ENTS 650: Network Security

Malware presented by:

Tom McManuels
Sumita Jonak
Zach Davis

Introduction to Malware

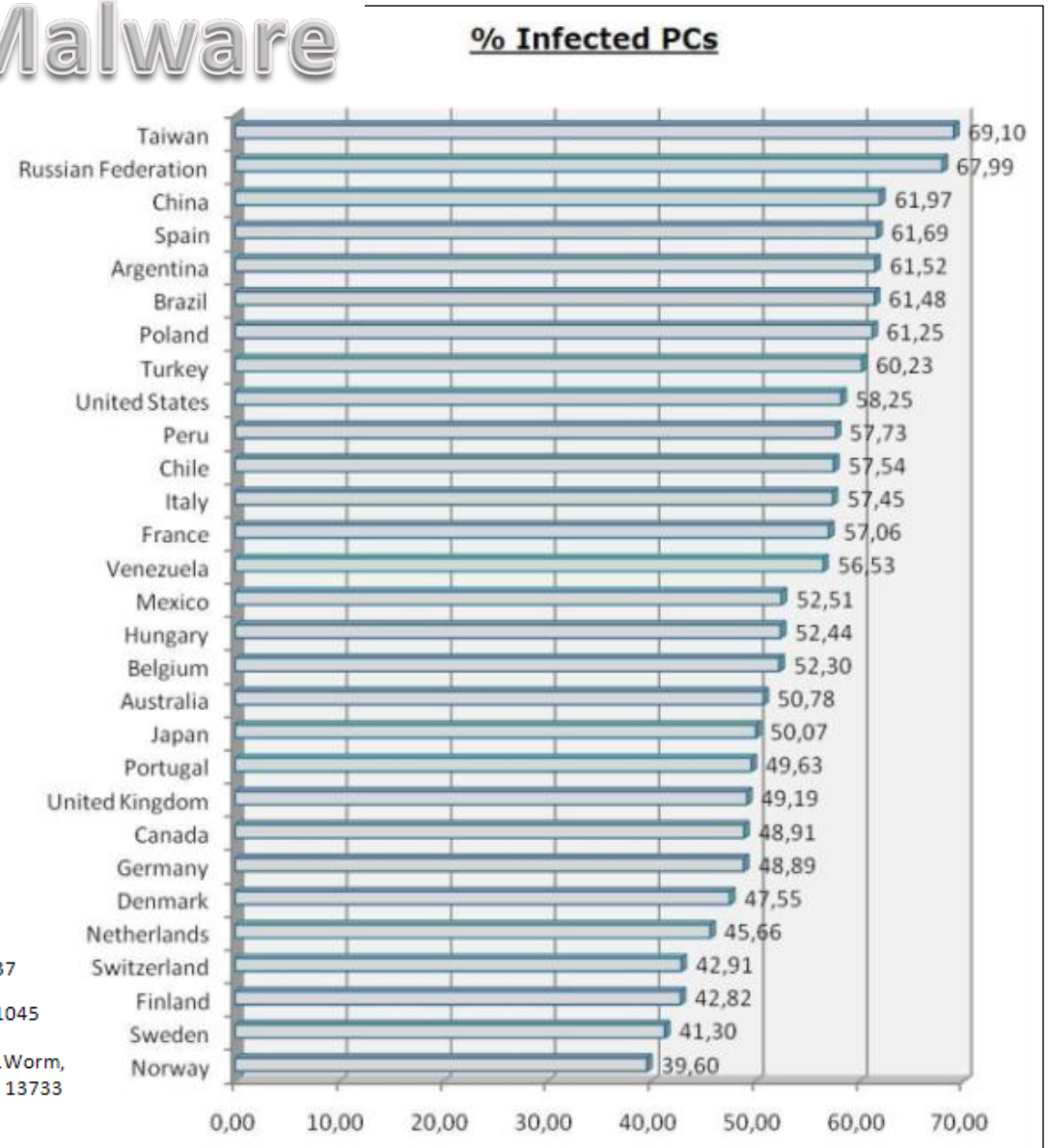
- Malicious software = Malware

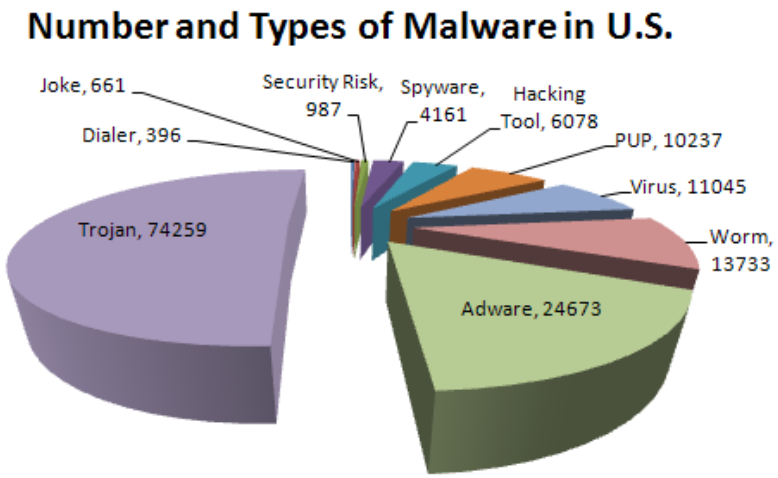
- Definition: software intended to damage a computer, computer system, or computer network, or to take partial control over its operation without the user's knowledge or consent

- Types of Malware:
  - Viruses
  - Worms
  - Trojan horses
  - Spyware
  - Any malicious/unwanted software

Introduction to Malware

- **2009 data reveals:**
  - **Trojans are biggest threat for US users**
  - **Taiwan/Russia/China have the highest infection rates**





Case Study 1: ILOVEYOU

- Early worm infection – most costly at the time
- Visual Basic Scripting (.VBS) – required user to run
- Used social engineering to entice user to run the script
  - Sent as attachment to email with subject “ILOVEYOU” or “IWANTYOU”
  - Message body reads “kindly check the attached LOVELETTER coming from me”
  - Attachment named “LOVE-LETTER-FOR-YOU.TXT.VBS”
  - By Windows defaults, .VBS extension hidden – looks like harmless text file to unaware user
  - File name and subject, coming from known sender, designed to trick user into opening and running attachment

Case Study 1: ILOVEYOU

Capabilities

- On execution, worm searches for files with many common extensions (for example, *.JPG, *.JPEG, *.VBS, *.VBE, *.JS, *.JSE, *.CSS, *.WSH, *.SCT, *.DOC, and *.HTA), overwrites the files with the worm, and adds a .VBS extension (hidden by default)
- Also hides *.MP2 and *.MP3 files and makes a copy of itself with the same filename with .VBS appended
- Sends itself to entries in Microsoft Address Book
- Adds registry keys that download and execute password-stealing trojan.
- Only infects Windows systems

Case Study 1: ILOVEYOU

Timeline and Effects

- May 4, 2000: Originated in Philippines. Spread to Hong Kong, then to Europe and USA in one day.
- May 8, 2000: CERT received reports of ~500K individual infected systems.
- By May 13, 2000, up to 50 million reported infections.
- Estimated $5.5B in damage – mostly from time and effort to clean systems
  - Numerous large organizations shut down mail systems to halt the spread
- Prevention:
  - Common sense: Don't open attachments if you don't know what they are.
  - Virus scanning software now detects this worm.

Case Study 2: ZEUS

ZEUS (aka ZBOT)

- Trojan and/or “bot” software
  - Name can also be used to refer to the more general toolkit for creating, distributing, and administering the botnet
- Once installed on a host, used to steal banking and other information via keystroke logging, form grabbing, custom form injection, and screenshot collection
- Bot can be controlled by an external server, which it can “phone home” for commands
- Injects code into winlogon.exe or explorer.exe, and from there into svchost.exe
- Distributed via phishing or other spam emails, and by drive-by downloads

Case Study 2: ZEUS

Capabilities

- Steal data from HTTP forms
- Steal account credentials from Windows Protected Storage
- Steal client-side X.509 certificates
- Steal POP and FTP account credentials
- Delete or steal cookies
- Modify HTML code of target sites in order to steal information
- Redirect from desired web pages to attacker-controlled sites
- Collect screen captures
- Upload files from the infected computer
- Modify local hosts file
- Download and execute arbitrary programs
- Delete registry keys, possibly entirely disabling Windows boot

Case Study 2: ZEUS

Email distribution

- Sample phishing attempt impersonating the FDIC:

From: FDIC
Date: [Header Details Removed]
To: [Header Details Removed]
Subject: FDIC alert: check your Bank Deposit Insurance Coverage

You have received this message because you are a holder of a FDIC-insured bank account.
Recently FDIC has officially named the bank you have opened your account with as a failed bank, thus, taking control of its assets.

You need to visit the official FDIC website and perform the following steps to check your Deposit Insurance Coverage:

- Visit FDIC website:
  http://www.fdic.gov/bankinsured/failed/personalfile/holder.php?email=[redacted]@[redacted]-[redacted]&id=36973428927474111305956910469273012541265 2
- Download and open your personal FDIC Insurance File to check your Deposit Insurance Coverage

FDIC Federal Deposit Insurance Corporation

- Other attempts have impersonated the IRS, social networking sites, and Microsoft

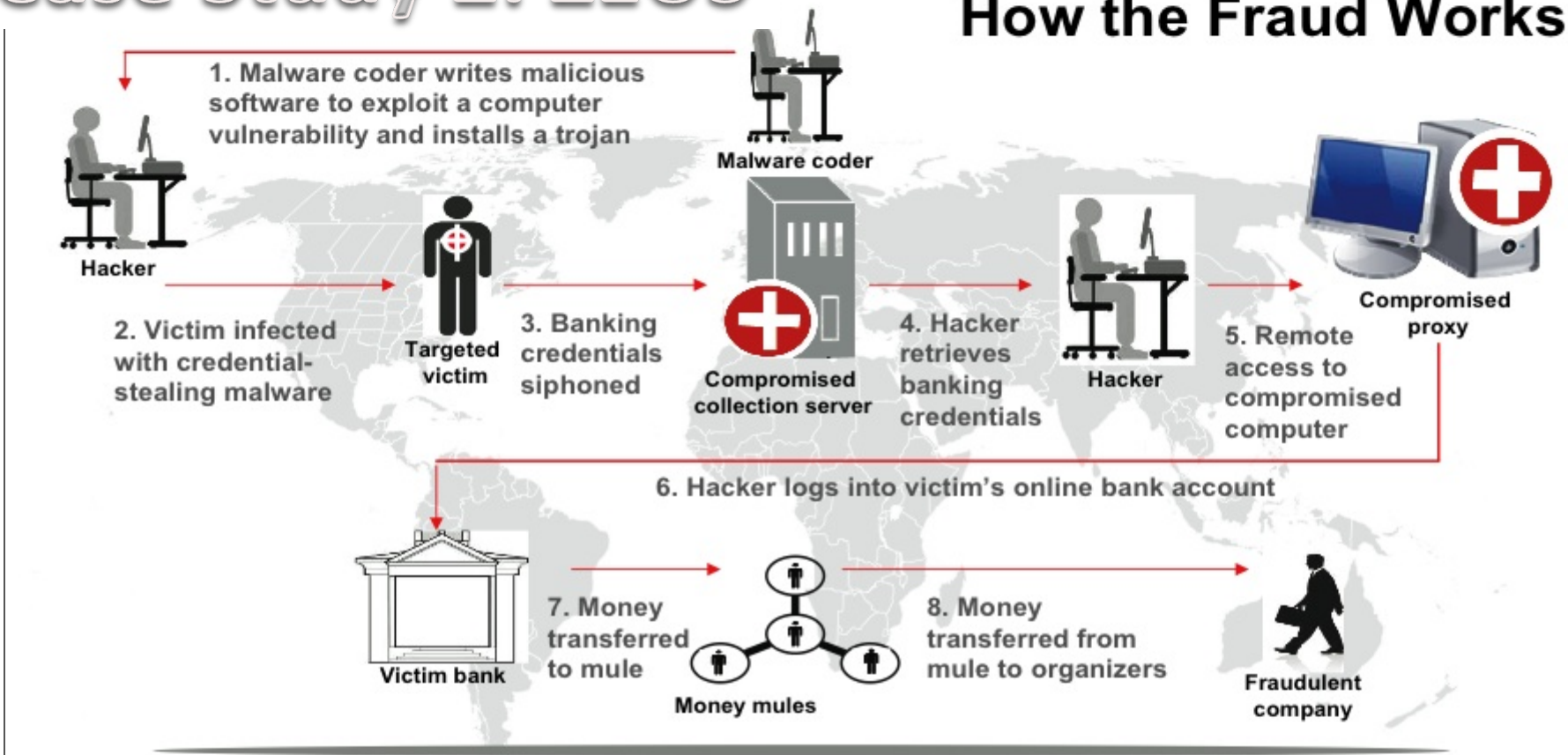
Case Study 2: ZEUS

Timeline

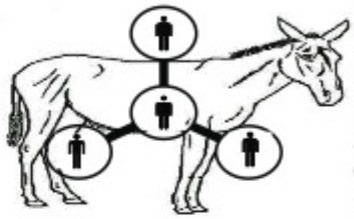
- July 2007: First identified when used to steal information from US Department of Transportation. Likely originated in Russia (based on early documentation)
- June 2009: Discovered to have compromised ~75K accounts on websites of major corporations
- October-November 2009: ~9M phishing emails sent
- July 2010: Kneber outbreak (similar/same tools). Report of compromise of credit cards of 15 US banks
- October 2010: FBI announces discovery of international cyber-crime network that used Zeus to steal ~$70M. Over 90 arrests made

Case Study 2: ZEUS

How the Fraud Works



Victims are both financial institutions and owners of infected machines.



Money mules transfer stolen money for criminals, shaving a small percentage for themselves.

Criminals come in many forms:

- Malware coder
- Malware exploiters
- Mule organization

Case Study 2: ZEUS

Distribution

- Toolkit available for sale in criminal underground
  - Reported prices range from $700 to $4K (with additional capabilities for additional fees)
- Tools allow control of the botnet and building and distribution of the individual bots to target computers
- Each build of the bot creates its own binary file (polymorphic) making it difficult for virus detection software to find it
- Only operable on Windows XP systems, although newer versions added Windows 7 and Vista support
- Botnet currently estimated to include ~3.6M compromised computers

Case Study 2: ZEUS

Detection and Avoidance

- Due to polymorphic nature, difficult for antivirus systems to detect and/or prevent
- Follow best practices:
  - Do not click on unknown or suspicious links in emails or on the web
  - Keep antivirus software updated
- Use different platforms for secure transactions from those used for routine browsing (not always feasible)
- Use non-Windows systems for guaranteed resistance to Zeus (not always feasible)

Case Study 3: Conficker

- Exploits a NetBIOS vulnerability in various Windows operating systems
- Downloads a copy of itself as a random DLL
- All variants try to patch the infected system to prevent re-exploitation
- Starts on system boot through registry manipulation
- Spreads

Case Study 3: Conficker

Agenda

- Timeline
- Conficker variants
- Delivery method(s)
- Domain name generation
- Threat assessment
- Technical assessment
- Detection and remediation

Case Study 3: Conficker

Conficker Timeline

October 23, 2008: Conficker exploit vector patched by Microsoft

November 21, 2008: First detection

December 29, 2008: Second variant, Conficker.B, detected

January 2009: 9 – 15 million infection rate

February 12, 2009: Industry goes on the offensive

February 13, 2009: $250,000 reward

February 20, 2009: Third variant, Conficker.C, detected

April 2009: Conficker.A update defeated

Case Study 3: Conficker

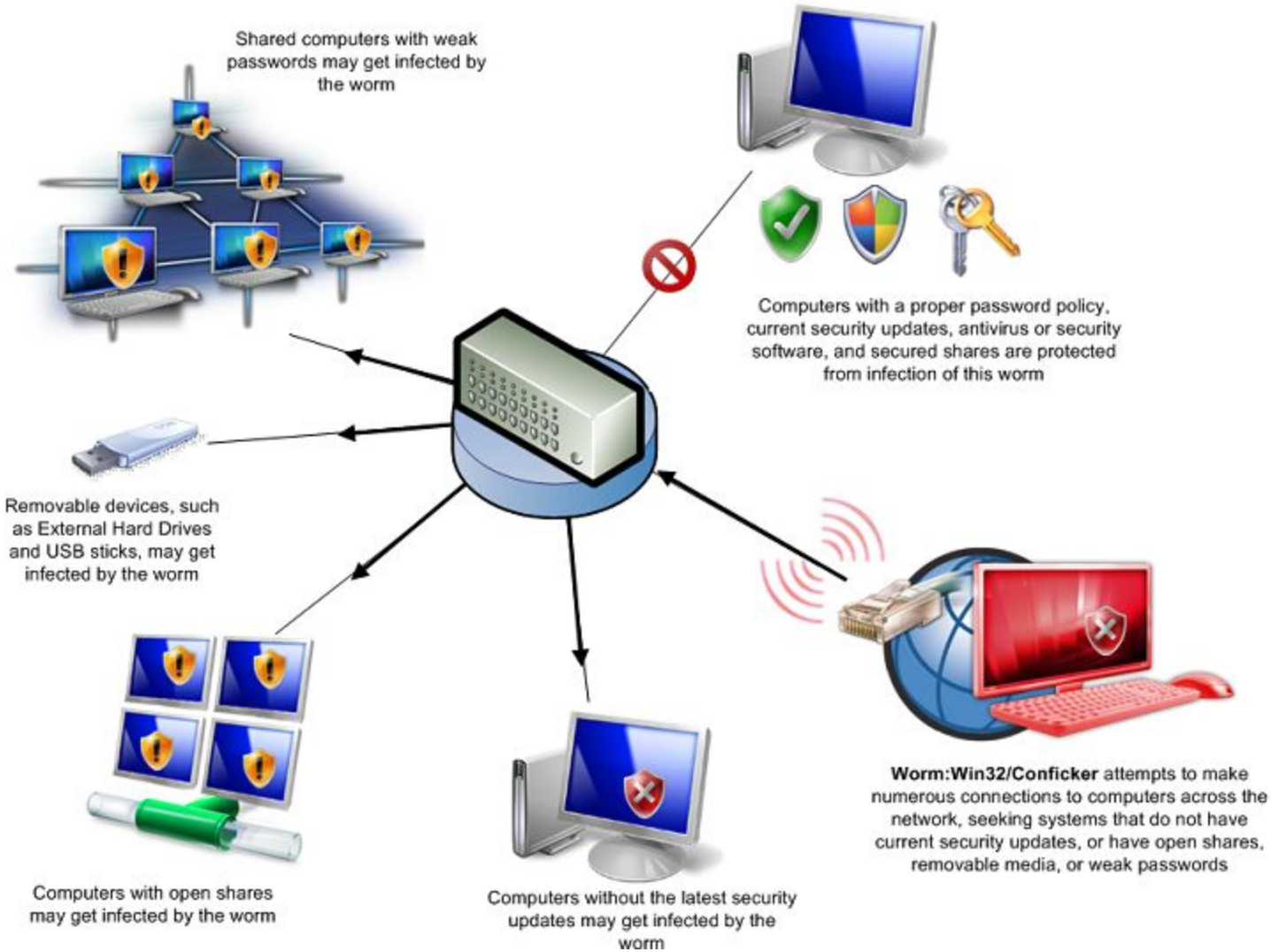
Delivery

- Randomly named Dynamic Link Library (DLL)
- Exploit vector is the MS08-067 vulnerability
- Injected into the running Windows server service
- Delivery via malformed RPC requests to vulnerable computers
- Delivery via the rundll32.exe application on USB drives or network shares
- Remote updates (pull)

MS08-67 is a critical vulnerability in the Windows Server Service on Windows 2008/Vista/2003/XP/2000 computers, which allows hackers to gain remote control of the affected computer with the same privileges as the logged user.

Case Study 3: Conficker

Delivery

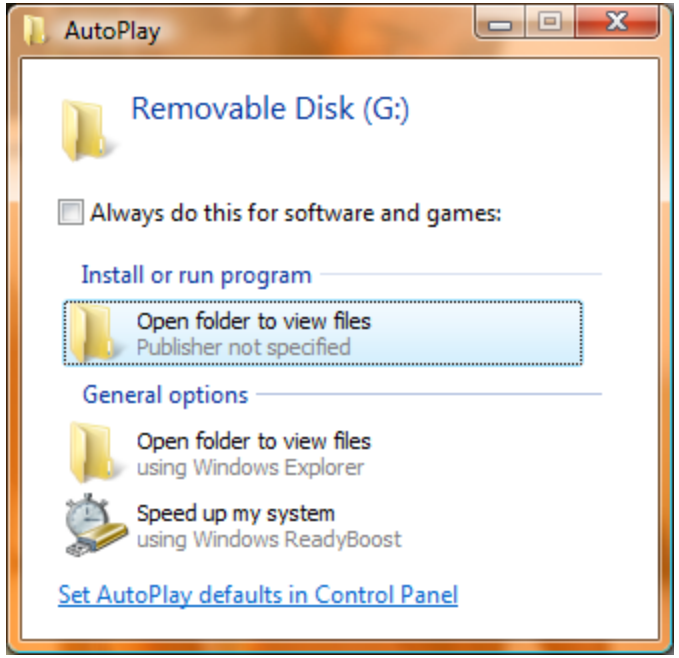


Case Study 3: Conficker

Delivery – rundll32.exe Vector

Infected autorun.inf file contains (cleaned up):

```
Action=Open folder to view files
Icon=%systemroot%\system32\shell32.dll,4
Shellexecute=.\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\jwgkvsq.vmx,ahaezedrn
```



"Install or run program" present because OS detected the autorun.inf file containing the shellexecute keyword.

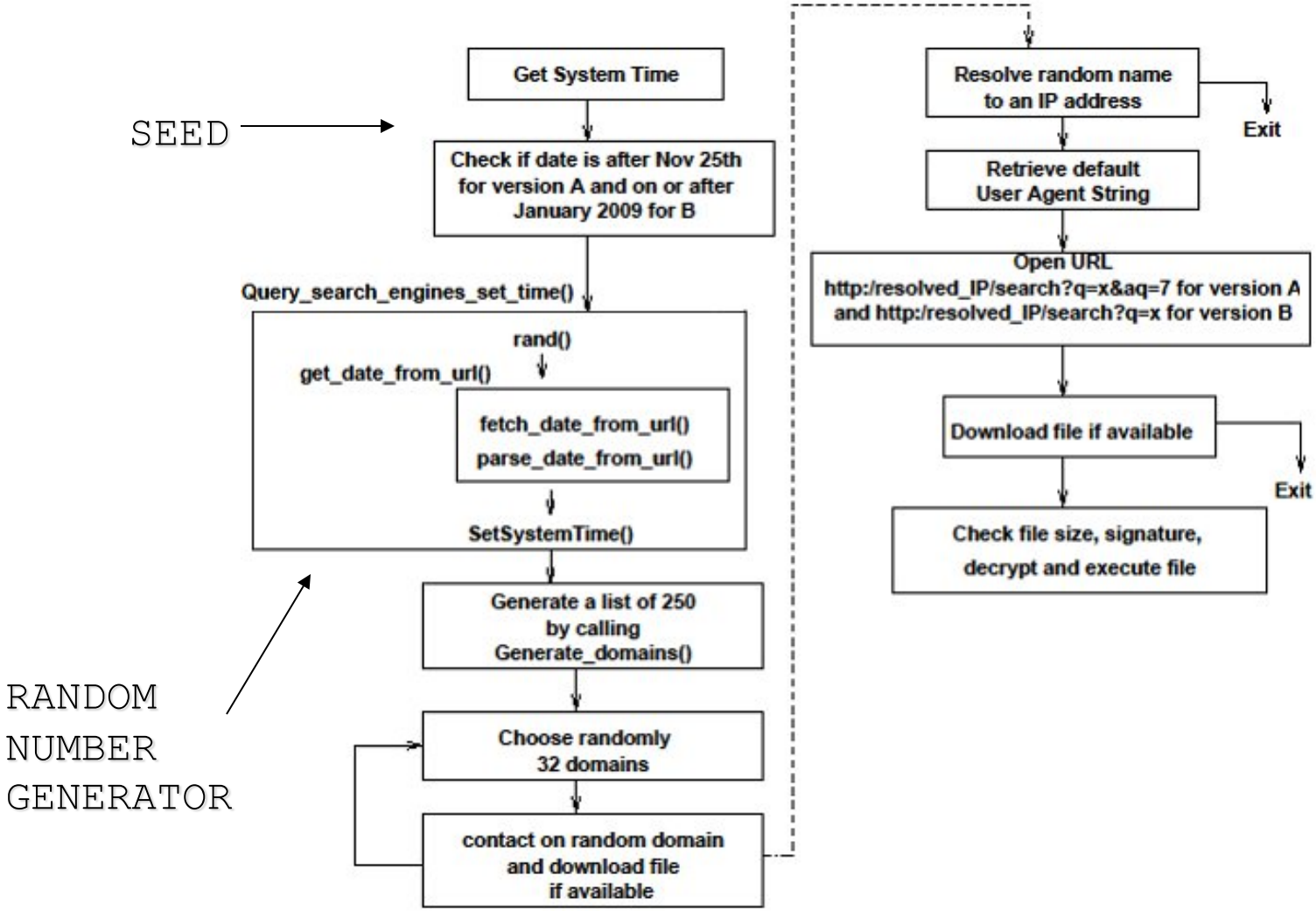
Case Study 3: Conficker

Delivery – Payload Update Vector

- Internet rendezvous points
- Effective updating service
- Highly mobile, location recomputed daily
- Authentication (secure hashing and RSA signature)

Case Study 3: Conficker

Delivery – Remote Update Vector



Case Study 3: Conficker

Conficker Variants

Variant	Detection Date	Exploit Vector	Update Method / Command and Control	Defense
Conficker.A	21-Nov-08	MS08-067 vulnerability Dictionary attack on Admin shares	*trafficconverter.biz (pull)* 250 pseudorandom domains (pull)	None
Conficker.B	29-Dec-08	MS08-067 vulnerability DLL Autorun trojan Dictionary attack on Admin shares	250 pseudorandom domains (pull) NetBIOS (push)	Block certain DNS lookup Disable autoupdate
Conficker.C	20-Feb-09	MS08-067 vulnerability Dictionary attack on Admin shares DLL Autorun trojan	250 pseudorandom domains (pull) NetBIOS (push)	Block certain DNS lookup Disable autoupdate
Conficker.D	4-Mar-09		50,000 pseudorandom domains (pull) P2P (push/pull)	Block certain DNS lookup Disable autoupdate Disable safemode Kills anti-malware
Conficker.E	7-Apr-09	MS08-067 vulnerability	NetBIOS (push) P2P (push/pull)	Block certain DNS lookup Disable autoupdate Kills anti-malware

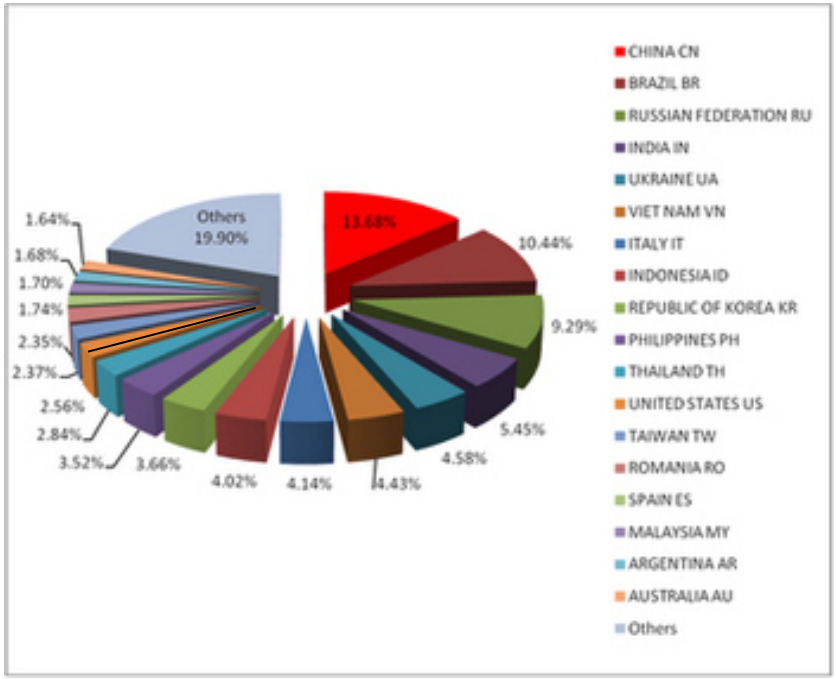
Case Study 3: Conficker

Warning Shot?

- January 2009: 8.9 million infected PC's
- April 2009: 3 million infected on a given day, 15 million total

- Multiple reports of pre-emptive network disruptions
- April Fools "threat" on April 1, 2009
- Varient E (Waledac and SpyProtect 2009)

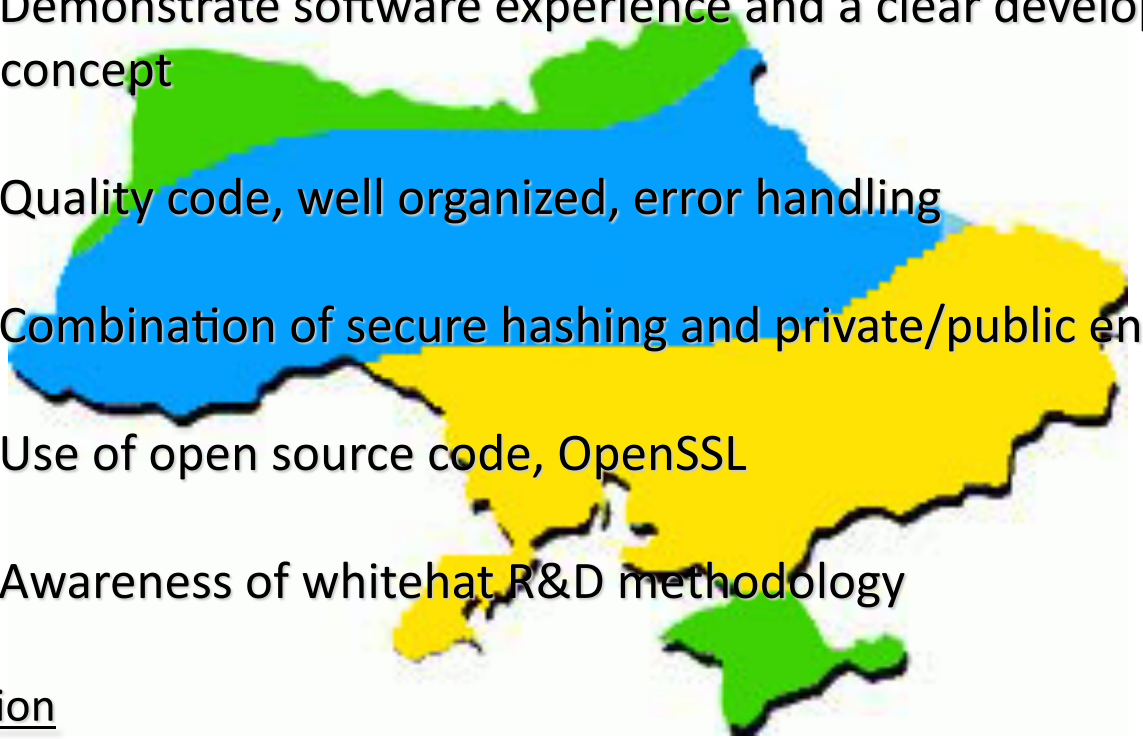
- 2010 Article: *"Effectively, nothing has happened to these (infected) machines," Weafer said. "But that doesn't mean it won't happen...it's still a significant botnet (network of infected bots) sitting out there."*



Case Study 3: Conficker

Technical Assessment

- Developed in a professional manner
- Demonstrate software experience and a clear development concept
- Quality code, well organized, error handling
- Combination of secure hashing and private/public encryption
- Use of open source code, OpenSSL
- Awareness of whitehat R&D methodology



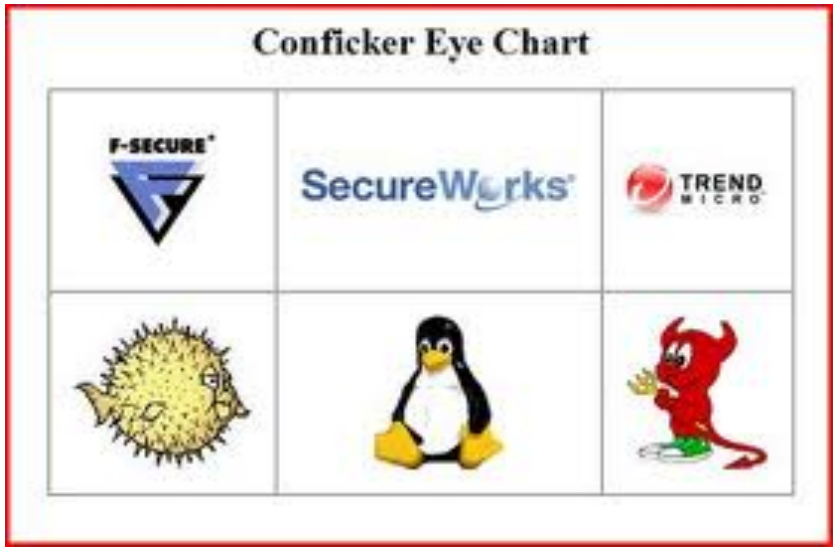
Attribution

- Working group members stated at the 2009 Black Hat conference that Ukraine is the probable origin of the virus, but declined to provide specific details.

Case Study 3: Conficker

Detection and remediation

- Enumerate by registering domains and sinkhole update requests
- Microsoft allows pirate and genuine Windows users to download critical security patches, but most pirate users have automatic update turned off
- Published removal guides
- Up to date antivirus signatures
- Disable AutoRun on removable media



Case Study 4: Stuxnet

- Highly specialized worm for Siemens Supervisory Control And Data Acquisition (SCADA) systems
- Windows computer worm discovered in July 2010
- Targets industrial software/equipment
- First worm to include a Programmable Logic Controller (PLC) rootkit
- 60% of infected computers were in Iran (Symantec, August 2010)
- Self-activated/targeted worm only against certain equipment

Case Study 4: Stuxnet

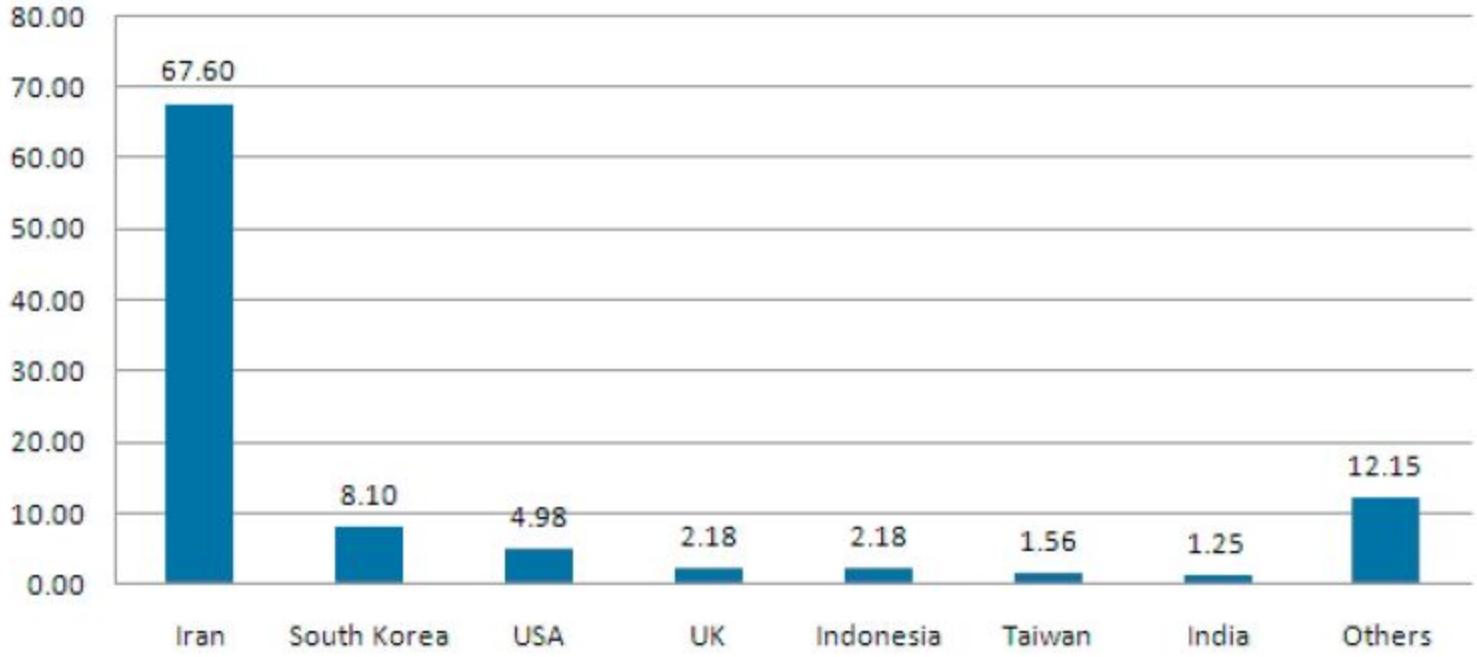
W32.Stuxnet Timeline

Date	Event
November 20, 2008	Trojan.Zlob variant found to be using the LNK vulnerability only later identified in Stuxnet.
April, 2009	Security magazine Hakin9 releases details of a remote code execution vulnerability in the Printer Spooler service. Later identified as MS10-061.
June, 2009	Earliest Stuxnet sample seen. Does not exploit MS10-046. Does not have signed driver files.
January 25, 2010	Stuxnet driver signed with a valid certificate belonging to Realtek Semiconductor Corps.
March, 2010	First Stuxnet variant to exploit MS10-046.
June 17, 2010	Virusblokada reports W32.Stuxnet (named RootkitTmphider). Reports that it's using a vulnerability in the processing of shortcuts/.lnk files in order to propagate (later identified as MS10-046).
July 13, 2010	Symantec adds detection as W32.Temphid (previously detected as Trojan Horse).
July 16, 2010	Microsoft issues Security Advisory for "Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)" that covers the vulnerability in processing shortcuts/.lnk files. Verisign revokes Realtek Semiconductor Corps certificate.
July 17, 2010	Eset identifies a new Stuxnet driver, this time signed with a certificate from JMicron Technology Corp.
July 19, 2010	Siemens report that they are investigating reports of malware infecting Siemens WinCC SCADA systems. Symantec renames detection to W32.Stuxnet.
July 20, 2010	Symantec monitors the Stuxnet Command and Control traffic.
July 22, 2010	Verisign revokes the JMicron Technology Corps certificate.
August 2, 2010	Microsoft issues MS10-046, which patches the Windows Shell shortcut vulnerability.
August 6, 2010	Symantec reports how Stuxnet can inject and hide code on a PLC affecting industrial control systems.
September 14, 2010	Microsoft releases MS10-061 to patch the Printer Spooler Vulnerability identified by Symantec in August. Microsoft report two other privilege escalation vulnerabilities identified by Symantec in August.
September 30, 2010	Symantec presents at Virus Bulletin and releases comprehensive analysis of Stuxnet.

Case Study 4: Stuxnet

Figure 4

Percentage of Stuxnet infected Hosts with Siemens Software installed



"Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?"

If an attacker succeeded in introducing Stuxnet in early or mid-2009 into vulnerable Iranian personal computers connected to the internet, the malware could have taken months to arrive at the Natanz centrifuge control systems. Because the Natanz control systems are not connected to the internet, Stuxnet would have needed to travel on a removable drive from an infected computer to the Natanz control system.

-ISIS, DEC2010

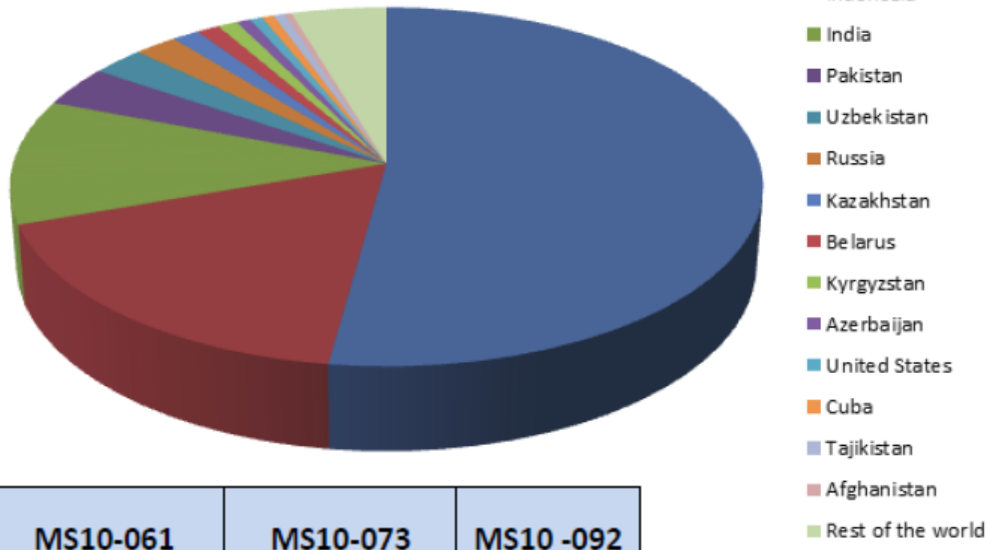
Case Study 4: Stuxnet

"Stuxnet is a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or power plant. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries. Stuxnet was discovered in July 2010, but is confirmed to have existed at least one year prior and likely even before. The majority of infections were found in Iran." – Symantec, FEB2011

Characteristics	Stuxnet
Target	Sites using SCADA systems but promiscuous dissemination
Multiple distribution vectors	yes
Payload	all in one malware
Code packing	yes
Code obfuscation	yes
Anti-AV functionality	yes
Masking under legal programs	yes
Architecture of malicious program	modular
Establishing a backdoor	no
Distributed C&C	no
Communications protocol	http
Custom encryption of communications protocol	yes
Modules with a legal digital signature	yes
Update mechanism	yes; downloads updates via WinAPI functions and runs them in memory, without creating any files
Uninstall mechanism	yes
Infection counter	yes
Availability of any modifications malicious program	yes

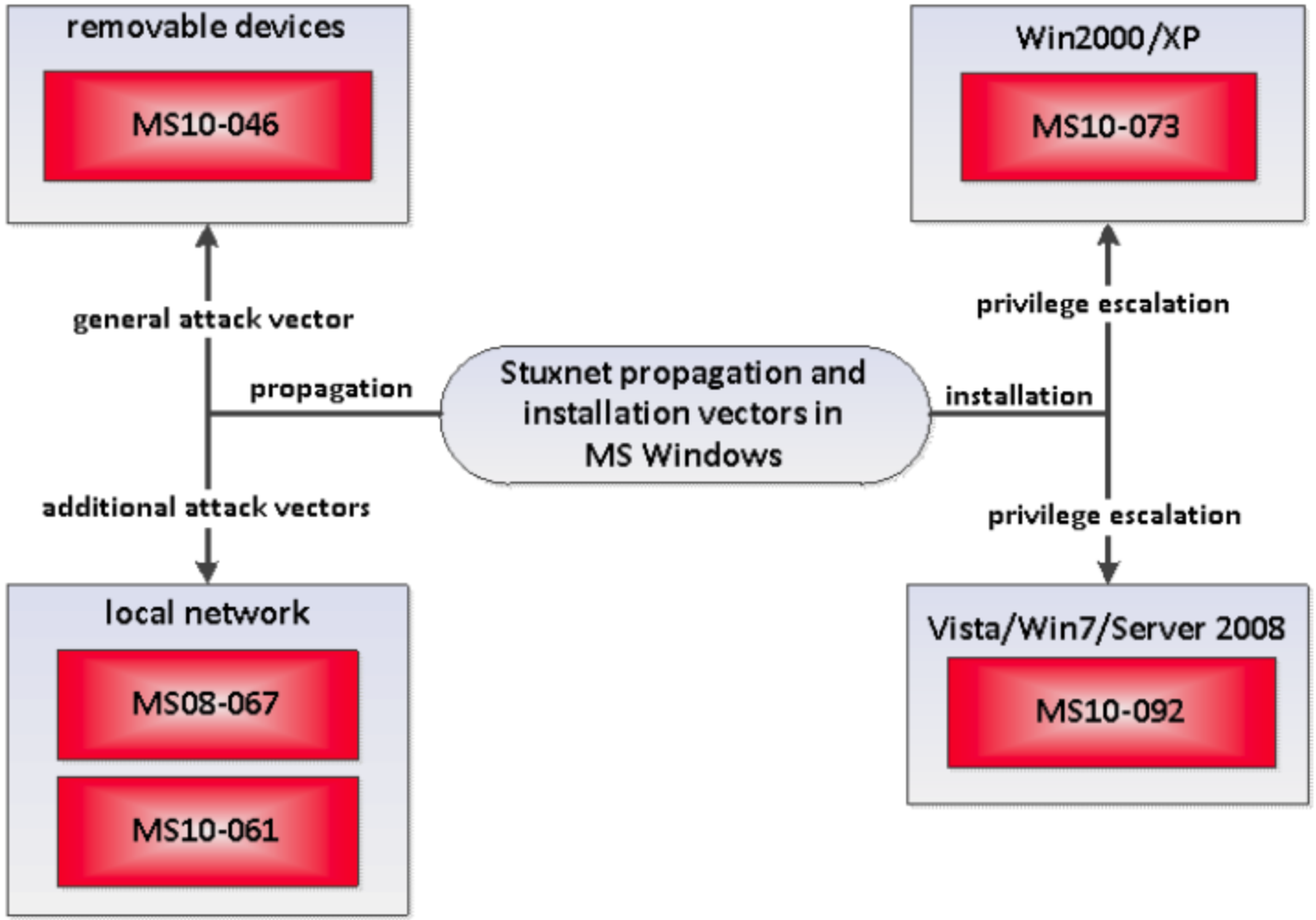
Case Study 4: Stuxnet

Characteristics	Stuxnet
Exploitation vector	MS10-046 (0-day) MS10-061 (0-day) MS10-073 (0-day) MS10 -092 (0-day) CVE-2010-2772 (0-day) MS08-067 (patched)
Targeted malicious program	Win32/Stuxnet



Characteristics	MS10-002	MS10-046	MS10-061	MS10-073	MS10 -092
Vulnerable versions	all versions of MS Internet Explorer (6, 7, 8)	all versions of MS Windows (WinXP, Vista, 7, ...)	all versions of MS Windows (WinXP, Vista, 7, ...)	WinXP and Win2000	Vista and Win7
Layered shellcode	yes	no	no	yes	no
Remote attacks	yes	yes	yes (only for WinXP)	no	no
Other vectors	no	yes	yes	no	no

Case Study 4: Stuxnet



Case Study 4: Stuxnet

Stuxnet feature highlights:

- Self-replicates through removable drives exploiting a vulnerability allowing auto-execution.
- Spreads in a LAN through a vulnerability in the Windows Print Spooler.
- Copies and executes itself on remote computers through network shares.
- Copies and executes itself on remote computers running a WinCC (specific to SCADA systems) database server.
- Updates itself through a peer-to-peer mechanism within a LAN.
- Exploits a total of four unpatched Microsoft vulnerabilities, two of which are previously mentioned vulnerabilities for self-replication and the other two are escalation of privilege vulnerabilities that have yet to be disclosed.
- Contacts a command and control server that allows the hacker to download and execute code, including updated versions.
- Contains a Windows rootkit that hide its binaries.
- Attempts to bypass security products.
- Fingerprints a specific industrial control system and modifies code on the Siemens PLCs to potentially sabo• tage the system.
- Hides modified code on PLCs, essentially a rootkit for PLCs

Conclusion

Malware is a part of the computing landscape.

- Threatens your information security
- Adaptable
- Weaponizable
- Responsible for a multi-billion dollar industry

Defense – ENTS650

Prevent malware infection

- Do not allow malware or virus on system
- Block modification of any files on system

IMPOSSIBLE

Conclusion

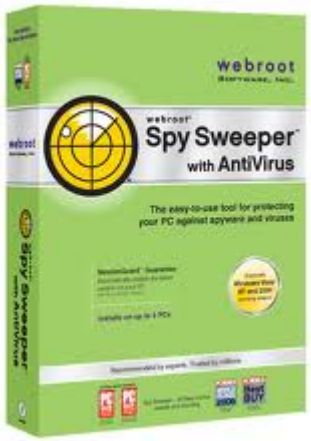
When prevention is not successful:

- Detection
- Identification
- Removal

As viruses have grown more complex, so has antivirus software:

- 1st generation: simple scanner
- 2nd generation: heuristic scanners
- 3rd generation: activity traps
- 4th generation: full-featured protection

PC Magazine editorial suggests Webroot and Ad-Aware Pro as providing the best protection overall.



Recommends Panda Cloud Anti-Virus 1.1 as best freeware.

References

ILOVEYOU/ZEUS

Wikipedia: “ILOVEYOU”. http://en.wikipedia.org/wiki/ILOVEYOU

CERT: “CERT Advisory CA-2000-04 Love Letter Worm”. May 9, 2000. http://www.cert.org/advisories/CA-2000-04.html

Chien, Eric. “VBS.LoveLetter and variants”, Symantec. Feb 13, 2007. http://www.symantec.com/security_response/writeup.jsp?docid=2000-121815-2258-99

Wikipedia: “Zeus (trojan horse)”. http://en.wikipedia.org/wiki/Zeus_%28trojan_horse%29

Westmoreland, Richard. “ZeuS”, Antisource. Feb 7, 2010. http://www.antisource.com/article.php/zeus-botnet-summary

Macdonald, Doug. “Zeus: God of DIY Botnets”, Fortiguard. Oct 14, 2009. http://www.fortiguard.com/analysis/zeusanalysis.html

Stevens and Jackson. “ZeuS Banking Trojan Report”, Dell SecureWorks. Mar 11, 2010. http://www.secureworks.com/research/threats/zeus/?threat=zeus

Falliere and Chien. “Zeus: King of the Bots”, Symantec Security Response. 2009. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/zeus_king_of_bots.pdf

References

Introduction/Stuxnet

http://extremevoltages.blogspot.com/2009_09_01_archive.html

http://dictionary.reference.com/browse/malware

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

http://en.wikipedia.org/wiki/Stuxnet

http://legalinsurrection.blogspot.com/2011/02/stuxnet-in-pictures.html

http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

http://www.isisnucleariran.org/news/detail/full-isis-coverage-of-stuxnet/

http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/

http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html

References

Conficker/Conclusion

Felix Leder, Tillmann Werner: Know Your Enemy, Containing Conficker: http://www.honeynet.org/files/KYE-Conficker.pdf

Ian Paul: Is Conficker Finally History?: http://www.pcworld.com/article/162570/is_conficker_finally_history.html

Erik Larkin: Protecting Against the Rampant Conficker Worm:
http://www.pcworld.com/article/157876/protecting_against_the_rampant_conficker_worm.html?tk=rel_news

Panda Security Assessment: Conficker.C:
http://www.pandasecurity.com/homeusers/security-info/204292/information/Conficker.C

Panda Security Assessment: MS08-067:
http://www.pandasecurity.com/homeusers/security-info/about-malware/encyclopedia/overview.aspx?idvirus=201683

Seungwon Shin, Guofei Gu: Conficker and Beyond, A Large-Scale Empirical Study:
http://faculty.cs.tamu.edu/guofei/paper/Shin_ACSAC10_Conficker.pdf

Bojan Zdrnja: Conficker's autorun and social engineering: http://isc.sans.edu/diary.html?storyid=5695

Wikipedia: Conficker. http://en.wikipedia.org/wiki/Conficker