RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: Tech-T08

Getting a Jump on Hackers

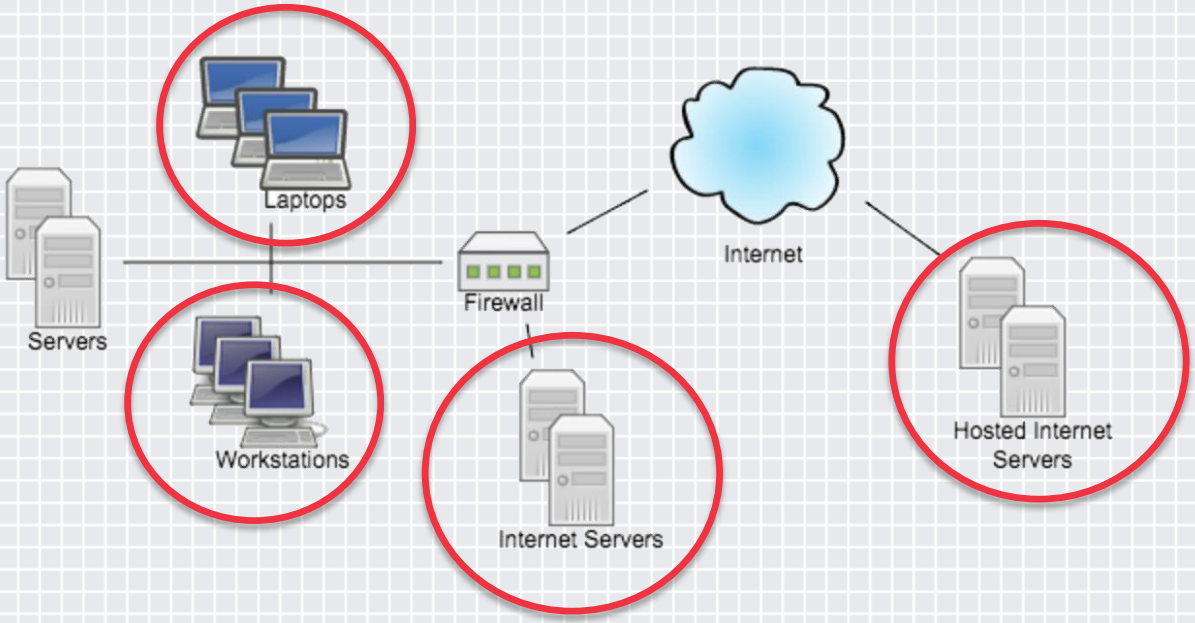
Wolfgang Kandek

CTO
Qualys
@wkandek

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
- Breaches

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

- BSI – C onstechnik
  - Digit
  - Situa
  - Digit
  - 95%
  - Attac
  - In a

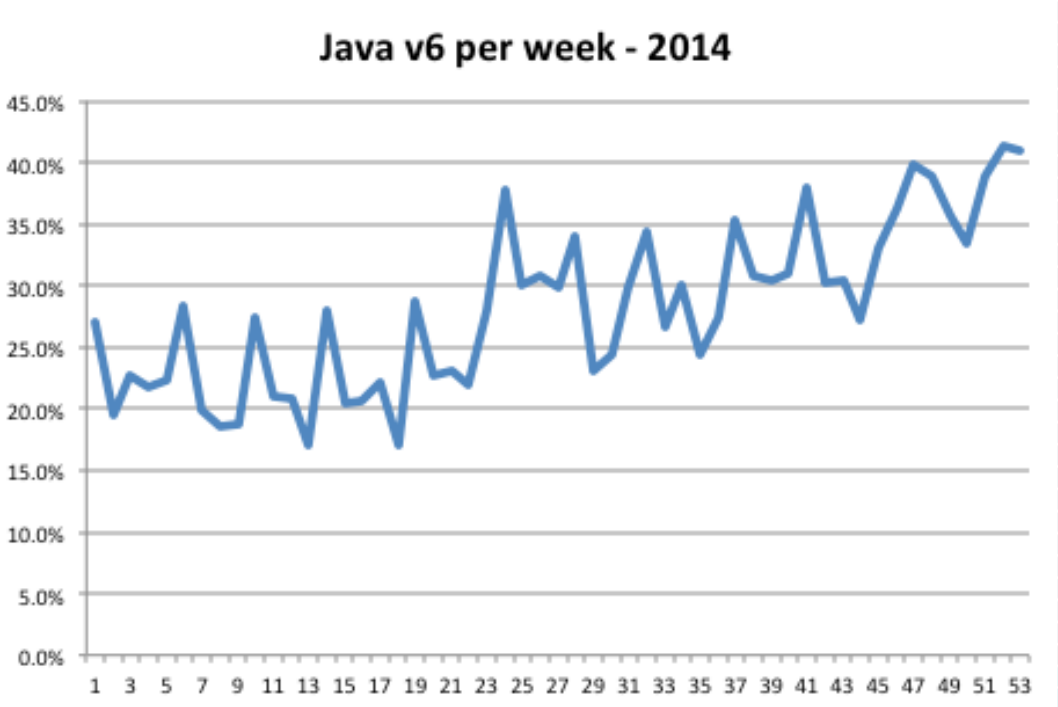
Softwareprodukte

- 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

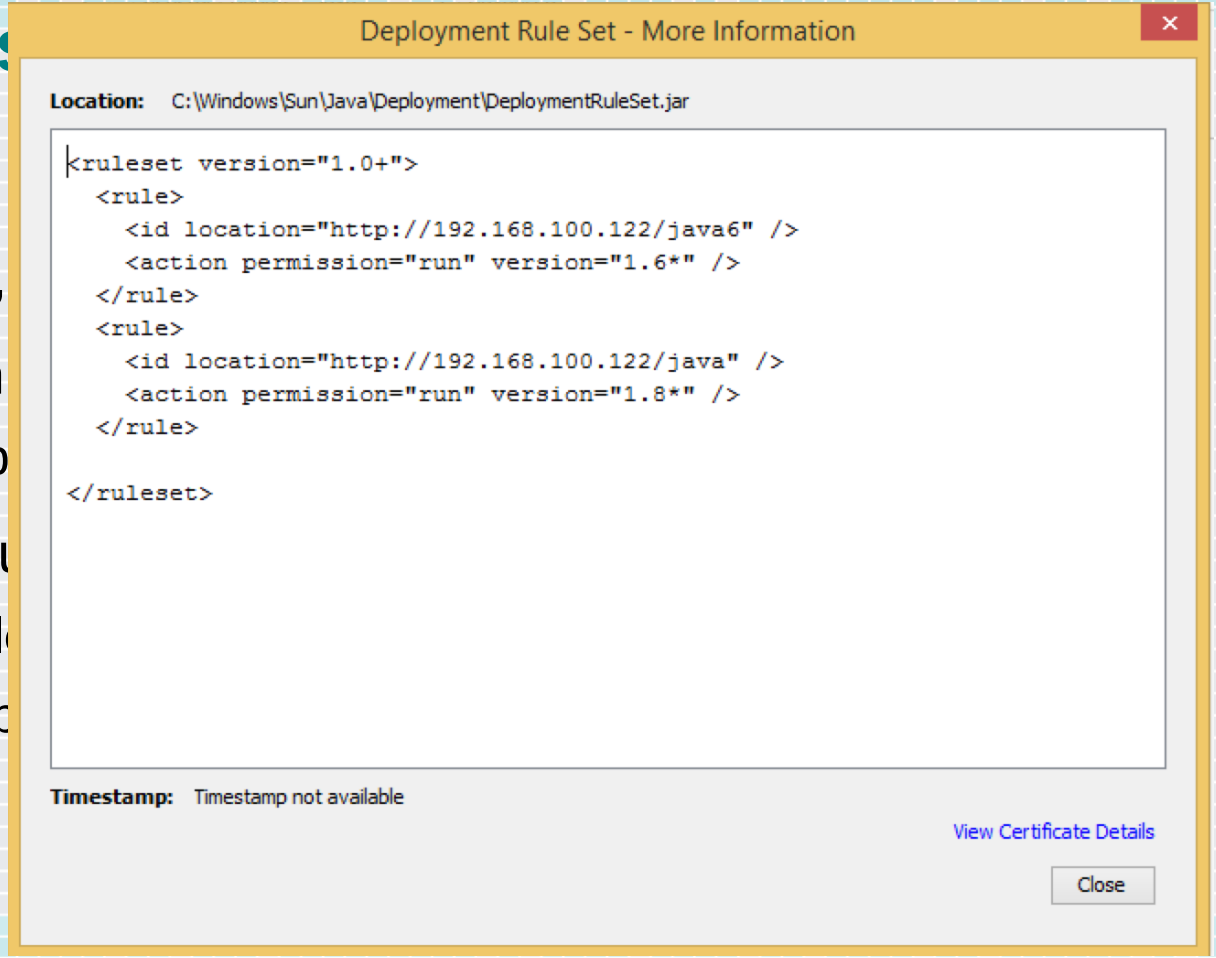


Hackers – Mass Malware - Java

- 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

- Java is
  - BTW,
- We can
  - Our b
- Yes, you
  - Oracl
  - Multip



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
  - 4x Internet Explorer in 2014
  - 3x 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

- 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

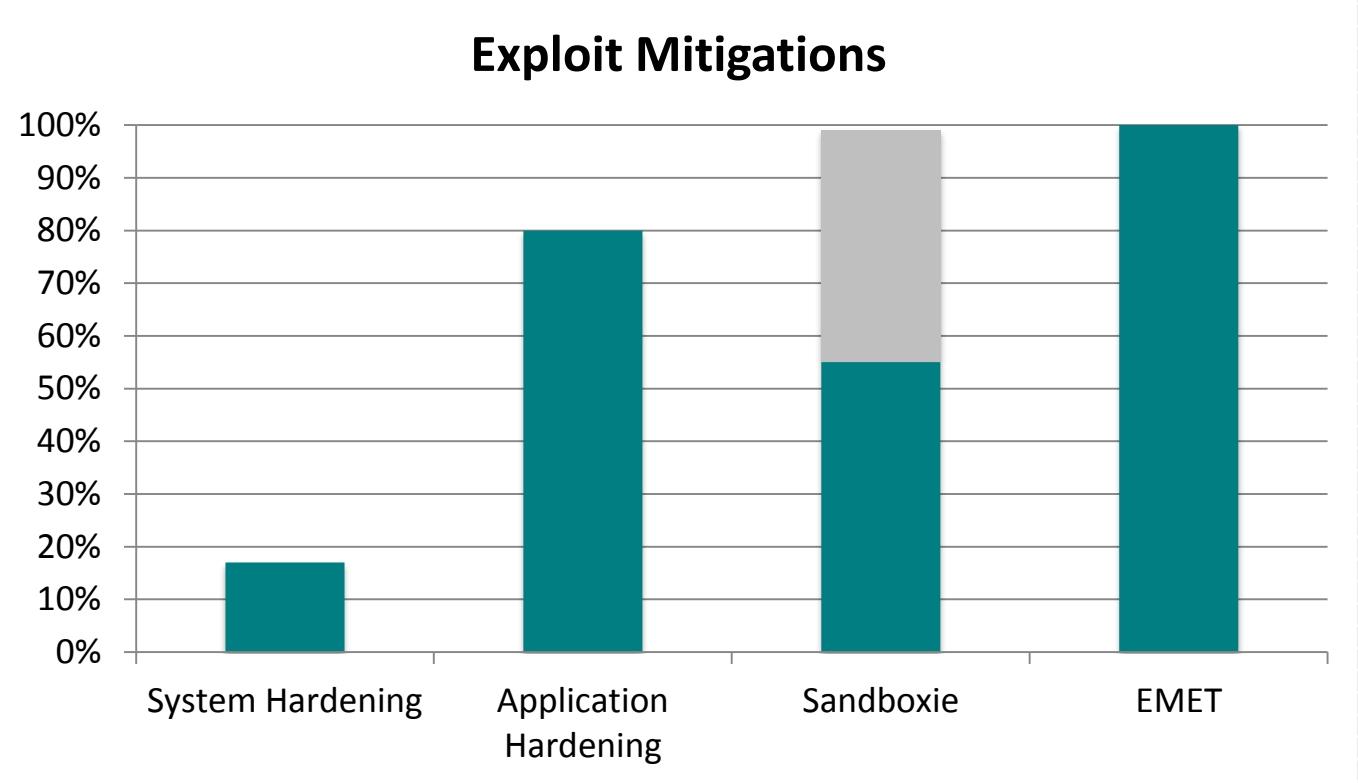
Hackers – APT and 0-days

- 0-days in 2014/2015
  - 2x Windows in 2014
  - 4x Internet Explorer in 2014
  - 3x 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



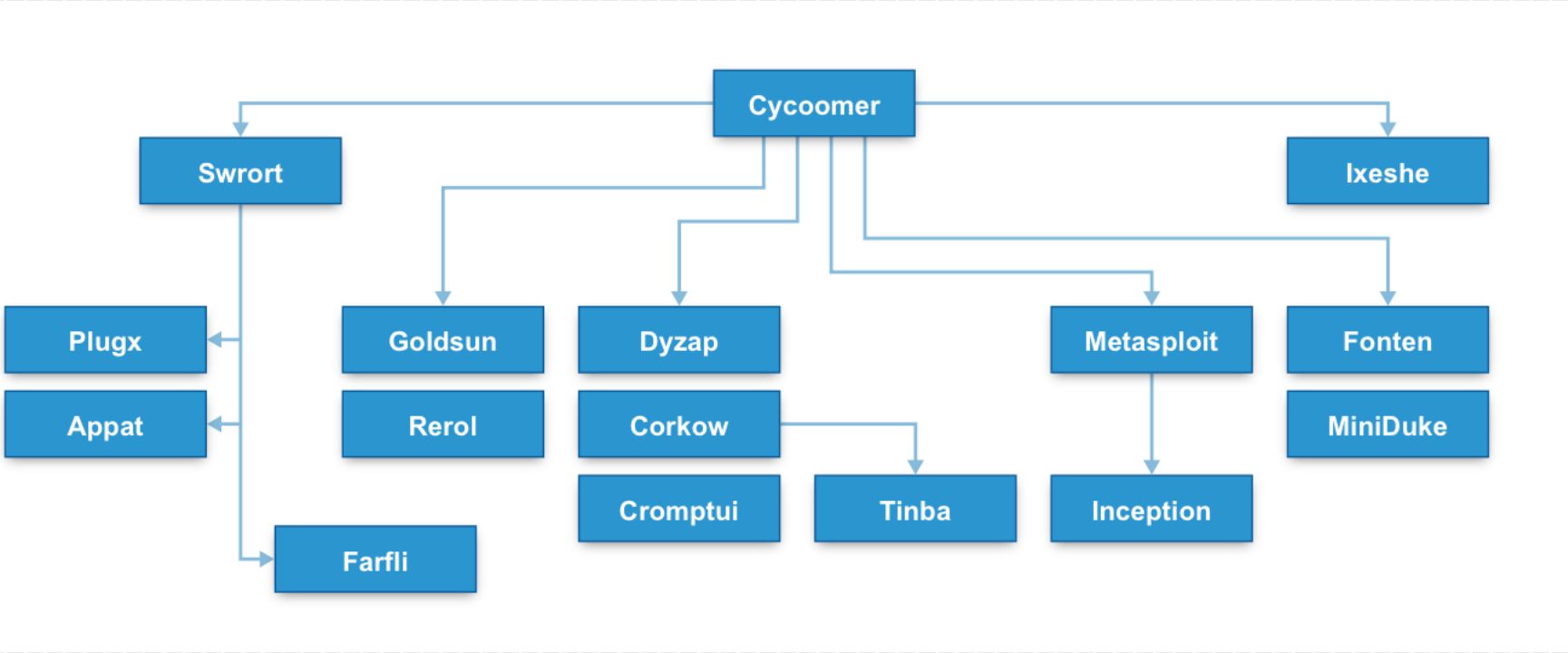
Hackers – APT and 0-days

- 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

- Dan Guido – Exploit Intelligence Project
- Focus on robust configurations to prevent future exploits
- Few vulnerabilities are relevant: 14 in 2009, 13 in 2010
- 20 in 2014
- Tighter Security Settings defeat new attacks

Hackers – APT and 0-days

- Dan Guic
- Focus on
- Few vuln
- 20 in 201
- Tighter S
  - DEP, A
  - EMET
  - Disable

Memory Corruption (19)	
Defeated by DEP	14
Defeated by ASLR	17
Defeated by EMET	19

Logic Flaws (8)	
No Java in Internet Zone	4
No EXEs in PDFs	1
No Firefox or FoxIt Reader	2

oits

L0

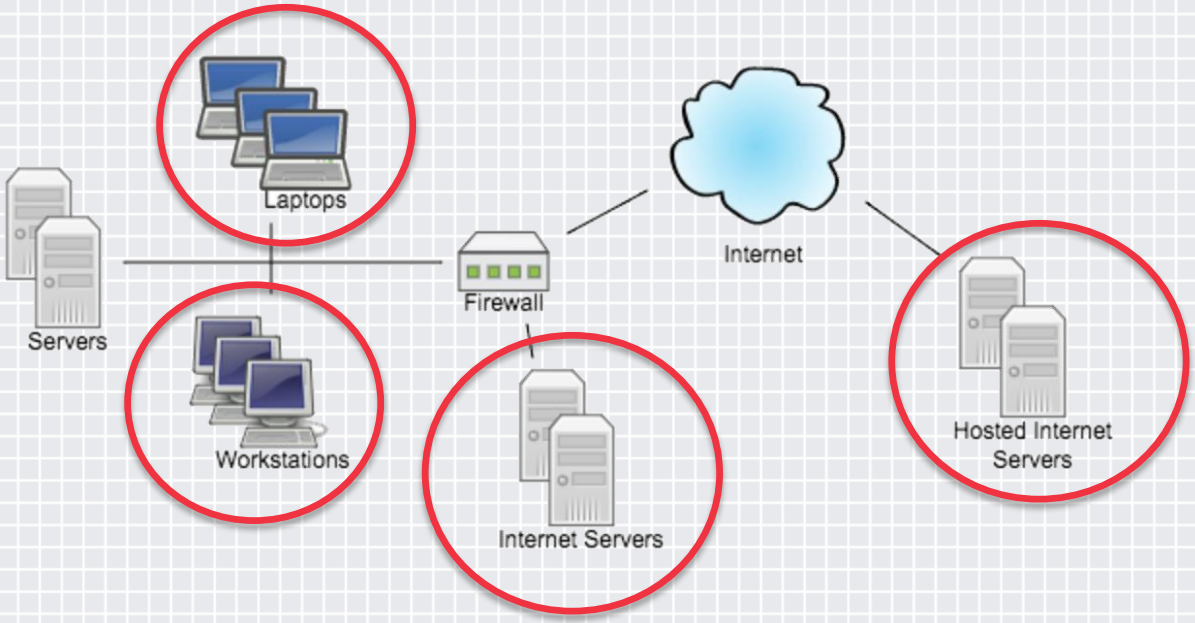
Hackers – APT and 0-days

- Dan Guido – Exploit Intelligence Project
- Focus on robust configurations to prevent future exploits
- Few vulnerabilities are relevant: 14 in 2009, 13 in 2010
- 20 in 2014
- Tighter Security Settings defeat new attacks
  - DEP, ASLR
  - EMET (btw, all IE 0-days in 2014)
  - Disable EXE/Javascript in PDF
  - Limit Java to internal Applications

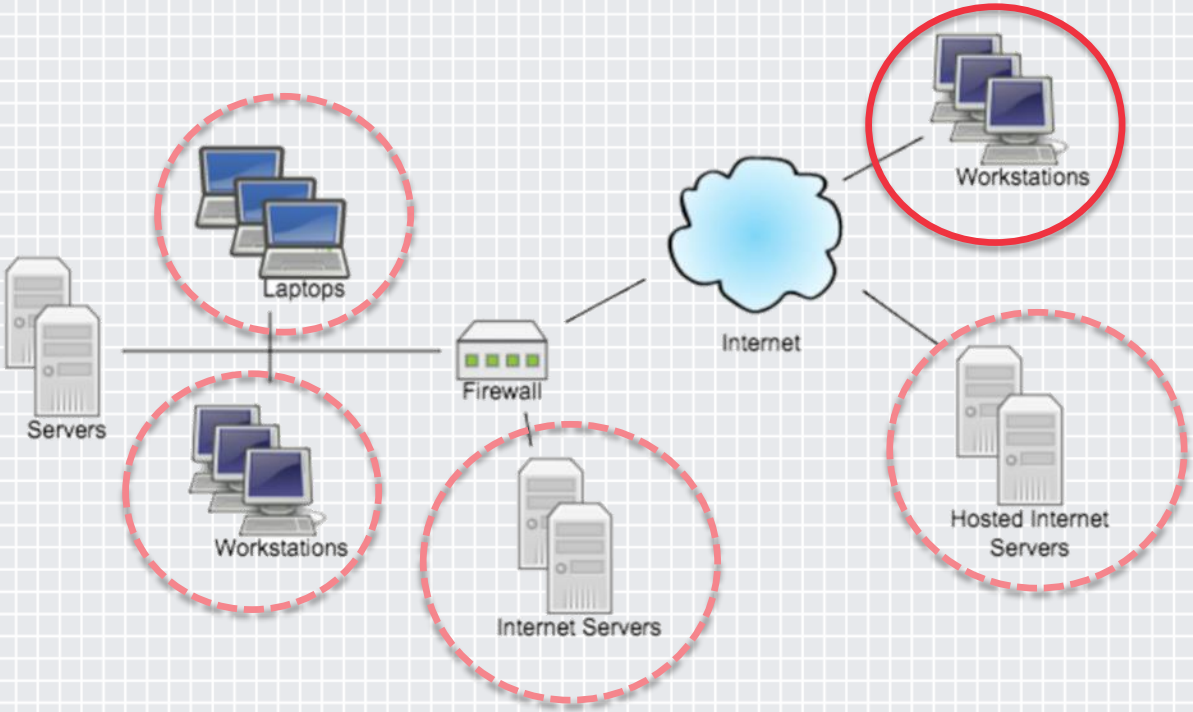
Hackers – APT and 0-days

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

Hackers – Attack Perimeter



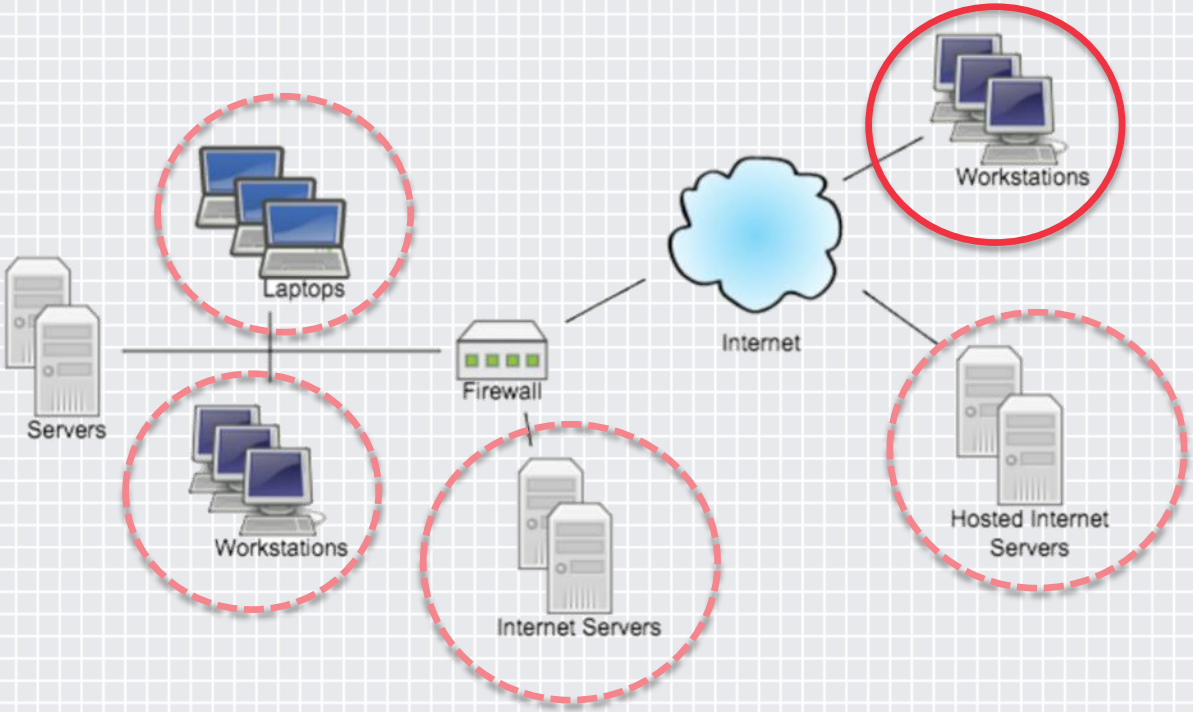
Hackers – Attack Perimeter



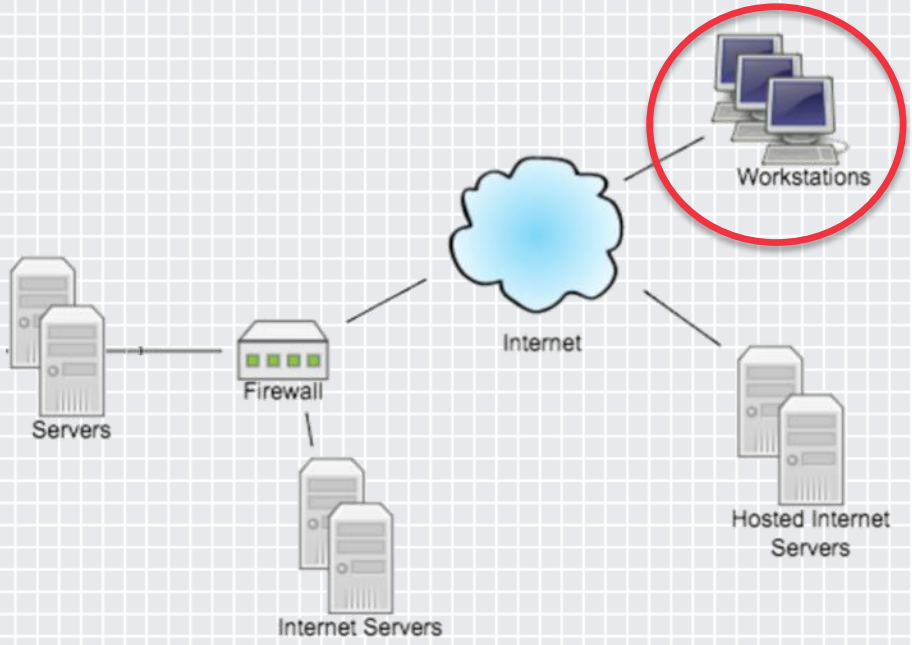
Hackers – Attack Perimeter

- Perimeter is everywhere
  - Mobility, Personal Devices
- 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

Hackers – Attack Perimeter



Hackers – Attack Perimeter



Hackers - Credentials

- Abuse worldwide connectivity (e-mail, mobile workstations, VPN)
- Steal credentials through phishing attacks (e-mail)
- Install undetectable malware
- Access VPNs

Hackers - Credentials

THE WALL STREET JOURNAL. | BUSINE

Target Breach Began Wit Electronic Billing Link

Fazio Mechanical Services Says It Was 'a Victir

By PAUL ZIOBRO
Feb. 6, 2014 6:59 p.m. ET

The hackers that carried out the massive data breach at T appear to have gained access via a refrigeration contracto Pittsburgh that connected to the retailer's systems to do billing.

Fazio Mechanical Services Inc., a privately held company 125 employees, said Thursday it was "a victim of a sophist cyberattack operation" and was cooperating with investig Secret Service.

SECTIONS | HOME | SEARCH | The New York Times

INVESTMENT BANKING | LEGAL/REGULATORY

Neglected Server Provided Entry for JPMorgan Hackers

By MATTHEW GOLDSTEIN, NICOLE PERLROTH and MICHAEL CORKERY DECEMBER 22, 2014 8:41 PM
79 Comments

The computer breach at JPMorgan Chase this summer — the largest intrusion of an American bank to date — might have been thwarted if the bank had installed a simple security fix to an overlooked server in its vast network, said people who have been briefed on internal and outside investigations into the attack.
...
The attack against the bank began last spring, after hackers stole the login credentials for a JPMorgan employee, these people said. Still, the attack could have been stopped there.

Hackers - Credentials

- Teach users to recognize attacks – ✓
- Require better passwords – ✓
- But limited effect > 2% will still click
- Password reuse rampant due to complicated rules
- Massive username/password databases available

Hackers - Credentials

- Teach
- Requir
- But lim
- Passw
- Massiv

Forbes ▾ | New Posts | Most Popular | Lists | Video

Log in | Sign up | Connect

SECURITY 2/10/2015 @ 4:30AM | 6,959 views

Researcher Releases 10 Million Usernames And Passwords In Fight Against Obama's War On Hackers

Thomas Fox-Brewster
Forbes Staff

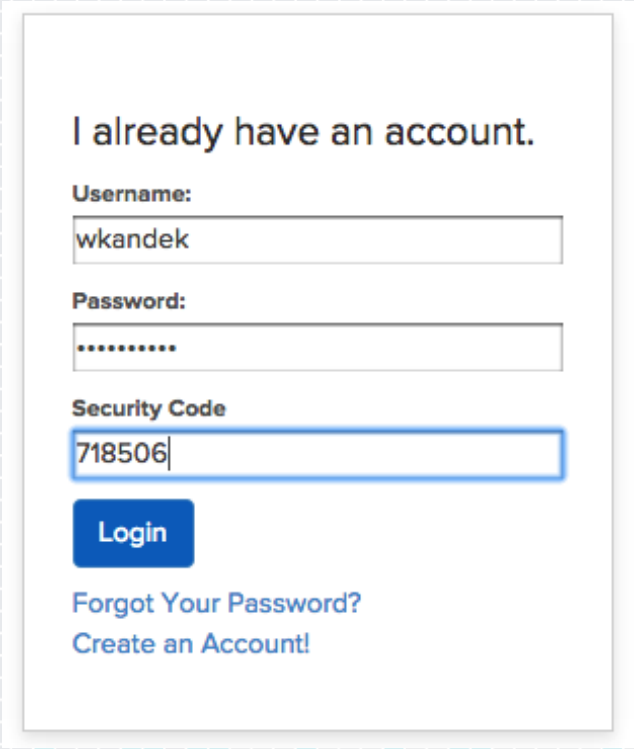
With the sentencing of Barrett Brown, a journalist who was convicted of numerous crimes and whose jail time was increased because he posted a link to stolen data, and some worrying cyber security proposals from the Obama administration that would appear to outlaw the everyday activities of researchers, both hacks and hackers have been anxious about the chilling effects on their work. Quinn Norton, a long-time security writer, said she would no longer report on leaked information for fear of arrest. Errata Security's Robert Graham said there was a war being waged on professional hackers who have only been trying to make the internet safer.

Hackers - Credentials

- Teach users to recognize attacks – ✓
- Require better passwords – ✓
- But limited effect > 2% will still click
- Password reuse rampant due to complicated rules
- Massive username/password databases available
- Password decoding/guessing in the realm of all attackers.

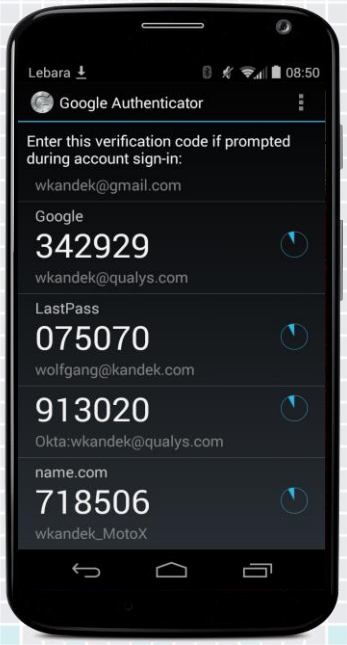
Hackers - Credentials

- Two factor authentication



Hackers - Credentials

- Two factor authentication



Hackers - Credentials

- Teach users to recognize attacks – ✓
- Require better passwords – ✓

- Teach your users to protect their own personal data
  - Banks, E-mail, Linkedin
- 2FA is mature now
- Implement 2FA for your systems

Act Now – x days

- x=30: Scan your Perimeter Server continuously, alert on changes
- x=60: Software inventory for Flash,Reader,IE,Office,Java
- x=90: Update versions- – Mass Malware cure
- x=90+: Address Vulnerabilities Quickly
- x=90+: Harden Setup - APT and 0-days
  - Newest Software, Use EMET, Safe neighborhoods
- x=90+: Authentication - Deploy 2-Factor
- Then: Watch Logs for Anomalies, Run Sandboxes

SESSION ID: Tech-T08

Thank you

http://laws.qualys.com
@wkandek
Wolfgang Kandek