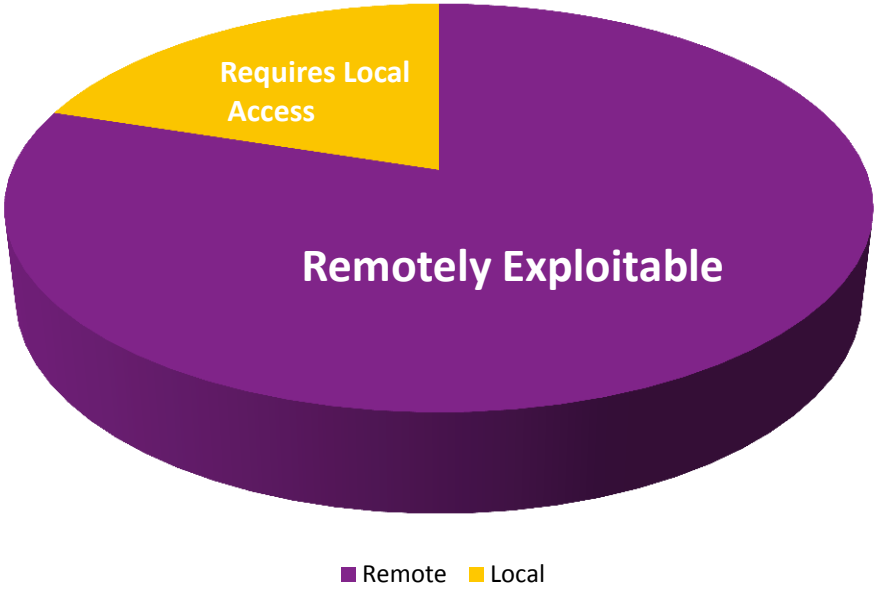


#3. Remote vs Local Exploits



#3. Remote vs Local Exploits

80% can be compromised Remotely

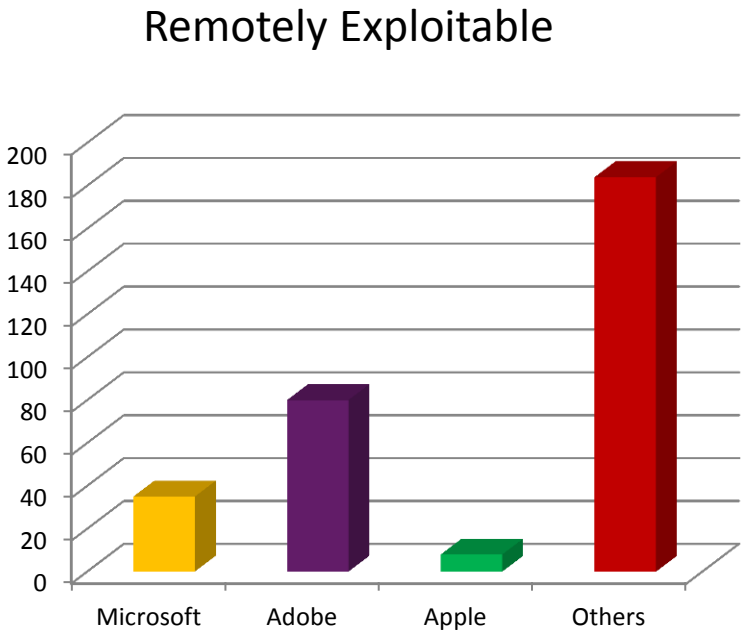


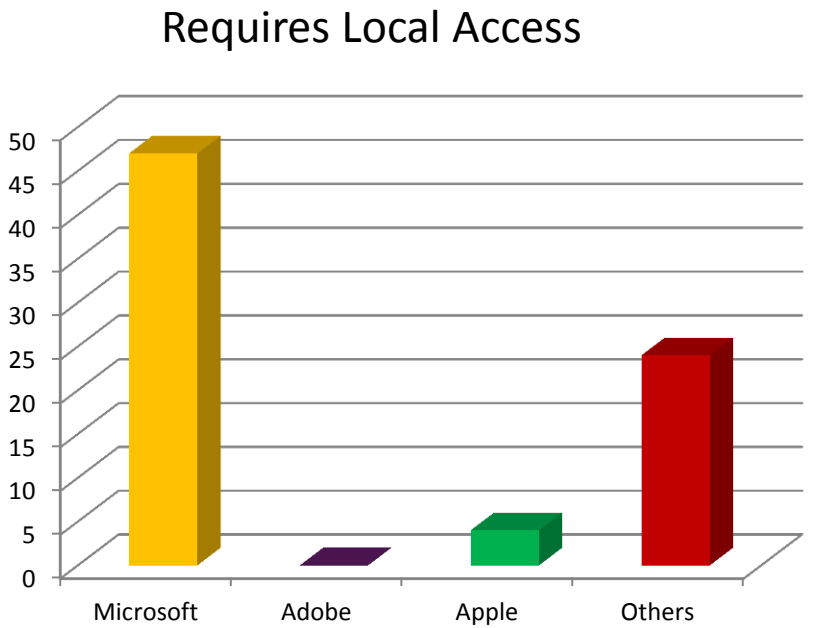
QUALYS®

#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





#4. Lateral Movement

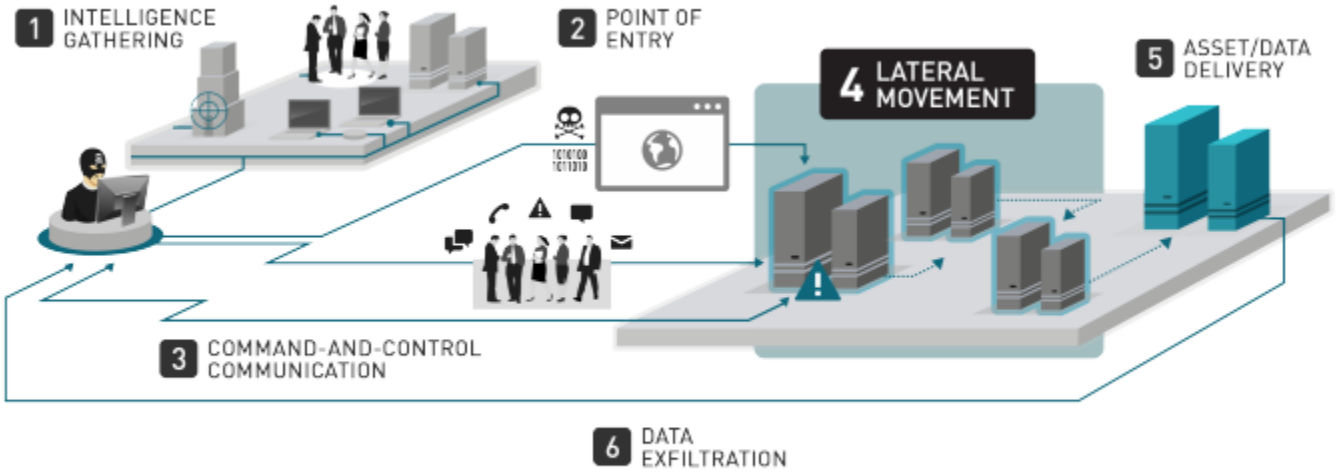


Figure 1. Six Stages of an APT attack

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

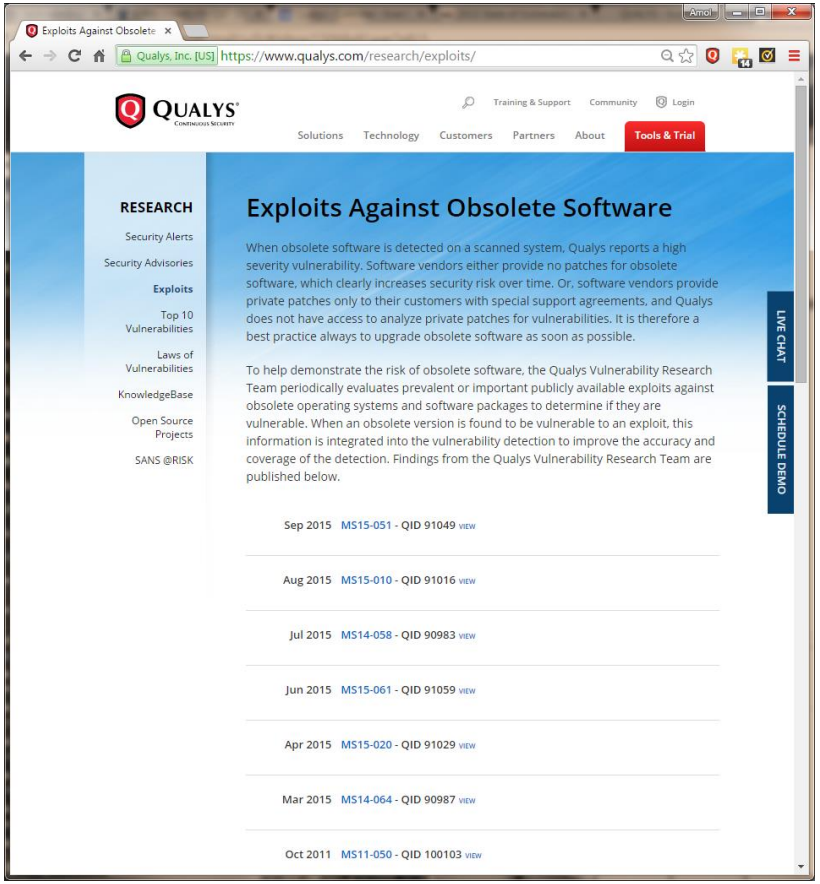
50% of Vulnerabilities had minimal Lateral Movement

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

QUALYS®

#5. Exploits for EOL Applications



Sep 2015 MS15-051 - QID 91049 HIDE

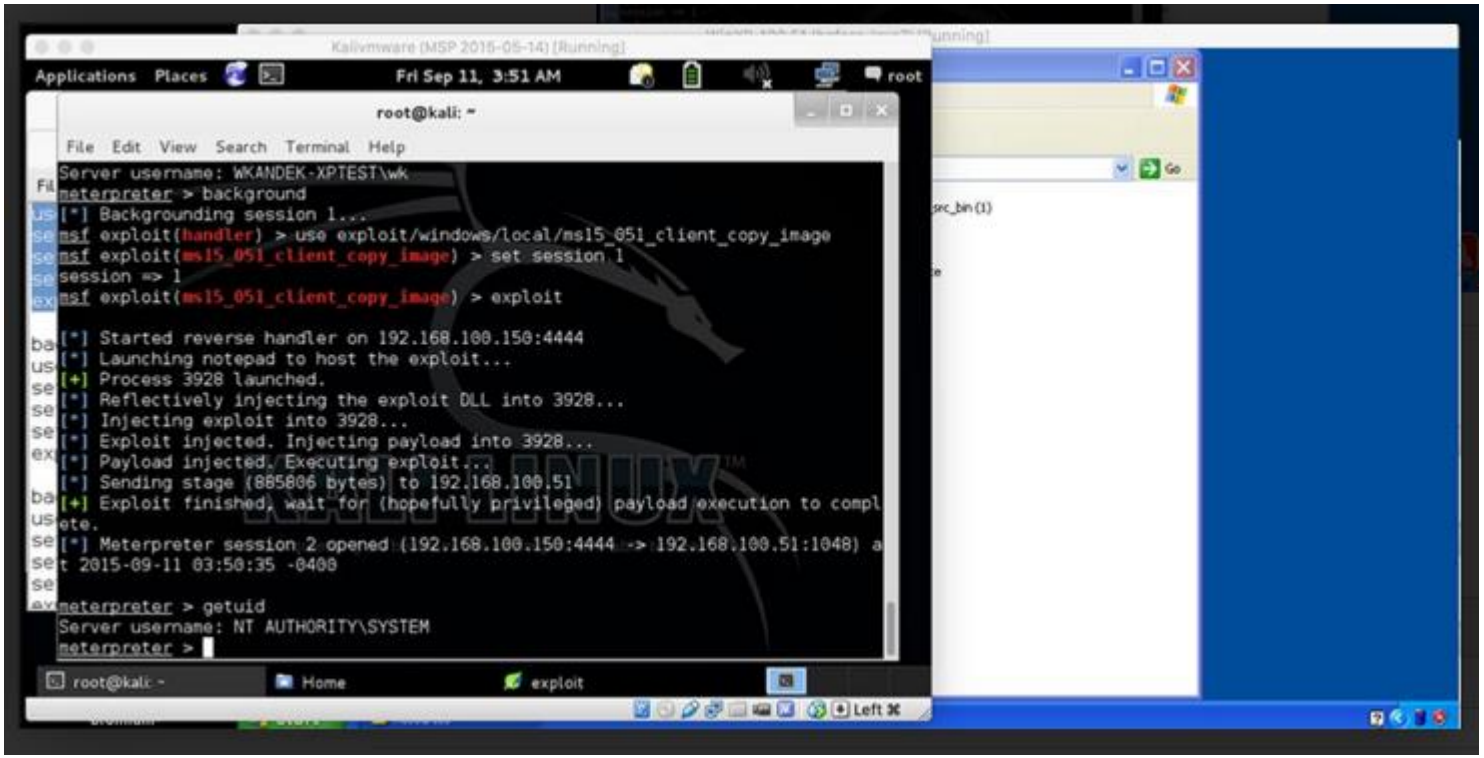
Vulnerable Software per Vendor Advisory: Windows 2003 - Windows 8.1 - see Microsoft Advisory for full detail

Exploit Used: Metasploit v4.11.4 - 2015071402

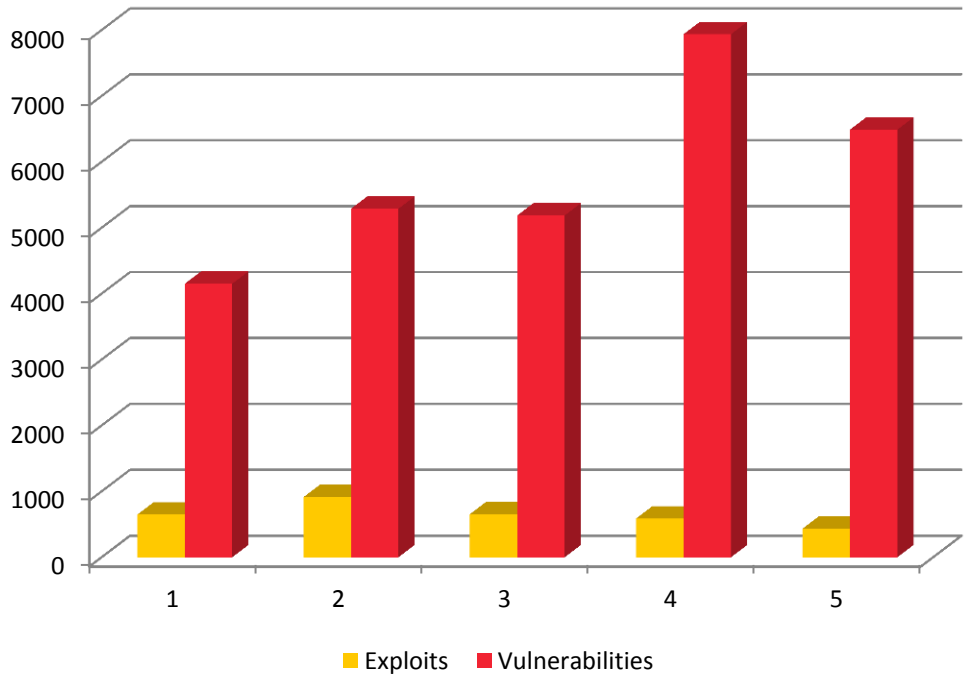
Findings:

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

#5
Exploits for EOL Applications



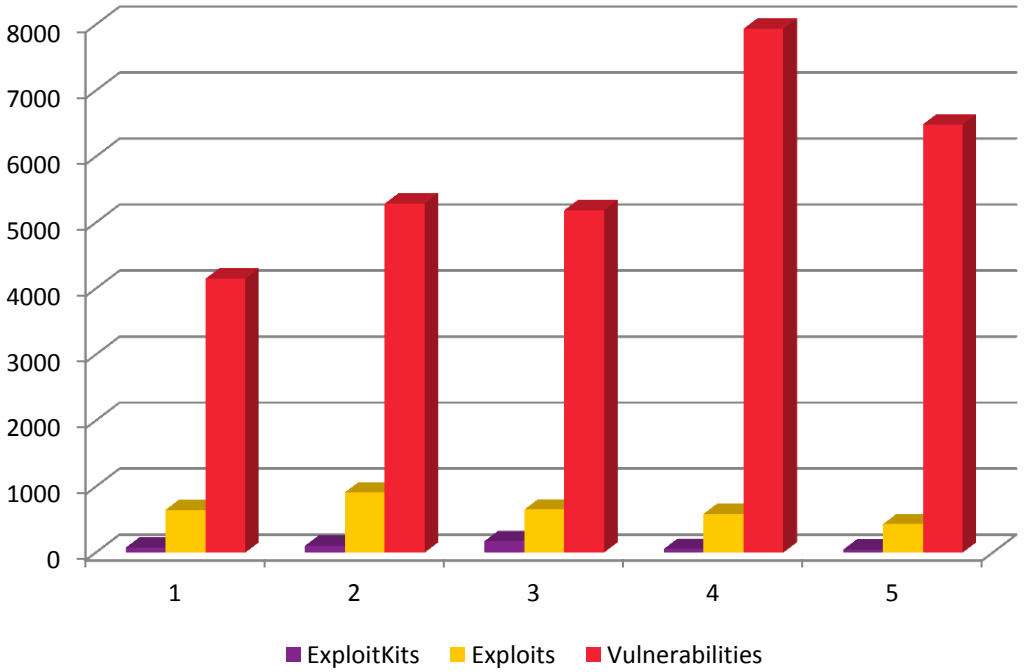
#6. Only 7% of Vulnerabilities in 2015 had an associated Exploit



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, Nutrino, 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, Nutrino, 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.

QUALYS®

Thank You

@amolsarwate