Security Becomes Continuous

Wolfgang Kandek
Qualys

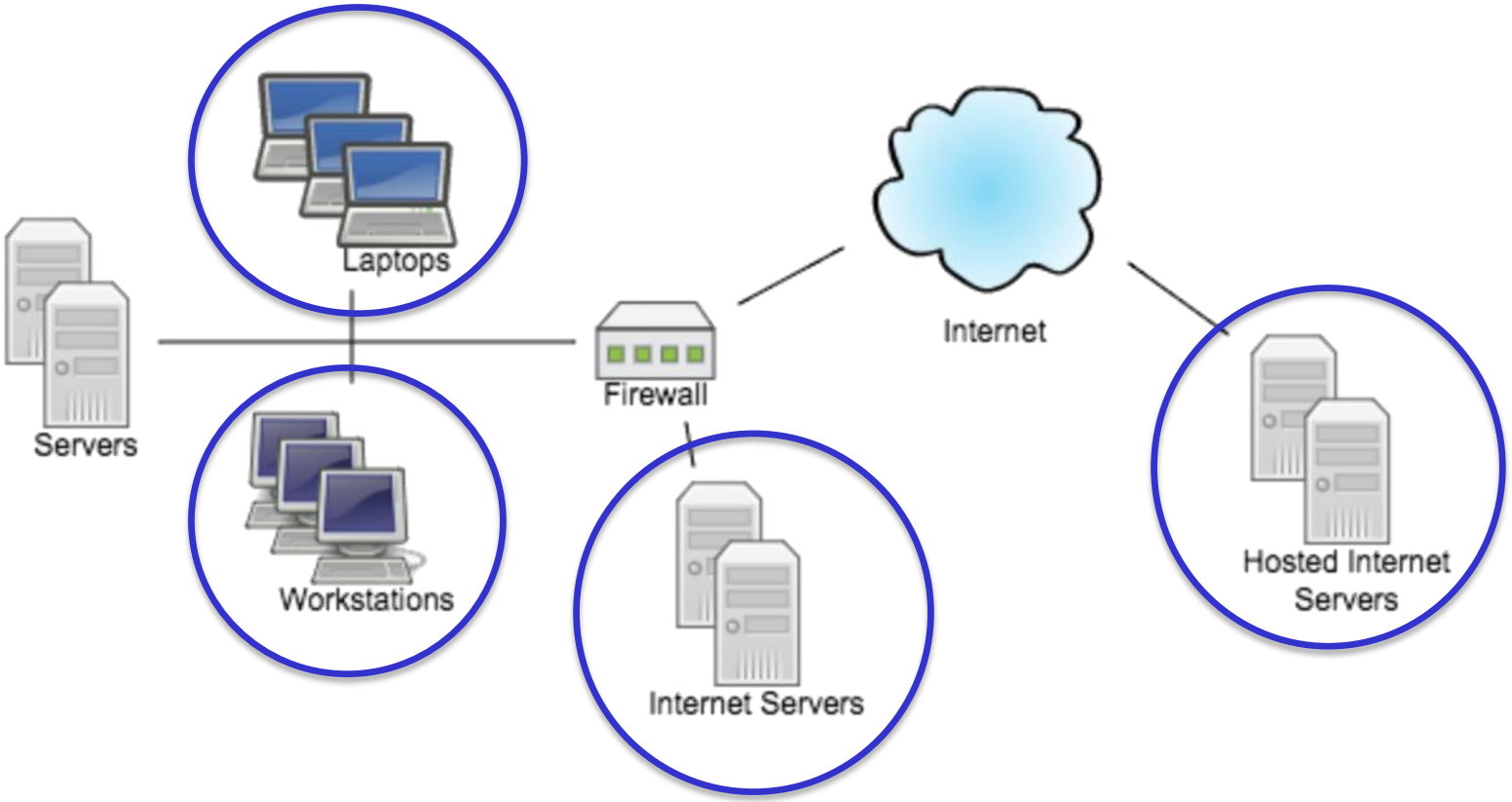
June 23, 2015 – SIGS Technology Summit

QUALYS®

Hackers

- Attack your Organization by continuously probing your organization for weaknesses.
- Find and catalog vulnerabilities, software flaws and misconfigurations
- Use exploits to gain control over your systems

Hackers - Attack Perimeter



Hackers

- We can get a jump on them by using their weak spots.
- Weak Spots:
  - Millions of Malware samples
  - Thousands of Vulnerabilities
  - Tens of Exploitation vectors

Hackers

- Mass Malware
- APT and 0-days
- Nation State

Hackers – Mass Malware

- Majority of all attacks
- Mature technologies (on both sides)
  - Exploit Kits (Angler, Nuclear, …)
  - Analysis and Patching
- “Digital Carelessness”
- Research

Hackers – Mass Malware

- BSI – German Bundesamt für Sicherheit in der Informationstechnik
  - Digital Situation Report December 2014
  - Situation is critical
  - Digitale Sorglosigkeit => “Digital Carelessness”
  - 95% of issues are easily addressed
  - Attackers use known vulnerabilities
  - In a limited set of software

Hackers – Mass Malware

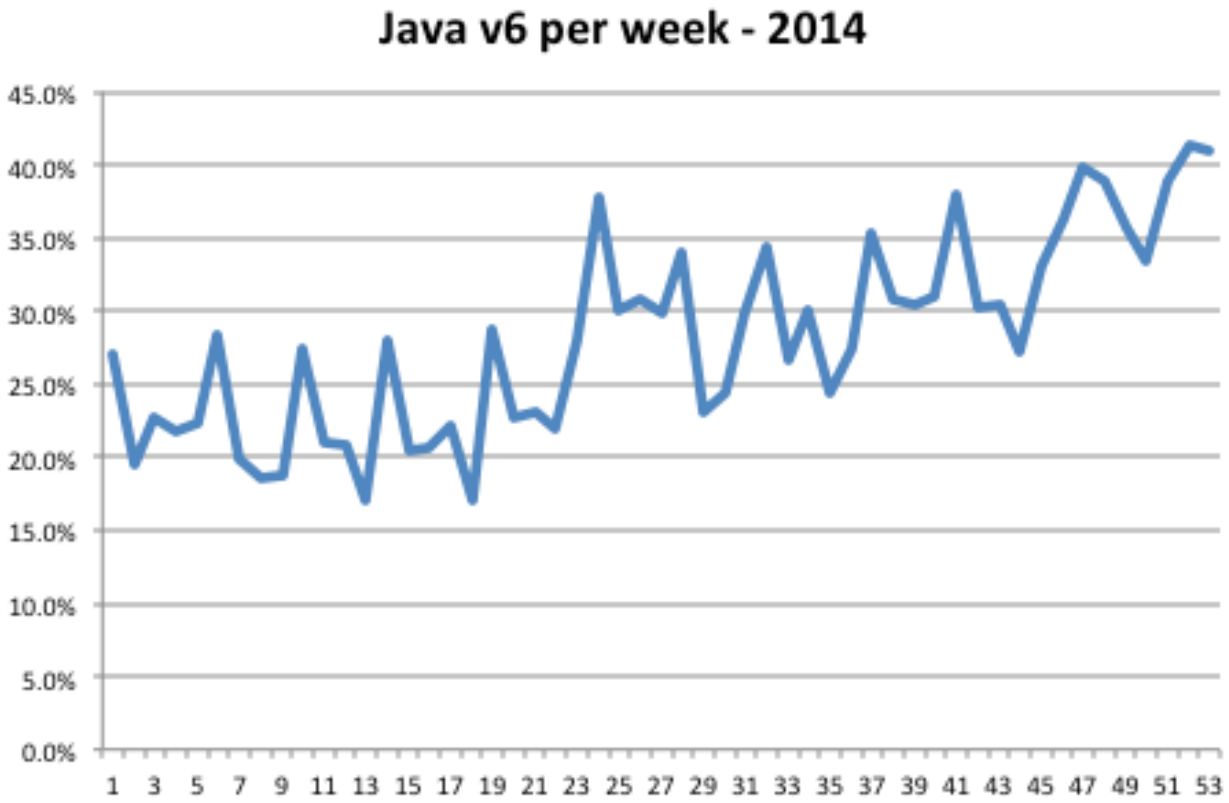
Softwareprodukte

- Adobe Flash Player
- Adobe Reader
- Apple OS X
- Apple Quicktime
- Apple Safari
- Google Chrome
- Linux Kernel
- Microsoft Internet Explorer
- Microsoft Office
- Microsoft Windows
- Mozilla Firefox
- Mozilla Thunderbird
- Oracle Java/JRE

Tabelle 1: Auswahl von Softwareprodukten mit hoher Relevanz

Hackers – Mass Malware - Java

- Java is on our top unpatched threat for the year



QUALYS® CONTINUOUS SECURITY

Hackers – Mass Malware - Java

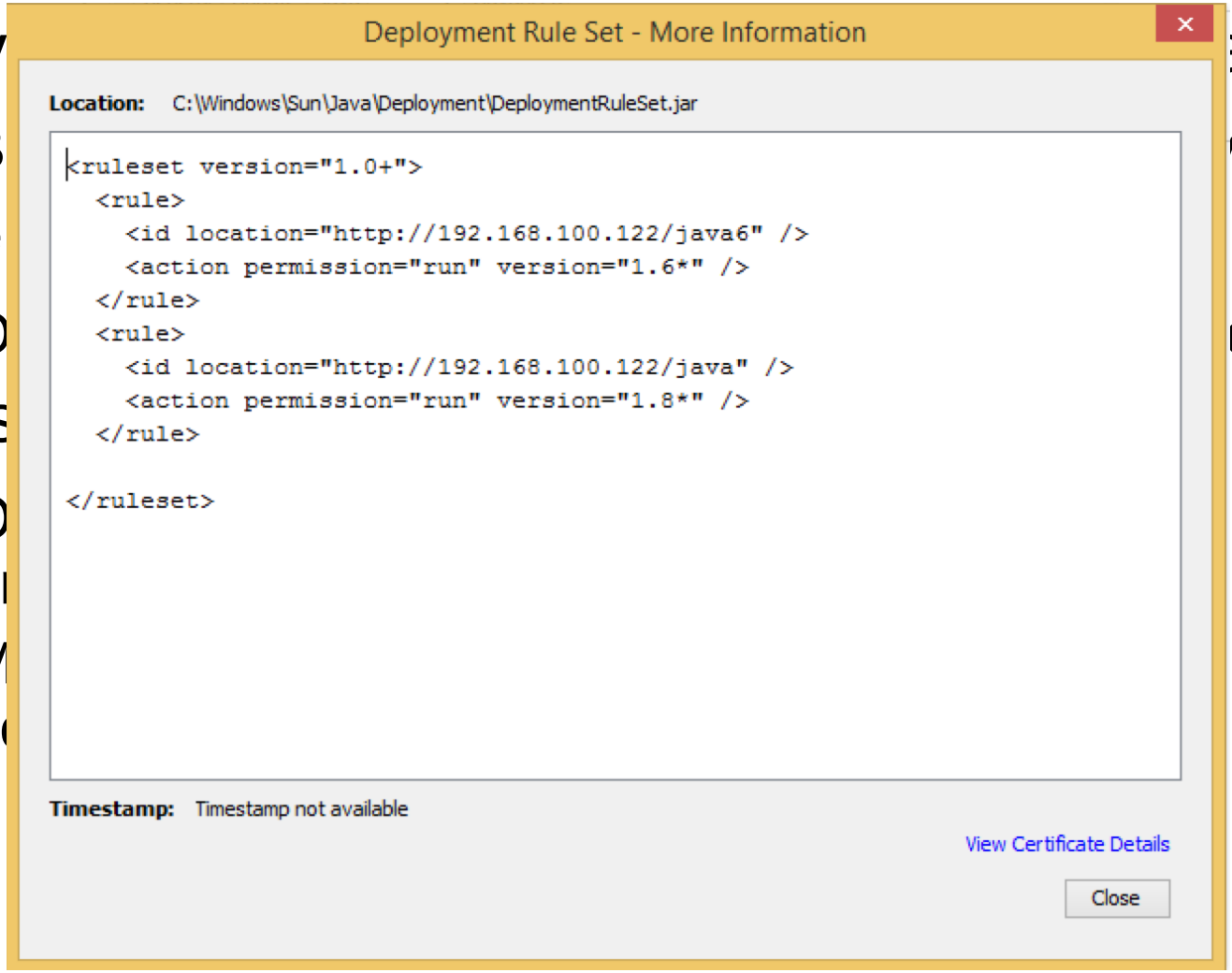
- Java is on our top unpatched threats for the year
  - BTW, attacks are on desktop not serverside Java
- We can’t patch Java
  - Our business critical timecard application requires it..

Hackers – Mass Malware - Java

- Java is on our top unpatched threats for the year
  - BTW, attacks are on desktop not serverside Java
- We can't patch Java
  - Our business critical timecard application requires it..
- Yes, you can.
  - Oracle Java v7 and v8 have a "Java Router" embedded
  - Multiple Javas on a machine can be selectively deployed

Hackers – Mass Malware - Java

- Jav … year
  - B … va
- We …
  - O … es it..
- Yes …
  - O … er
  - M … de



QUALYS® CONTINUOUS SECURITY

Hackers – Mass Malware - Java

- Java is on our top unpatched threats for the year
  - BTW, attacks are on desktop not serverside Java
- We can't patch Java
  - Our business critical timecard application requires it..
- Yes, you can.
  - Oracle Java v7 and v8 have a "Java Router" embedded
  - Multiple Javas on a machine can be selectively deployed
  - Deployment Rulesets - by URL, by checksum, by…

Hackers – Mass Malware - Java

Demo

Hackers - APT and 0-days

- 0-days in 2014/2015
  - 2x Windows in 2014, 1x2015 (June)
  - 4x Internet Explorer in 2014, 1x2015
  - 4x Adobe Flash in 2015

Hackers - APT and 0-days

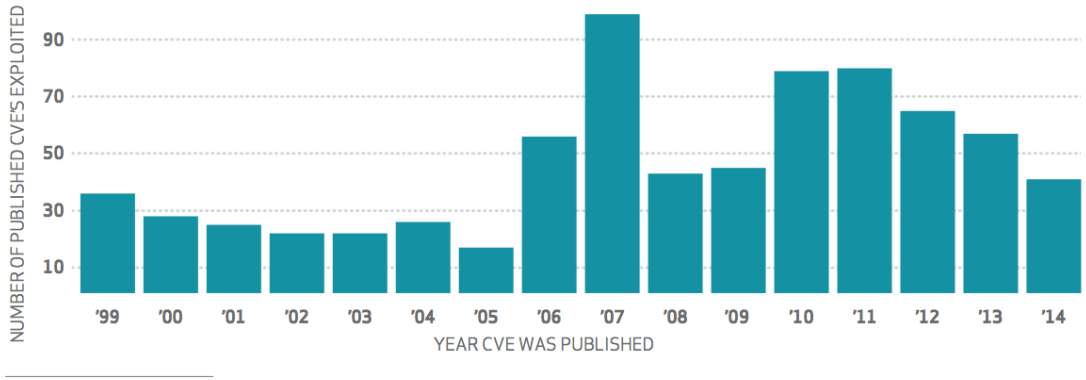
- 0-days in 2014/2015
  - 2x Windows in 2014
  - 4x Internet Explorer in 2014, 1x2015
  - 4x Adobe Flash in 2015
- Use Safe Neighborhood Software
  - Alternative OS: Mac OS X
  - Alternative Browser: Chrome

Hackers - APT and 0-days

- Alternative Browser: Chrome
- 60% Marketshare
- 220 critical vulnerabilities in 2012-2014
- 0 known attacks
- Aggressive Autoupdate & Fast Patching: 24 hours to 7 days
  - Faster than typical exploits
- Sandboxing

Hackers - VDBIR 2015

- Few Vulnerabilities are being exploited – 40 in 2014



- 99.9% of Vulnerabilities exploited are > 1 year old
- 50% of 2014 CVE exploits happened within 2 weeks
- Lesson: Patch all, decide which to patch faster (pg 17)
  - Exploitable Attribute: most important factor (pg 17)

QUALYS® CONTINUOUS SECURITY

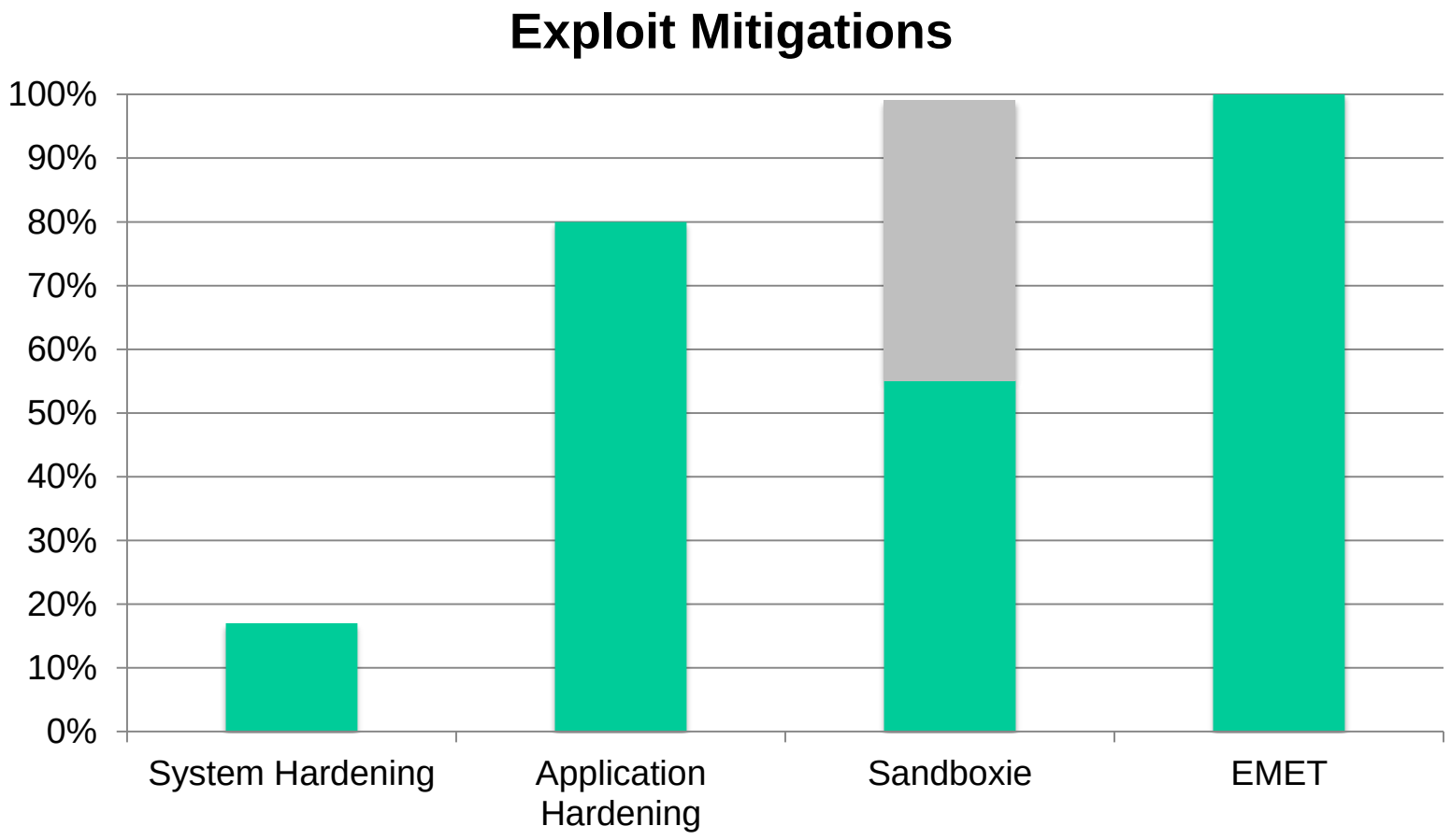
Hackers - APT and 0-days

- 0-days in 2014/2015
  - 2x Windows in 2014
  - 4x Internet Explorer in 2014,1x2015
  - 4x Adobe Flash in 2015
- Use Safe Neighborhood Software
  - Alternative OS: Mac OS X
  - Alternative Browser: Chrome
  - Alternative Flash: HTML5?
    - Sandbox: Chrome/Flash combo not attacked

Hackers - APT and 0-days

- Sandboxing
- Jarno Niemela's (F-Secure) VB 2013 Paper
- 930 APT malwares against Hardening

Hackers - APT and 0-days



QUALYS® CONTINUOUS SECURITY

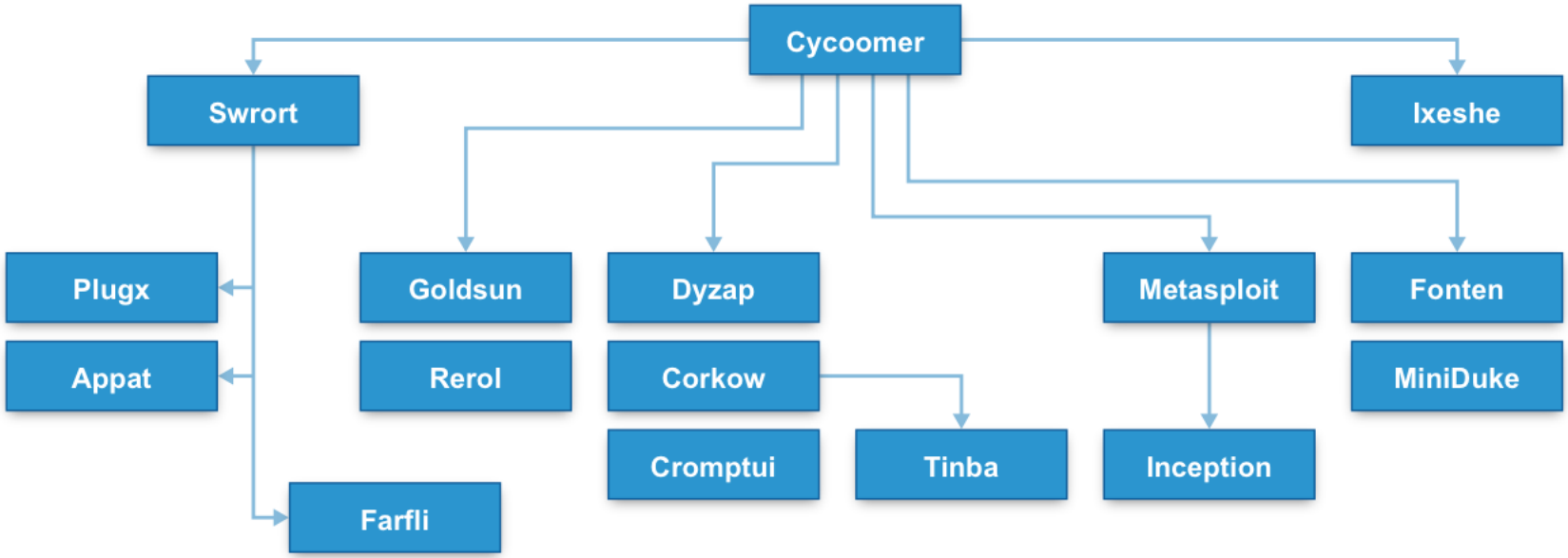
Hackers - APT and 0-days

- Sandboxing
- Jarno Niemela's (F-Secure) VB 2013 Paper
- 930 APT malwares against Hardening
- Sandbox testing not conclusive
- Application Hardening and EMET are free

Hackers - APT and 0-days

- But APT means attacker can do anything
- Bypass your Hardening, the Sandbox, EMET…
- How good are they?
- Sophos: CVE-2014-1761 (Word RTF) analysis
- 15+ sample families assessed

Hackers - APT and 0-days



Hackers - APT and 0-days

- But APT means attacker can do anything
- How good are they?
- Sophos: CVE-2014-1761 (Word RTF) analysis
- 15+ sample families assessed
- 7 skill categories

Hackers - APT and 0-days

	Zero	Basic	Intermediate	Skilled	Advanced	Pro	Neo
Generate sample with Metasploit	✔	✔	✔	✔	✔	✔	✔
Replace payload in existing sample	-	✔	✔	✔	✔	✔	✔
Modify shellcode	-	-	✔	✔	✔	✔	✔
Trivial modification in ROP chain	-	-	-	✔	✔	✔	✔
Significant modification in ROP chain	-	-	-	-	✔	✔	✔
Trivial modification in exploit trigger	-	-	-	-	-	✔	✔
Significant modification in exploit trigger	-	-	-	-	-	-	✔

Hackers - APT and 0-days

- But APT means attacker can do anything
- How good are they?
- Sophos: CVE-2014-1761 (Word RTF) analysis
- 15+ sample families assessed
- 7 skill categories
- Mixed results 50% trivial, 50% advanced

Hackers - APT and 0-days

Zero	Basic	Intermediate	Skilled	Advanced	Pro	Neo
	Goldsun		Metasploit	MiniDuke	Fonten	Cycoomer
	Swrort		Inception		Dyzap	
	Plugx				Tinba	
	Appat				Corkow	
	Farfli				Cromptui	
	Rerol				Ixeshe	

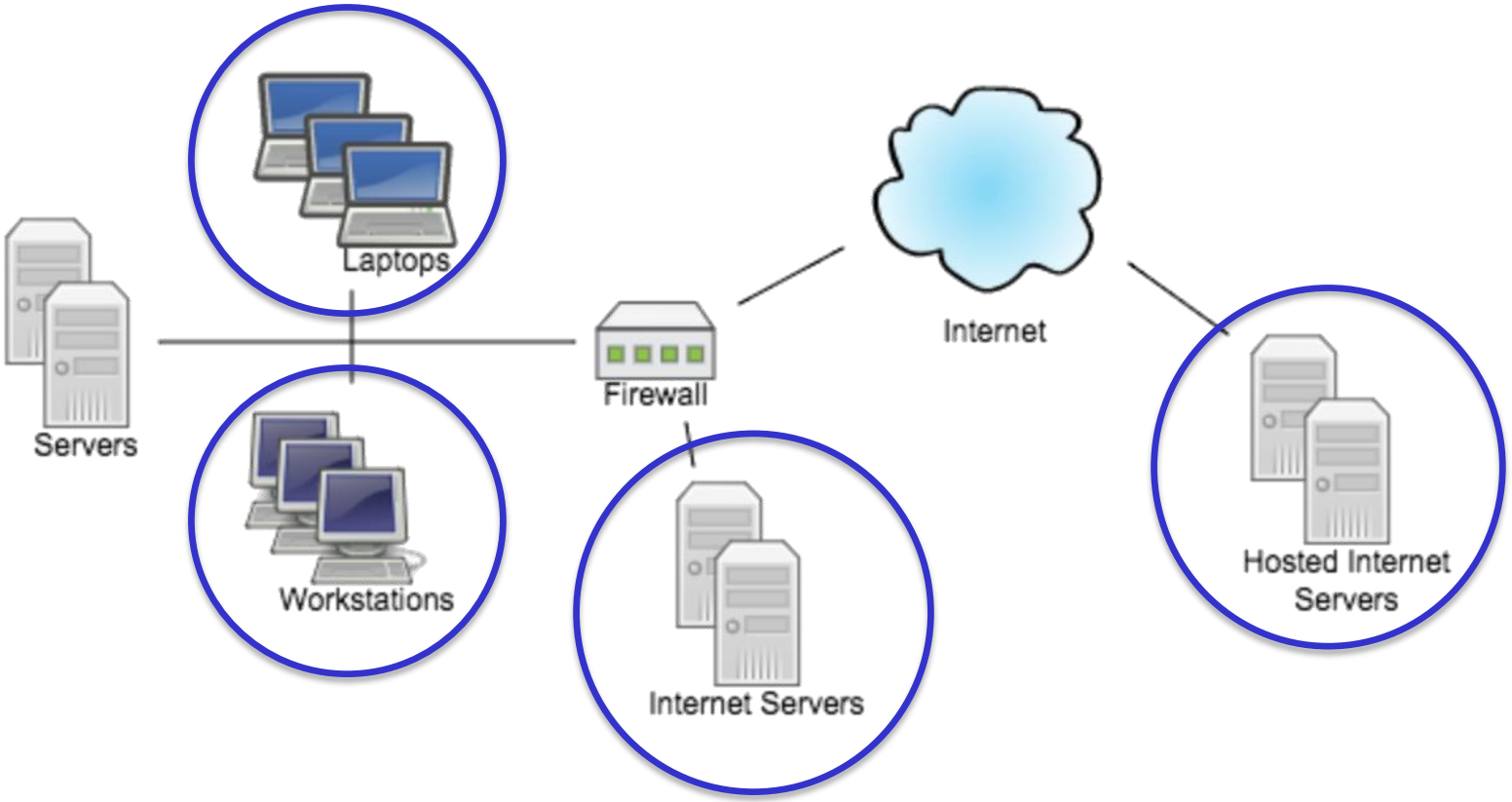
Hackers - APT and 0-days

- But APT means attacker can do anything
- How good are they?
- Sophos: CVE-2014-1761 (Word RTF) analysis
- 15+ sample families assessed
- 7 skill categories
- Mixed results 50% trivial, 50% advanced
- All (!) attacked only 1 software version – Office 2010 (SP2, 32bit)

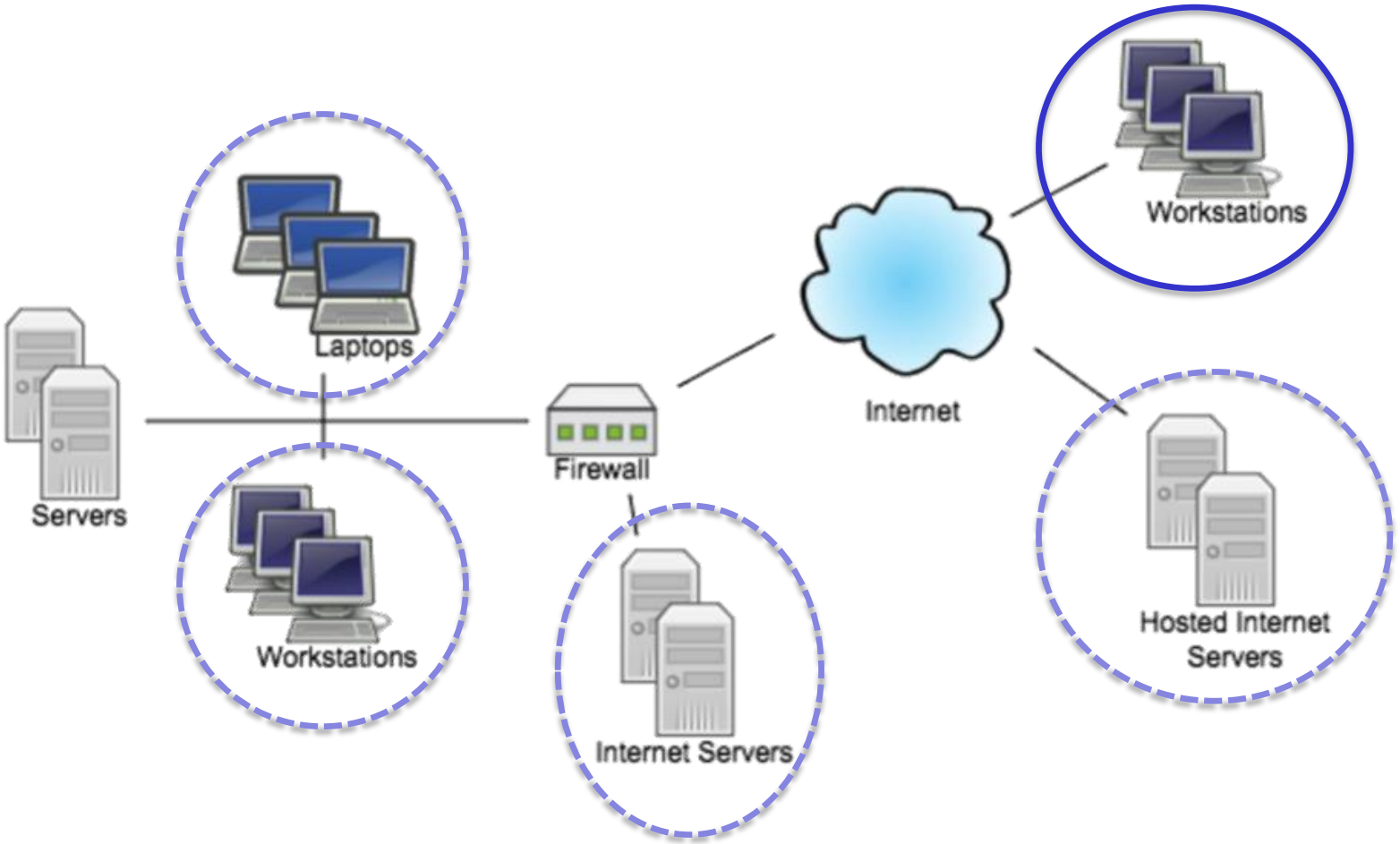
Hackers - APT and 0-days

- Harden Applications and deploy EMET
- Safer Neighbourhoods - Alternative Technology stacks
- Limit Java to internal/known Applications – Deployment Rulesets

Hackers - Attack Perimeter



Hackers – Attack Perimeter



Hackers - Attack Perimeter

- Perimeter is everywhere
  - Mobility, Personal Devices
  - Beyondcorp

Google Moves Its Corporate Applications to the Internet

AUTHENTICATION BEYONDCORP CORPORATE NETWORK CYBERSECURITY GOOGLE

Email Print

By RACHAEL KING

Google Inc. GOOGL -0.85%, taking a new approach to enterprise security, is moving its corporate applications to the Internet. In doing so, the Internet giant is flipping common corporate security practice on its head, shifting away from the idea of a trusted internal corporate network secured by perimeter devices such as firewalls, in favor of a model where corporate data can be accessed from anywhere with the right device and user credentials.

Hackers - Attack Perimeter

- Perimeter is everywhere
  - Mobility, Personal Devices
  - Beyondcorp
- SaaS Applications enable
- Security Pros
  - All Machines Internet hardened
  - No Client/Peer networking = no malware lateral growth
- Security Cons
  - Traditional Non-Internet Tools challenged
- Internet Agent Solutions

Internet Agent

Demo

Action - Short and Medium term

- Scan your Perimeter continuously, alert on changes
- Inventory for Flash, Reader, IE, Office, Java
- Update versions – Mass Malware cure

- Address Vulnerabilities Quickly
- Harden Setup - APT and 0-days
  - Newest Software, Use EMET, Safe neighborhoods

- Later - Watch Logs for Anomalies, Run Sandboxes

Vielen Dank

Wolfgang Kandek
wkandek@qualys.com
@wkandek

http://www.qualys.com

QUALYS®