

# Defense is Possible!

Kevin Cardwell

# Agenda

- ▶ Dispelling myths
- ▶ Ingress and Egress
- ▶ Hardening
- ▶ The good and the bad
- ▶ Memory analysis
- ▶ Server 2008/2012 security enhancements
- ▶ BYOD security
- ▶ “out of the box” network design

# Myth or Fact?

Mobile – 71%

- ▶ The compromise was inevitable!
  - APT, sophisticated attackers etc etc
  - **MYTH!**

2012 – 78% low difficulty



## WHAT COMMONALITIES EXIST?

79% of victims were targets of opportunity (-4%)

96% of attacks were not highly difficult (+4%)

94% of all data compromised involved servers (+18%)

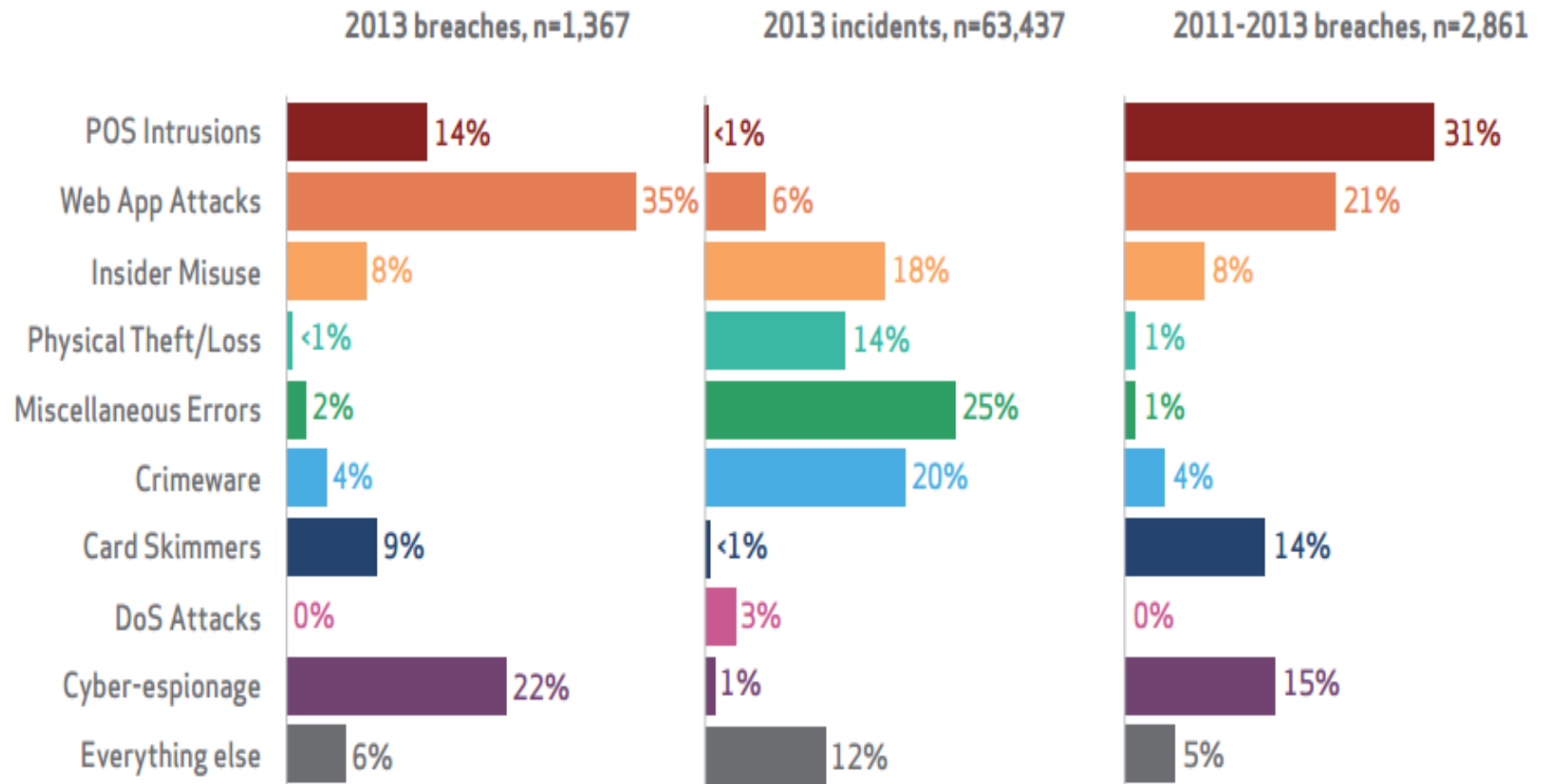
85% of breaches took weeks or more to discover (+6%)

92% of incidents were discovered by a third party (+6%)

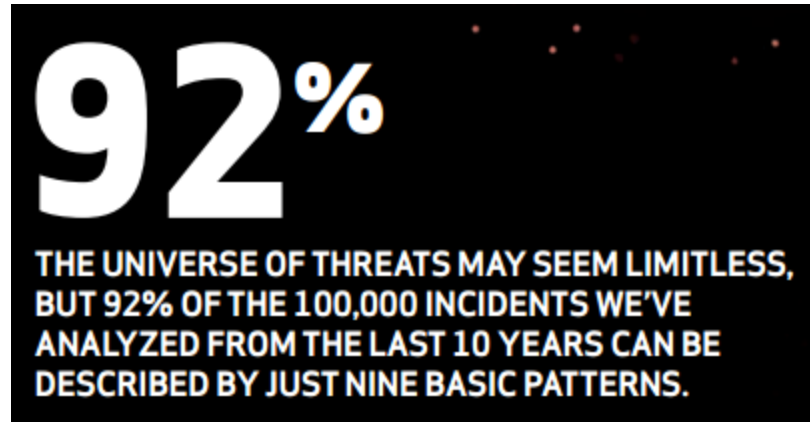


97% of breaches were avoidable through simple or intermediate controls (+1%)

# 2011-2013 Data Breach Report



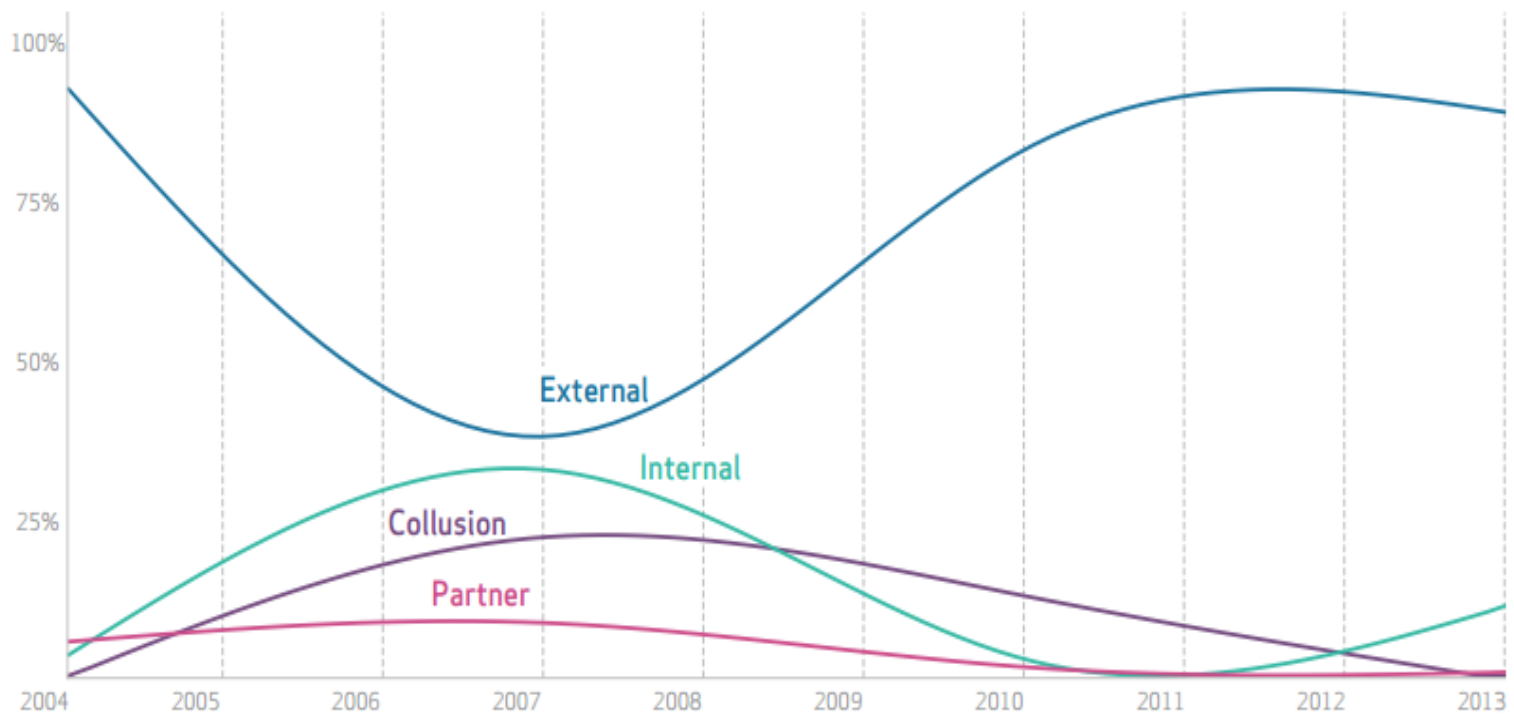
# Shift of Focus



---

*2013 may be remembered as the “year of the retailer breach,” but a comprehensive assessment suggests it was a year of transition from geopolitical attacks to large-scale attacks on payment card systems.*

# Insider Threat



# Ingress Filtering

- ▶ Traffic coming into your network
- ▶ Implemented by almost all organizations
- ▶ Security policy determines what is allowed and configured in the filters
- ▶ No traffic arriving at the perimeter should have an internal source address
  - Commonly referred to as *sanity checking*
- ▶ RFC 2267 provides guidance for filters to prevent denial-of-service attacks
- ▶ Block ICMP Echo Reply messages to the broadcast address
- ▶ Bogon Filtering

CaseStudy of malware infection => **64% of traffic** blocked by bogon filtering

# Egress Filtering

- ▶ One of the most neglected areas of filtering
  - Most organizations neglect to filter traffic leaving their network
  - Even after the rise of DDoS attacks, many organizations still do not
  - There will always be some out there who never will
- ▶ These sites are used as amplifiers to attack other networks
- ▶ The concept is simple:
- ▶ Most attacks use a spoofed address to attack as the source
  - When you egress filter, then the packet is dropped
- ▶ Blackhole routing

**Do not allow traffic to leave your network that does not have a source address from within your network**

DDoS = distributed denial of service

# Egress Filtering (cont)

- ▶ If site is not 24/7
  - Shut off access going out to the Internet
    - Block the well known malware ports of communication
      - http
      - ssh
      - https
      - Etc
  - Monitor for attempts
    - All malware will attempt outbound connections
    - If no one is there, should be none
- ▶ If 24/7
  - Only monitor critical systems
    - Servers should not initiate connections to the Internet
  - Subscribe to a service
    - Watch for lookups of known malware nets

# Web Applications

- ▶ Harden them!
- ▶ OWASP application testing guide
- ▶ [www.owasp.org](http://www.owasp.org)
- ▶ Harden the SQL databases
  - Upgrade MS to SQL Server 2008 or beyond
  - Follow application hardening guides

# Hardening Systems

- ▶ NSA Guides

- [http://www.nsa.gov/ia/guidance/security\\_configuration\\_guides/index.shtml](http://www.nsa.gov/ia/guidance/security_configuration_guides/index.shtml)

- ▶ Center for Internet Security

- Benchmarks
    - [www.cisecurity.org](http://www.cisecurity.org)

# Security Compliance Manager

- ▶ Provided by Microsoft
- ▶ Can customize
- ▶ Allows for baseline comparisons



# Top 4 Controls

- ▶ Application Whitelisting
- ▶ Patch Applications
- ▶ Patch Operating System
- ▶ Minimize the number of users with privileged rights
  - Disable the local admin account on domain computers

# SANS Critical Security Controls

## 20 Critical Security Controls - Version 4.1

- Critical Control 1: Inventory of Authorized and Unauthorized Devices
- Critical Control 2: Inventory of Authorized and Unauthorized Software
- Critical Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
- Critical Control 4: Continuous Vulnerability Assessment and Remediation
- **Critical Control 5: Malware Defenses**
- Critical Control 6: Application Software Security
- Critical Control 7: Wireless Device Control
- Critical Control 8: Data Recovery Capability
- Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps
- Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services
- Critical Control 12: Controlled Use of Administrative Privileges
- Critical Control 13: Boundary Defense
- Critical Control 14: Maintenance, Monitoring, and Analysis of Audit Logs
- Critical Control 15: Controlled Access Based on the Need to Know
- Critical Control 16: Account Monitoring and Control
- Critical Control 17: Data Loss Prevention
- Critical Control 18: Incident Response and Management
- Critical Control 19: Secure Network Engineering
- Critical Control 20: Penetration Tests and Red Team Exercises

# Good and the Bad

- ▶ We have gotten better at security
- ▶ The hackers have gotten better at hacking
- ▶ Patch system is broken
- ▶ Residual risk
- ▶ [www.zerodayinitiative.com](http://www.zerodayinitiative.com)

ZDI-CAN-2152	Juniper	CVSS: 10	2014-02-18 (177 days ago)	2014-08-17
Discovered by: Anonymous				
ZDI-CAN-2152	Juniper	CVSS: 10	2014-02-18 (177 days ago)	2014-08-17
Discovered by: Anonymous				
ZDI-CAN-2151	Juniper	CVSS: 10	2014-02-18 (177 days ago)	2014-08-17
Discovered by: Anonymous				
ZDI-CAN-2049	AlienVault	CVSS: 7.9	2014-01-13 (213 days ago)	2014-07-12
Discovered by: Brandon Perry				

# The Bad

## (0Day) F5 Data Manager discoverFilerBasicInfo.jsft fileName SQL Injection Remote Code Execution Vulnerability

**ZDI-14-293:** August 12th, 2014

### CVE ID

---

CVE-2014-2949

### CVSS Score

---

6.8, (AV:N/AC:M/Au:N/C:P/I:P/A:P)

### Affected Vendors

---

F5

### Affected Products

---

Data Manager

### Vulnerability Details

---

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of F5 Data Manager. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the discoverFilerBasicInfo.jsft page. An attacker is able to inject SQL through the fileName field in this page, and use that to gain full administrator credentials for Data Manager.

# The Ugly

## Vendor Response

---

### F5 states:

This vulnerability is being disclosed publicly without a patch in accordance with the ZDI 120 day deadline.

05/02/2014 - ZDI disclosed vulnerability to vendor

05/12/2014 - Vendor acknowledged

06/16/2014 - ZDI wrote F5 to ask for clarification about: <http://support.f5.com/kb/en-us/solutions/public/15000/300/sol15310.html>

06/16/2014 - Vendor wrote that they notified ZDI of closure on 06/09/2014 (this was not received) and indicated that "our publications team has determined that this release provides the appropriate level of disclosure"

06/17/2014 - ZDI acknowledged

06/18/2014 - ZDI wrote to confirm mitigation only

06/18/2014 - Vendor requested contact

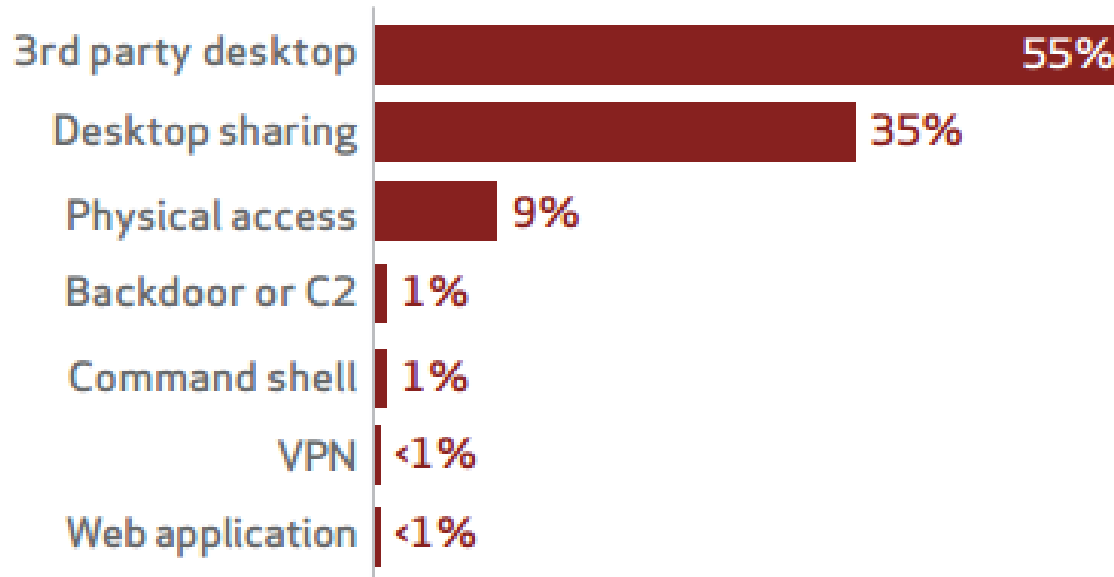
06/19/2014 - ZDI replied

07/25/2014 - ZDI again wrote to confirm our understanding

08/12/2014 - ZDI published advisory

# Clients

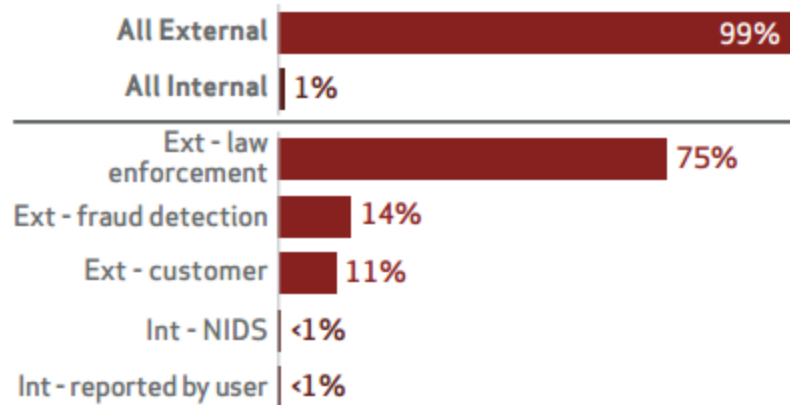
## Hacking vector within POS Intrusions (n=187)



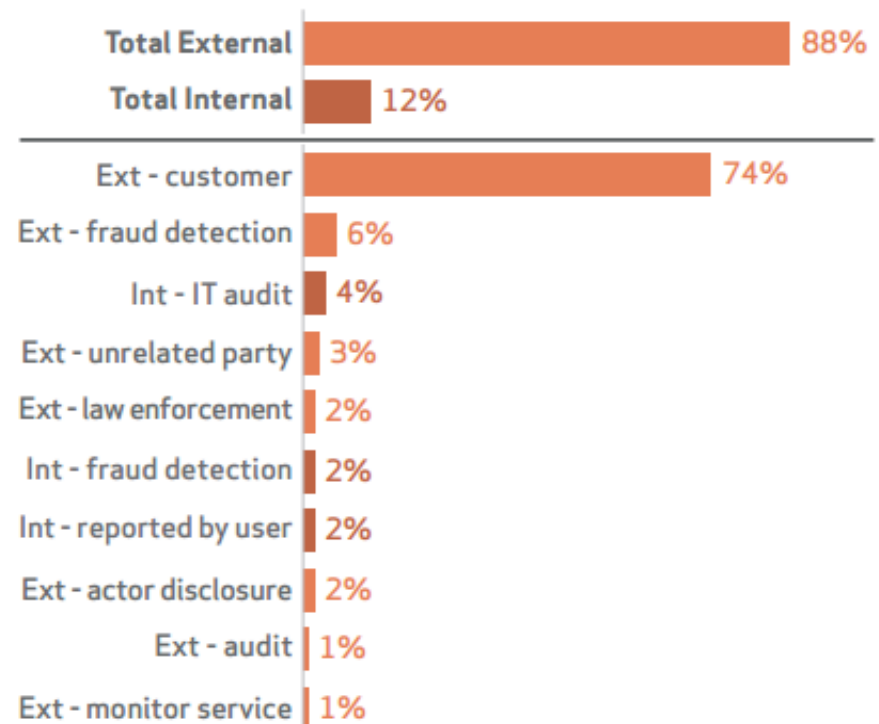
# POS and Web

- ▶ Attacks of choice
- ▶ **Security is a process and methodology not a product!**

Top 5 discovery methods for POS Intrusions (n=197)

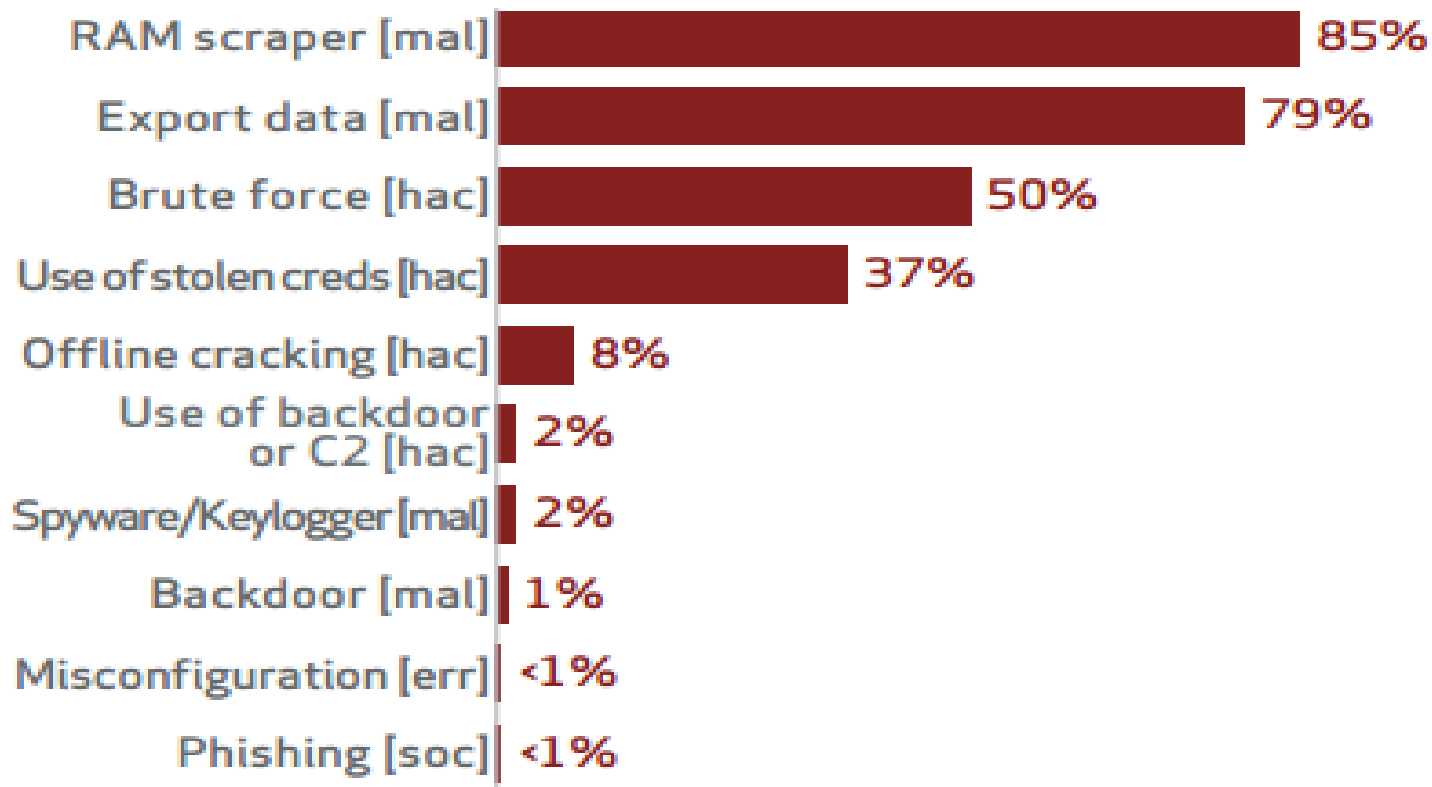


Top 10 discovery methods for financially motivated incidents within Web App Attacks (n=122)



# The How

## Top 10 threat action varieties within POS Intrusions (n=196)



# Memory Analysis



# Running Processes

- ▶ We have to run several tools to extract needed information
  - Executable image
  - Command used to invoke
  - Runtime
  - Security context
  - DLLs and modules
  - Memory

# Pslist

Process information for INTERNALHOST:

Name	Pid	Pri	Thd	Hnd	Prio	CPU Time	Elapsed Time
Idle	0	0	1	0	0	0:50:51.812	0:00:00.000
System	4	8	52	434	0	0:00:15.984	0:00:00.000
smss	604	11	3	21	168	0:00:00.109	0:52:42.320
csrss	676	13	12	398	1728	0:00:14.562	0:52:41.133
winlogon	700	13	22	516	7568	0:00:02.718	0:52:40.820
services	744	9	15	272	1956	0:00:04.953	0:52:40.258
lsass	756	9	20	345	3712	0:00:01.515	0:52:40.070
svchost	916	8	16	191	2996	0:00:00.171	0:52:38.758
svchost	1004	8	9	241	1700	0:00:00.406	0:52:38.367
svchost	1120	8	68	1452	13288	0:00:10.078	0:52:38.258
svchost	1172	8	6	80	1216	0:00:00.218	0:52:38.164
svchost	1292	8	14	204	1680	0:00:00.375	0:52:37.383
spoolsv	1476	8	10	129	3596	0:00:00.593	0:52:36.336
inetinfo	1656	8	25	456	5576	0:00:02.843	0:52:29.992
wdfmgr	1744	8	4	65	1488	0:00:00.046	0:52:29.461
UMwareService	1872	13	3	57	976	0:00:03.937	0:52:26.274
winvnc	1936	8	4	80	1148	0:00:00.140	0:52:26.024
alg	588	8	6	102	1124	0:00:00.062	0:52:21.671
explorer	944	8	18	643	20472	0:00:18.062	0:35:27.890
QkRes2k	1460	8	1	19	500	0:00:00.046	0:35:26.875
UMwareTray	1272	8	1	24	716	0:00:00.078	0:35:26.781
UMwareUser	244	8	5	65	1276	0:00:00.625	0:35:26.703
firefox	680	8	10	228	26732	0:00:18.437	0:17:51.984
nc	468	8	1	31	576	0:00:00.046	0:01:54.406
svchost	2044	8	1	31	576	0:00:00.078	0:00:14.437
cmd	900	8	1	31	1944	0:00:00.062	0:00:04.734
pslist	1820	13	2	102	1000	0:00:00.109	0:00:00.140

# Pslist -t

Process information for INTERNALHOST:

Name	Pid	Pri	Thd	Hnd	UM	WS	Priv
Idle	0	0	1	0	0	28	0
System	4	8	52	434	1876	236	0
smss	604	11	3	21	3800	388	168
csrss	676	13	12	396	25844	3988	1728
winlogon	700	13	22	516	52532	3008	7568
services	744	9	15	272	36320	3980	1956
alg	588	8	6	102	32536	3372	1124
svchost	916	8	16	191	60412	4592	2996
svchost	1004	8	9	241	34412	3992	1700
svchost	1120	8	67	1449	133656	22868	13264
svchost	1172	8	6	80	29604	3100	1216
svchost	1292	8	14	204	36776	4280	1680
spoolsv	1476	8	10	129	42416	5584	3596
inetinfo	1656	8	25	456	59008	9276	5576
wdfmgr	1744	8	4	65	14648	1636	1488
UMwareService	1872	13	3	57	28752	2624	976
winvnc	1936	8	4	80	31876	3456	1148
lsass	756	9	20	343	41080	2712	3712
nc	468	8	1	31	18548	1820	576
explorer	944	8	17	634	95852	27824	20340
UMwareUser	244	8	5	60	35780	3584	1276
firefox	680	8	10	228	99192	34536	26696
cmd	900	8	1	31	29924	2368	1944
pslist	1844	13	2	102	28448	2296	1000
UMwareTray	1272	8	1	24	27904	2632	716
QkRes2k	1460	8	1	19	24192	1772	500
svchost	2044	8	1	31	18548	1820	576

# Tasklist

C:\>tasklist /svc

Image Name	PID	Services
System Idle Process	0	N/A
System	4	N/A
smss.exe	604	N/A
csrss.exe	676	N/A
winlogon.exe	700	N/A
services.exe	744	Eventlog, PlugPlay
lsass.exe	756	PolicyAgent, ProtectedStorage, SamSs
suchost.exe	916	DcomLaunch, TermService
suchost.exe	1004	RpcSs
suchost.exe	1120	AudioSrv, Browser, CryptSvc, Dhcp, dmserver, ERSvc, EventSystem, helpsvc, lanmanserver, lanmanworkstation, Netman, Nla, RasMan, Schedule, seclogon, SENS, SharedAccess, ShellHWDetection, TapiSrv, Themes, TrkWks, W32Time, winmgmt, wscsvc, wuauser, WZCSUC
suchost.exe	1172	Dnscache
suchost.exe	1292	LmHosts, RemoteRegistry, SSDPSRV, WebClient
spoolsv.exe	1476	Spooler
inetinfo.exe	1656	IISADMIN, SMTPSVC, W3SVC
wdfmgr.exe	1744	UMWdf
UMwareService.exe	1872	UMTools
winvnc.exe	1936	winvnc
alg.exe	588	ALG
explorer.exe	944	N/A
QkRes2k.exe	1460	N/A
UMwareTray.exe	1272	N/A
UMwareUser.exe	244	N/A
firefox.exe	680	N/A
nc.exe	468	N/A
suchost.exe	2044	N/A
cmd.exe	900	N/A
tasklist.exe	1164	N/A
wmiprvse.exe	1724	N/A

# Process Memory Dumps (cont)

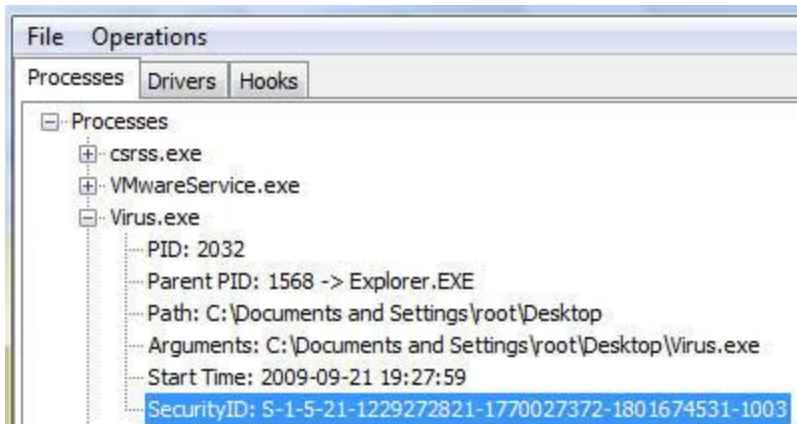
- ▶ Process dissection
  - *Process explorer*

Process	PID	CPU	Description	Company Name
System Idle Process	0	96.97		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4			
smss.exe	604		Windows NT Session Mana...	Microsoft Corporation
csrss.exe	676		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	700		Windows NT Logon Applicat...	Microsoft Corporation
services.exe	744	1.52	Services and Controller app	Microsoft Corporation
svchost.exe	916		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1004		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1120		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1172		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1292		Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	1476		Spooler SubSystem App	Microsoft Corporation
inetinfo.exe	1656		Internet Information Services	Microsoft Corporation
wdfmgr.exe	1744		Windows User Mode Driver ...	Microsoft Corporation
VMwareServic...	1872		VMware Tools Service	VMware, Inc.
winvnc.exe	1936		VNC server for Win32	UltraVNC
alg.exe	588		Application Layer Gateway S...	Microsoft Corporation
userdump.exe	1444		User Dump Service/Comma...	Microsoft Corporation
lsass.exe	756		LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	944		Windows Explorer	Microsoft Corporation
QkRes2k.exe	1460			
VMwareTray.exe	1272		VMware Tools tray application	VMware, Inc.
VMwareUser.exe	244		VMware Tools Service	VMware, Inc.
firefox.exe	680		Firefox	Mozilla Corporation
notepad.exe	1088		Notepad	Microsoft Corporation
cmd.exe	532		Windows Command Processor	Microsoft Corporation
procexp.exe	976	1.52	Sysinternals Process Explorer	Sysinternals - www.sysinter..
nc.exe	468			
svchost.exe	2044			

# Sophisticated Malware

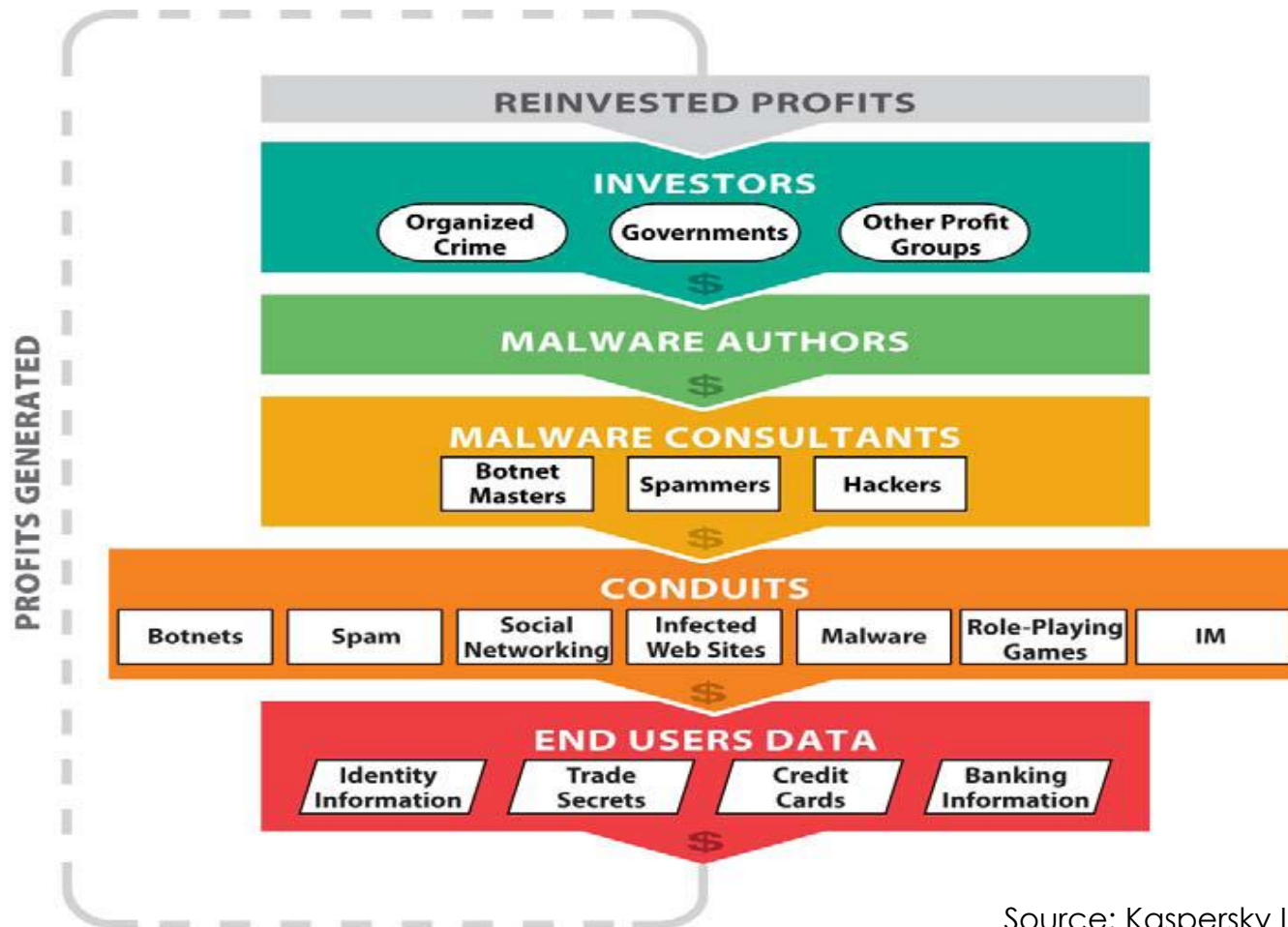
- ▶ None of the previous tools will work in most cases
- ▶ Perpetrators write their tools to avoid these
- ▶ Have to analyze the raw image
- ▶ Can do manually
- ▶ Tools work the best

# Sophisticated Malware (cont)



Processes Drivers Hooks			
System Service Descriptor Table Hooks		Interrupt Descriptor Table Hooks	Driver IRP Hooks
HookedFun...	HookedM...	HookingModule	HookingAddress
NtEnumerat...	ntoskrnl.exe	\\??C:\WINDOWS\hide_evr2.sys	0xf8c46608
NtFreeVirtu...	ntoskrnl.exe	\\??C:\FLYPAPER.sys	0xf6bc0bf0
NtQueryDire...	ntoskrnl.exe	\\??C:\WINDOWS\hide_evr2.sys	0xf8c46734
NtQuerySys...	ntoskrnl.exe	\\??C:\WINDOWS\hide_evr2.sys	0xf8c468da
0x101	ntoskrnl.exe	\\??C:\FLYPAPER.sys	0xf6bc0db0
0x102	ntoskrnl.exe	\\??C:\FLYPAPER.sys	0xf6bc0cb0
0x115	ntoskrnl.exe	\\??C:\FLYPAPER.sys	0xf6bc0b30

# Malware Ecosystem



Source: Kaspersky Lab US

# Help!

- ▶ Enhanced Mitigation Experience Toolkit
  - Microsoft tool
    - DEP and others => adds obstacles to exploitation
  - Permanent protection against targeted applications
    - Adobe etc
- ▶ All 2013 IE exploits stopped by version 3.0  
=> at version 5 now

# EMET

## System Settings

Mitigation	XP	Server 2003	Vista	Server 2008	Win7	Server 2008 R2
DEP	Y	Y	Y	Y	Y	Y
SEHOP	N	N	Y	Y	Y	Y
ASLR	N	N	Y	Y	Y	Y

## Application Settings

DEP	Y	Y	Y	Y	Y	Y
SEHOP	Y	Y	Y	Y	Y	Y
NULL Page	Y	Y	Y	Y	Y	Y
Heap Spray	Y	Y	Y	Y	Y	Y
Mandatory ASLR	N	N	Y	Y	Y	Y
EAF	Y	Y	Y	Y	Y	Y
Bottom-up	Y	Y	Y	Y	Y	Y

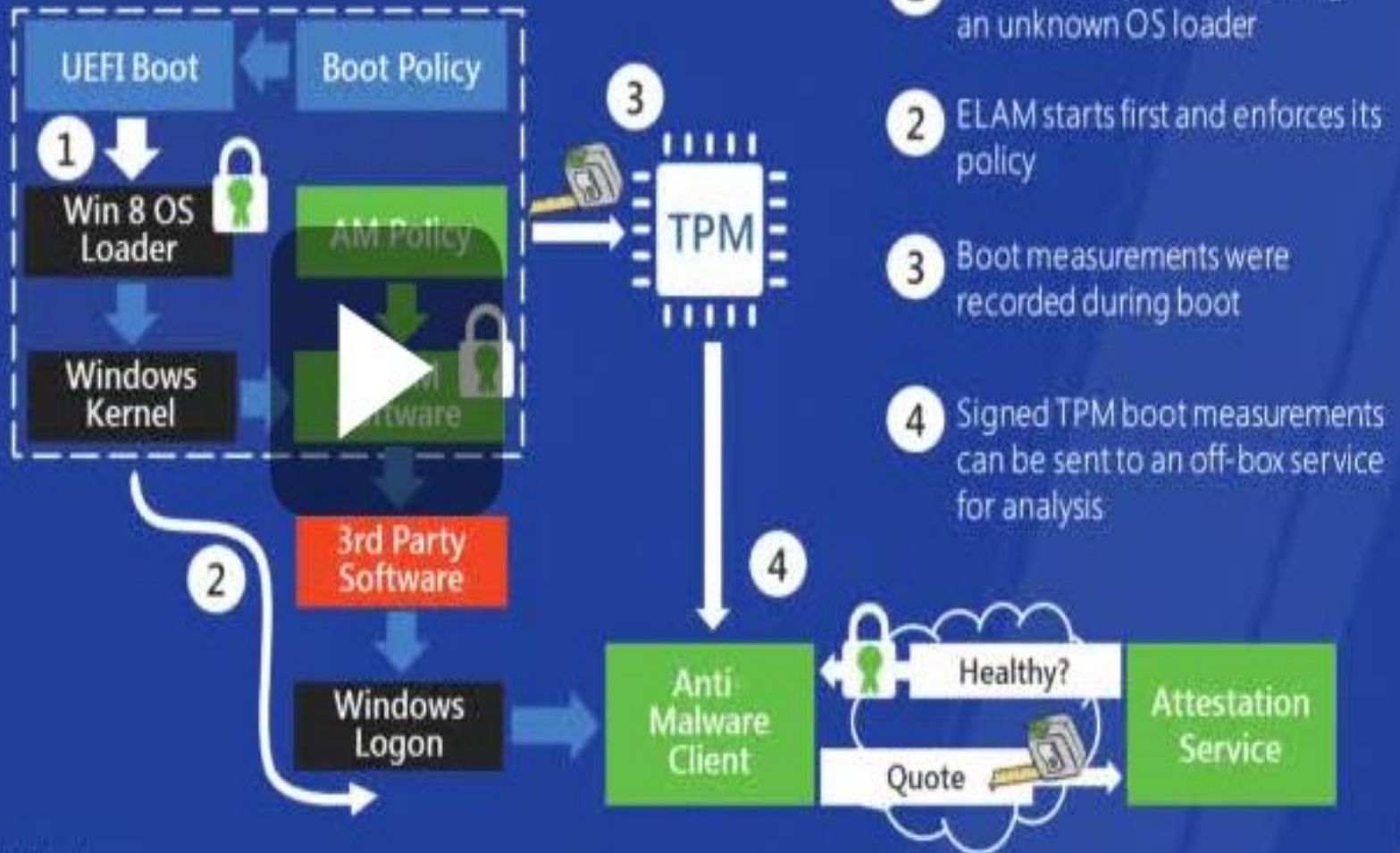
# Server 2008 Components

- ▶ Network Access Protection
  - Restrict access based on client health
- ▶ Public Key Infrastructure
  - Bind user identity to a public key
    - Trace origin of ownership
  - Distributed trust hierarchies
- ▶ RODC
  - Read Only Domain Controllers
- ▶ Software restriction policies
  - Can allow or block based on hash, name, signature or origin

# Server 2012

- ▶ Secure boot
  - Taken from Windows 8
  - Hardware protection capable
- ▶ DNSSEC
  - Robust and improved from Server 2008
- ▶ Data classification built-in
- ▶ ServerCore
  - Can optionally load GUI and unload it

# Secured boot architecture



www.buildwindows.com

Source: [www.buildwindows.com](http://www.buildwindows.com)

# Secure Device Identity

*802.1AR*

## **802.1AR - Secure Device Identity**

It is desirable to authenticate entities attached to a network in a secure fashion; e.g., by means of the mechanisms defined in IEEE Std 802.1X. A standardized device identity facilitates interoperable secure device authentication. User organizations have identified this as a desirable capability to simplify and standardize security management in their networks. The IETF has identified DevID or an equivalent capability as an enabling component of a solution to security issues in several of their protocols, e.g. ARP. DevID is specifically conceived to address this need. This standard will be of benefit to manufacturers of conformant LAN equipment, their customers, and users of LANs or LAN services that are based on such equipment.

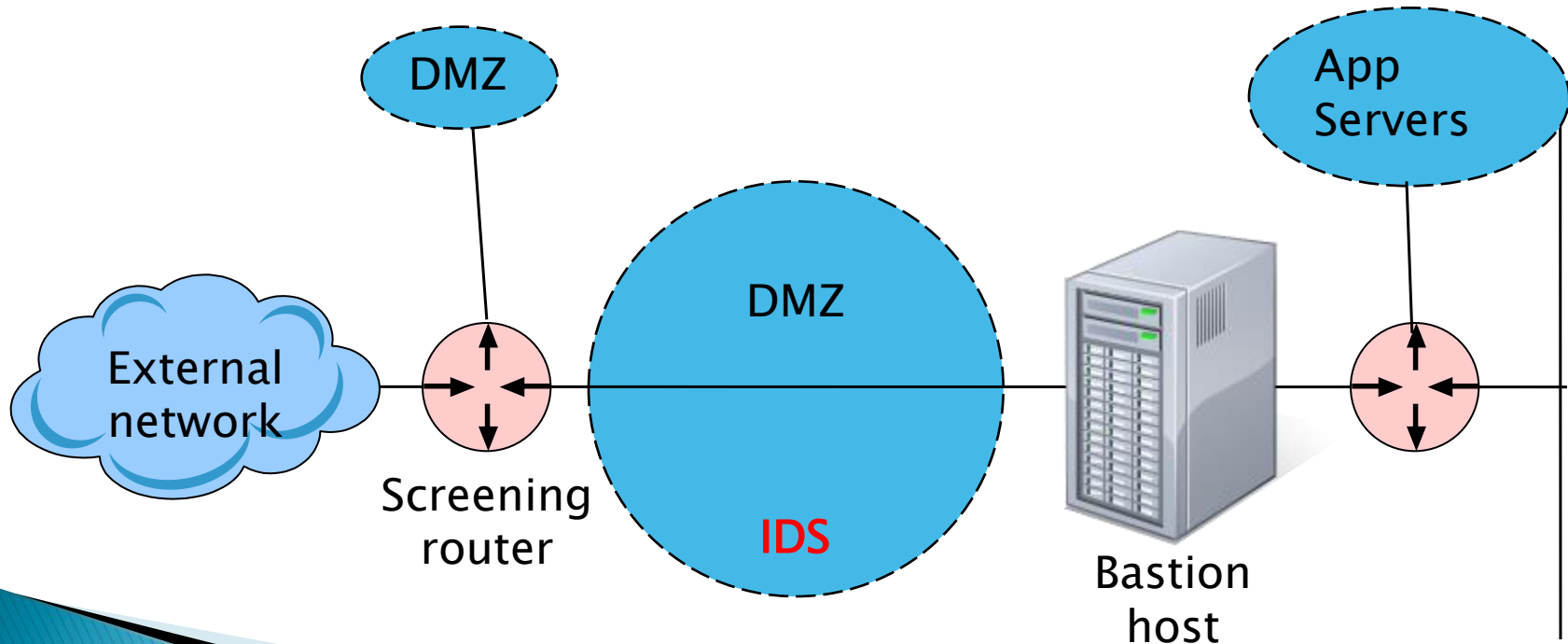
- ▶ **Standard as of 2009**
  - Assigns a DevID to a device
    - Hardware based
      - TPM?

# Phones


- ▶ Attacks are on the rise
- ▶ MTPM
  - Expected release ?
    - Was in 2012
  - Provides hardware based protection of phones
    - Device identity
  - Similar to the TPM
    - Optimized for mobile platform
  - Apple?
    - Did not participate
      - Proprietary solution – ?????

# Secure Network Architectures

- ▶ Segmentation and isolation
- ▶ Bind ports inside the bastion host



# Bastion Host Ingress



Express 3.0

Control About Services **Networking** VPN Logs Tools Maintenance

shutdown | help ?

incoming outgoing internal external access ip block timed access qos advanced ppp interfaces

Forward ports from your external IP address to ports on machines inside your local networks.

**Add a new rule:**

Protocol: TCP

External source IP (or network):

Source port or range: User defined

Port:

Destination IP:

Destination port: User defined

Port: \*

Comment:

Enabled: ☒

Add


\* If blank, then the source port will be used as the destination port.


**Current rules:**

Protocol <input checked="" type="checkbox"/>	External source IP	Source port	Destination IP	Destination port	Enabled	Mark
Comment						

Remove Edit

# Bastion Host Egress



Express 

Control About Services **Networking** VPN Logs Tools Maintenance

shutdown | help

incomingoutgoing**internal**external accessip blocktimed accessqosadvancedpppinterfaces

Add rules to control local machine's access to external services.

Interface defaults:

Traffic originating on GREEN is: 

Blocked with exceptions

Save

Add exception:

Interface: 

GREEN

Application or service(s): 

User defined







 Port:

Comment:

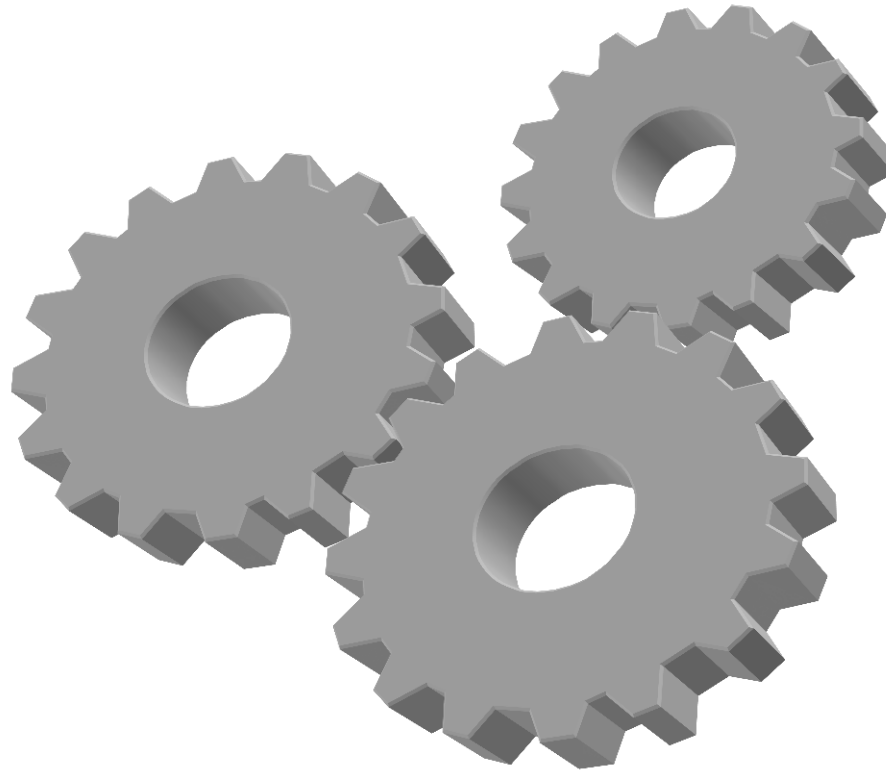
Enabled: ☒

Add

Current exceptions:

Interface 	Application or service(s) Comment	Enabled	Mark
GREEN	Web		<input type="checkbox"/>
GREEN	File transfer		<input type="checkbox"/>
GREEN	Email and News		<input type="checkbox"/>
GREEN	Instant Messaging		<input type="checkbox"/>
GREEN	Multimedia		<input type="checkbox"/>

# Demo: Windows Firewall

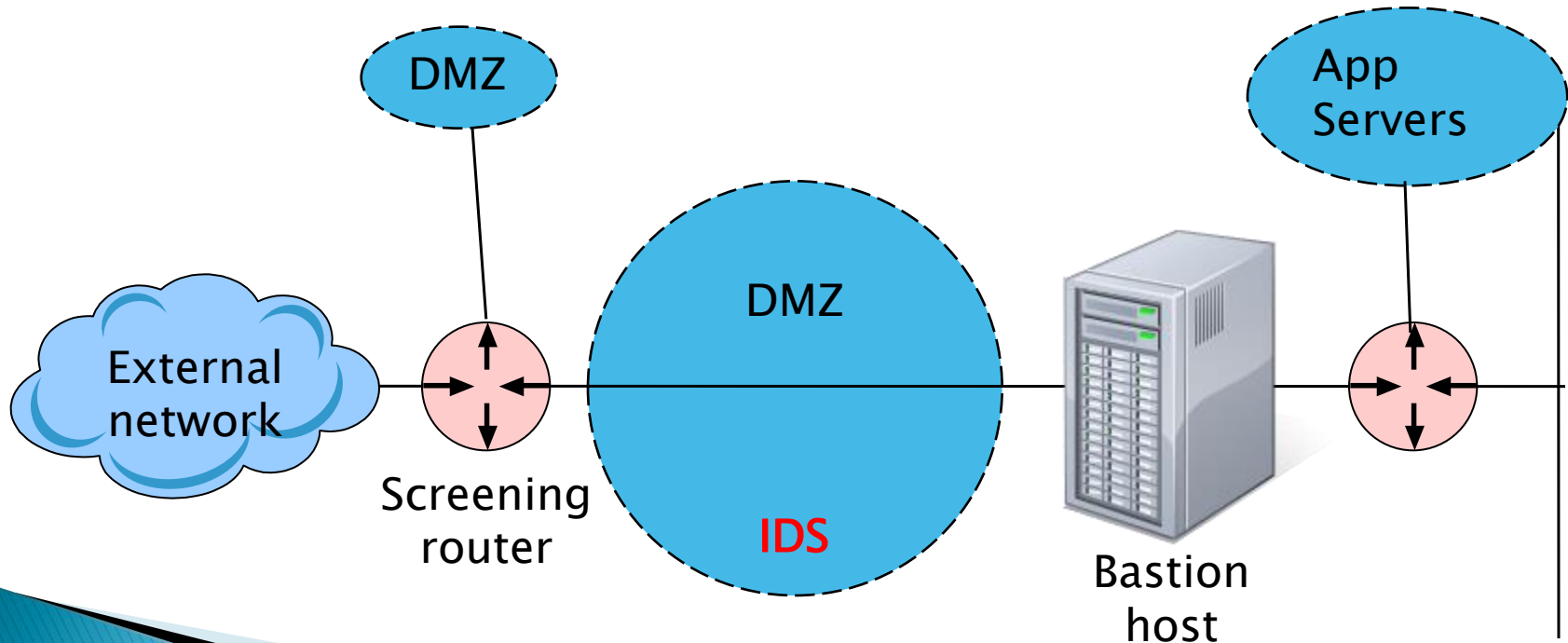


# Closing

- ▶ Case Study – 2012 Olympics
- ▶ Blackhole or Sinkhole routing
- ▶ Internal Honeypots!

# Secure Network Architectures

- Segmentation and isolation



# Thank You

- ▶ We can defend!
- ▶ [cesi@ieee.org](mailto:cesi@ieee.org)