RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

SESSION ID: SPO1-T06

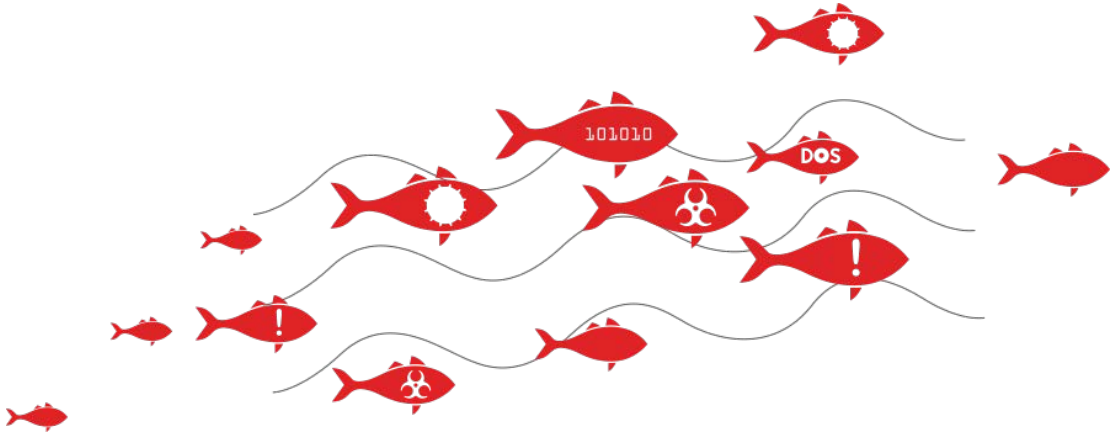
Evaluating Vulnerability Risk Exposure to Prioritize Remediation and Patching in Heterogeneous Environments

Hadi Jaafarawi

Managing Director
Qualys Middle East
@hjaafarawi

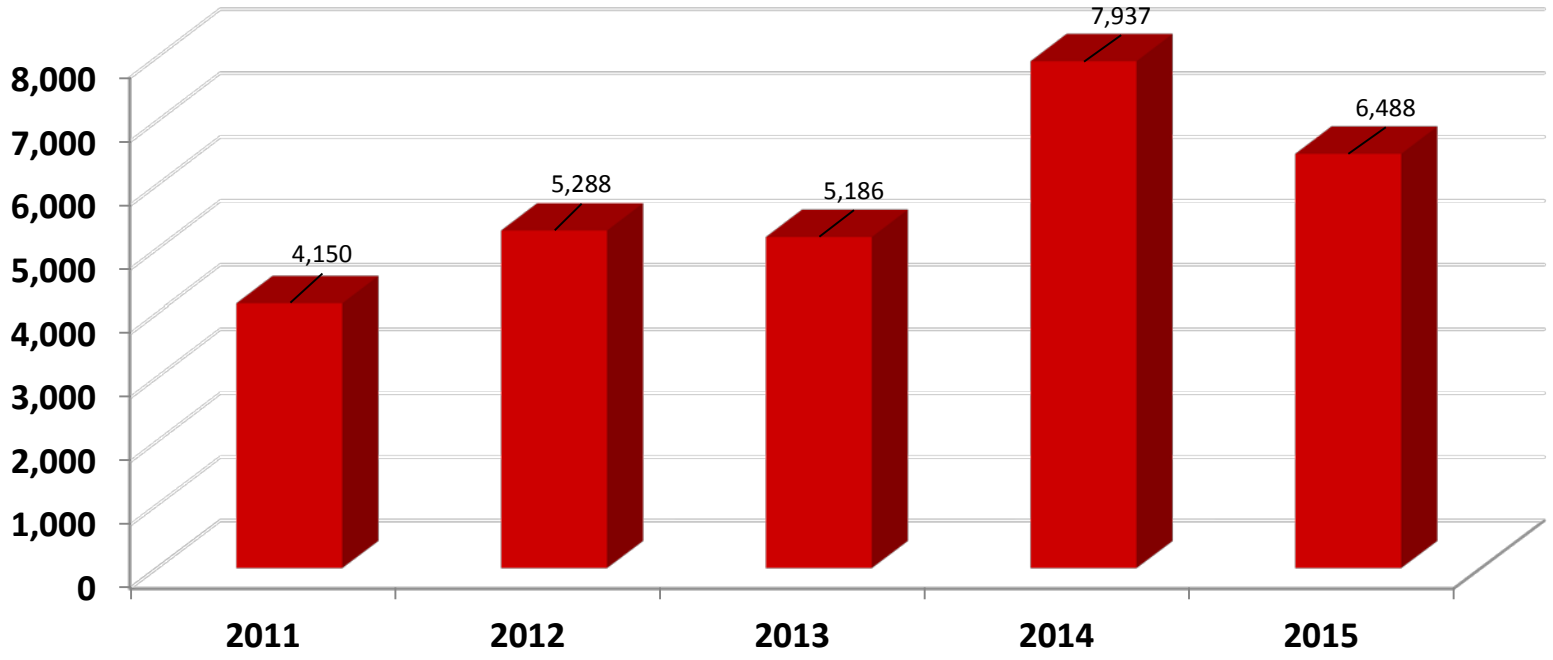
#RSAC

Constant stream of vulnerability disclosures



… plug into the fire hose of external vulnerability disclosures, so you're aware of the latest threats out in the wild.

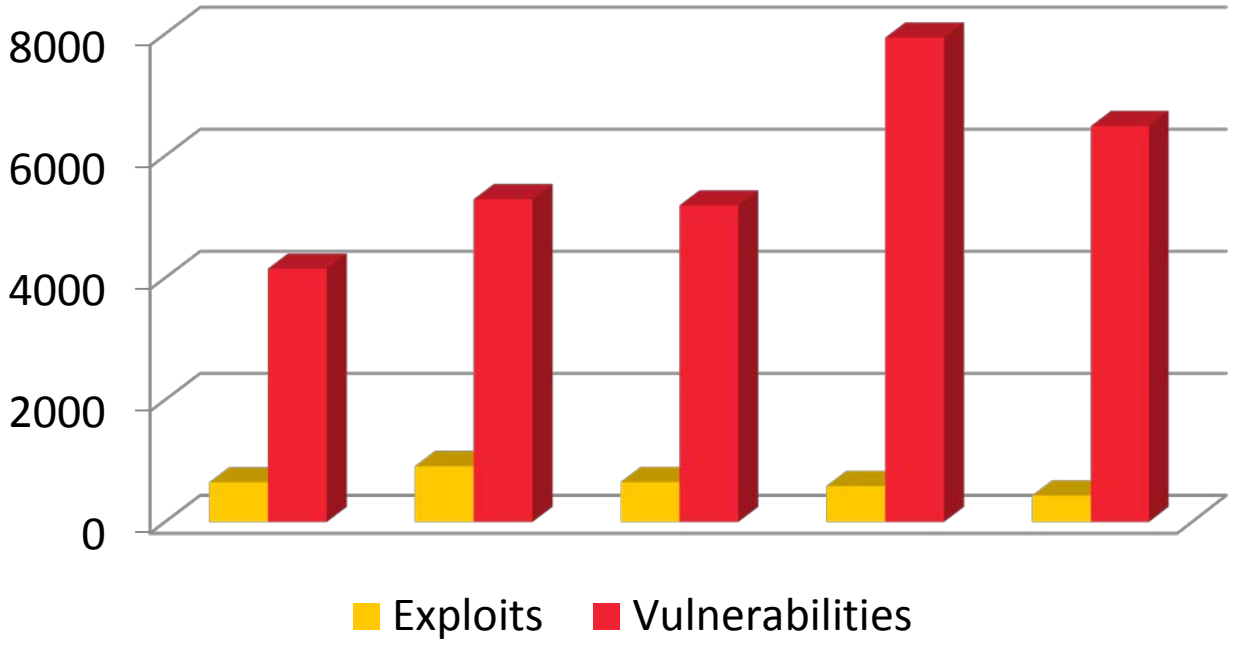
Vulnerabilities: Year Over Year



Notice, React, Remediate

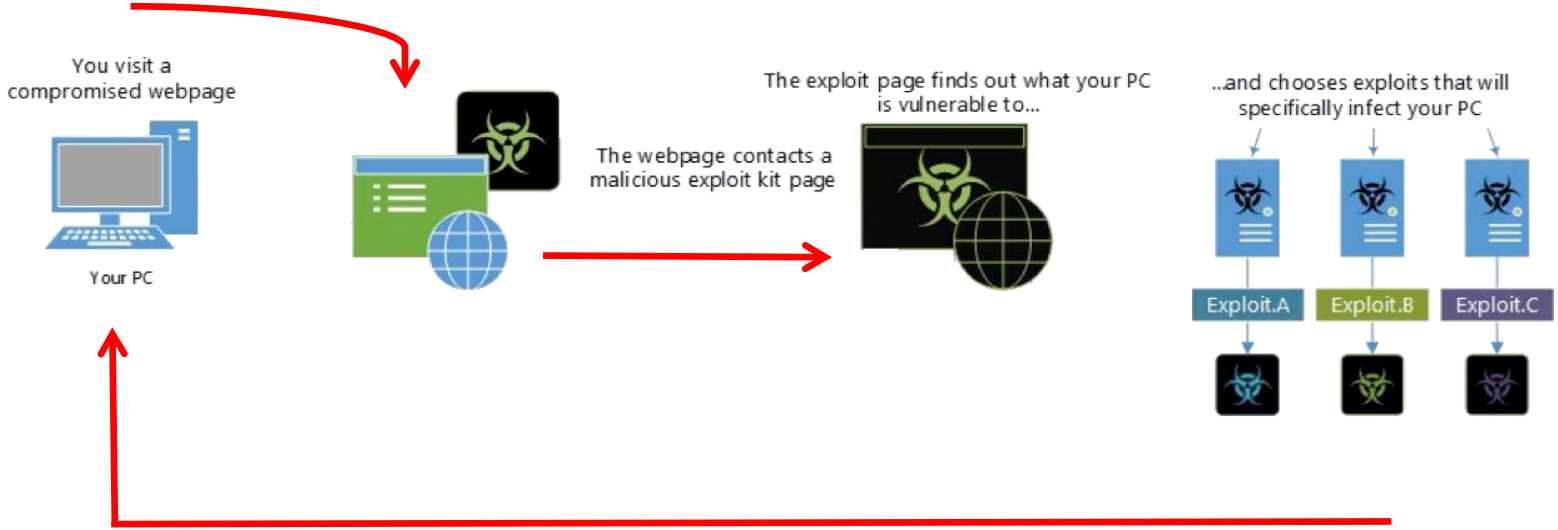
Where do I start?

Exploit vs Vulnerabilities



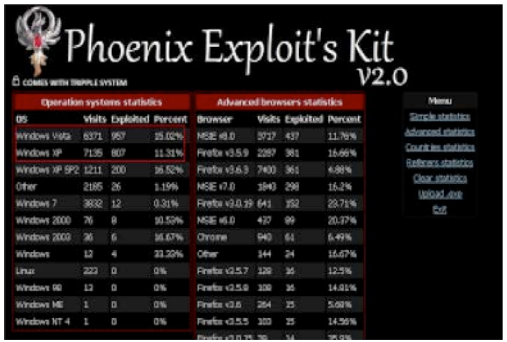
Only **7%** of Vulnerabilities had Exploits

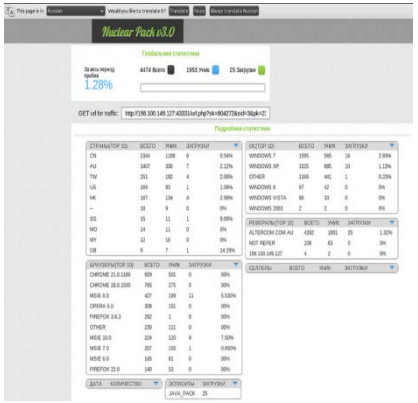
Exploit Kits



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

Exploit Kits





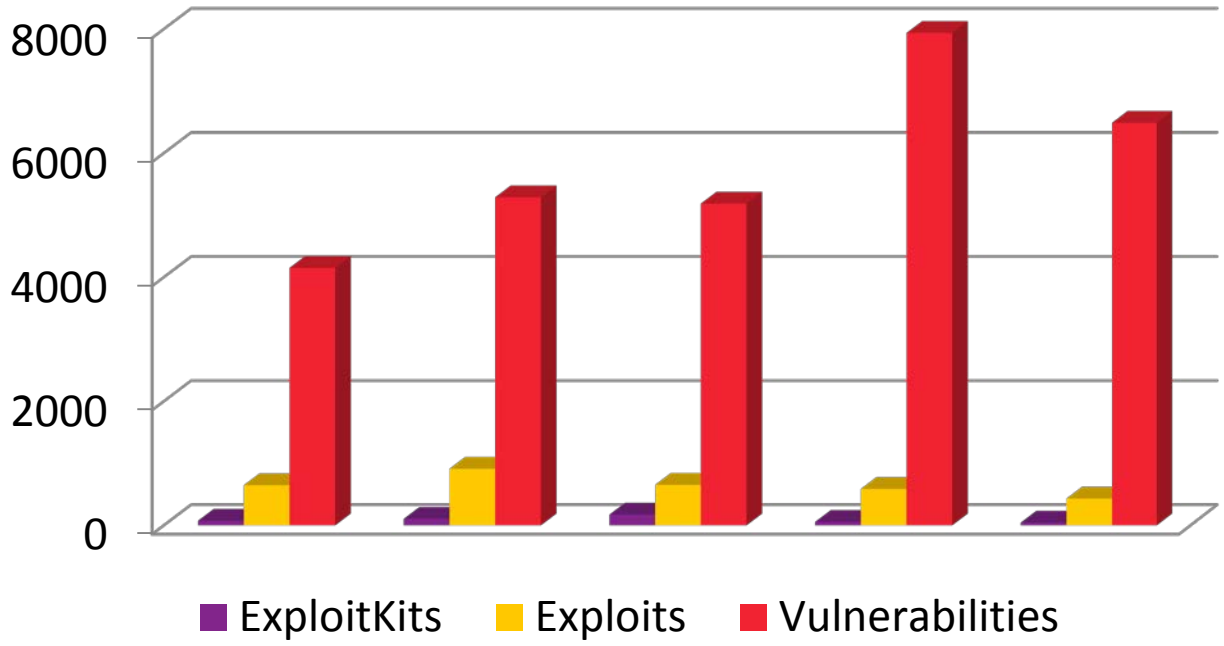
Exploit Kit Examples

QUALYS

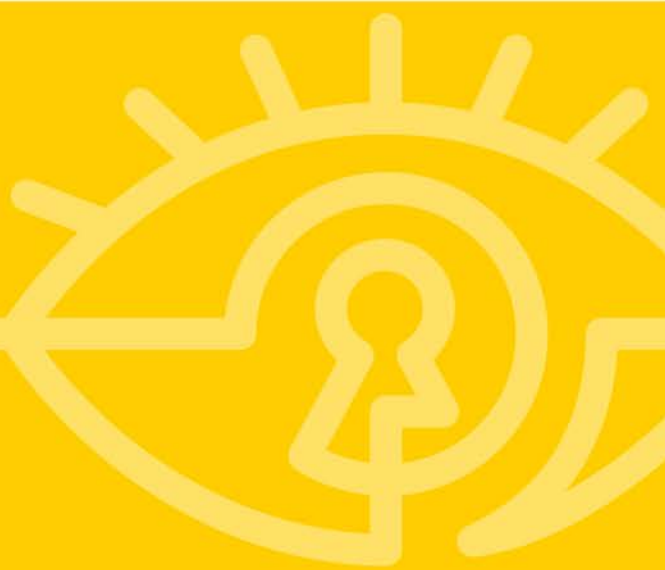
Vulnerabilities With Exploit Kit

CVE	VULNERABILITY	EXPLOIT KIT
CVE-2015-0313	Adobe Flash Player RCE Vulnerability (APSB15-04)	Hanjuan, Angler,
CVE-2015-0311	Adobe Flash Player RCE Vulnerability (APSB15-03)	SweetOrange, Rig, Fiesta, Nuclear, Nutrino, Angler
CVE-2015-2419	Microsoft Internet Explorer Security Update (MS15-065)	RIG,Nuclear Pack, Neutrino, Hunter,Angler
CVE-2015-0312	Adobe Flash Player RCE Vulnerability (APSB15-03)	Magniture, Angler
CVE-2015-0359	Adobe Flash Player Multiple RCE 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 RCE Vulnerability (APSB15-05)	Angler
CVE-2015-5560	Adobe Flash Player and AIR Multiple Vulnerabilities (APSB15-19)	Nuclear Pack
CVE-2015-2426	Microsoft Font Driver RCE Vulnerability (MS15-078)	Magnitude
CVE-2015-5122	Adobe Flash Player Multiple Vulnerabilities (APSB15-18)	Hacking Team, Nutrino, Angler, Magnitude, Nuclear
CVE-2015-5119	Adobe Flash Player Multiple Vulnerabilities (APSA15-03,B15-16)	Neutrino, Angler, Magnitude, Hanjuan, NullHole
CVE-2015-1671	Microsoft Font Drivers RCE Vulnerabilities (MS15-044)	Angler
CVE-2015-3113	Adobe Flash Player Buffer Overflow Vulnerability (APSB15-14)	Magnitude, Angler, Rig, Neutrino
CVE-2015-3104/5	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 RCE Vulnerability (APSB15-05)	Nuclear,Angler, Neutrino, Magnitude

Exploit Kits vs. Vulnerabilities

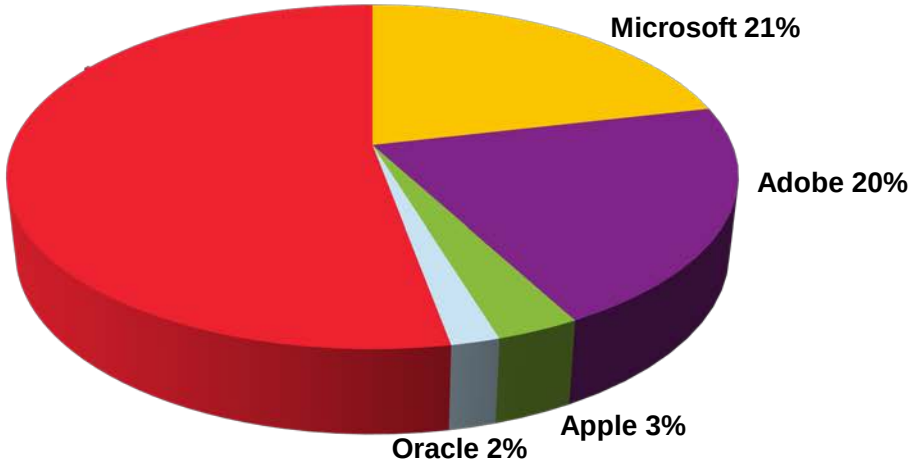


Only **1%** of Vulnerabilities are supported by Exploit Kits



Exploit Trends
2015 - 2016

Most Affected Vendors

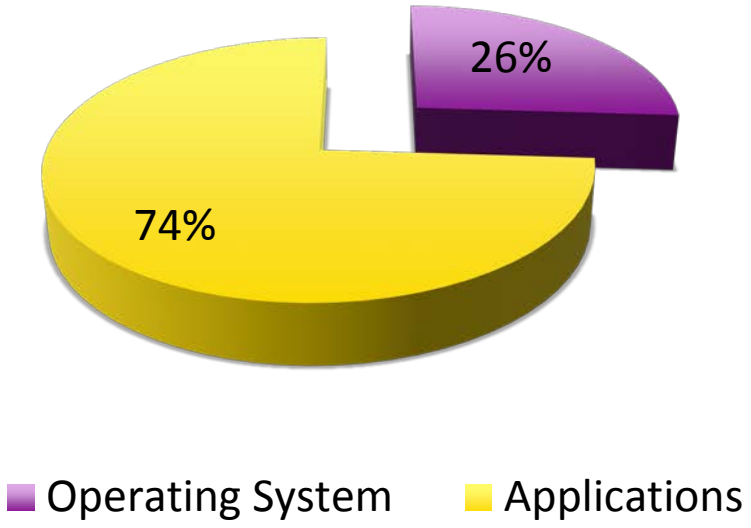


- microsoft
- joomla
- elasticsearch
- symantec
- cmsjunkie
- metalgenix
- web-dorado
- akronymmanager_project
- betster_project
- cs-cart
- elegant_themes
- h5ai_project
- kcodes
- milw0rm_project
- palosanto
- adobe
- pixabay_images_project
- fortinet
- wpml
- dell
- novius-os
- x2engine
- apache
- bisonware
- cups
- endian_firewall
- horde
- libmimedir_project
- moodle
- pcman%27s_ftp_server_project
- apple
- redhat
- foxitsoftware
- ajsquare
- emc
- refbase
- xceedium
- arubanetworks
- boxautomation
- cybernetikz
- ericsson
- hp
- linux
- npds
- persistent_systems
- oracle
- ansible
- igniterealtime
- apport_project
- etouch
- samsung
- yuba
- atlassian
- centreon
- e107
- feedwordpress_project
- insanevisions
- maarch
- ntop
- pfsense
- ferretcms_project
- citrix
- jakweb
- apptha
- f5
- sefrengo
- zohocorp
- auto-exchanger
- clip-bucket
- easy2map_project
- fork-cms
- ipass
- magic_hills
- nvidia
- photocati_media
- goautodial
- debian
- mozilla
- bitrix
- genixcms
- simple_ads_manager_project
- accunetix
- avinu
- cloudbees
- ecommercemajor_project
- freereprintables
- isc
- manageengine
- oxwall
- php
- google
- d-link
- novell
- cisco
- magmi
- thecartpress
- adb
- beehive_forum
- crea8social
- ektron
- gsm
- job_manager
- mcafee
- palo_alto_networks
- phpmybackuppro

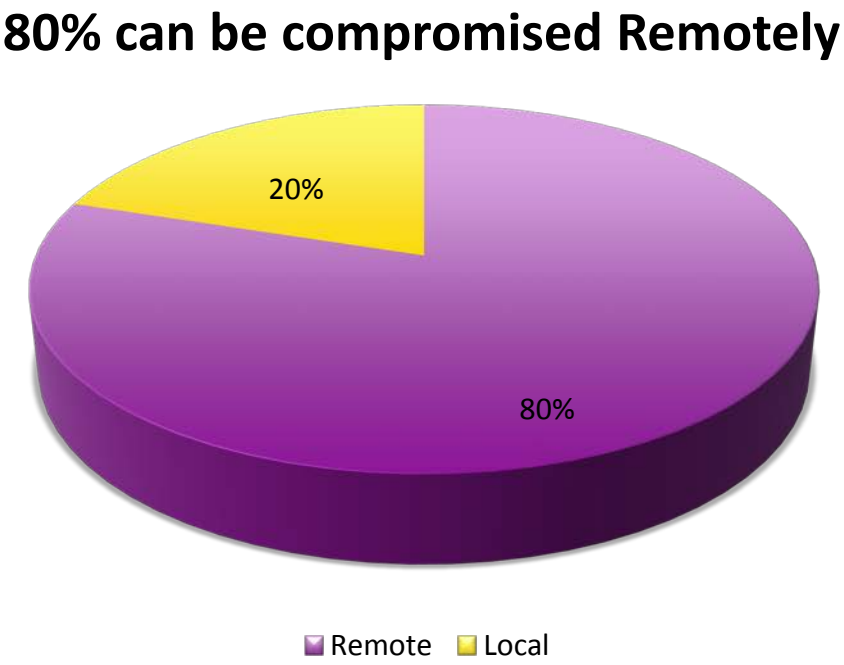
QUALYS

Applications vs Operating Systems

Applications 3x more frequent



Remote vs Local Exploits

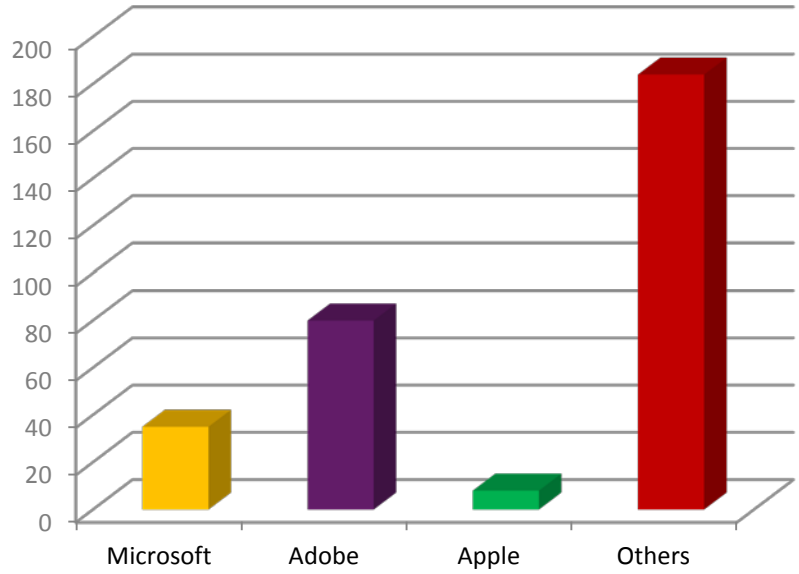


Remote vs Local Exploits

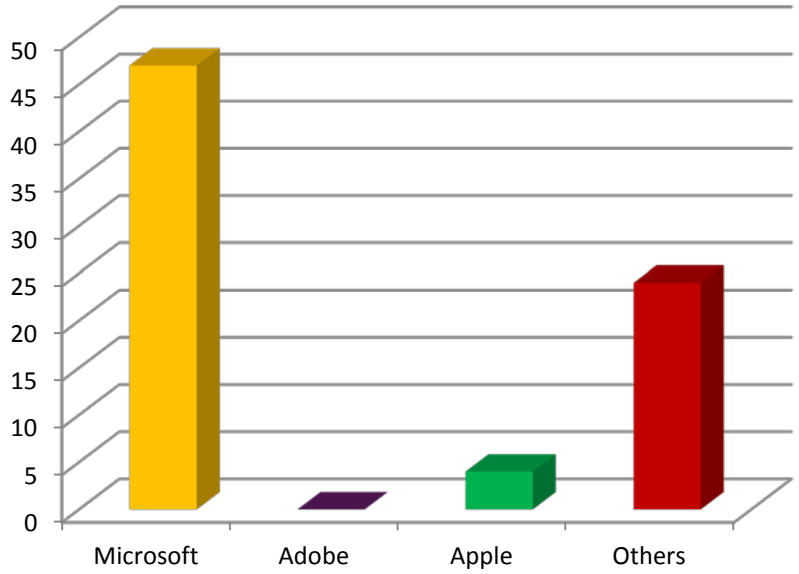
REMOTE	LOCAL
CVE-2015-0349: Adobe Flash Player APSB15-06 Multiple Remote Code Execution Vulnerabilities	CVE-2015-2789: Foxit Reader CVE-2015-2789 Local Privilege Escalation Vulnerability
CVE-2015-2545: Microsoft Office CVE-2015-2545 Remote Code Execution Vulnerability	CVE-2015-2219: Lenovo System Update '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

Remote vs Local Exploits

Remotely Exploitable



Requires Local Access



Lateral Movement

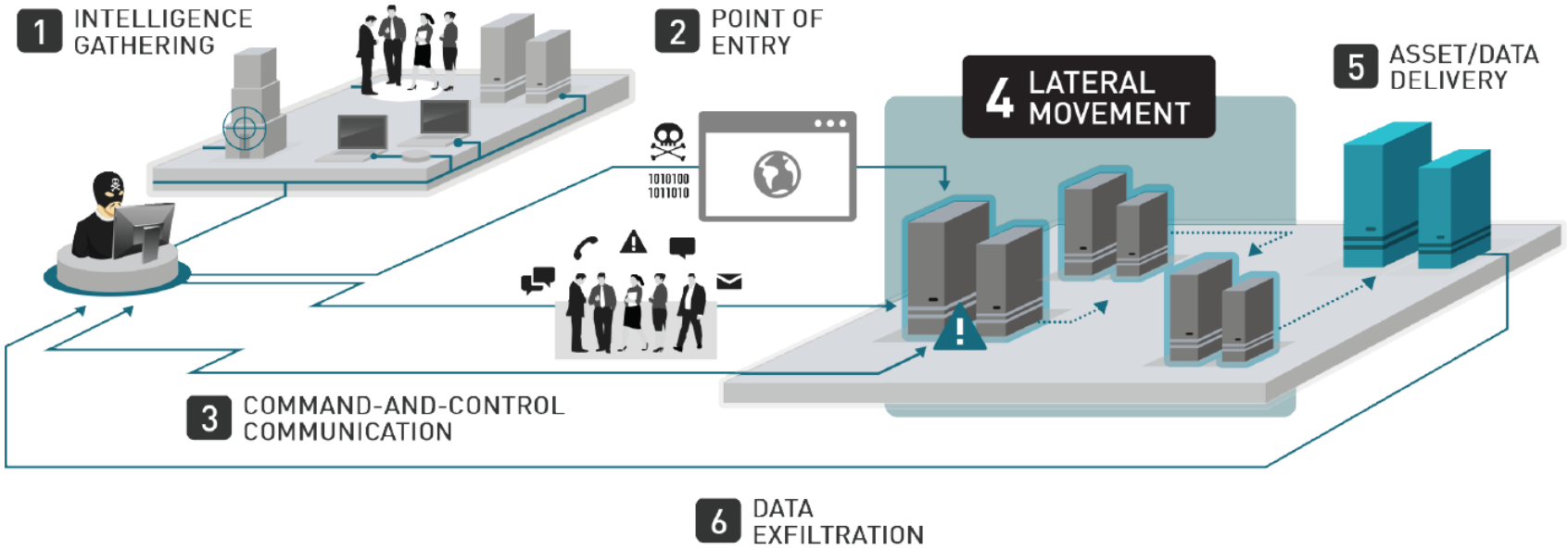


Figure 1. Six Stages of an APT attack

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

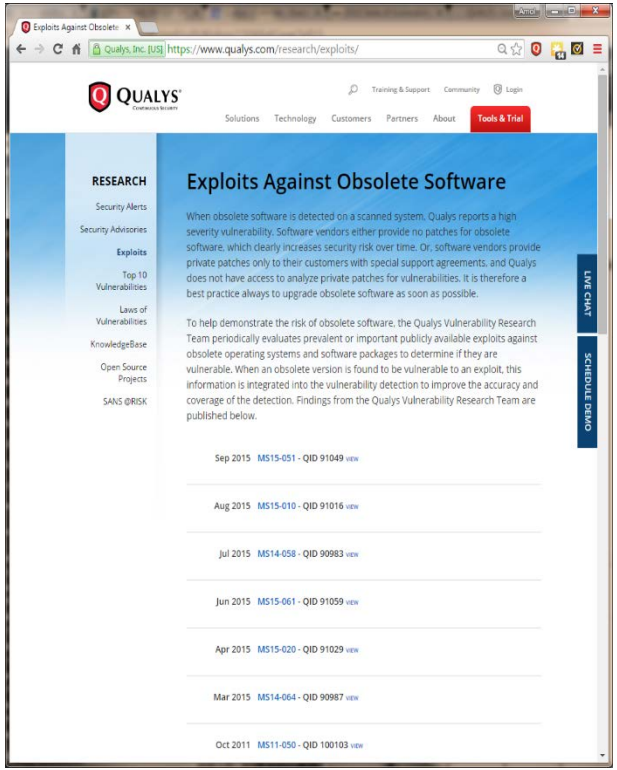
Lateral Movement

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

Almost ½ of Vulnerabilities had High Lateral Movement

Examples:	Remote + High Lateral Movement
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

Exploits of 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 Key Elements for Successfully Prioritizing Vulnerability Remediation

- A comprehensive and continuously updated view of all your IT assets.
- Knowledge of the constant stream of vulnerability disclosures.
- The ability to correlate external threat information with your vulnerability gaps.
- Dashboard tools to visualize your threat landscape.
- Precise assessments of your organization's threat scenarios.

Applying Exploit Knowledge

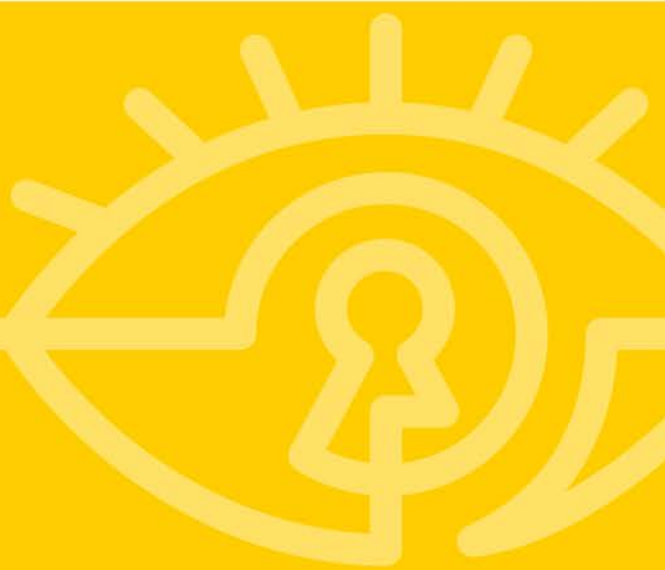
- **Next Week: Create inventory of:**
  - Applications with weaponized Exploit pack.
  - EOL Applications and EOL Operating Systems.
  - Vulnerabilities with working exploits.
  - Vulnerabilities that can be remotely compromised.

Applying Exploit Knowledge

- **Next Month:**
  - Upgrade EOL applications.
  - Patching all vulnerabilities with Exploit packs and exploits.

Applying Exploit Knowledge

- **Next Quarter:**
  - Automatic inventory and alerting.
  - Debate if most exploited applications, like Flash, are required for business.



Thank you

hjaafarawi@qualys.com