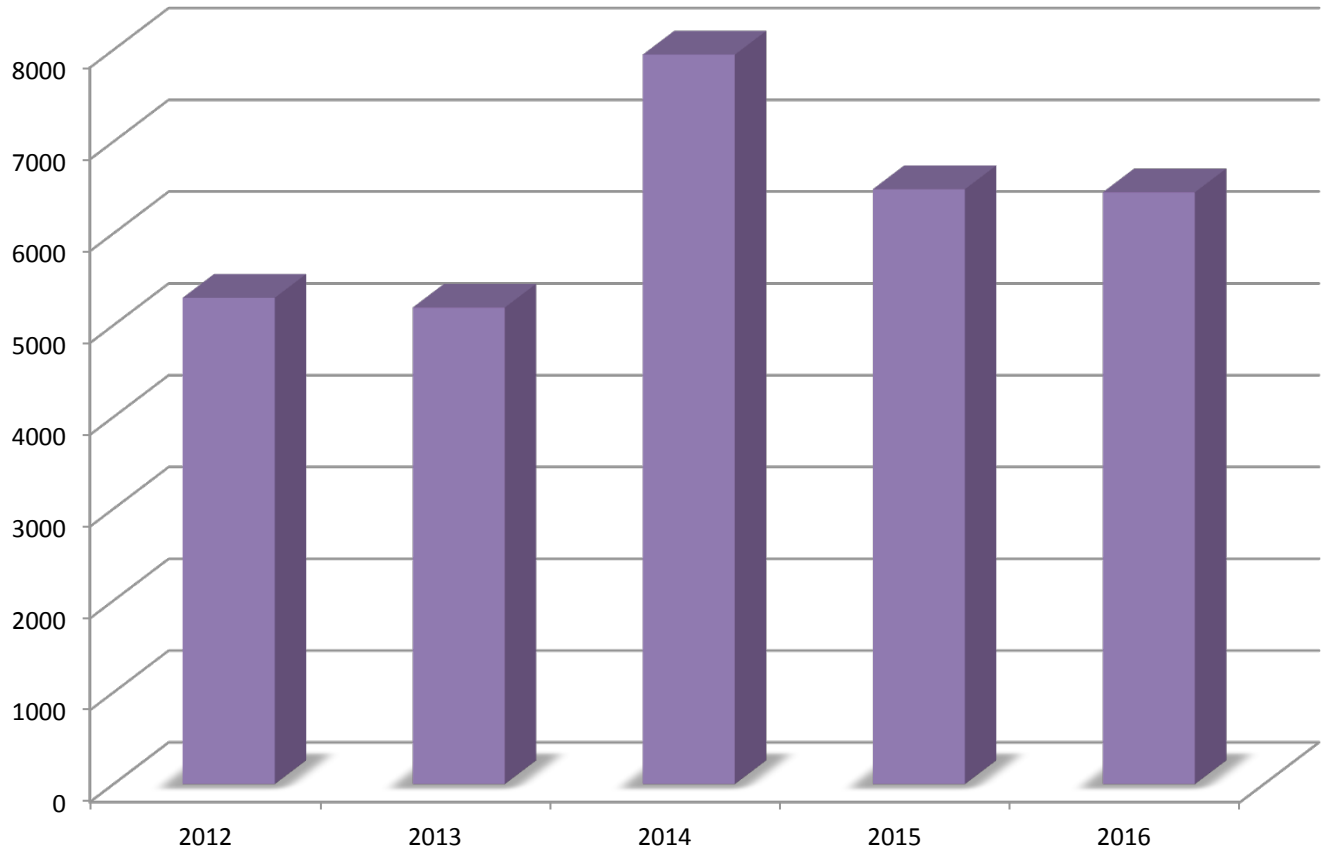
Qualys

SECTOR
Security Education Conference

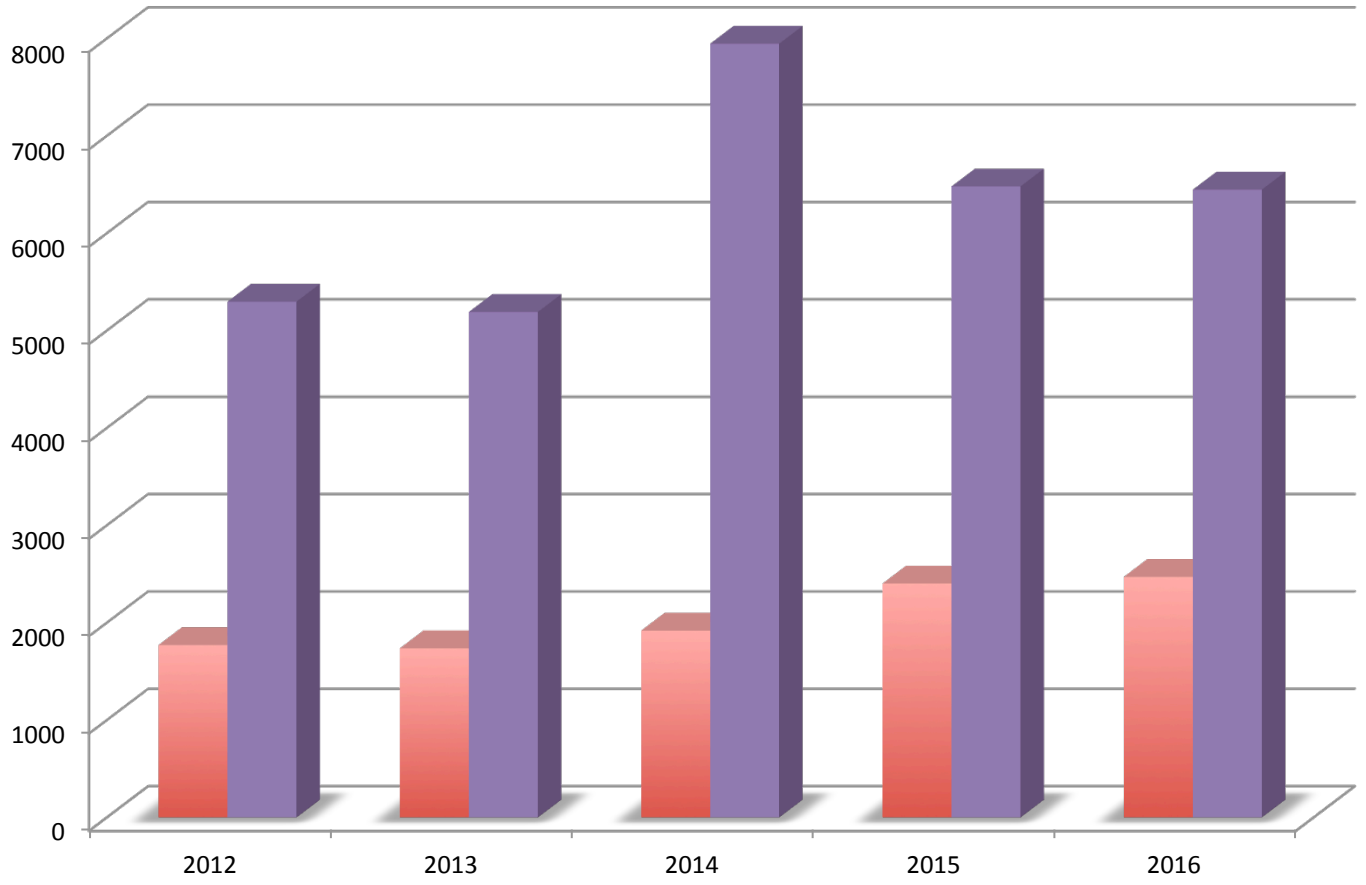
Prioritizing Vulnerability Remediation From Attacker's Perspective

Bharat Jogi
Senior Manager, Vulnerability & Threat Research

Vulnerabilities

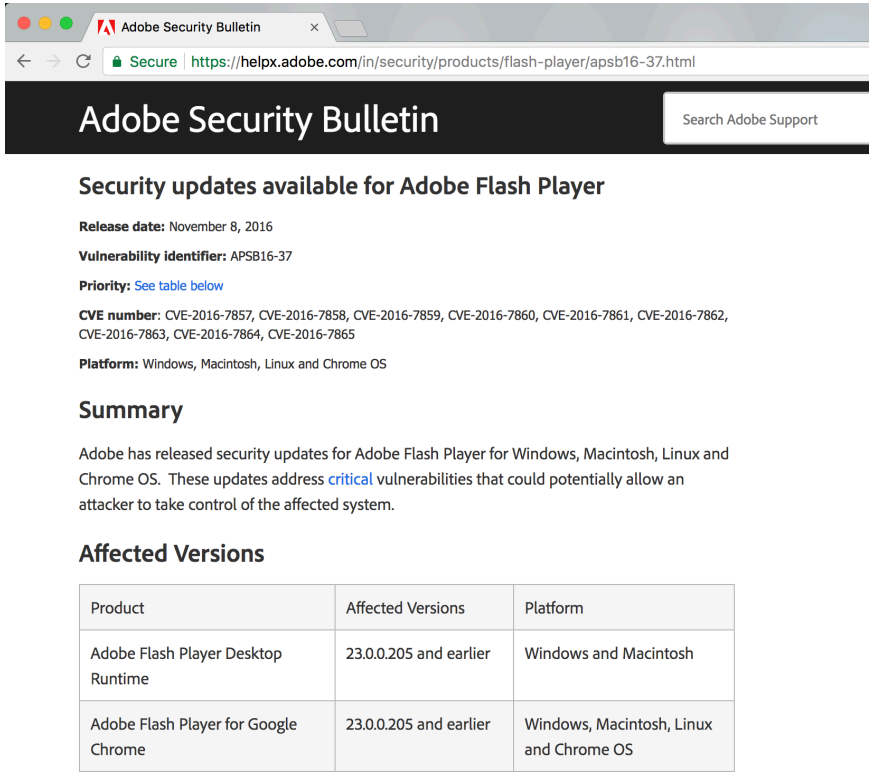


Vulnerabilities



Vulnerabilities

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



Exploit

An Exploit tries to turn a vulnerability into an actual means to **breach** *a system*

EXPLOIT DATABASE

Apache Struts 2.3.x Showcase - Remote Code Execution (PoC)

EDB-ID: 42324	**Author**: Vex Woo	**Published**: 2017-07-07
CVE: CVE-2017-9791	**Type**: Webapps	**Platform**: Multiple
Aliases: N/A	**Advisory/Source**: Link	**Tags**: N/A
E-DB Verified: ✓	**Exploit**: Download / View Raw	**Vulnerable App**: N/A

« Previous Exploit Next Exp

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

# Just a demo for CVE-2017-9791


import requests


def exploit(url, cmd):
    print("[+] command: %s" % cmd)

    payload = "%{"
    payload += "(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)."
    payload += "(#_memberAccess?(#_memberAccess=#dm):"
    payload += "((#container=#context['com.opensymphony.xwork2.ActionContext.container'])."
    payload += "(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))."
```

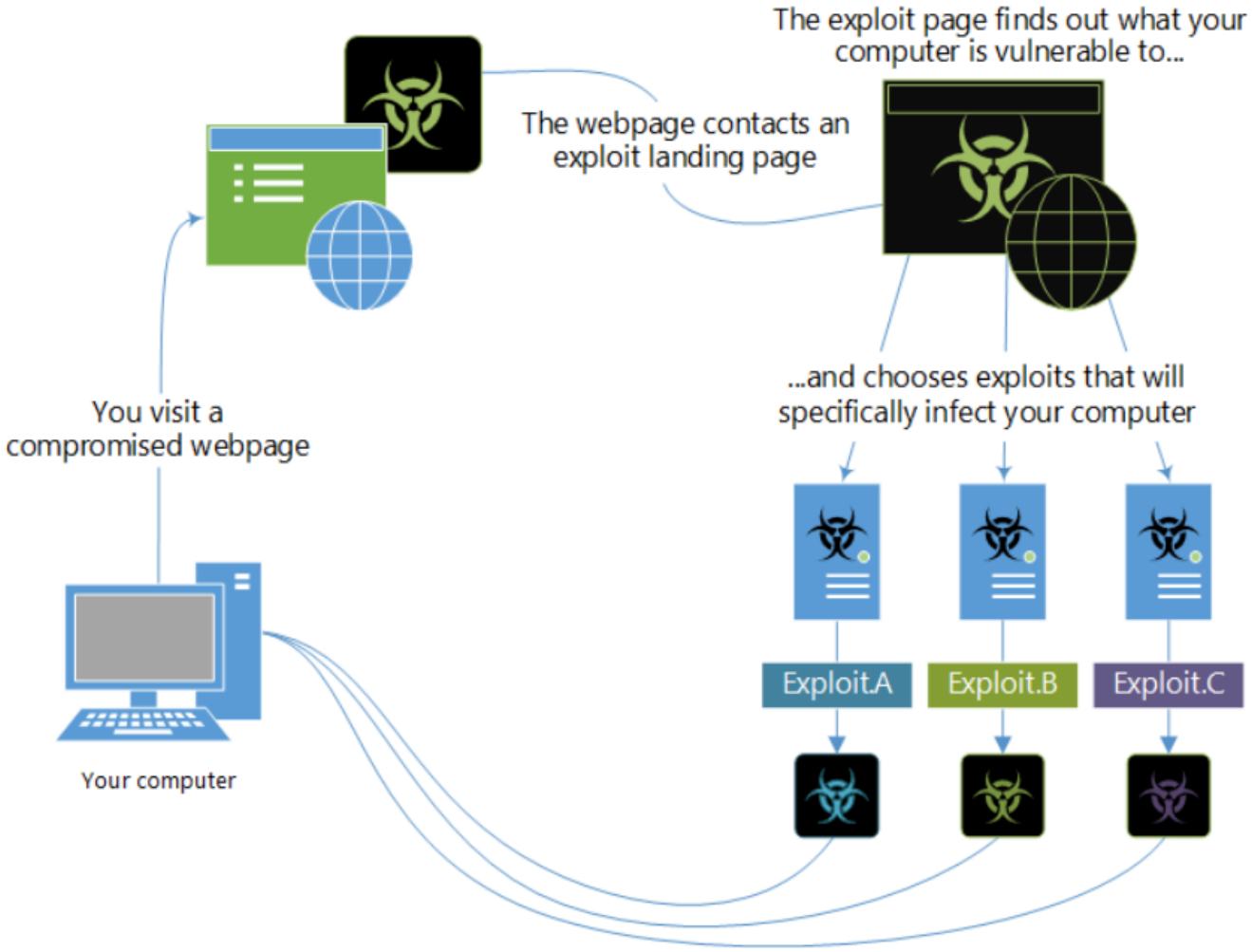
Exploit

An Exploit tries to turn a vulnerability into an actual means to ***breach*** *a system*

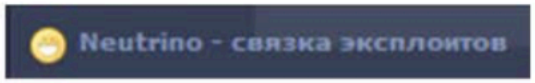
Exploit Kits

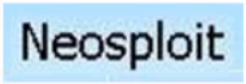
An exploit kit or exploit pack is a type of a toolkit cybercriminals use to attack vulnerabilities in systems so they can distribute ***malware*** *or perform other malicious activities.*

Exploit Kits



Exploit Kits Examples





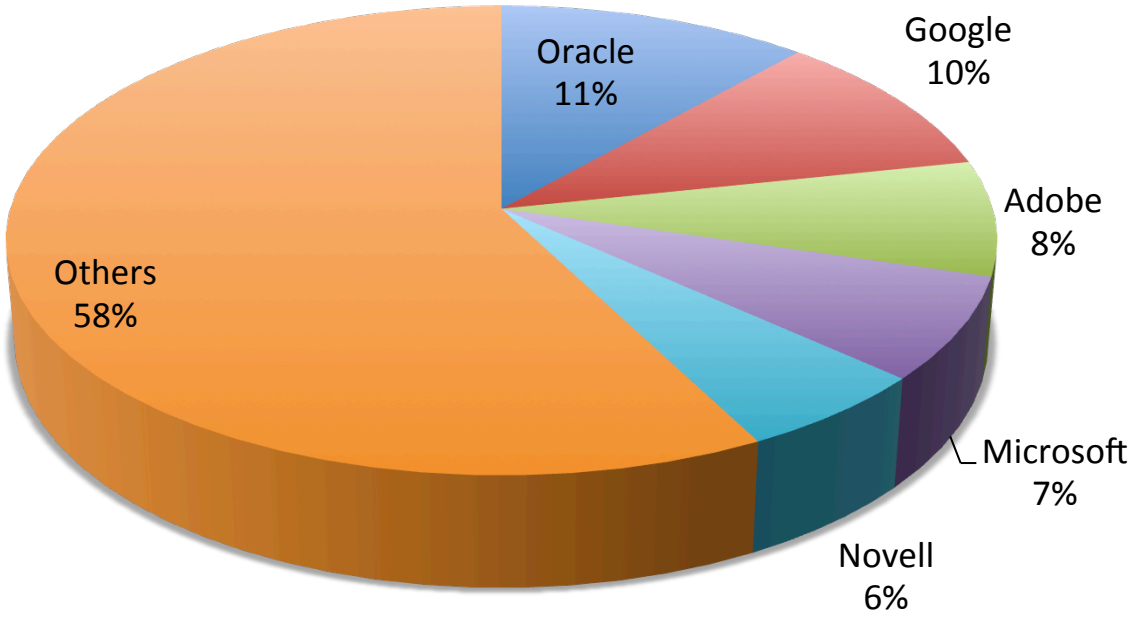
Qualys

SECTOR
Security Education Conference

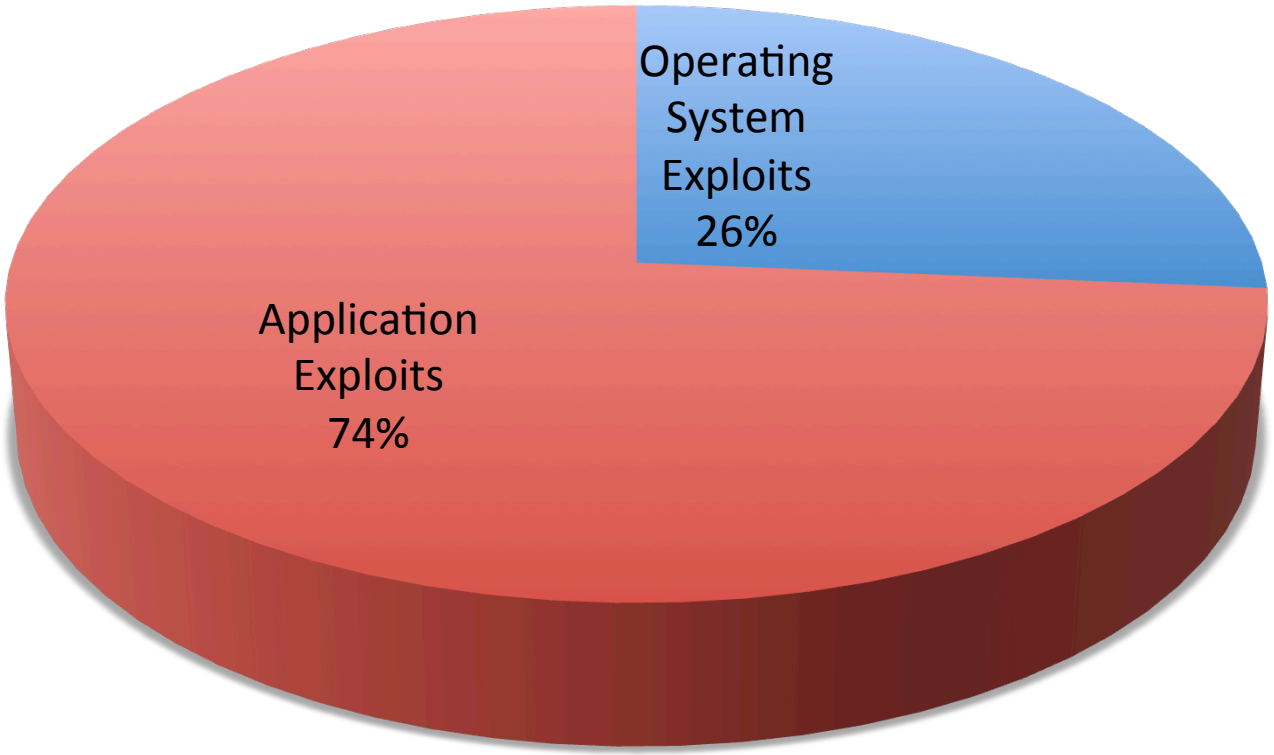
Exploit and Vulnerability Trends

and how to use them to our advantage

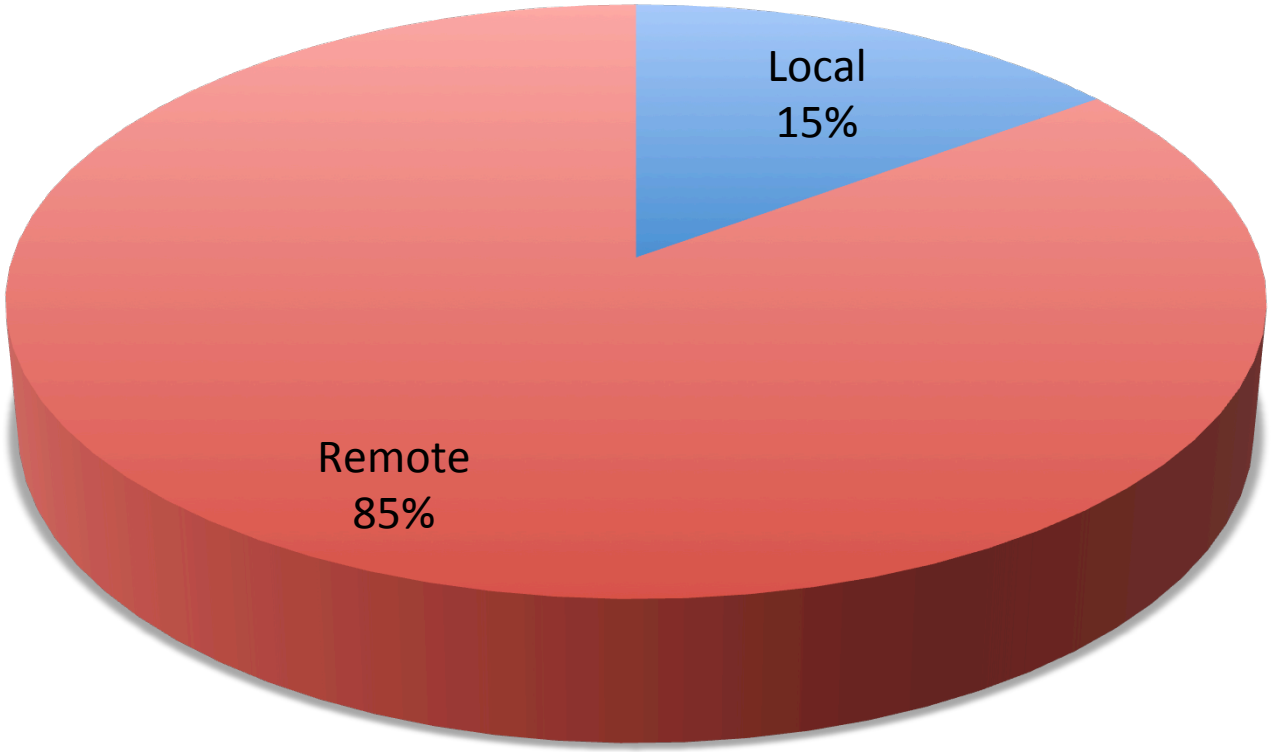
#1 Most Affected



#2 Operating System vs Applications



#3 Remote Vs Local



Remote Vs Local

Remote	Local
CVE-2016-0985: Adobe Flash Player Remote Code Execution Vulnerabilty (APSB16-04)	CVE-2016-7237: Microsoft Windows LSASS Memory Corruption DoS (MS16-137)
CVE-2016-10033: PHPMailer Remote Code Execution Vulnerability	CVE-2016-7225: Microsoft Windows ZwDeleteFile Arbitrary File Deletion Privilege Escalation (MS16-138)
CVE-2016-2004: HP Data Protector Multiple Security Vulnerabilities (HPSBGN03580)	CVE-2016-5195: Linux Kernel 2.6.22 < 3.9 - 'Dirty COW' 'PTRACE_POKEDATA' Race Condition Privilege Escalation
CVE-2016-3081: Apache Struts Dynamic Method Invocation RCE Vulnerability (S2-032)	CVE-2016-1793: Mac OSX Kernel Null Pointer Dereference Vulnerability
CVE-2016-3642: Solarwinds Virtualization Manager Java JMX-RMI Remote Code Execution Vulnerability	CVE-2016-3220: Microsoft Windows Kernel - 'ATMFD.dll' NamedEscape 0x250C Pool Corruption
CVE-2016-6366: Cisco ASA SNMP Remote Code Execution Vulnerability (EXTRABACON)	CVE-2016-3216: Microsoft Windows 'gdi32.dll' Heap Based Memory Disclosure (MS16-074)

#4 Lateral Movement

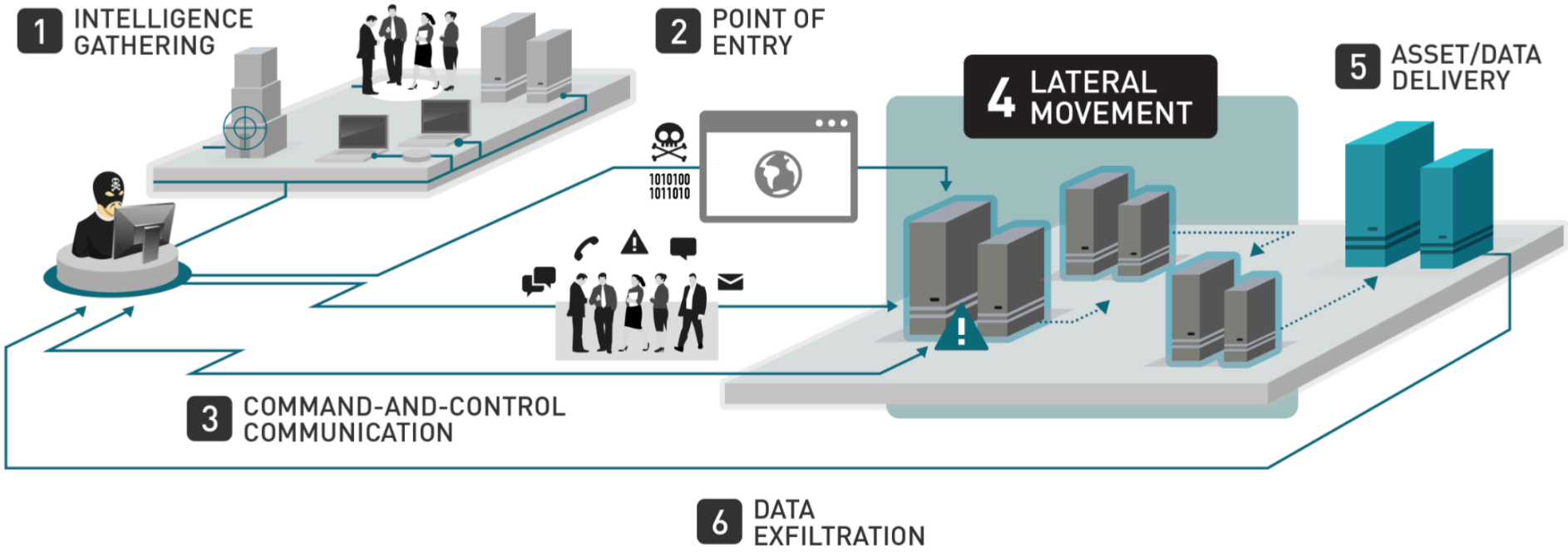


Figure 1. Six Stages of an APT attack

#4 High Lateral Movement

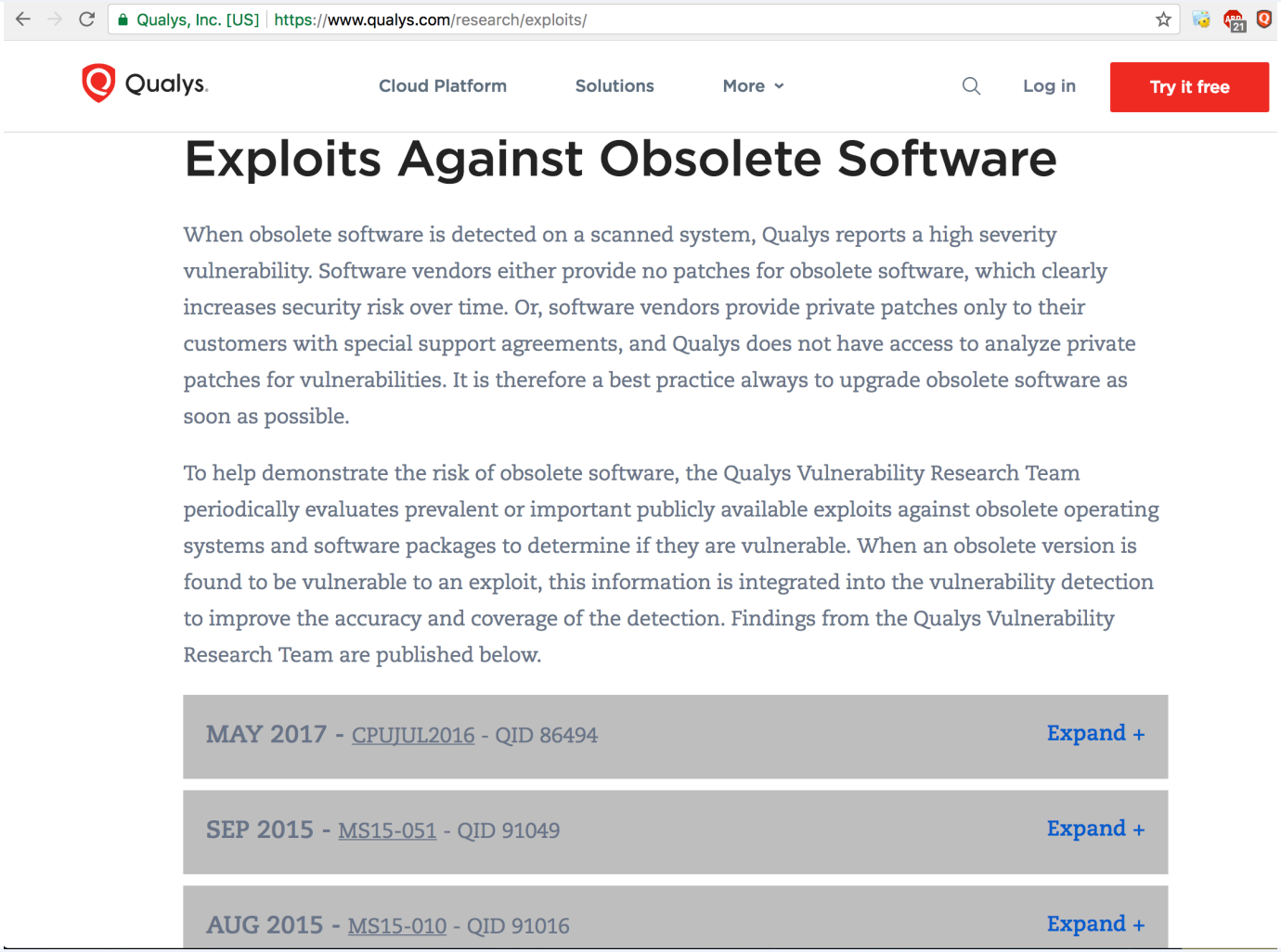
CVE	Vulnerability
CVE-2016-3643	Solarwinds Virtualization Manager Local Privilege Escalation Vulnerability
CVE-2016-1464	Cisco WebEx Meetings Player for WRF Files Code Execution Vulnerability
CVE-2016-2298	Meteocontrol WEBlog Password Extractor
CVE-2016-1909	FortiOS Fortimanager_Access SSH Interactive Login Vulnerability
CVE-2016-0099	Microsoft Windows Secondary Logon Elevation of Privilege Vulnerability (MS16-032)
CVE-2016-2005	Hewlett Packard Enterprise Data Protector EXEC_BAR User Name Buffer Overflow Exploit
CVE-2016-3646	Symantec Multiple Products Decomposer Engine Multiple File Parsing Vulnerabilities (SYM16-010)

#4 High Lateral Movement

CVE	Vulnerability
CVE-2016-3643	Solarwinds Virtualization Manager Local Privilege Escalation Vulnerability
CVE-2016-1464	Cisco WebEx Meetings Player for WRF Files Code Execution Vulnerability
CVE-2016-2298	Meteocontrol WEBlog Password Extractor
CVE-2016-1909	FortiOS Fortimanager_Access SSH Interactive Login Vulnerability
CVE-2016-0099	Microsoft Windows Secondary Logon Elevation of Privilege Vulnerability (MS16-032)
CVE-2016-2005	Hewlett Packard Enterprise Data Protector EXEC_BAR User Name Buffer Overflow Exploit
CVE-2016-3646	Symantec Multiple Products Decomposer Engine Multiple File Parsing Vulnerabilities (SYM16-010)

50% of exploits had lateral movement potential

#5 Exploits for EOL Systems



#5 Exploits for EOL Systems

Qualys, Inc. [US] | https://www.qualys.com/research/exploits/

Qualys. Cloud Platform Solutions More Log in Try it fre

Vulnerable Software per Vendor Advisory

Oracle WebLogic Server, version(s) 10.3.6.0, 12.1.3.0, 12.2.1.0

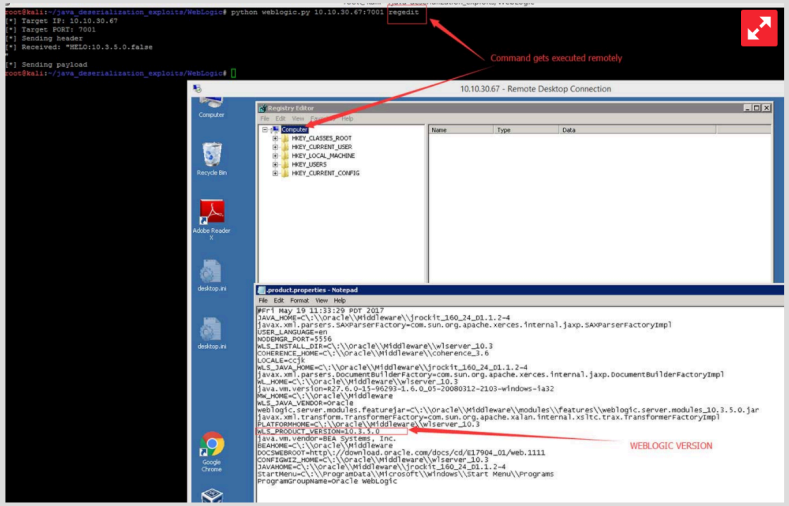
Exploit Used

https://github.com/CoalfireLabs/java_deserialization_exploits/blob/master/WebLogic/weblogic.py

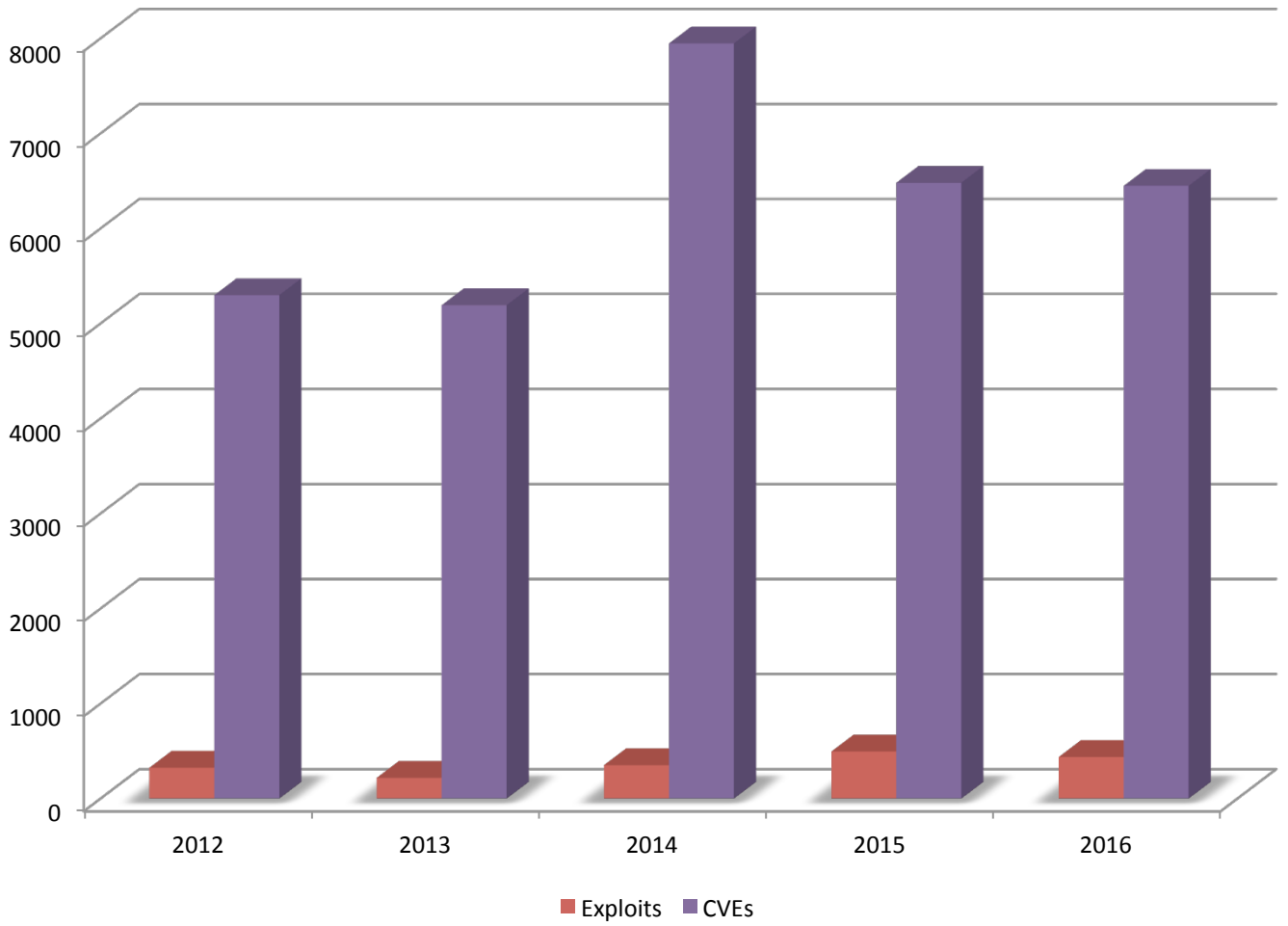
Findings

Additional Vulnerable Software
Oracle WebLogic Server, version(s) 10.3.5.0

Impact of Exploit
Remote Code Execution



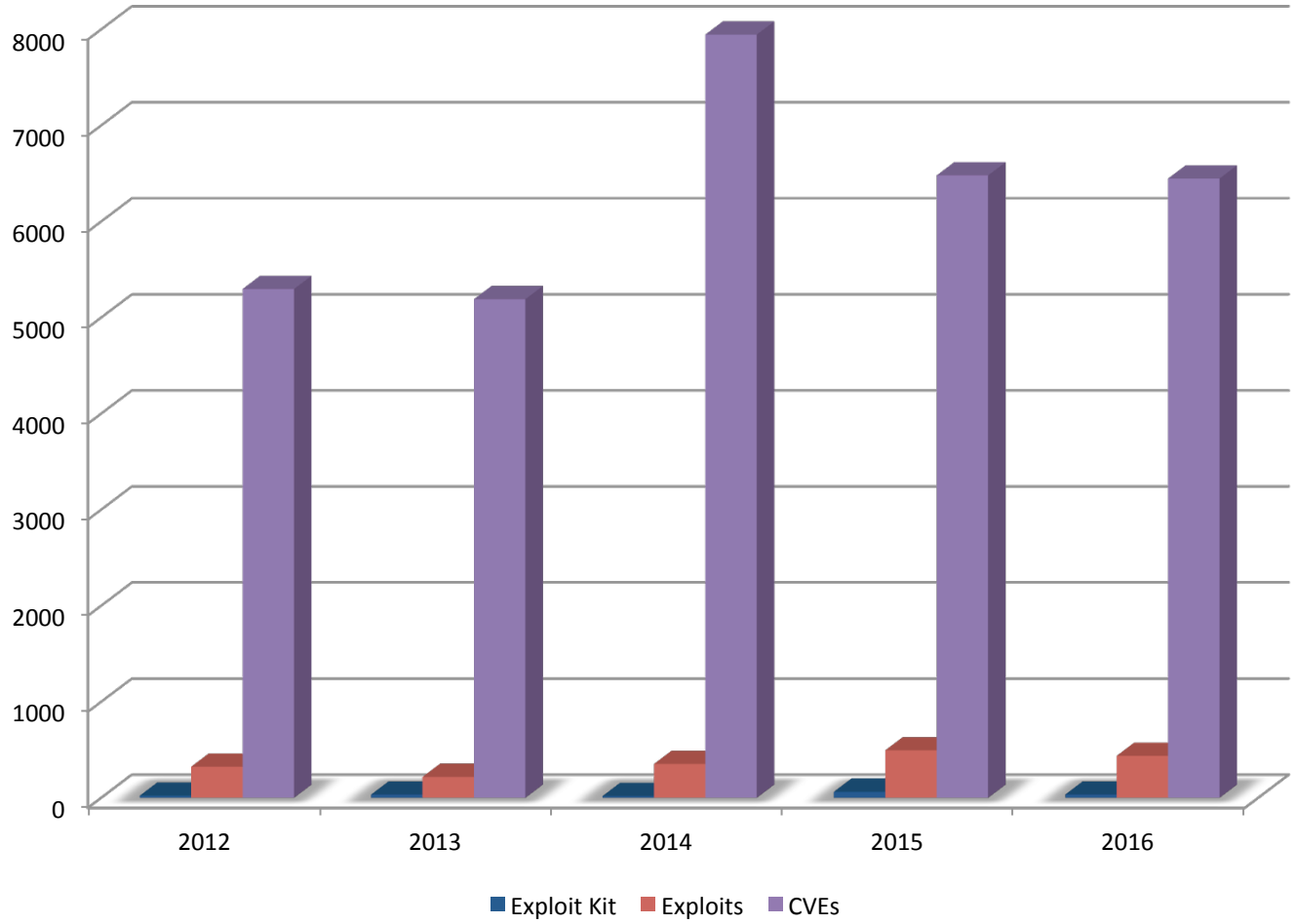
#6 < 7% of vulnerabilities had exploits



Exploit Kits from Last Year

CVE	Vulnerability	Exploit Kit
CVE-2016-0034	Microsoft Silverlight Remote Code Execution Vulnerability (MS16-006)	Angler EK , RIG
CVE-2016-0189	Microsoft JScript and VBScript Remote Code Execution Vulnerabilities (MS16-053)	Neutrino Sundown,RIG,Magnitude
CVE-2016-7201	Microsoft Edge Cumulative Security Update (MS16-129)	Sundown,Neutrino
CVE-2016-7202	Microsoft Edge Cumulative Security Update (MS16-129)	Sundown,Neutrino
CVE-2016-4117	Adobe Flash Player and AIR Multiple Vulnerabilities (APSA16-02) (APSB16-15)	Magnitude, Nutrino,Angler,Sundown
CVE-2016-1001	Adobe Flash Player and AIR Security Update (APSB16-08)	Angler
CVE-2016-1019	Adobe Flash Player and AIR Multiple Vulnerabilities (APSA16-01) (APSB16-10)	Nuclear Pack, Magnitude , Neutrino

#7 < 1% of vulns are in exploitkits



Applying Exploit Knowledge

Next Week: Create inventory of:

- *Applications with weaponized Exploit*
- *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*

Next Quarter:

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

Qualys

SECTOR
Security Education Conference

Thank You

Bharat Jogi
Senior Manager, Vulnerability & Threat Research