Chapter 17

Cyber Security Overview

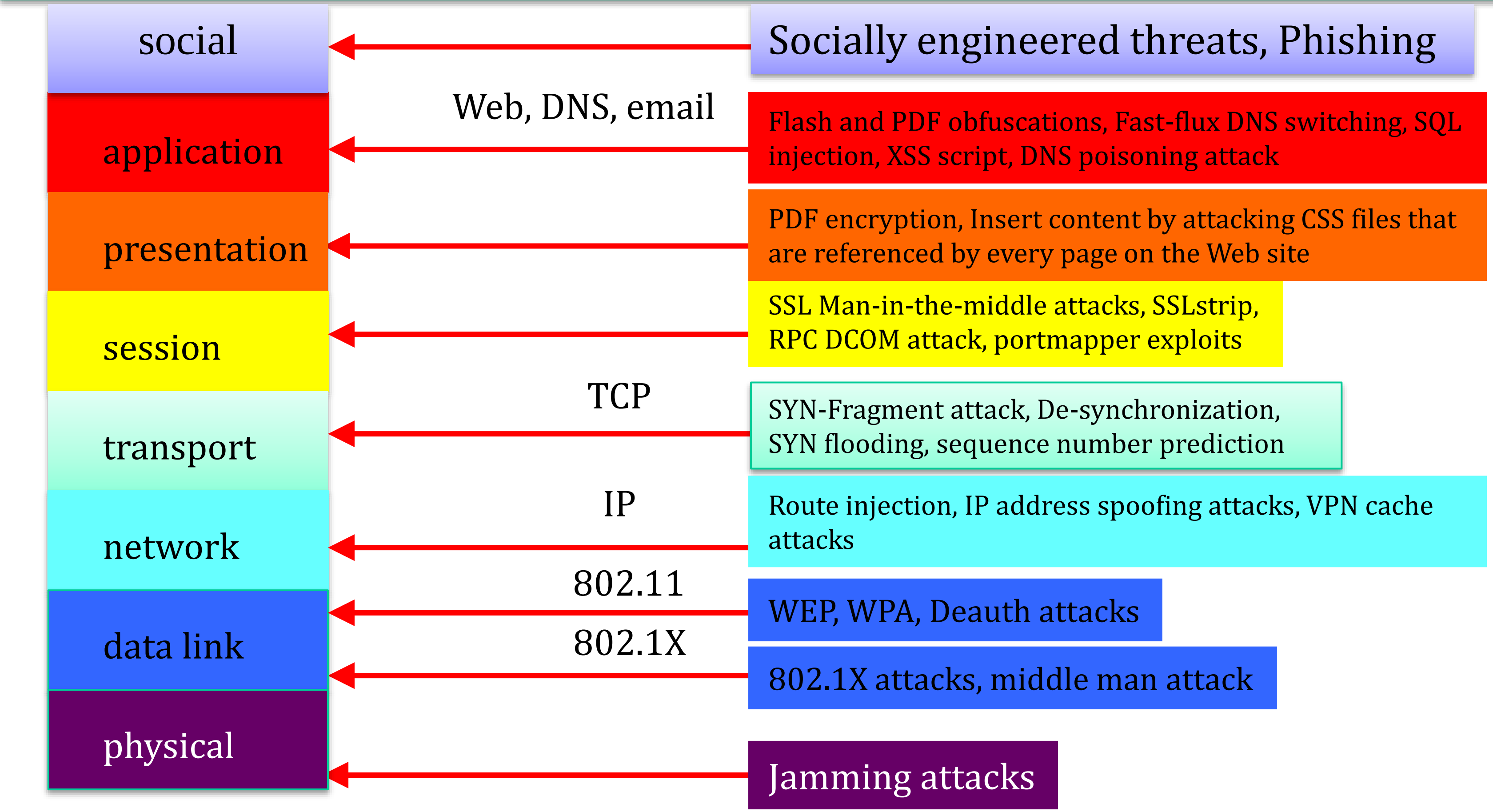
Outline

- Security overview
- Attacks and malware trends
- Attack/malware types
- Mutation of Malware
- Attacker's motivation and tactics
- Zero-day vulnerability
- Attacks to the Power Grid
- Network and Information Infrastructure Defense overview

Network and Information Security

- Security goals:
  - Confidentiality:
    - Only intended receiver or user can understand contents
  - Authentication:
    - Confirm identity
  - Accountability and non-repudiation:
    - Another notch of authentication’s feature
  - Integrity:
    - ensure information not altered
      - Integrity of routing and DNS infrastructure
  - Access control:
    - a security measure to permit the access to resources for user/process
  - Availability:
    - services must be accessible and available to allowed users/processes in an information infrastructure

Attacking Network Stack and Beyond



social ← Socially engineered threats, Phishing

application ← Web, DNS, email ← Flash and PDF obfuscations, Fast-flux DNS switching, SQL injection, XSS script, DNS poisoning attack

presentation ← PDF encryption, Insert content by attacking CSS files that are referenced by every page on the Web site

session ← SSL Man-in-the-middle attacks, SSLstrip, RPC DCOM attack, portmapper exploits

transport ← TCP ← SYN-Fragment attack, De-synchronization, SYN flooding, sequence number prediction

network ← IP ← Route injection, IP address spoofing attacks, VPN cache attacks

data link ← 802.11 ← WEP, WPA, Deauth attacks

data link ← 802.1X ← 802.1X attacks, middle man attack

physical ← Jamming attacks

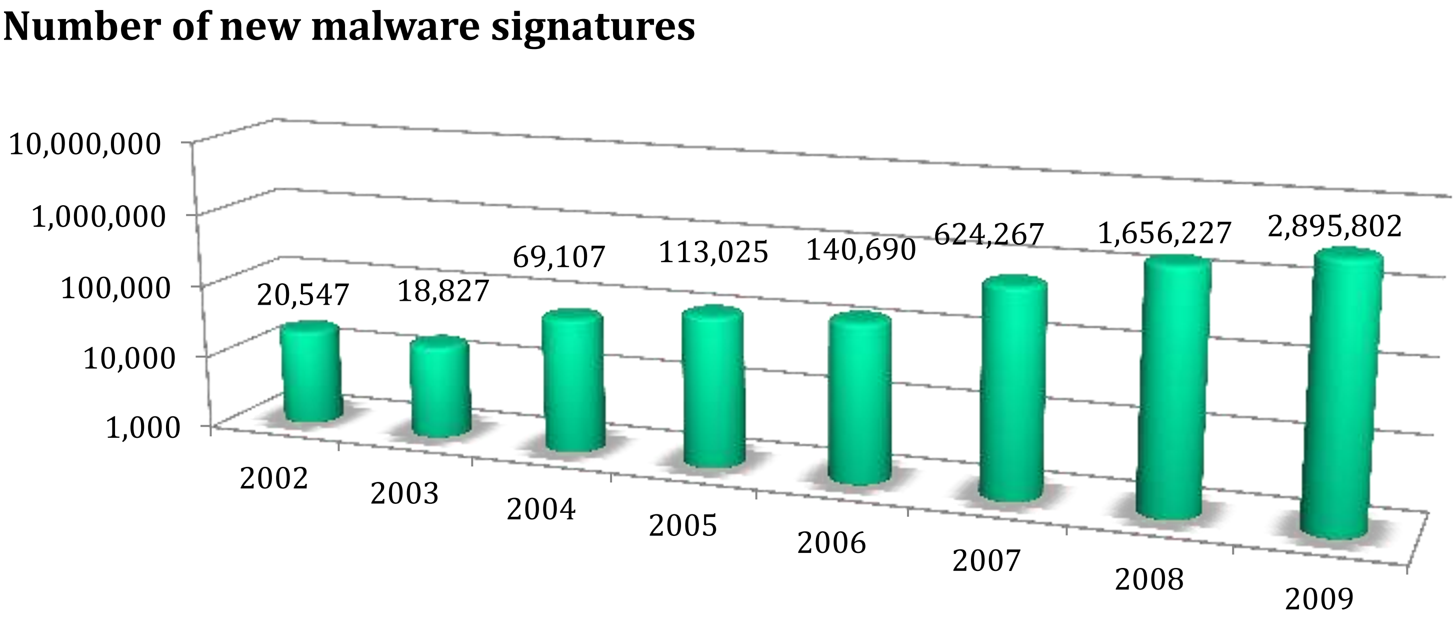
Weakest layer/component/module will be attacked

Attacks to Internet: Network-based exploits

- Attacks to OS, applications, hardware, and network equipment vulnerabilities
  - Malware
  - Configuration weakness
  - Syntax and semantics weakness
  - Validation weakness
- Attacks to confidentiality
  - Memory scraping
  - eavesdropping
  - packet sniffing
- Attacks on integrity
  - Modify content

- Attack on Authenticity
  - Identity theft
  - Password crack
  - Phishing attack
  - DNS attack
  - Cache poisoning
- Evasion on security equipment/measures
  - Mutated attacks
- Attacks on Availability
  - Distributed denial of service (DDoS)
- Social engineering

The exponential rise in new malware (threats) signatures

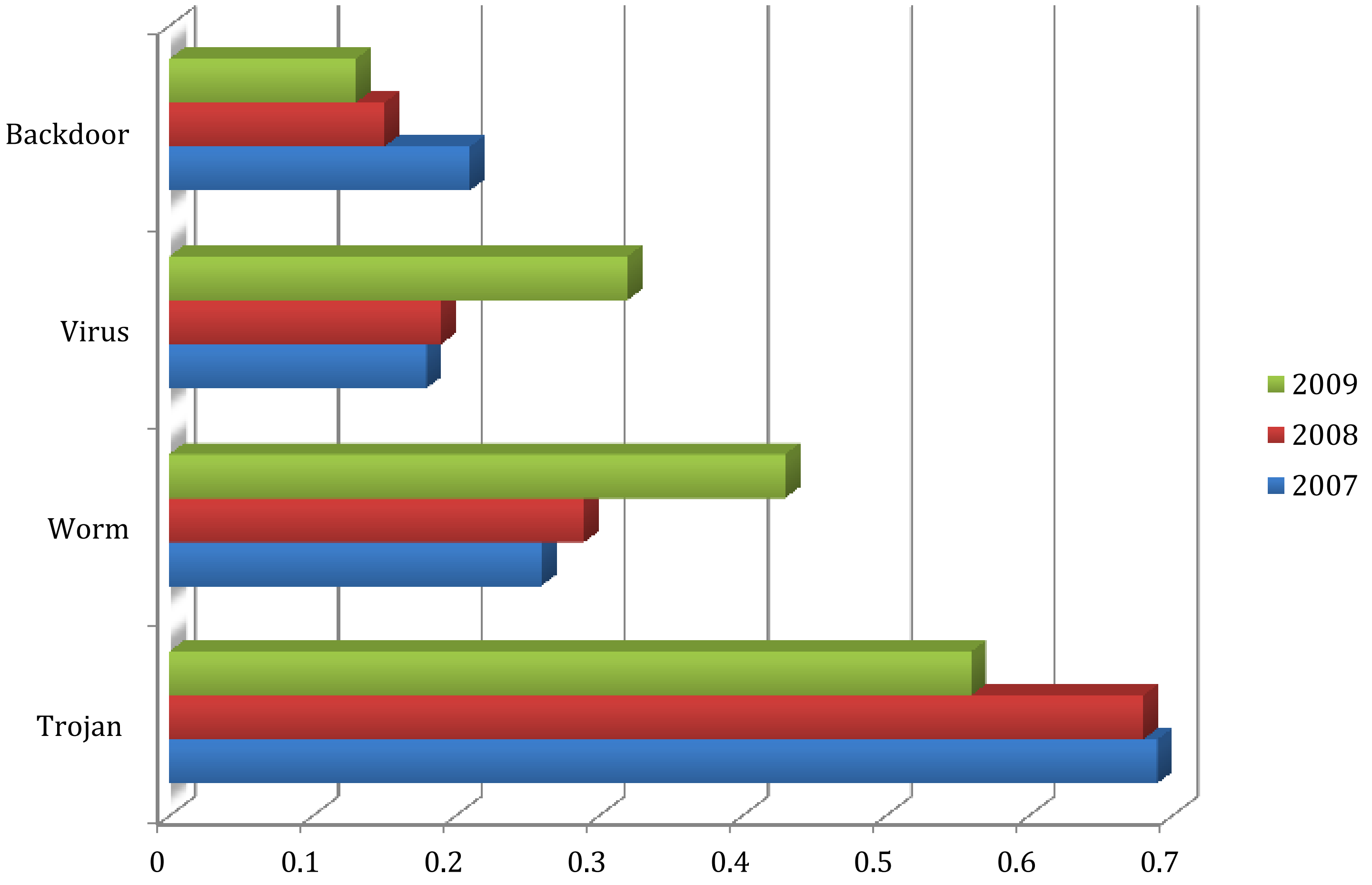


The McAfee Threat Report states that the average daily malware growth has reached its highest levels, with an average of 60,000 new pieces of malware identified per day in 2010, almost quadrupling since 2007

Polymorphism and new delivery mechanisms

- Symantec encountered more than 286 million unique variants of malware in 2010
- Symantec discovered 240 million unique threat samples in 2009
  - created 2.9 million new malware signatures in the same period
  - Symantec stopped reporting the number of new signatures since 2010
- Signature-based protection, intrusion prevention, behavioral and heuristic detection capabilities are not enough for defending malware
  - This shift has made it nearly impossible for security vendors to discover, analyze and protect against every threat and placed a significant burden on traditional approaches to malware detection
- Reputation-based approach: a security rating for each file, based on information about the context of the file – where it came from, how old it is and its adoption patterns across Symantec's user population
- There is a delay for effective defense similar to signature-based protection

Distribution of Malware Types



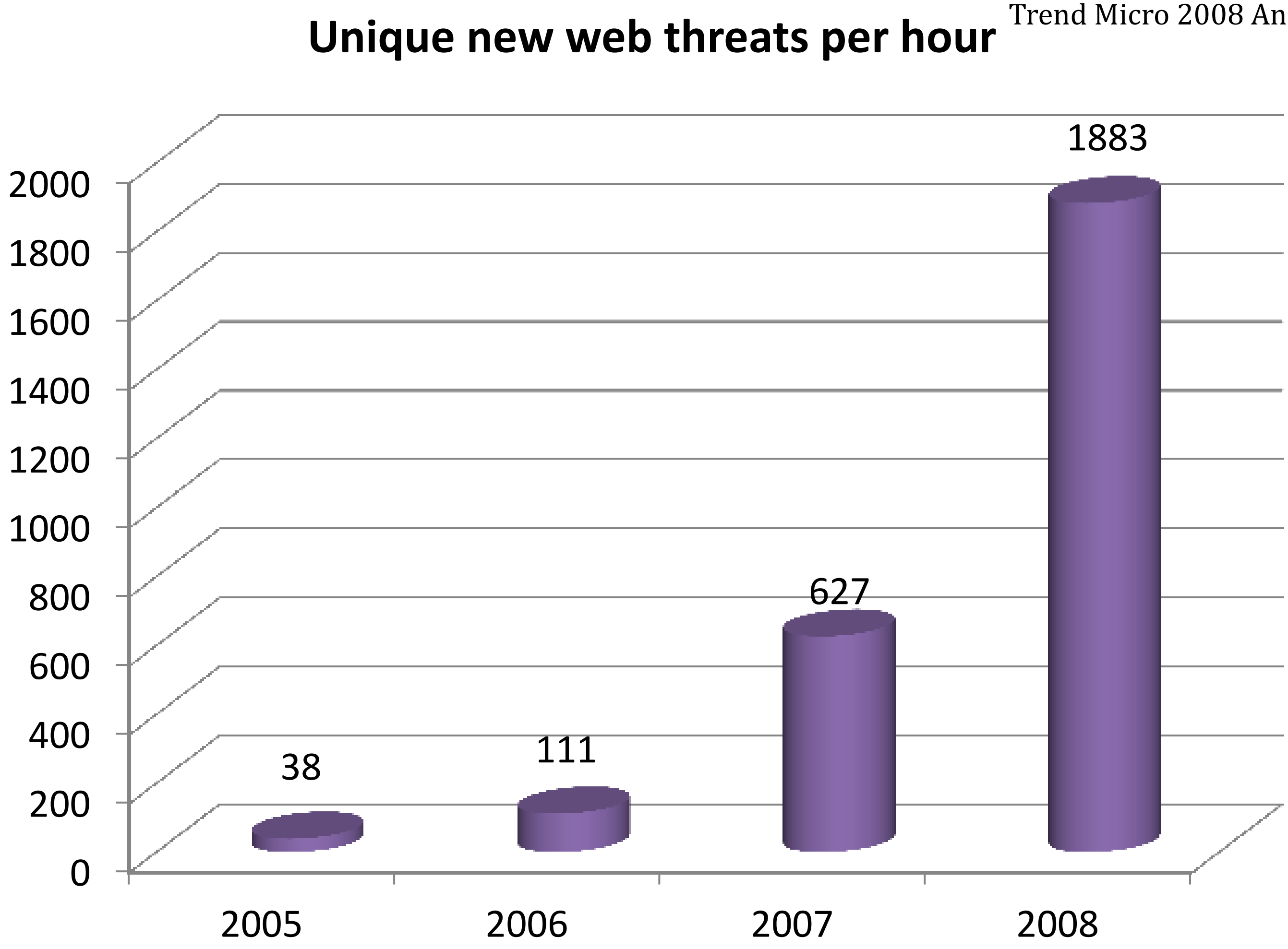
Source: Symantec Global Internet Security Threat Report

Web-based malware and Phishing

- The significant growth of social networking
- Web-based malware has now become more attractive to cyber-criminals as they present an opportunity to capitalize on users' unfamiliarity with the nature of Web-based threats
  - New toolkits were successful in exploiting web sites with weak security
    - Trend Micro discovered that in March of 2008 there were more than 400 phishing kits designed to generate phishing sites for targeting the top Web 2.0 sites as well as other popular venues for social networking, video sharing, free email service, banks, and the like
- The Blue Coat Web Security Report for 2009 noted that the average lifespan of malware had dropped to two hours in 2009
  - The rapid change in preferred toolkits is probably driven by the need to adapt and constantly adjust in order to avoid detection by anti-phishing software

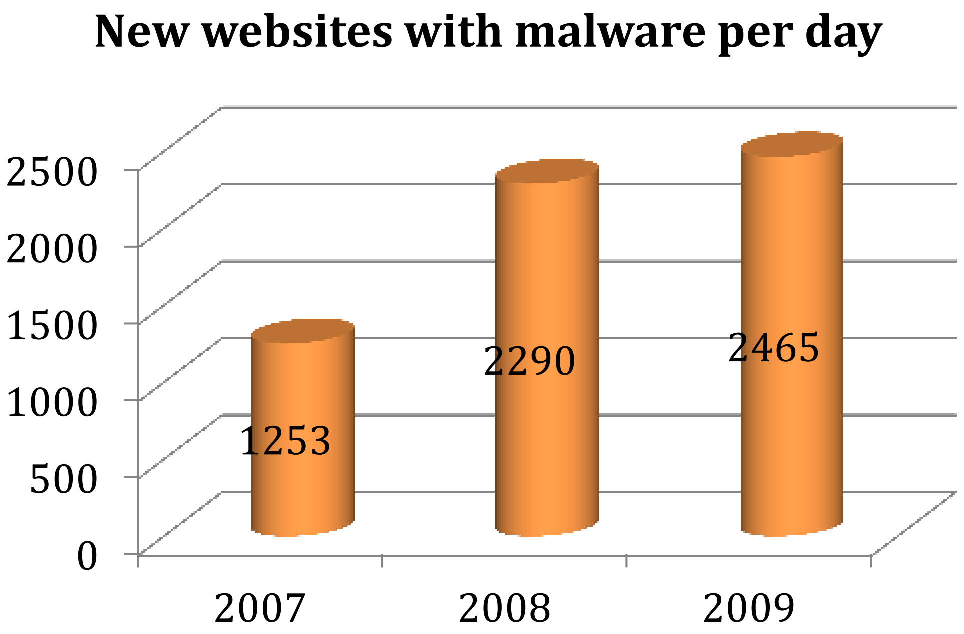
Unique new web threats per hour

Trend Micro 2008 Annual Threat Roundup



New websites with malware per day

MessageLabs



Malware

- Malicious code often masquerades as part of useful software/message/information
- Malware exploits existing vulnerabilities on systems making quiet and easy entry
- Some malicious programs need host programs to hide their tracks
  - Trojan horses, spyware, viruses, and rootkits
- Others can exist and propagate independently
  - Worms, automated viruses and zombies

Worms

- Propagation mechanisms
  - Sharing files
    - USB flash drives
      - In the second half of 2007, 40 percent of malicious code that propagated did so as a significant increase from 14 percent in the first half of 2007
      - Nov 2008: agent.btz affected the Pentagon's networks; The malware is able to spread to any flash drive plugged into an infected computer; DoD ban use of external drives
      - Nov 2008: Conficker worm
      - 2011: Stuxnet worm
  - P2P, IRC
  - Instant messaging
  - SQL injection
  - Web pages
  - Buffer Overflow
  - emails

Conficker.A worm

- The Conficker worm, discovered in November 2008, leveraged
  - an extremely new vulnerability discovered in September 2008
    - the MS08-67 vulnerability in the Microsoft Windows server service
  - the Server Message Block (SMB) path traversal and password guessing
  - peer-to-peer (P2P) update mechanism
- SRI:
  - caused such a broad spectrum of antivirus tools to do such a consistently poor job of detecting malware binary variants

Conficker.B worm

- Propagation mechanisms
  - through open *NetBIOS* network shares as well as brute force password attempts using a list of over 240 common passwords
  - using a Universal Serial Bus (USB) drive to copy itself as the autorun.inf to removable media drives in the system
- SRI'S cumulative census :
  - Conficker.A has affected more than 4.7 million IP addresses
  - Conficker.B, has affected 6.7M IP addresses
- China's National Computer Network Emergency Response Technical Team (CNCERT) reported in the 2009 annual security report that China had about 7 million Internet Protocol (IP) addresses infected with Conficker B at the end of 2009

Conficker.C worm

- A rootkit in that it obfuscates its presence and protects itself, a Trojan/backdoor, a polymorphic virus and a botnet
- Major functional additions
  - a security product disablement thread that disables critical host security services, such as anti-malware software, Windows defender, and Windows services that deliver security patches
    - deactivates the safeboot mode as a future reboot option
    - kills processes whose names match a blacklisted set of 23 security products, hot fixes, and security diagnosis tools
    - modifies the host domain name service (DNS) APIs to block various security-related network connections
  - Conficker.C installs itself into the user file system and configures the registry appropriately to invoke its DLL at host startup
  - P2P coordination channel
  - a revision of the domain name generation algorithm

Phishing and Identity Theft

- Phishing is essentially an online con game and phishers are nothing more than tech-savvy con artists and identify thieves.
  - They use SPAM, malicious Web sites, email messages and instant messages to trick people into divulging sensitive information, such as bank and credit card accounts
- The phish sites can look remarkably like legitimate sites because they tend to use the copyrighted images from legitimate sites
- Fraudulent messages are often not personalized
- Spear phishing contains very personal messages
  - FBI director Robert Mueller fell prey to a phishing scheme in 2009
    - Responding to a legitimate-looking email purporting to be from his bank and requesting that he "verify" some of his personal information

Phishing Toolkit

- There are two types of phishing toolkits:
  - Domain-based phishing toolkits that require the phisher to own and register a unique domain, such as "devil.com" and host it somewhere like a botnet or on an ISP
  - Defacement-based phishing toolkits that do not require the registration of domains or DNS servers so they are easier to setup
    - Defacement-based phishing toolkits require a phisher to compromise existing Web pages, after which the phisher can simply upload the page of the spoofed brand

Big News Event

- Manipulating search engine results is one example of where criminals are showing increasing "mastery" of skills
- A big news event
  - when pop star Michael Jackson passed away in June 2009
  - Internet service actually slowed down on the day of Jackson's death because so many people were online searching for the same information at the same time
  - many of the highest-ranking search results related to his death on major search engines were actually malicious websites
  - Cisco researchers identified eight different botnet organizations using the Michael Jackson lure, including the Zeus Trojan

Transformer 3 in a phishing scheme

- On 4/26/2010, security testers at the Guam Air Force base's 36th Communications Squadron had to send out a clarification notice after an in-house test
  - an operational readiness exercise (ORE) in Air Force parlance, indicating how airmen would respond to a phishing e-mail
  - The e-mail said that crews were going to start filming "Transformers 3" on Guam and invited airmen to fill out applications on a Web site if they wanted to work the shoot
  - Unfortunately, many of Andersen's personnel responded to this phishing site and submitted their personal information to the Web site, and forwarded the information outside of Andersen
  - The rumor soon spread to other Transformers fan sites, including Seibertron.com and Tformers.com
  - As the rumor spread that the hotly anticipated film was coming to Guam, local media started calling the base

Trojan Horse and Backdoor

- Program with hidden malware
  - Programs are usually superficially attractive
    - E.g. game, s/w upgrade etc
  - Plus additional malicious tasks
    - allows attacker to gain access that they are not allowed
- Used to propagate a virus/worm or install a backdoor

- Backdoor
  - secret entry point into a program
  - allows those who know access bypassing usual security procedures

Sinowal/Mebroot Trojan (1)

- Researchers at RSA Security Inc.'s FraudAction Research Labs tracked the Sinowal Trojan horse, also known as Mebroot and Torpig (10/31/2008)
  - Infected hundreds of thousands of PCs worldwide
  - Rootkit elements infect the PC's master boot record (MBR), the first sector of a hard drive
    - Because that sector is loaded before loading anything else, Windows included, the Sinowal is nearly invisible to security software
- Trojan waits for the user to enter the address to an online bank, credit card company site or another financial URL, then substitutes a phishing site
  - Triggered by more than 2,700 specific Web addresses, a massive number compared with other Trojan horses

Sinowal/Mebroot Trojan (2)

- Fake sites collect log-on usernames and passwords to banks and other financial institutions
  - Dupe users into disclosing information those organizations never collect online, such as Social Security numbers
  - Transmits the stolen credentials and data to the drop server
- A sophisticated cybercrime group that has maintained an especially devious Trojan horse for nearly three years since Feb 2006
  - stolen the log-ons to more than 300,000 online bank accounts and 300,000 credit cards during that time
  - The Trojan horse has been revised in a number of variants

Sinowal/Mebroot/Torpig Trojan, April, 09 (1)

- Researchers were able to monitor more than 180,000 hacked computers by exploiting a weakness within the command-and-control network used by the hackers to control the computers
  - It only worked for 10 days, however, until the hackers updated the command-and-control instructions
  - The botnet, known as Torpig or Sinowal
  - In that short time, about 70GB of data were collected from hacked computers
  - While it is difficult to precisely estimate the value of the information collected over the 10 days, it could be worth between $83,000 to $8.3 million, the research paper said
    - Source: Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Chris Kruegel, and Giovanni Vigna, "Your Botnet is My Botnet: Analysis of a Botnet Takeover," UCSB Technical Report, Santa Barbara, CA, April 2009, http://www.cs.ucsb.edu/~seclab/projects/torpig/index.html

Sinowal/Mebroot Trojan, April, 09 (2)

- Torpig/Sinowal can infect a PC if a computer visits a malicious Web site that is designed to test whether the computer has unpatched software, a technique known as a drive-by download attack
  - If the computer is vulnerable, a low-level piece of malicious software called a rootkit is slipped deep into the system
  - The researchers found out that Torpig/Sinowal ends up on a system after it is first infected by Mebroot, a rootkit that appeared around December 2007
- Torpig/Sinowal is customized to grab data when a person visits certain online banking and other Web sites
- It is coded to respond to more than 300 Web sites, with the top targeted ones being PayPal, Poste Italiane, Capital One, E-Trade and Chase bank

Limbo malware and HTML injection

- Uri Rivner, at RSA Consumer Solutions, a division of EMC: 10/30/2008
  - A trojan horse program can add extra data-entry fields to legitimate online banking sites and trick visitors into giving up bank card numbers, PINS, and other valuable data
    - Abnormal behavior: ask user to provide some information that were never asked to give before
  - The Limbo malware insinuates itself into a Web browser using HTML injection
    - while the user is at a genuine bank site and can surreptitiously change the actual layout of that real site
- Like other malware, Limbo can infiltrate a computer through many paths:
  - pop-up messages that ask you to download an (often security-themed) fake application
    - drive-by downloads from hacked Web sites that invisibly attack holes in vulnerable outdated software, and other means
- Fraudsters can buy Limbo via a complex underground market, and it is getting cheaper: It costs about $350, down from about $1000 a year ago

Zeus Trojan

- Available as a toolkit that can be purchased
  - creates new variants of the Trojan, providing each new version with a unique signature that enables it to evade detection by anti-virus programs
- The malware can monitor computer activity and, through this intelligence gathering, steal login names and passwords for banking and email accounts
  - Even defeat hardware tokens and one-time passwords (OTP) that people assume provide protection from this type of attack
  - When the malware is operational on secure sites that require OTP for logins, the Trojan will ask the user to generate several of these passwords, usually from a hardware token
  - The malware will then deliver these legitimate passwords to the botmaster, instead of the banking website
- Peer-to-peer functionality, including update to Zeus Trojan, offers resistance to take-downs

BIOS Trojans (1)

- Chinese AV vendor 360 has discovered a virus in the wild that makes its home in a computer's BIOS, where it remains hidden from virus scanners
  - The contaminant, called Mebromi, first checks to see whether the victim's computer uses an Award BIOS
    - If so, it uses the CBROM command-line tool to hook its extension into the BIOS
    - The next time the system boots, the BIOS extension adds additional code to the hard drive's master boot record (MBR) in order to infect the winlogon.exe / winnt.exe processes on Windows XP and 2003 / Windows 2000 before Windows boots
  - The next time Windows launches, the malicious code downloads a rootkit to prevent the drive's MBR from being cleaned by a virus scanner

BIOS Trojans (2)

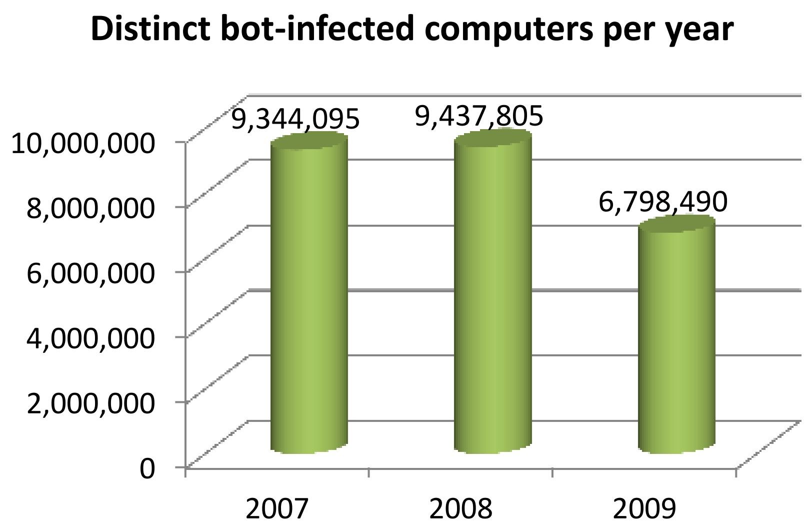
- But even if the drive is cleaned, the whole infection routine is repeated the next time the BIOS module is booted
  - Mebromi can also survive a change of hard drive
  - If the computer does not use use an Award BIOS, the contaminant simply infects the MBR and control the Windows boot process

  http://www.h-online.com/security/news/item/Return-of-the-BIOS-trojans-1341421.html

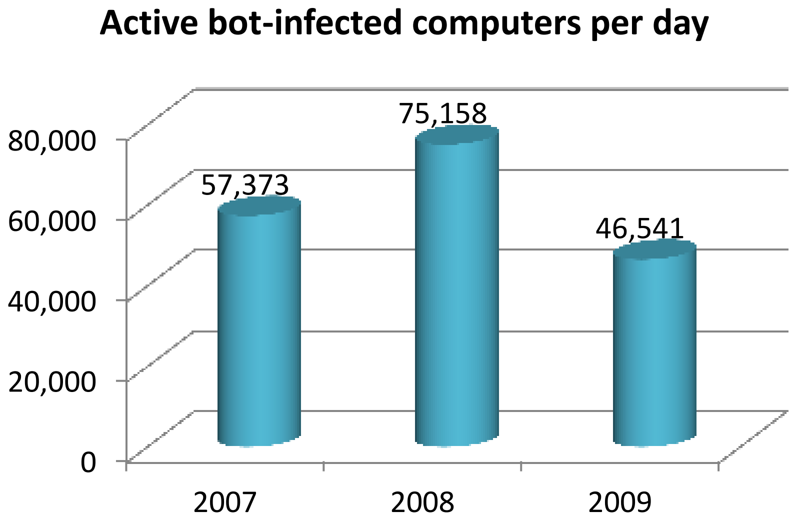
Botnet/Zombie

- Botnet
  - network of hosts capable of acting on instructions
    - Program secretly takes over another Internet host
    - Capable of exploiting vulnerabilities and propagating automatically
  - Typically a large group of remotely controlled “zombie” systems
    - up to several million
    - Host owners are not aware they have been compromised
  - Botnet control is accomplished through Bot command-and-control (C&C) servers
    - Controlled and upgraded via IRC, P2P, HTTP-based, fast-flux DNS or the hybrid
- Used for attacks
  - Distributed denial of service
  - Spam and clickjacking
  - Launching pad for new exploits/worms/spams
- A business for rent
  - that the Conficker worm is the biggest cloud service on the planet

Distinct bot-infected computers per year



Active bot-infected computers per day



SPAM Rate in Botnet

- One bot-infected PC = 600,000 spam messages a day (4/24/09)
- Source: TRACElabs, Marshal8e6, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131984&source=NLT_PM

Botnet	Number of SPAM messages /hour
Rustock	25,000
Xarvester	25,000
Mega-D	15,000
Donbot	8,000
Srizbi	8,000
Bobax	7,200
Waledac	7,000
Gheg	7,000
Pushdo	4,500
Grum	4,000

BOT messages per hour

Botnet control

- Bot command-and-control servers are computers that botnet owners use to relay commands to bot-infected computers
  - Bot locates IRC server, connects, joins channel
  - Typically need DNS to find out server's IP address
    - Especially if server's original IP address has been blacklisted
  - Authentication password often stored in bot binary
- Botnet master issues authenticated commands

- New trend
  - move away from traditional IRC bot command-and-control communication frameworks for botnet owners
  - a decentralized command-and-control using P2P
    - Storm was the first to introduce a fully P2P control channel and utilize a peer-based coordination scheme
    - providing better security for their botnets
    - making them more difficult to detect and disable
  - Examples are P2P networks such as the botnets associated with the Conficker

Fast-flux DNS for evasion (1)

- P2P botnet owners typically use a fast-flux domain name service scheme
- Fast-flux switching mechanism combines
  - peer-to-peer networking
  - distributed command and control
  - Web-based load-balancing
  - proxy redirection
- Researchers were struggling to identify malicious Storm domains in February 2008

- Storm was pinpointed as the spam source linked to a fake Canadian pharmacy
  - fraudulent pharmaceutical sites hosted on nodes in the fast-flux Storm botnet
  - Although the domains involved in this spamming operation seemed to be pointing to the same IP, the links in the spammed messages were actually changing, creating detection difficulties

Fast-flux DNS for evasion (2)

- Fast-flux helps phishing sites stay up for longer periods to lure more victims
- Rock Phish toolkit, a sophisticated technology framework that helps criminals create and carry out phishing attacks, uses fast-flux technology to maintain phishing sites for a longer period
- Cyber criminals are now encrypting P2P networks to disguise botnet activity
  - Encryption is also being used on VoIP to hide mobile malware threats
- Obfuscation techniques are becoming more sophisticated as cyber criminals develop new ways to hide malicious script
- Srizbi bots (that was rated no. 1 in size) connect with new servers via domains that dynamically generated by algorithm
  - The domain names are generated on a three-day cycle

Zbot

- Zbot, also known as Zeus, is a malware package that is readily available for sale
  - The package contains a builder that can generate a bot executable and Web server files, e.g. PHP, images and SQL templates, for use as the command and control server
  - a set of data-stealing Trojans that spreads through email phishing attacks as well as drive-by downloads
  - According to a report published by SecureWorks in March 2010 [25], the basic Zeus Builder kit runs $3,000 to $4,000, with another $1,500 for the "Backconnect" module which is used to connect back to an infected host in order to make financial transactions
  - To hack Windows 7 or Vista computers, criminals will have to pay an extra $2,000 or be limited to Windows XP systems
- Infecting nearly 4 million computers worldwide in 2009
- The Zeus malware monitors for signs that a user is logging in to an account, such as bank account or webmail, and then collects the necessary authentication credentials and passes them to the botmaster

ZeuS P2P botnet: 10/13/2011

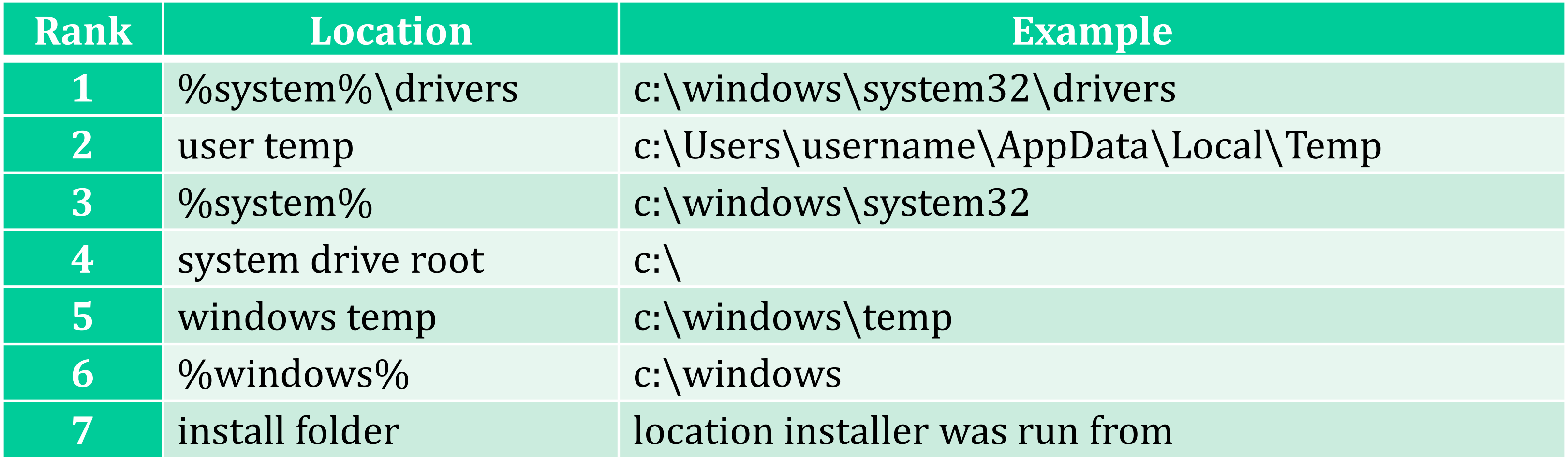
- ZeuS is using a ***IP list*** which contains IP addresses of other drones participating in the P2P botnet.
  - An initial list of IP addresses is hardcoded in the ZeuS binary
  - As soon as a computer gets infected, ZeuS will try to find a active node by sending UDP packets on high ports
  - If the bot hits an active node, the remote node will response with a list of current IP addresses that are participating in the P2P network
  - Additionally, the remote node will inform the requesting node its *binary* and *config version*
    - If the remote node is running a more recent version, the bot will connect to it on a **TCP high port** to download a binary update and/or the current config file
    - Afterwards the bot will connect to the C&C domain listed in the config file using HTTP POST
      - The HTTP protocol is only being used to drop the stolen data to the Dropzone and/or to receive commands from the botnet master.
- Source: http://www.abuse.ch/?p=3499

DDoS Attacks

- A report by Arbor Networks in 2011
- Botnet-driven DDoS attacks are likely to continue as a low cost, high-profile form of cyber-protest
- Maximum attack sizes reached 100 Gbps for the first time in 2010
  - double that for 2009, and ten times the peak size seen as recently as 2005
- Application-layer DDoS attacks target data center infrastructure
  - increasingly in the form application attacks rather than simple packet flooding
- Attack frequency also appears to be increasing, with 25 percent of survey respondents seeing 10 or more DDoS attacks per month, and 69 percent experiencing at least one

Rootkits (1)

- A *Rootkit* is a set of Trojan system binaries
- Its primary characteristic is stealth
  - burrows deep into the operating system
  - modifying OS at a low-level in order to hide itself and other malware, in order to avoid removal
  - the modified binaries have the same checksum as the original ones
- The most popular locations for hidden rootkit binaries on a Windows hard disk



Rank	Location	Example
1	%system%\drivers	c:\windows\system32\drivers
2	user temp	c:\Users\username\AppData\Local\Temp
3	%system%	c:\windows\system32
4	system drive root	c:\
5	windows temp	c:\windows\temp
6	%windows%	c:\windows
7	install folder	location installer was run from

Rootkits (2)

- Drivers (.sys) are the most prevalent file being hidden on user's computers
  - 59% of rootkits hide in .sys files (e.g. acpi.sys)
  - 40% in .exe files and 1% in .dll files
- A sniffer to record user passwords
- Its typical infection paths are a website visit and *Clickjacking*
  - also use a stolen password or a dictionary attack
  - buffer overflow
- Types of Rootkits:
  - user mode
  - kernel mode
  - Master Boot Record (MBR) mode

Types of Rootkits (1)

- User Mode Rootkits
  - hooking the user or application space in such a way that whenever an application makes a system call, the predetermined path of the system's execution permits a Windows Rootkit to hijack the system call at many points along the path
  - One of the most common user mode techniques is the in-memory modification of system DLLs

- Kernel-mode Rootkits
  - As a system call's execution path leaves user mode and enters kernel mode, it must pass through a gate that prevents the user mode code from accessing kernel mode space
    - Only the super-user or equivalent process can access the kernel
    - In older versions of Windows, this gate is accessed via interrupts while in newer versions of Windows this is done via model specific registers (MSRs)

Types of Rootkits (2)

- Kernel-mode Rootkits use methods
  - (1) An attacker can directly execute the rootkit, rather than the original kernel mode code, by hooking both gate mechanisms
  - (2) A rootkit can modify the System Service Descriptor Table (SSDT), which is a function pointer table in kernel memory that holds all of the addresses of the system call functions
    - By simply modifying this table, the rootkit can redirect the execution to its code instead of the original system call
  - (3) A rootkit can also simply remove itself and other malicious processes in order to hide from this active process list by modifying the data structures in kernel memory

Types of Rootkits (3)

- Master Boot Record (MBR) Rootkit
  - Since a MBR rootkit, such as Mebroot, loads prior to anything else and is nearly invisible to security software, once the machine is infected, the hacker controlling the Rootkit has complete control of the victim's machine
  - Most MBR rootkits can defend itself by disabling all security related updates and patches as well as malware detection functions during PC boot process
- A more deeply embedded rookit is the BIOS Trojans

Rootkits for Cisco routers

- Sebastian Muniz, a researcher with Core Security Technologies, has developed malicious rootkit software for Cisco's routers
  - unveiled on May 22, 2008 at the EuSecWest conference in London
- It is written for IOS, the Internetwork Operating System used by Cisco's routers
  - It could work on several different versions of IOS
- The software cannot be used to break into a Cisco router
  - an attacker needs to have some propagation means, or an administrative password on the router to install the rootkit

Viruses (1)

- Self-replicating code attached to some other code
  - biological virus
- Propagating itself and carries a payload
  - carries code to make copies of itself
  - modifies the OS or the application's portable executable (PE) files
    - it needs to understand how some executables are executed in the operating system
    - To infect a particular program file, the virus will parse it, copy itself into the program and/or modify the header to get executed, whenever the program is executed
  - performs some covert task

Viruses (2)

- Virus phases:
  - Dormant: waiting for a trigger event
  - Propagation: using exploits for replicating to other host
  - Triggering: by event to execute payload
  - Execution of payload
    - downloading files and/or executing programs

Common Vulnerabilities and Exposures (CVE)

- The CVE vulnerability naming scheme is for a dictionary of unique, common names for publicly known software flaws
- The MITRE Corporation assigns CVE IDs to publicly known vulnerabilities in commercial and open source software
- General information on CVE is available at http://cve.mitre.org/

- CVE provides the following:
  - A comprehensive list of publicly known software flaws
  - A globally unique name to identify each vulnerability
  - A basis for discussing both the priorities and risks of vulnerabilities
  - A way for a user of disparate products and services to integrate vulnerability information

CVE Example

- A CVE vulnerability entry consists of a unique identifier number, a short description of the vulnerability, and references to public advisories on the vulnerability

Name: CVE-2004-0356

Description:

Stack-based buffer overflow in a Supervisor Report Center in the SL Mail Pro 2.0.9 and earlier versions allows remote attackers to execute arbitrary code via an HTTP request with a long HTTP sub-version. Status: Entry

Reference: BUGTRAQ:20040305 SLMail Pro Supervisor Report Center Buffer Overflow (#NISR05022004a)

Reference: URL:http://marc.theaimsgroup.com/?l=bugtraq&m=107850488326232&w=2

Reference: CONFIRM:http://216.26.170.92/Download/webfiles/Patches/SLMPPatch-2.0.14.pdf

Reference: MISC:http://www.nextgenss.com/advisories/slmailsrc.txt

Reference: XF:slmail-src-stack-bo(15398)

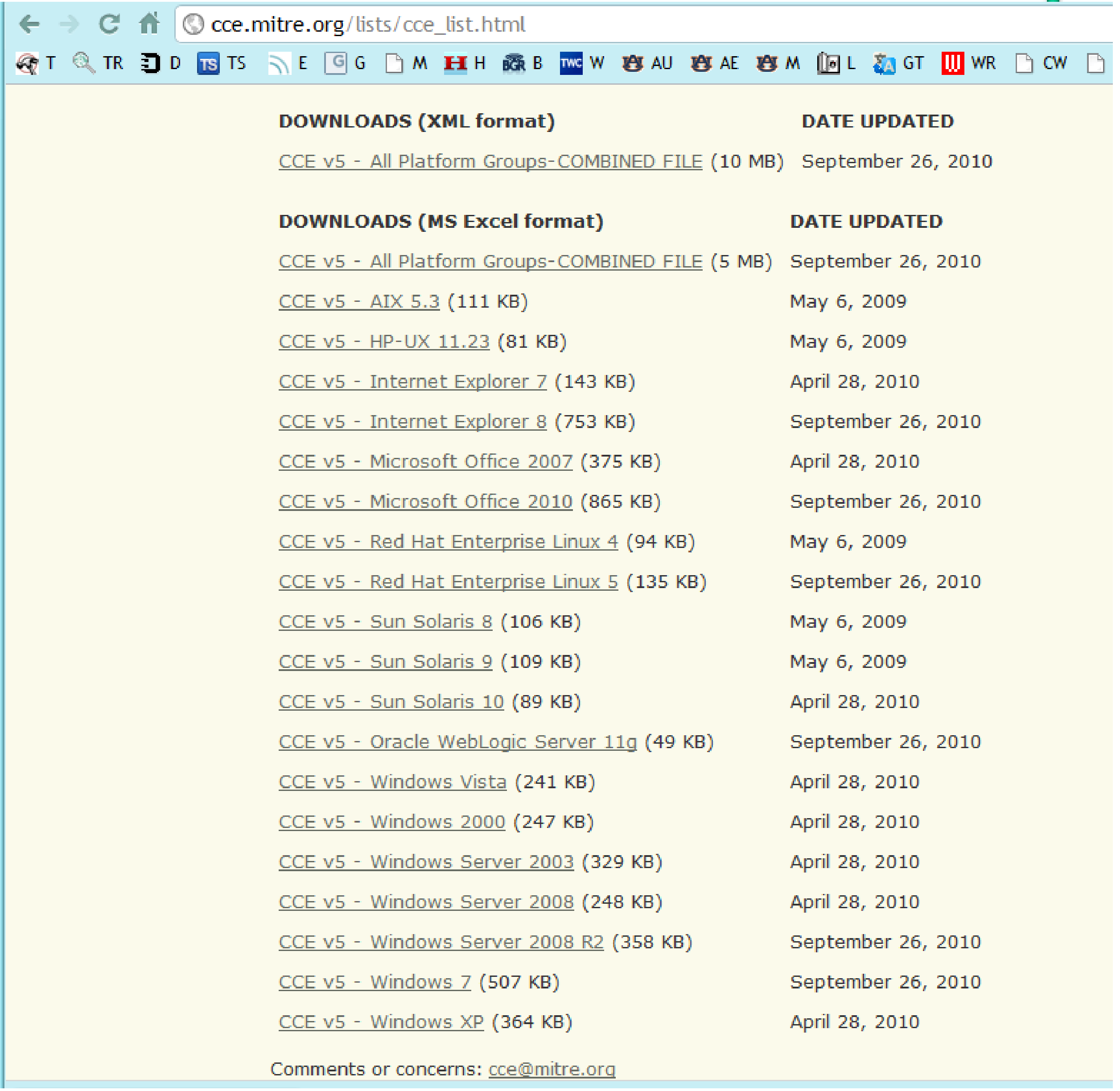
Reference: URL:http://xforce.iss.net/xforce/xfdb/15398

Reference: BID:9809

Reference: URL:http://www.securityfocus.com/bid/9809

Common Configuration Enumeration (CCE)

- The CCE version 5 List provides unique identifiers for software *security configuration* settings
- The settings are recommendations for securing an OS or application
- The MITRE Corporation maintains and publishes the lists of CCE names. The lists, and additional information on CCE, are available at http://cce.mitre.org/



DOWNLOADS (XML format)	DATE UPDATED
CCE v5 - All Platform Groups-COMBINED FILE (10 MB)	September 26, 2010

DOWNLOADS (MS Excel format)	DATE UPDATED
CCE v5 - All Platform Groups-COMBINED FILE (5 MB)	September 26, 2010
CCE v5 - AIX 5.3 (111 KB)	May 6, 2009
CCE v5 - HP-UX 11.23 (81 KB)	May 6, 2009
CCE v5 - Internet Explorer 7 (143 KB)	April 28, 2010
CCE v5 - Internet Explorer 8 (753 KB)	September 26, 2010
CCE v5 - Microsoft Office 2007 (375 KB)	April 28, 2010
CCE v5 - Microsoft Office 2010 (865 KB)	September 26, 2010
CCE v5 - Red Hat Enterprise Linux 4 (94 KB)	May 6, 2009
CCE v5 - Red Hat Enterprise Linux 5 (135 KB)	September 26, 2010
CCE v5 - Sun Solaris 8 (106 KB)	May 6, 2009
CCE v5 - Sun Solaris 9 (109 KB)	May 6, 2009
CCE v5 - Sun Solaris 10 (89 KB)	April 28, 2010
CCE v5 - Oracle WebLogic Server 11g (49 KB)	September 26, 2010
CCE v5 - Windows Vista (241 KB)	April 28, 2010
CCE v5 - Windows 2000 (247 KB)	April 28, 2010
CCE v5 - Windows Server 2003 (329 KB)	April 28, 2010
CCE v5 - Windows Server 2008 (248 KB)	April 28, 2010
CCE v5 - Windows Server 2008 R2 (358 KB)	September 26, 2010
CCE v5 - Windows 7 (507 KB)	September 26, 2010
CCE v5 - Windows XP (364 KB)	April 28, 2010

Comments or concerns: cce@mitre.org

Obfuscation techniques

- Obfuscation techniques are used by malware to avoid detection and analysis
  - Polymorphism: changing the encryption/decryption routine
    - The malware employs a very large pool of encryption/decryption routines and are much harder to detect using signatures.
    - This high number of encryption/decryption routines is delivered by the use of a mutation engine
  - Metamorphism: changing the virus body but performing the same task
    - using equivalent functions (or code)
    - changing the sequence of codes
    - Inserting unneeded functions (or code)
      - Malware Mutation includes polymorphism and metamorphism
  - entry point obfuscation (EPO)
- The malware can use multiple obfuscation techniques and fragmented call routines to make detection very difficult
- Ref: Aman Hardikar, Malware 101 - Viruses

Malware Mutation

- Malware mutates in order to disguise itself in an effort to evade detection
  - Mutation is common in macro and script malwares, since they are typically interpreted and not compiled
  - The techniques of polymorphism and metamorphism change the form of each instance of software in order to evade pattern matching, i.e. signature detection
    - Malware may change itself every time it replicates
      - Polymorphism and metamorphism result in the automatic creation of large numbers of unique, but functionally identical, files as part of the malware replication process
    - Server-side polymorphism and metamorphism are used by a server that is configured to serve a different version of a file every time it is accessed, typically in an effort to foil detection signatures
    - This can result in hundreds or thousands of unique files with different hash values but identical functionality, which inflates the number of samples

NP-complete

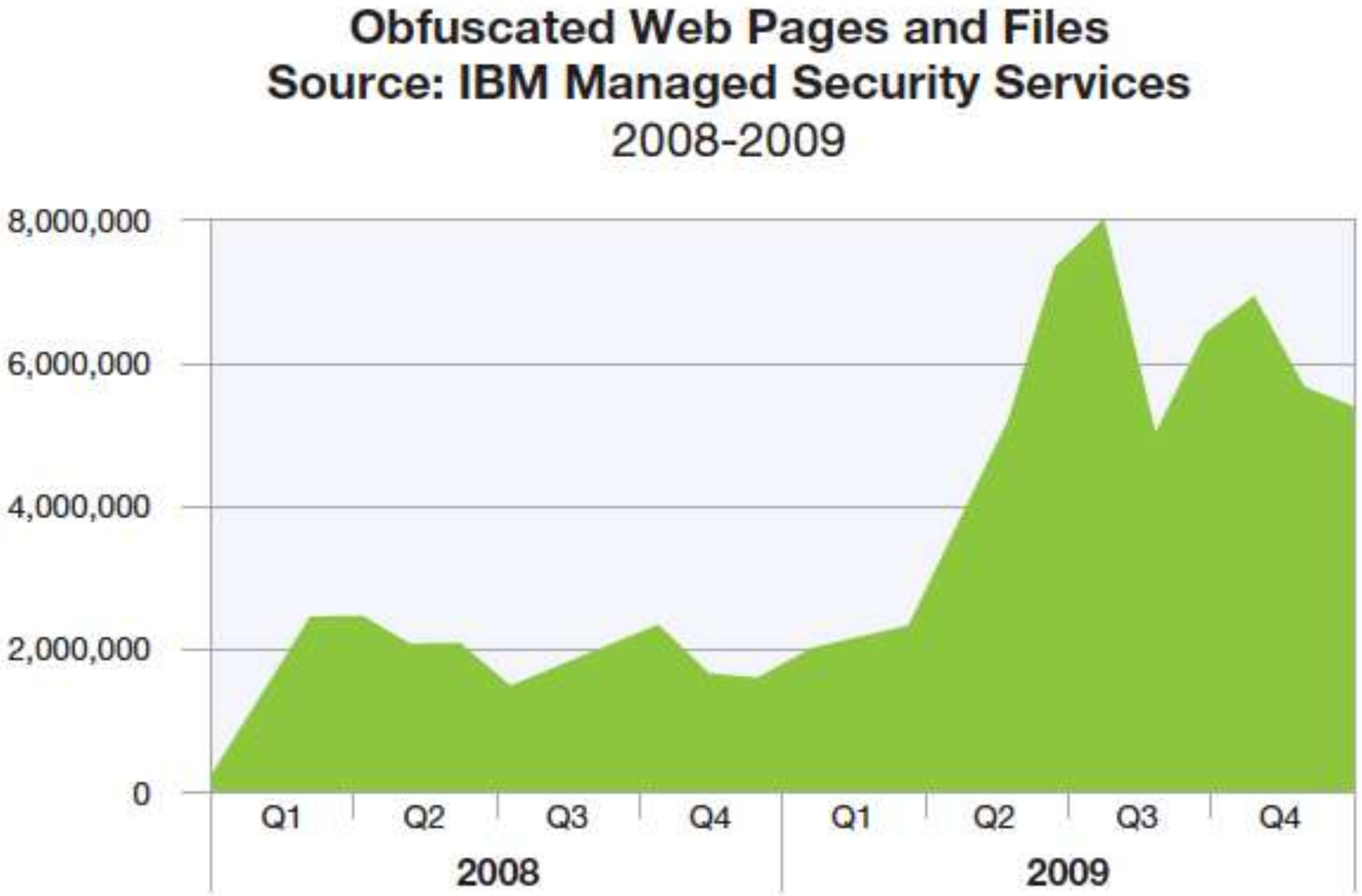
- Spinellis [64] has shown that the detection of mutating size-bounded viruses by signature is NP-complete
- The characteristic of a NP-complete problem is that no solution can be found in polynomial time
- Polynomial time means that the running time of an algorithm has an upper bound set by a polynomial that is the size of the input for the algorithm
- For metamorphic viruses, whose size in unbounded, the result is even worse [65].

Mutation Trend

- Top malware families with more than 1 million unique samples detected in both 1H09 and 2H09
  - The decrease in the Password Stealers & Monitoring Tools category was primarily due to Win32/Lolyda, which declined from 5.7 million samples in 1H09 to less than 100,000 in 2H09
  - This fact also indicates a rapid pace of the malware evolution and their life cycles

Top 5 Family in 1H09	Most Significant Category	Total Samples	Top 5 Family in 2H09	Most Significant Category	Total Samples
Win32/Parite	Viruses	40,932,141	Win32/Parite	Viruses	33,906,946
Win32/Virut	Viruses	15,217,839	Win32/Virut	Viruses	17,376,150
Win32/Agent	Trojans	6,720,422	Win32/Sality	Viruses	10,033,778
Win32/Lolyda	Password Stealers & Monitoring Tools	5,671,251	Win32/Agent	Trojans	6,901,068
Win32/Vundo	Trojans	5,130,143	Win32/FakeXPA	Trojans	5,457,424

Obfuscated web sites and files



Executable Packing/Compression (1)

- Executable packing/compression is also frequently used to deter reverse engineering or to obfuscate the contents of the executable
  - A software vendor wants to protect their code from reverse engineering, while hackers want to hide the presence of malware from anti-malware scanners through the use of proprietary packing methods and/or added encryption
    - Executable packing can be used to prevent direct disassembly, mask string literals and modified signatures
    - Although this does not eliminate the chance for reverse engineering and debugging analysis, it can make the process more difficult and costly
- An executable packer compresses an executable file and combines the compressed data with the decompression code it needs into a single executable

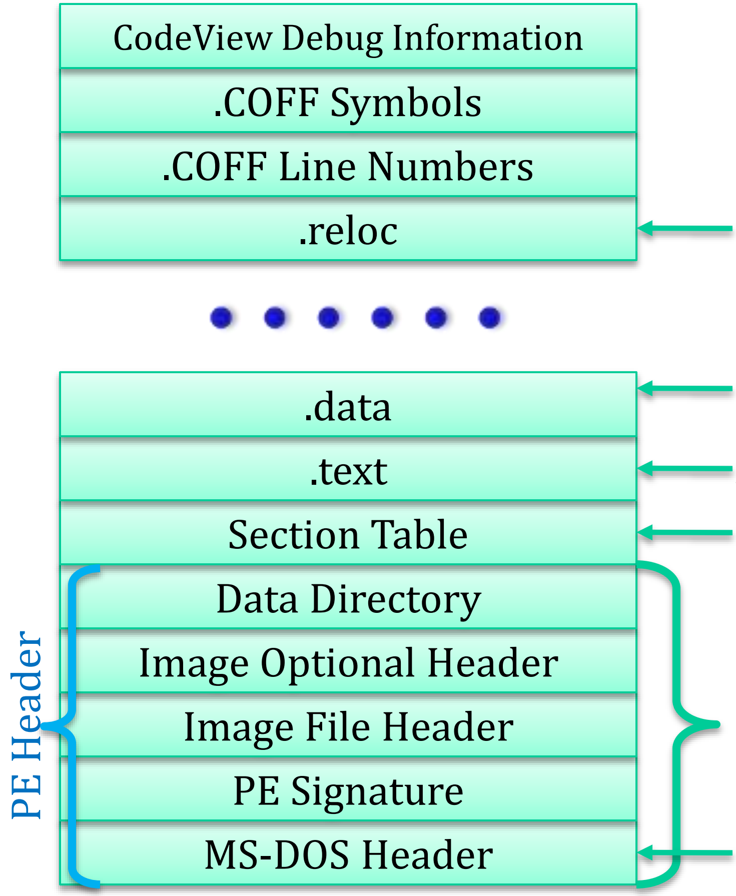
Executable Packing/Compression (2)

- A packed executable is one variety of a self-extracting archive in which compressed data is packaged along with the relevant decompression code in an executable file
  - Executing a packed executable transfers control to it
  - executes the decompression code
  - unpacks the original executable code
  - then runs the unpacked code
- There are free, open-source executable packers, such as UPX, that are widely used by hackers
  - UPX supports Windows Portable Executable (PE) file format, DOS executables, and the Executable and Linkable Format (ELF)
    - ELF is widely used in UNIX, Linux and embedded systems, whereas the old UNIX format is a.out

Windows PE file and Loader

- PE file on disk is very similar to what the module will look like after Windows has loaded it
  - The Windows loader does not need to work extremely hard to create a process from the disk file
  - The loader uses the memory-mapped file mechanism to map the appropriate pieces of the file into the virtual address space
  - Relative Virtual Address (RVA). Many fields in PE files are specified in terms of RVAs. An RVA is simply the offset of another item, relative to where the file is memory-mapped.

PE file format



CodeView Debug Information

.COFF Symbols

.COFF Line Numbers

.reloc

.data

.text

Section Table

Data Directory

Image Optional Header

Image File Header

PE Signature

MS-DOS Header

PE Header

COFF (Common Object File Format)

The .reloc section holds a table of base relocations. A base relocation is an adjustment to an instruction or initialized variable value if the loader could not load the file where the linker assumed it would. If the loader is able to load the image at the linker's preferred base address, the loader completely ignores the relocation information

The .data section contains initialized data. This data consists of global and static variables that are initialized at compile time.

All general-purpose code generated by the compiler or assembler

The section table is essentially a map containing information about each section in the image. The sections in the image are sorted by their starting address (RVAs), rather than alphabetically.

This header contains information such as the locations and sizes of the code and data areas, what operating system the file is intended for, the initial stack size, and other vital pieces of information: the RVA where the file's code sections begin, the RVA where the file's data sections begin, etc.

The MS-DOS stub is a tiny program that prints out something to the effect of "This program cannot be run in MS-DOS mode."

DotFixNiceProtect: packing and mutation engines (1)

- DotFixNiceProtect, a commercial software, provides packing in PE format as well as both polymorphism and metamorphism mutation engines
- NiceProtect also provides the following protection measures:
  - Erase packer signature:
    - The signatures of the most popular packers are erased, which disables the ability to unpack the program automatically
  - Encrypt original entry point:
    - Encrypting part of the code located after the entry point (from 10 to 500 bytes) is translated into metamorphic instructions and then partially compiled into the code that only the Virtual Machine (VM) interpreter understands
    - This option provides the program with protection against identifying the entry point of the protected code and disassembling it
  - Encrypt code section:
    - Protects the code section against disassembling for analysis

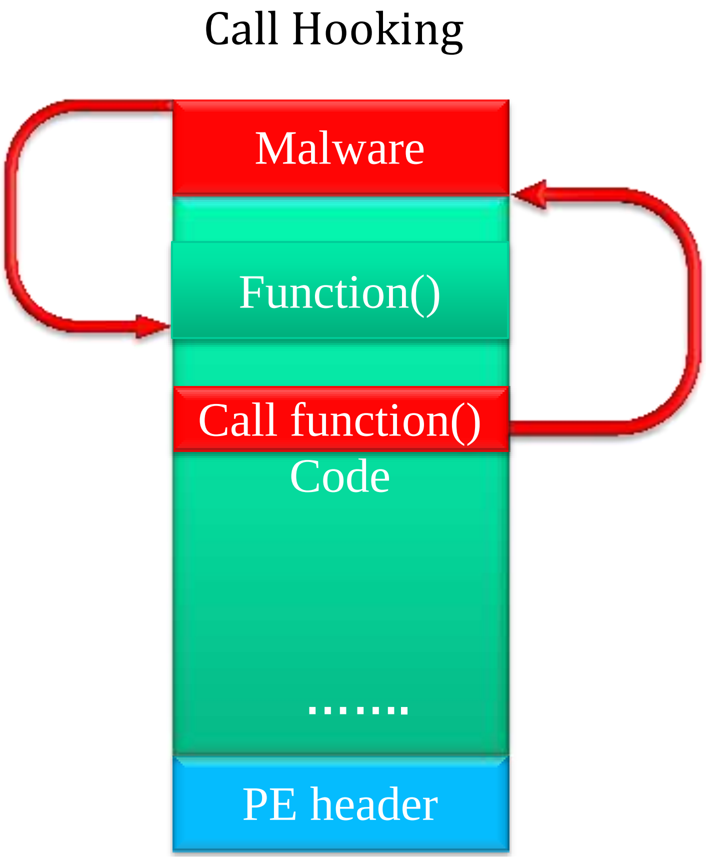
DotFixNiceProtect: packing and mutation engines (2)

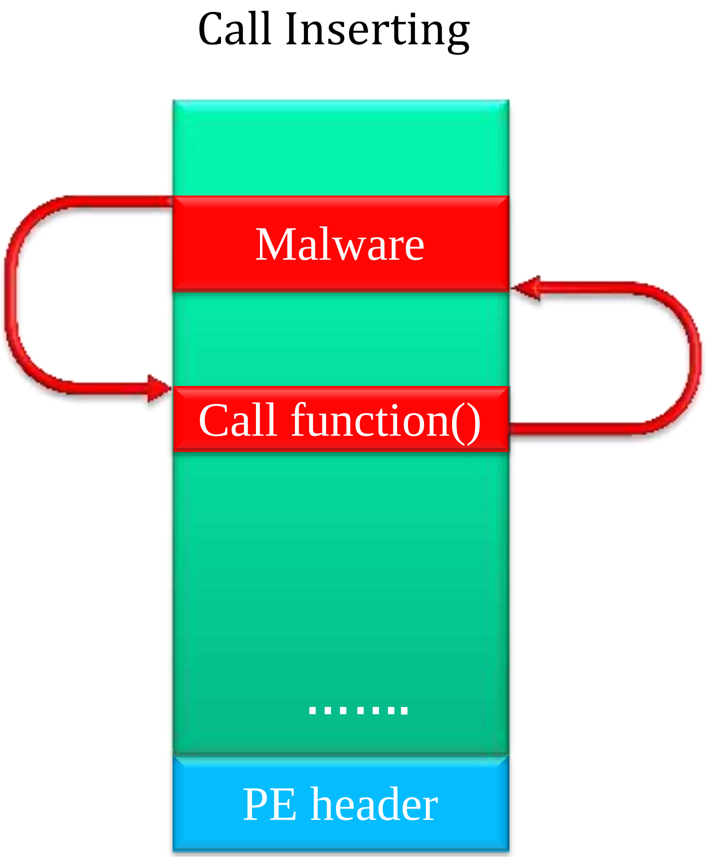
- Virtual Machine:
  - This virtual machine interpreter is built into the packed program and interprets this block of commands
  - It makes detecting malware much more complicated
- Anti-tracing engine:
  - Tracing means debugging the program code step by step
  - This feature prevents the use of tracing malware and thus makes the use of this malware more difficult
- Anti-debug protection:
  - It detects an active debugger in the system and exits the protected program.
- Run-Time Type Information (RTTI) obfuscator:
  - A C++ system, e.g. Visual C++, provides run-time type information about an object's data type in memory at runtime, e.g. simple data types, such as integers and characters, or generic objects
  - The RTTI obfuscator changes all the names of forms, objects, unit declarations as well as the name of events

Entry Point Obfuscation (EPO)

- This type of malware changes a random location in the host file data instead of the changing the headers (PE headers in Windows) or the initial host file data, so that the entry point of the malware is hidden in the host file
  - Call hooking: Using a function call routine to get itself executed: aka call hooking
    - The malware first scans the targeted program code (in .text area of PE) for any function or subroutine calls or for certain APIs
      - For example, a relocation table in PE can be modified to direct control to malware code
    - It then changes one of the subroutine calls to gain execution control and passes the control to the actual subroutine after execution
  - Call inserting: Inserting a subroutine call into the host program code
    - The control is transferred to the malware via an inserted subroutine call that is embedded in the host program code
    - After the execution is complete, the control is transferred back to the host program

Call Hooking and Call Inserting





EPO detection difficulty

- Embedding the call/jump to the malware code deep within a target executable prevents tracing the execution path of an EPO-infected file provides no guarantee that the virus code itself will ever be called
- EPO disables the static detection method of malware, as it removes the ability for a scanner to trace into the virus code with guarantee
- In other words, the scanner is unable to detect its exact location in order to emulate it
- It is also very difficult to clean up an infected host due to the modifications to host programs performed by malware

Polymorphic Malware

- Encrypted malware
  - The malware containing a constant decryptor, followed by the encrypted malware body
  - Relatively easy to detect because decryptor is constant
- Polymorphism includes encryption, and junk instruction insertions
  - Constantly create new random encryption routines of the same malware body
    - Conficker, Marburg (Win95), HPS (Win95), Coke (Win32)
  - Malware includes an mutation engine for creating new keys and new encryptions of the malware body
    - Crypto (Win32) decrypts its body by brute-force key search to avoid explicit decryptor code
  - Decryptor can start with millions of NOPs to defeat emulation
    - Emulation: execute a code in order to tell if it is malicious
      - the anti-malware uses a simulated environment for emulating the execution of instructions in CPU, registers, memory etc.
      - emulating code is significantly slower than executing it on a real CPU

Polymorphism Weakness

- Decryptor may be detected
- If it hides signature of decryptor, one can use *code emulator* to decrypt putative malware dynamically
  - Decrypted malware body is constant
  - Signature detection is possible
- Microsoft proposed a *Dynamic Translation* method for speeding up the execution of emulation involved in decrypting polymorphic malware
  - This method relies on dynamically disassembling the analyzed code and then performing a just-in-time translation, i.e. compilation, code targeted for the host CPU

Conficker.C polymorphic worm (1)

- Conficker.C uses the triple layers of packing, encryption and code obfuscation to further hinder binary detection.
- The Conficker authors hindered detection through code obfuscation by impeding the identification of Windows API calls, which it does using a mapping of obfuscated APIs to code offsets, as well as other code obfuscations to hinder analysis.
- This sophisticated technique provides the Conficker bot with a secure binary updating service that effectively allows them to secure the control of bots.
- It also prevents infected computers from accessing anti-malware vendor and security websites.
- Conficker.C begins obfuscating its presence at the moment its bootstrapping DLL is initialized on the victim host.

Conficker.C polymorphic worm (2)

- Upon initialization, the DLL creates a protected memory segment, and then spawns this segment as a remote thread to the netsvcs or explorer processes, depending on the OS.
- NETSVC.EXE is a command line utility, which allows one to administer, query and display services on a Windows NT workstation or server.
  - It sets the NETSVC display name to nil, does not return from the loadlib initialization function, and effectively prevents standard Windows service utilities from listing its DLL as loaded and active.
- Conficker.C also alters the registry to ensure that its DLL is reloaded at next boot.
  - To cloak its registry key settings, Conficker.C randomly selects and sets various registry keys to obfuscate the modifications that it made to the svchosts or netsvcs registry segments.

Conficker.C polymorphic worm (3)

- Once the process is activated, it stores its DLL under a randomly generated filename with DLL extension, and sets the date of the DLL to that of kernel32.dll.
- The file is then stored on disk in the following manner:
  - first, it attempts to place the DLL in the System32 directory; otherwise, it attempts to place the DLL inside the Program Files directory.
    - Here it attempts to select one of the following subdirectories: \\Movie Maker, \\Internet Explorer, \\Windows Media Player, or \\Windows NT. If both fail, then it places the DLL in the user temp directory.

Polymorphism detection (1)

- Cryptanalysis (X-Ray), dedicated decryption routines, and emulation
  - X-Ray can only handle simple decryptions
  - dedicated routines require significant development effort
  - neither scale well with the number of detected malwares.
- X-Ray scanning targets the encryption by attempting simple, standard decryption algorithms based on simple arithmetic operations and a fragment of decrypted code, which is part of the signature.
  - For a single decryption algorithm, X-Ray computes the encrypted code and decrypted code as a function of the decryption key
  - When the decryption algorithm is simple, X-Ray can be effective
  - In contrast, a dedicated decryption routine is useful in detecting complex and multiple layer encryptions.
    - However, one must analyze the malware and all possible variants in order to detect it.
    - This approach is not feasible for defense against the current polymorphic malware.

Polymorphism detection (2)

- Heuristic-based recognition provides protection against new and unknown threats, but is usually time consuming and may fail to detect new malicious executables.
- Heuristic methods can be either static or dynamic.
  - Static heuristics can be based on an analysis of the file format and the code structure of the malware fragments.
  - Dynamic heuristics use code emulation to simulate the processor and operating system and detect suspicious operations while the malware code is executed on a virtual machine.

Polymorphism detection (3)

- Code emulation executes the malware in a small virtual machine in attempt to find the end of the decryption routine included.
  - But it is difficult to reliably halt the execution of the malware when the decryption is complete.
  - Therefore, emulation uses a sandbox around untrusted programs and executes the suspect programs in a restricted environment where the malicious software can be executed and detected with no harm to the file system.
- A code emulator can dynamically decrypt a putative malware regardless of the type and numbers of the encryption algorithms and layers.
  - During execution in the emulator, the malware scanner checks the program's memory image against its signature database, in addition to heuristic analyses, after a decryption is assumed complete.
    - When the decrypted malware body is constant, signature detection is possible through comparisons.
    - A memory content hash is one way of detecting a known signature.
    - String scanning, which scans the particular files for common substrings that are only found in specific malware, is more accurate than checking hash.
    - Smart scanning is a special form of wildcard scanning that omits irrelevant parts of the inspected file, such as obvious junk code used to combat mutation.

Polymorphism detection (4)

- Because a virtual machine is complicated, the anti-malware uses a simulated environment for emulating the execution of instructions in CPU, registers, memory etc.
  - emulating code is significantly slower than executing it on a real CPU.
  - Therefore a very complex polymorphic malware would take unreasonably long to emulate until it is decrypted.
  - For example, it is infeasible to detect Win32.Crypto using an exhaustive search for a decryption key.
- Microsoft proposed a *Dynamic Translation* method for speeding up the execution involved in decrypting polymorphic malware
  - This method relies on dynamically disassembling the analyzed code and then performing a just-in-time translation, i.e. compilation, code targeted for the host CPU.
  - The translated code obtained can be safely executed on the host CPU, with little degradation in execution speed, when compared to the original code.
  - This approach provides the same flexibility as emulation, but the execution speed is dramatically improved.
  - The detection of the precise moment for completing the decryption is still an open, challenging issue.

Polymorphism detection (5)

- Newsome, Karp, and Song proposed *polygraph*, an algorithm to automatically generate signatures for polymorphic worms.
  - They found that even though polymorphic worms change the payload dynamically, certain contents may not be changed.
  - Polygraph leverages the insight that in order for a real-world exploit to function properly, multiple invariant substrings must often be used in all variants of a payload; these substrings typically correspond to protocol framing bytes, e.g., GET and HTTP protocol indicator, as well as values used for a return address or a pointer to overwrite a jump target.
  - For instance, some malware may obtain a decryption key from certain Internet domains.
- Polygraph can generate signatures as tokens that consist of multiple disjoint content substrings.
  - The system generates tokens automatically and detects worms based on these tokens.

Polymorphism detection (6)

- Geometric detection, which is another approach, is based on the file geometry and the execution flow geometry, if it is tailored to specific malware families.
- More generic detections are based on typical malware heuristics, such as entry points in the last section of the infected file, suspicious code flow redirections, or inconsistent file header values
- The probability of detecting a file-infecting malware that morphs into a host program is an even more difficult task but can be improved by better scanning for typical anomalies in executable files, i.e. changes to the host program of specific file-infecting malware or unusual layout inside the malicious programs themselves

Metamorphism (1)

- Cloned malware/worm can be detected
  - Common signature on every copy
  - Detect once, detect everywhere (DODE)
- “Good” metamorphic software…
  - Mitigate buffer overflow attacks
- Malware
  - Avoid malware/worm signature detection
- Metamorphic malware
  - Each copy has different signature
  - Same detection does not work against every copy
  - Analogous to genetic diversity in biology
  - Source: M. Stamp and W. Wong, “Hunting for metamorphic engines,” www.cs.sjsu.edu/faculty/stamp/ppt/metamorphic.ppt

Metamorphism (2)

- Mutate malware body
  - malware needs to find an installed compiler or assembler in the targeted host in order to compile itself
    - Unix/Linux machines have C compilers installed by default
    - An assembler may be in the malware body
  - malware mutates its source and recompiles itself
    - New mutated binary looks completely different
- Mutation techniques:
  - permutation of subroutines
  - insertion of garbage/jump instructions
  - substitution of instructions

Metamorphic code generation

- Disassembles the viral code into an intermediate form, independent of the CPU and OS
- Shrinks the intermediate form, by removing the redundant and unused instructions
  - Earlier replications added these instructions to interfere with the disassembly by antivirus
- Permutates the intermediate form
  - register swapping
  - code substitution
  - reordering subroutines
  - separating blocks of code and linking them with jump instructions
  - Code Insertion
  - New metamorphic instructions
- Expands the code, by adding redundant and unused instructions
- Reassembles the intermediate form into a final native form that will be added to infected files

Metamorphic Methods

- Code Insertion
  - This is one of the most complex methods
  - The malware weaves itself into the binary code of its host
  - Entry Point Obfuscation (EPO)
    - malware will patch the target executable in the middle of its execution train with jump/call instructions and receive control
    - hijacking some functions from the import address table
    - EPO will fool the scanner that looks for a modified entry point as part of its heuristics engine
    - W32.Bolzano

- New metamorphic instructions
  - Part of the malware located after the entry point (from 10 to 500 bytes) is translated into metamorphic instructions and then partially compiled into the code that only the VM interpreter can understand
  - This interpreter is built into the packed program and interprets this block of commands

Metamorphic methods

Name	Description
Register Swapping	While all x86 CPU registers were designed with specific instructions and resultant optimizations in mind, they can also be used interchangeably as is the case in the Win95/Regswap virus.
Code Substitution	Switching instructions for equivalent variants that will result in a different binary code but accomplish the same task. For example, the call to a subroutine can be replaced by push registers and a jump to a subroutine, i.e. xor/sub and test/or instructions can be easily interchanged.
Branch Condition Reversing	Stateless reordering of branch conditionals.
Subroutine Reordering	Moving the order of subroutines so that they are called in a random order, thus adding a layer of complexity equal to n!, where n denotes the number of routines reordered.
Code Insertion	This is one of the most complex methods in which the malware will actually weave itself into the binary code of its host. Entry Point Obfuscation (EPO) is a technique used by malware authors to dissuade anti-malware scanners from investigating the files that have been invaded. EPO-enabled malware will patch the target executable somewhere in the middle of its execution train with jump/call instructions and receive control in that manner. By doing this, EPO will fool the scanner that looks for a modified entry point as part of its heuristics engine.
New metamorphic instructions	Part of the malware located after the entry point (from 10 to 500 bytes) is translated into metamorphic instructions and then partially compiled into the code that only the VM interpreter can understand. This interpreter is built into the packed program and interprets this block of commands.

Metamorphic Malware

- Example:
  - W32.Evol is the first 32-bit metamorphic virus
    - using a 32-bit true metamorphic engin
    - replicate on Windows 9x as well as Windows NT and 2000
  - PE_MERGORY.A (Windows 95 to XP)
    - It appends its code to .EXE and .SCR (Script) host files located in the Windows system and current folder
    - metamorphic engine differentiates the code of each infected file
    - The generation of a unique code corrupts the said file, thus the host code fails to execute
- Mutation is common in macro and script viruses
  - Macros/scripts are usually interpreted, not compiled

Creating polymorphic/metamorphic viruses by toolkit

- VX Heavens (http://vxheavens.com/): lists well over a hundred virus generation toolkits
- NGVCK (Next Generation Virus Creation Kit)
  - all created viruses are completely different in structure and opcode
  - impossible to catch all variants with one or more scan strings
- G2 (Second Generation virus generator):
  - different viruses may be generated from identical configuration files
- PS-MPC (Phalcon/Skism Mass-Produced Code) generator
  - Not only polymorphic, but their decryption routines and structures change in variants
- MPCGEN (Mass Code Generator)
- OverWritting Virus Construction Toolkit
  - The perfect choice for beginners

Suggestions

- Demo: use toolkits to generate code to escape IDS
- A good paper: CODE OBFUSCATION AND VIRUS DETECTION
  - http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&sqi=2&ved=0CEUQFjAF&url=http%3A%2F%2Fwww.cs.sjsu.edu%2Ffaculty%2Fstamp%2Fstudents%2Fashwini_venkatesan_cs298report.doc&ei=VfIWT63pF9STtwfL8MWGAw&usg=AFQjCNGKFjUaG_JEDVWIVcn144lf_RdPeA&sig2=YAsqs-UwmpzIOVxZ5Cj4BQ
- METAMORPHIC VIRUSES WITH BUILT BUFFER OVERFLOW
  - http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&sqi=2&ved=0CFAQFjAG&url=http%3A%2F%2Fwww.cs.sjsu.edu%2Ffaculty%2Fstamp%2Fstudents%2Fshah_ronak.pdf&ei=VfIWT63pF9STtwfL8MWGAw&usg=AFQjCNGKlP5ZwgQmXPIOSwwluTXbd3q8Zw&sig2=E-o3qxXjk_qlWyjxiBS8xQ

Example of a combined polymorphic and metamorphic virus

- Win32/Simile: March 2002
  - highly obfuscated
  - decryptor, whose location in the file is variable, allocates a large chunk of memory (about 3.5 Megabytes)
  - then proceeds to decipher the encrypted body in a most unusual manner
    - to avoid triggering some of the decryption-loop recognition heuristics: it decrypts the encrypted data in a seemingly random order rather than going through the encrypted data linearly
- Source: Symantec, “Striking Similarites: Win32/Simileand Metamorphic Virus Code, “

Impeding analysis and detection (1)

- The W32.Waledac binary is packed by several packers to hinder analysis and detection
- Anti-unpacking techniques are functionalities that are employed by the packer to prevent the binary from being unpacked.
  - The first layer of packing on Waledac is a freely available packer (UPX), and the second layer is a custom packer.
  - During the unpacking process for the second layer of packing, the malware gradually reconstructs the instructions of the core program and passes control to it.
  - The unpacked instructions are written in stages, so that the same memory location can change among several values before it is finally assigned the correct value.
  - These writing cycles are interspersed with other instructions, most of which aim to complicate the manual unpacking process

Impeding analysis and detection (2)

- Code obfuscation is achieved with a large number of jump instructions that frequently redirect code execution along with several call chain loops.
  - Call chain loops start within a function that contains a call to another function, which in turn calls another function until a call is made to the initial function, completing the loop.
    - Most of the functions in the loop do not actually make use of a return instruction to return the execution back to the function that called them.
      - Instead, they just keep calling the next function in the loop and pass control to it.
    - This hampers some function analysis because there is no return instruction marking an exit point for analysis
- anti-debugging functions
  - detect stepping that is being done by a debugger.
  - If detected, Waledec creates a code path that eventually leads to an invalid instruction.

Counter metamorphic malware

- All known metamorphic techniques can be thwarted by the use of an emulator coupled with heuristics capable of coalescing the effects of multiple instructions into a sequence of actions
- Chronological order of actions
  - This "ordering" information can be crucial in discriminating between a sequence of actions which is viral, and a sequence of actions which is harmless
  - Hidden Markov models (HMMs) that trained to recognize the sequence of actions are effective (source: "Hunting for metamorphic engines,")
- Source: Myles Jordan, "Anti-Virus Research - Dealing with Metamorphism," http://www.ca.com/us/securityadvisor/newsinfo/collateral.aspx?cid=48051

Profit is the motivation (1)

- Profit-driven cyber criminals have replaced high school script kitties
  - No more fighting for bragging rights
  - Lay low with pin point accuracy for profits
- New generation of malware tools utilized in a powerful underground economy
- Consumer Reports estimates that U.S. consumers lost more than $7 billion over the last two years (2005-2006) to viruses, spyware, and phishing schemes
- Source: ConsumersUnion.org, August 6, 2007, “U.S. Consumers Lose More Than $7 Billion to Online Threats,” Consumer Reports,” https://secure.consumersunion.org/site/Advocacy?JServSessionIdr007=jkjuzxI2t1.app43a&cmd=display&page=UserAction&id=1799.

Profit is the motivation (2)

- Cyber criminals are presently selling bank accounts and credit card numbers
  - bank account : the most frequently advertised item observed on underground economy servers
  - bank account details $10 to $1,000
    - depending on the amount of funds available and the location of the account
    - Bank accounts that included higher balances, such as business accounts, and EU accounts, were advertised for considerably more
    - bank accounts that bundled in personal information such as names, addresses and dates of birth were advertised at higher prices
  - Source: The Economic Times, May 4, 2008, "Credit Card Numbers Up for Grabs at Rs 16," http://economictimes.indiatimes.com/ rssarticleshow/msid-3009404,prtpage-1.cms.
- Symantec observed an 86 percent increase in potential banking Trojan infections in the second half of 2007

Profit is the motivation (3)

- Credit card numbers for $0.40 to $20 (USD)
  - Credit cards were the second most commonly advertised item on underground economy servers during this reporting period, accounting for 13 percent of all advertised goods
  - This was a decrease from 22 percent in the first six months of 2007
    - The decrease in credit cards being advertised may be due to the recent high-profile reports on lost credit card data, such as the TJX loss
      - TJX breach: credit card number stolen through wireless networks
    - consumers and credit card companies may be more diligent in monitoring customers' credit card activities and quicker to inform customers of suspicious transactions

Profit is the motivation (4)

- A black market for zero-day vulnerabilities has emerged that has the potential to put them into the hands of criminals and other interested parties
  - Zero-day flaws in the Windows kernel can easily cost upwards of $10,000 in the underground market
  - malware such as Trojan horses used to steal online account information can fetch $1,000-$5,000 (USD)

  Source: Byron Acohido and Jon Swartz, USA TODAY "Cybercrime flourishes in online hacker forums," October 11, 2006, http://www.usatoday.com/tech/news/computersecurity/ infotheft/2006-10-11-cybercrime-hackerforums_x.htm.
- Yaneza of Trend Micro has linked Storm and other botnets with the Russian Business Network (RBN), a shadowy network of malicious code and hacker hosting services
  - RBN pulled up stakes and moved most of its operations/services to servers based in China and Asian countries
  - avoid attention and possible action by law enforcement

Profit is the motivation (5)

- The significant increase in new threats indicates the increasing professionalization of malicious code and the existence of organizations that employ programmers dedicated to the production of these threats
  - As these groups of programmers must be paid, professionally written malicious code requires a profit return
  - It is in the interests of these organizations to constantly produce new threats to infect the largest number of computers
  - Many of these threats can be used for financial gain by performing actions such as stealing confidential information that can be sold online

Sensitive information

- Between July 1, 2007 and June 30, 2008, Symantec monitored 44,752 unique samples of sensitive information publicly posted on underground economy servers, which accounted for 10 percent of the total distinct messages (source: http://www.symantec.com/business/theme.jsp?themeid=threatreport)
- The distribution of the sampled sensitive information:

2009 Rank	Name	2009	2008	2007	Range of Prices
1	Credit card information	19%	32%	21%	$0.85–$30
2	Bank account credentials	19%	19%	17%	$15–$850
3	Email accounts	7%	5%	4%	$1–$20
4	Email addresses	7%	5%	6%	$1.70/MB–$15/MB
5	Shell scripts	6%	3%	2%	$2–$5
6	Full identities	5%	4%	6%	$0.70–$20
7	Credit card dumps	5%	2%		$4–$150
8	Mailers	4%	3%	5%	$4–$10
9	Cash-out services	4%	3%	5%	$0–$600 plus 50%–60%
10	Website administration credentials	4%	3%		$2–$30

Attack Tactics

- Multistage attacks
  - staged downloaders consisting of an initial Trojan, e.g., Trojan.Farfli, designed to establish a beachhead
    - Additional threats can be downloaded and installed in the compromised host for next stage of attack
      - These threats allow an attacker to change the downloadable component to any type of threat that meet next objectives
      - For example, if the targeted computer contains no data of interest, the attacker can install a worm/trojan to attack other hosts
      - As the attacker's objectives change, change any later components that will be downloaded to perform the requisite tasks
- Attributed to the continuing increase in new Trojans
  - Since the initial stage usually involves minimal functionality, it is relatively easy for attackers to create numerous variations of these simple Trojans
  - The concentration of Trojans in North America may be indicative of enterprises and ISPs taking more active steps to prevent the propagation of worms

Attacks to a region

- Keep a low profile attack to avoid detection for a longer period
- Farfli Trojans was written to target a certain group of users that are using two browsers developed and maintained by Chinese companies
- Changes the search settings to use a popular Chinese search engine
- Author of the Trojan is specifically targeting Chinese users

Phishing Kits

- In March 2008, over 400 phishing kits designed to generate phishing sites were targeting top Web 2.0 and other popular sites
  - i.e., social networking, video sharing, and VoIP sites, free email service providers, banks, and popular e-commerce Web sites
- Source: Trend Micro Threat Roundup and Forecast—1H 2008, June 2008

Rapidly evolving tactics

- Three phishing toolkits were responsible for 26 percent of all phishing attacks observed by Symantec in the second half of 2007
- This is a decrease from the first half of 2007, when three phishing toolkits were responsible for 42 percent of all phishing attacks
- Two of the three most prevalent phishing toolkits from the first half of 2007 were no longer commonly used in the second half of the year
- The rapid change in preferred toolkits is likely driven by a need for phishers to adapt and constantly change the toolkits to avoid detection by anti-phishing software

Phishing activity distribution by sector

Sector	2009	2008	2007
Financial	74%	79%	83%
ISP	9%	8%	7%
Retail	6%	4%	4%
Insurance	3%	2%	2%
Internet community	2%	2%	2%
Telecom	2%	2%	<1%
Computer hardware	1%	1%	1%
Government	1%	1%	1%
Computer software	<1%	<1%	1%
Transportation	<1%	<1%	1%

Source: Symantec Global InternetSecurity Threat Report

The top five brands of phishing targets for the first half of 2008

January	Attack #	February	Attack #	March	Attack #	April	Attack #	May	Attack #
PayPal	757	PayPal	852	eBay	1333	HSBC	1499	PayPal	382
eBay	739	eBay	612	PayPal	1216	NatWest	1497	Wachovia	303
Regions Bank	662	Citibank	355	Halifax Bank	431	eBay	1207	eBay	216
Citibank	545	Bank of America	291	Wachovia	359	PayPal	1125	Bank of America	149
Abbey National PLC	512	Posteitaliane	251	Citibank	334	Wachovia	697	Royal Bank of Scotland	142

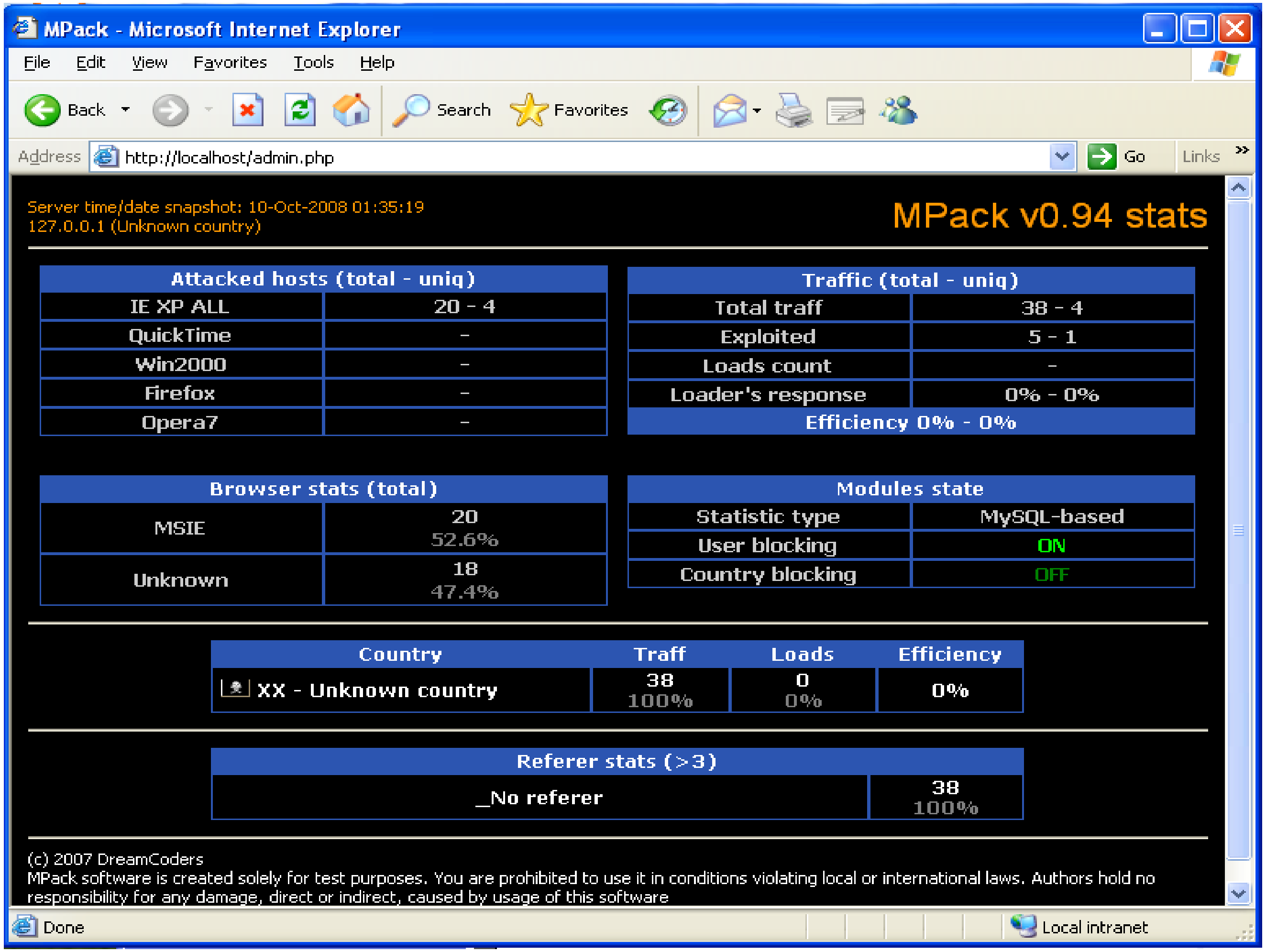
Automated web-based attack package

- The Russian Business Network is one organization that is highly effective in its exploitation efforts
  - Source: . "Russian Business Network Study," http://www.bizeul.org/files/RBN_study.pdf
- Research was performed on the tools they employ
  - MPack
  - These tools allow automatic exploitation of vulnerable systems
  - When a user visits a malicious site, MPack analyzes them for vulnerabilities, and automatically exploits vulnerabilities in its set
    - Source: . Vincente Martinez, "MPack Uncovered," http://pandalabs.pandasecurity.com/blogs/images/PandaLabs/2007/05/11/MPack.pdf
  - Research shows more than 100,000 computer were infected utilizing Mpack
    - Source: Luis Corrons, "MPack uncovered," http://pandalabs.pandasecurity.com/archive/MPack-uncovered_2100_.aspx
  - Other similar tools identified include IcePack, FirePack, n404, Neosploit, and Zeus

MPack Attack Set

Microsoft Security Bulletin	Name
ms06_014	Internet Explorer (MDAC) Remote Code Execution Exploit
ms06_044	Microsoft Management Console Vulnerability
ms06_055	Vulnerability in Vector Markup Language
ms06_071	Vulnerability in Microsoft XML Core Services
ms06-006	Windows Media Player Plug-in EMBED Overflow

Mpack control console



MPack - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://localhost/admin.php Go Links
Done
Local intranet

Server time/date snapshot: 10-Oct-2008 01:35:19
127.0.0.1 (Unknown country)

MPack v0.94 stats

Attacked hosts (total - uniq)	
IE XP ALL	20 - 4
QuickTime	-
Win2000	-
Firefox	-
Opera7	-

Traffic (total - uniq)	
Total traff	38 - 4
Exploited	5 - 1
Loads count	-
Loader's response	0% - 0%
Efficiency 0% - 0%	

Browser stats (total)	
MSIE	20 52.6%
Unknown	18 47.4%

Modules state	
Statistic type	MySQL-based
User blocking	ON
Country blocking	OFF

Country	Traff	Loads	Efficiency
XX - Unknown country	38 100%	0 0%	0%

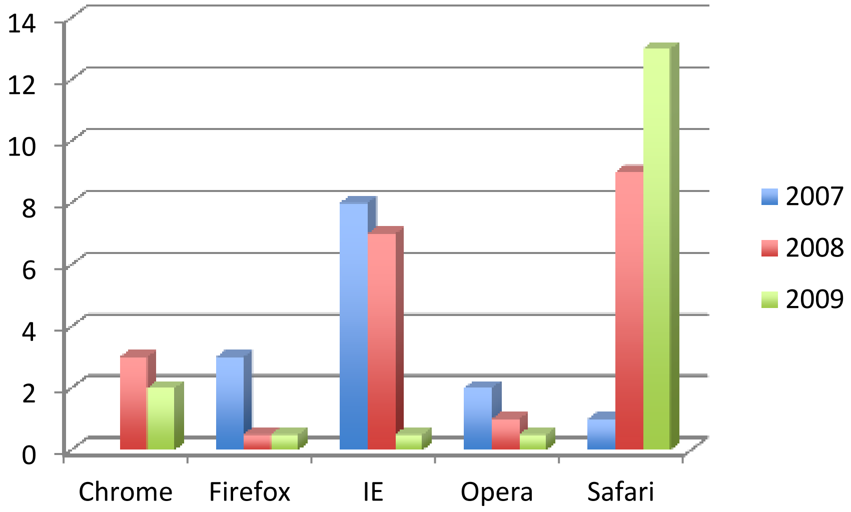
Referer stats (>3)	
_No referer	38 100%

(c) 2007 DreamCoders
MPack software is created solely for test purposes. You are prohibited to use it in conditions violating local or international laws. Authors hold no responsibility for any damage, direct or indirect, caused by usage of this software

Zero-day vulnerability

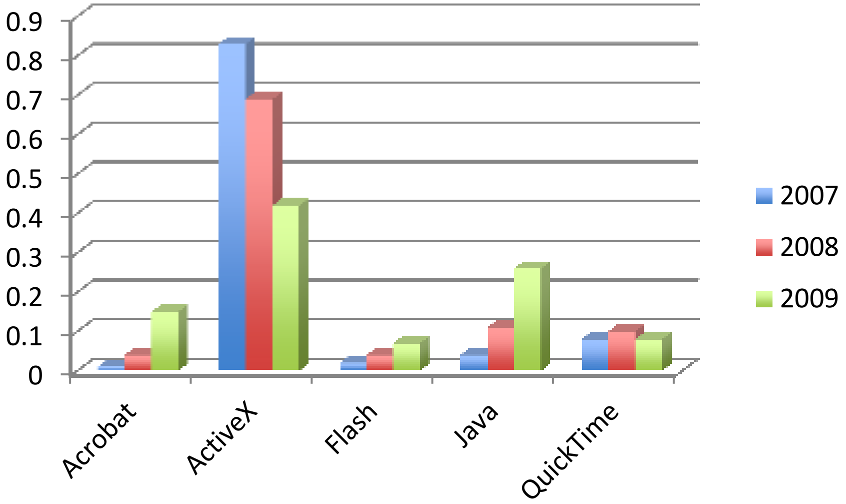
- May not be known to the vendor prior to exploitation
  - No released patch at the time of the exploit activity
  - Zero-day vulnerabilities likely will be able to evade purely signature-based detection
- May be used in targeted attacks and in the propagation of malicious code
  - Raytheon detected 138 zero-day attacks against some 5,000 employees in 2010
  - Symantec documented
    - nine zero-day vulnerabilities in the second half of 2007
      - All the zero-day vulnerabilities documented during this period targeted third-party applications for Microsoft Windows
      - Eight of the nine zero-day vulnerabilities were also client-side in nature, the majority of which affected ActiveX components
    - six in the first half of 2007
      - a portion of the zero-day vulnerabilities affected Microsoft Office

Zero-Day attacks: Window of Exposure for Web browsers



Source: Symantec Global Internet Security Threat Report

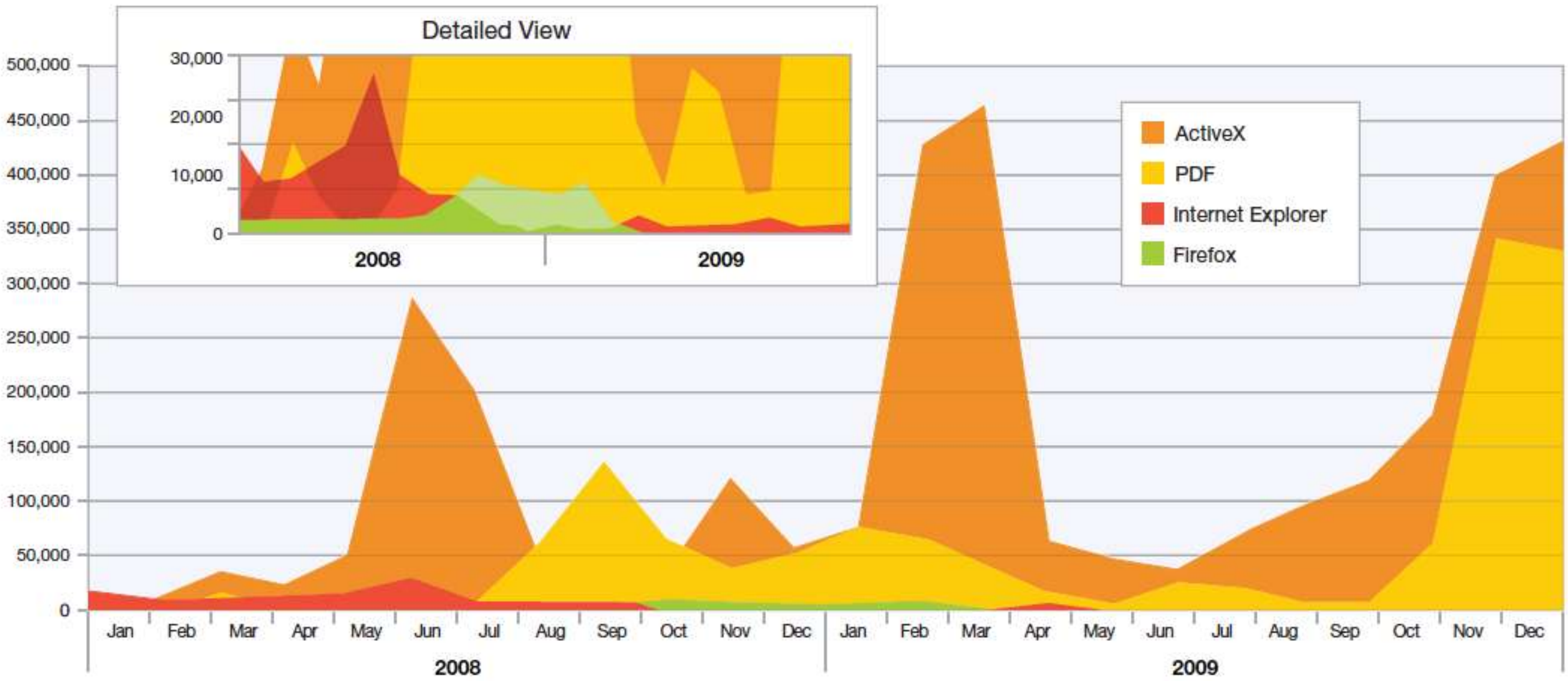
The distribution of vulnerabilities in common browser plugins



The volume of attacks is a different story

The number of monthly attacks using ActiveX, PDF, IE & Firefox

Browser and PDF Exploitation
Source: IBM Managed Security Services
2008-2009



Low-profile zero-day attacks in a region

- Once an avenue of attack has proven successful, attackers often search for similar vulnerabilities in the same types of applications popular in one region
  - an active community of attackers based in a region focusing on users within their own region instead of exploiting vulnerabilities with a higher profile on the global scale
- Balance between vulnerabilities that affect a large user base versus lower profile issues that are less likely to draw public attention
- High profile vulnerabilities are more likely to be patched or mitigated by organizations,
- Lower profile vulnerabilities will remain unpatched for a longer period

Protect against zero-day vulnerabilities

- Deploy network and host-based IDS/IPS
  - Anomaly-based methods
- Regularly updated antivirus software
- Security vendors may provide rapid response to recently discovered zero-day vulnerabilities in the wild

Attacks to Power Grids 1/18/08

- CIA Confirms Cyber Attack Caused Multi-City Power Outage On 1/18/2008
  - "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."
- Attack avalanches!

Power grid is found susceptible to cyber attack

- Advanced Metering Infrastructure (AMI) Smart Grid systems use a variety of low-power processors along with custom-designed firmware and operating systems and can be equipped with a variety of wireless protocols, which can give attackers different ways to break into the systems
- In 2007 Goodspeed demonstrated that it was is possible to write a worm that would spread among Msp 430 chips, which are processors used by some Smart Grid device makers
- IOActive researchers confirmed a number of the theoretical vulnerabilities identified by Goodspeed, who has researched vulnerabilities in the Texas Instruments MSP430 chip used by some Smart Grid devices

Source: 3/23/2009, http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Security&articleId=9130178&taxonomyId=17&pageNumber=2

Malware in Power Grid

- The hackers who reportedly planted malware on key parts of the U.S. electrical grid, perhaps with the intent to cripple the country's power infrastructure, most likely gained access like any other cybercriminal -- by exploiting a bug in software such as Windows or Office in PCs connected to the Internet, a security researcher said 4/8/2009
- Hackers from China, Russia and elsewhere have penetrated the U.S. power grid, extensively mapped it, and installed malicious tools that could be used to further attack not only the electrical infrastructure, but others as well, including water and sewage systems
- *The Wall Street Journal*: The discoveries were made by U.S. intelligence agencies, not the utilities' security teams 4/8/2009
  - http://online.wsj.com/article/SB123914805204099085.html

Source: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131297&source=NLT_PM

Hackers penetrating industrial control systems (1)

- Stuxnet: World's most sophisticated malware ever
  - Discovered in 2010
    - aimed at industrial Supervisory Control and Data Acquisition (SCADA) systems
  - Stuxnet is designed to attack the Siemens Simatic WinCC SCADA system
    - These SCADA systems are installed in big facilities (like nuclear plants and utility companies) to manage operations
    - Step 7 is the Siemens software used to program and configure the German company's industrial control system hardware
- Stuxnet works by infecting Windows machines
  - It uses four zero-day vulnerabilities
    - One zero-day is used to spread the worm to a machine by a USB stick.
    - A Windows printer-spooler vulnerability is used to propagate the malware from one infected machine to others on a network
    - The last two help the malware gain administrative privileges on infected machines to feed the system commands
  - The Step 7 propagation vector would insure that already-cleaned PCs would be re-infected if they later opened a malicious Step 7 project folder

Duqu (1)

- 10/1/2011
- Duqu and Stuxnet share a lot of common code and functions.
  - While Stuxnet binaries have been floating around for some time, the actual source code itself has not been publicly available. The fact that Duqu contains Stuxnet code has led some to believe that Duqu's authors either have direct access to Stuxnet code -- or were the authors of Stuxnet. Duqu also uses an installation driver that is signed using a stolen or forged digital certificate belonging to a Taiwanese company called JMicron. Stuxnet used certificates belonging to the same company.
- Duqu appears designed to steal information from vendors of industrial control systems. It is an intelligence-gathering agent. Stuxnet on the other hand was designed to cause actual physical damage to industrial control systems. Security vendor Symantec and others believe that Duqu is being used to steal information that can eventually be used to craft another Stuxnet.

Duqu (2)

- Duqu infects systems in ways that are not entirely understood yet. In one instance, a Duqu installer took advantage of a zero-day kernel-level vulnerability in Microsoft's Win32k TrueType font parsing engine to install the malware on a vulnerable computer. The malware was delivered via a malformed Word document that was sent to the target organization as an email attachment. Clicking on the document causes the exploit to be triggered.
- Once installed, the malware communicates with a command-and-control server, which then instructs it to download additional data stealing malware or to spread itself via network shares to other computers on the same network. Duqu is not designed to propagate on its own. It is also programmed to delete itself from an infected computer after 36 days.
- Stolen data is encrypted and then sent out to the C&C servers as JPG image files.

Hackers penetrating industrial control systems (2)

- Joseph Weiss, managing partner of control systems security consultancy Applied Control Solutions, didn't detail the breach that caused deaths during his testimony before a U.S. Senate committee, but he said he's been able to find evidence of more than 125 control systems breaches involving systems in nuclear power plants, hydroelectric plants, water utilities, the oil industry and agribusiness.
- "The impacts have ranged from trivial to significant environmental damage to significant equipment damage to deaths," he told the Senate Commerce, Science and Transportation Committee. "We've already had a cyber incident in the United States that has killed people."
- Weiss has talked about a June 1999 gasoline pipeline rupture near Bellingham, Wash. That rupture spilled more than 200,000 gallons of gasoline into two creeks, which ignited and killed three people. Investigators found several problems that contributed to the rupture, but Weiss has identified a computer failure in the pipeline's central control room as part of the problem.
- (source: 3/20/09 http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130080&source=NLT_AM)

Security Issues in Information Infrastructure

- Information sharing are global
  - Increased exposure, easier to cover tracks
  - Multiple organization must closely share critical information
- Feature-rich systems are poorly developed for security
  - Web 2.0/AJAX have too many weakness
- Implementations are impossible to consider all possibilities
  - Buffer overflows are the "IED"
- Protocol implementation weakness
  - DNS
  - Older version of SSL, SSH, Sendmail, FTP etc.
- Many attacks are not even technical in nature
  - Phishing, impersonation, social engineering, etc.

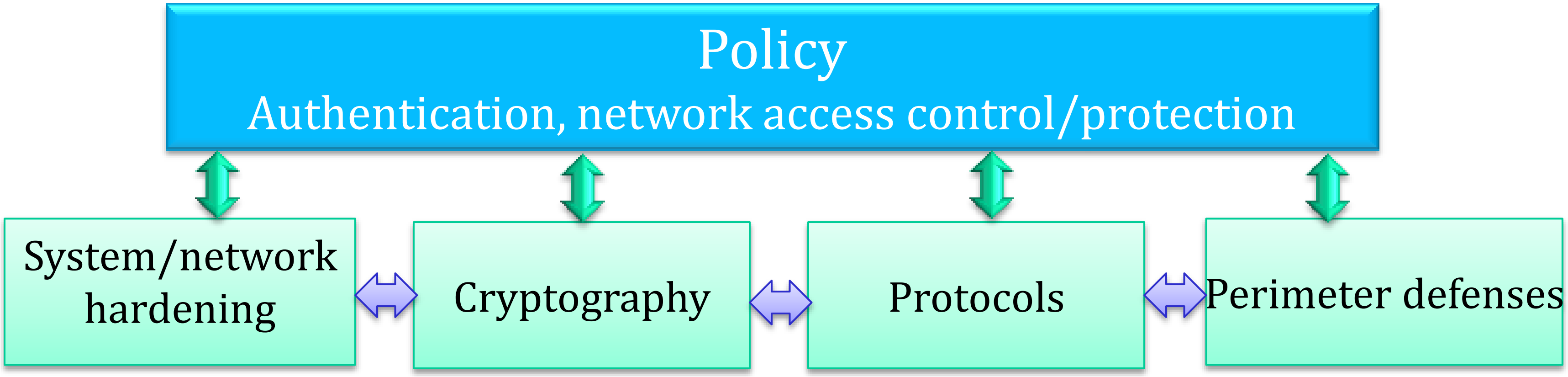
Security Mechanisms (1)

- Hardening of OS and applications using configuration in
  - smartphones/computers/servers
  - switches and routers
- Patch OS and applications by security updates
- Local, domain and public security policy for
  - smartphones/computers/servers/users
  - access control/protection
- Cryptography
  - Cryptographic hash functions for authentication
  - Symmetric encryption
  - Public-key infrastructure and certificates
  - Pseudo-random generators to ensure freshness and stop replaying
- Authentication and key establishment within a domain
  - Kerberos

Security Mechanisms (2)

- IP security
  - IPSec protocol suite: Virtual private tunnel
- Web/ transport security
  - SSL/TLS (Transport Layer Security): Virtual private tunnel
- Perimeter security
  - Firewall
    - Host-based
    - Network-based
  - Intrusion detection/prevention system (IDS/IPS)
    - Host-based
    - Network-based

Network and Information Infrastructure Defenses



Policy

Authentication, network access control/protection

System/network hardening

Cryptography

Protocols

Perimeter defenses

Configuration, anti-malware, security patches, host intrusion prevention, host firewall

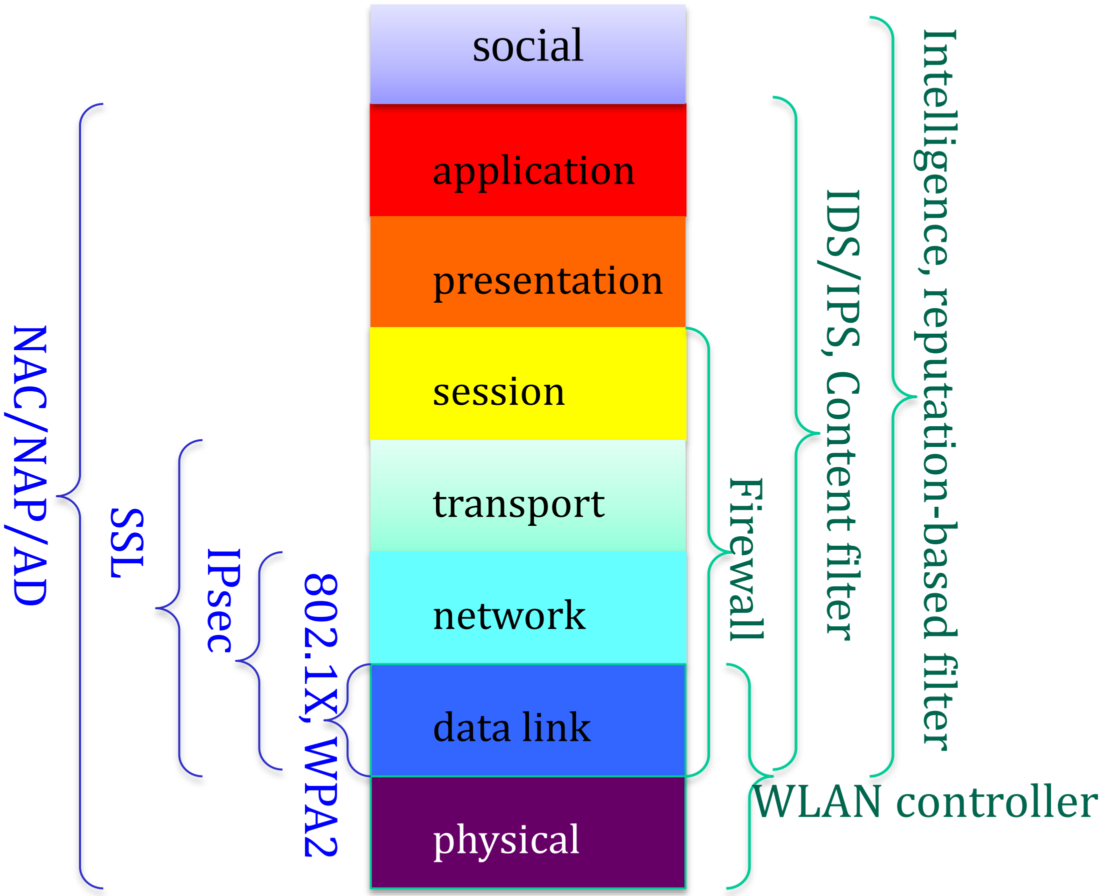
3DES, AES, RSA, DSS, SHA

SSL/TLS, IPSec, IMAP, 802.11i, 802.1x

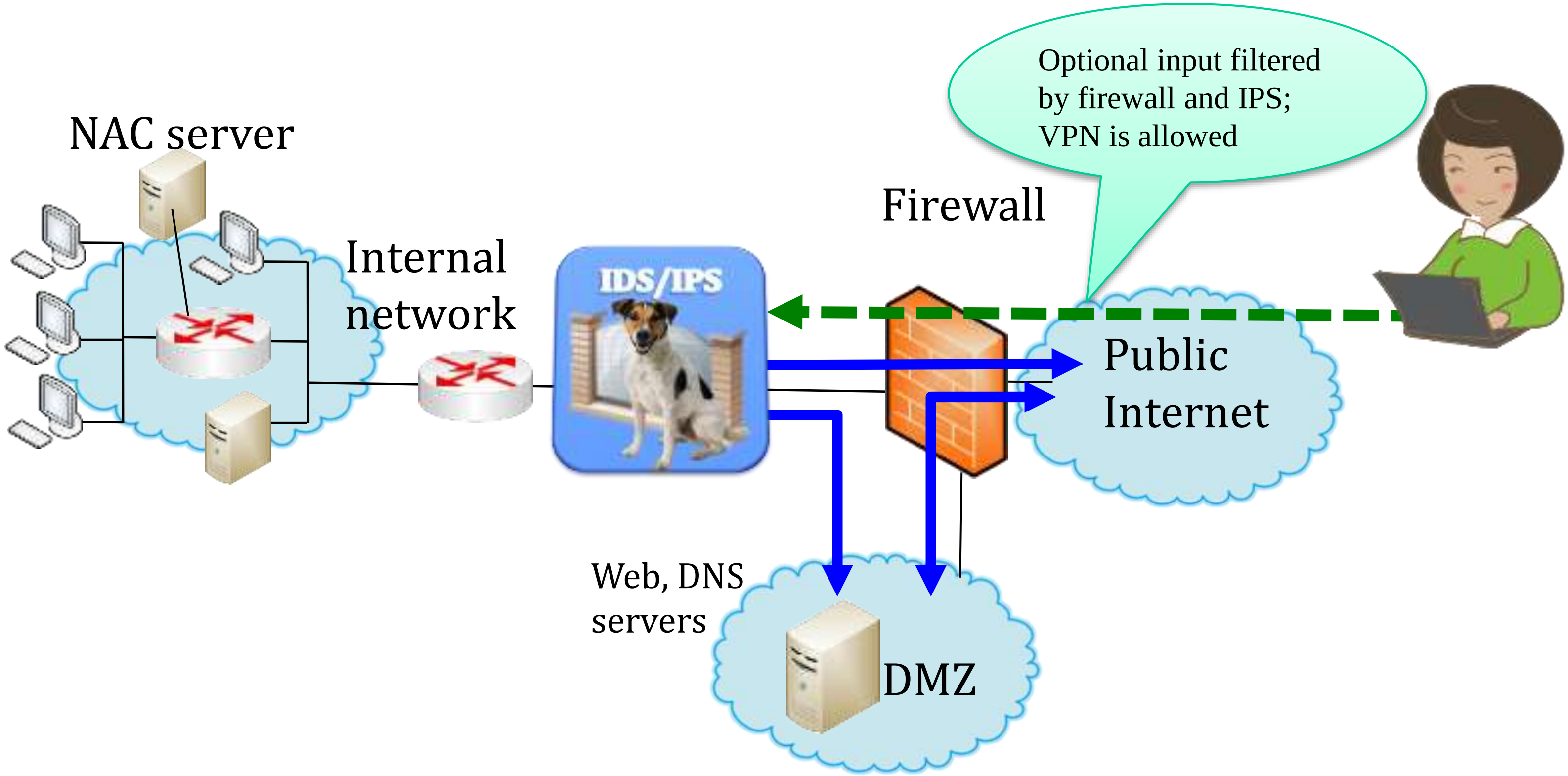
Firewalls/ intrusion detection/prevention

- Cooperative protection uses all hosts, and network/security equipment
- Centralized management

Defense hardware/software and protocols

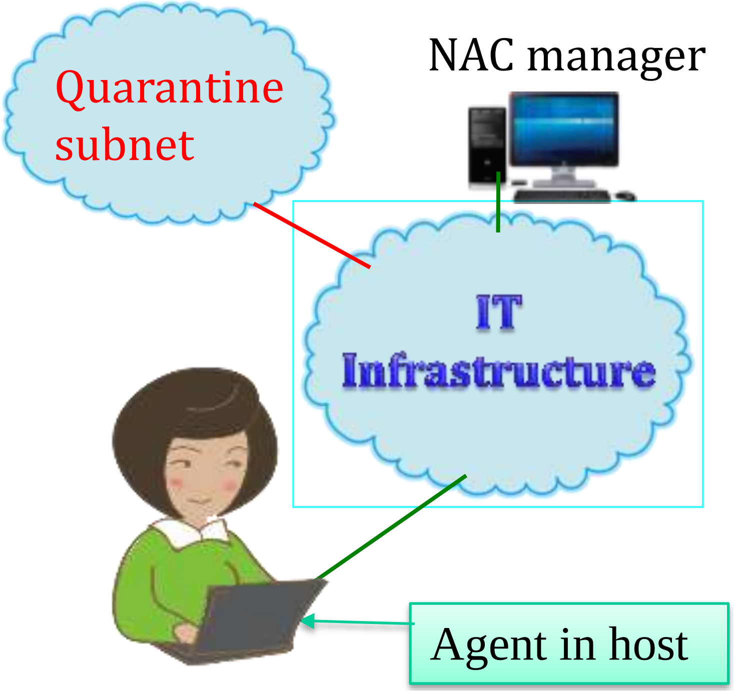


Typical Enterprise Network



Distributed and Coordinated Defense using NAC

- Network access control (NAC) uses policies to protect information infrastructure
  - Central management server/appliance
    - Set and enforce policies for agent
    - Management for policies and hosts
  - Agent (software) is running in a host
- NAC procedure
  - When a host joins the infrastructure, an agent (software) in the host inspects the health of the host
    - Health: OS/application patches, anti-malware updates, malware in the host, etc
  - When the health state of the host is acceptable, it can join the infrastructure; otherwise the host is quarantined in a subnet for remediation
  - After the host joins the infrastructure, its health is constantly monitored by the agent and the NAC manager



Host protection

- Anti-malware
- OS and application security patches
- Host-based firewall
- Host-based intrusion detection/protection
  - Signature-based analysis looks for patterns of specific known exploits and vulnerabilities
  - Behavioral-based analysis watches for
    - suspicious behavior that is commonly associated with a type of attack, such as buffer overflow
    - profile that the operations taking place on a system and then prevent any behavior outside of that profile
  - Most product support both signature- and behavior-based intrusion detections
- Configuration hardening

Host Intrusion Detection (HIDS)

- Host IDS uses signature analysis across multiple events/logs and/or time
- Heuristic profiling and behavior rules:
  - Monitoring resources consumed in OS and applications as well as system calls and processes in a host, including CPU, memory, disks, and I/O bandwidth, file access, registry access, and module/DLL loading
  - Analyze applications/process behaviors of against typical behaviors
  - Not signature based
  - Against zero-day attacks from Trojans, worms and key loggers
  - useful way to spot nefarious activity

Network Access Control/Protection (NAC/NAP)

- NAC/NAP needs a
  - Server side: server/appliance
  - Client side: an agent (software process) in a host
- Agent reports the health state of the host to NAC/NAP server
  - Security patches for OS and applications
  - Anti-malware updates
- Policies for user/group/process access rights
  - Microsoft NAP is built upon Active Directory
  - Cisco uses ACS (access control server)
  - Symantec Endpoint Protection Manager
- Name for NAC:
  - Cisco: network admission control (NAC)
  - Microsoft: NAP
  - Symantec and McAfee: NAC (network access control)

Crypto and Protocols

- Symmetric key crypto
  - Confidentiality: encryption
  - Authentication: Hash
- Public key crypto
  - Public key encryption
  - Signature
  - Public key certificate: authentication
- Protocols are based on Crypto
  - SSL protects transport layer using public key crypto for
    - Authentication
    - Establish a symmetric key
  - SSL using Symmetric key crypto for encryption
  - VPN for network layer

Perimeter protection

- Guarding the entrance of important assets
  - Perimeter: physical (such as router interface) or virtual (such as VLAN)
- Firewall
  - Inspection on IP and transport headers
  - Filter outgoing and incoming packets using source/dest. IP address/port
- IDS/IPS
  - Inspection on packet payload
  - Inspection on IP and transport headers
  - IDS: report detected malicious packets
  - IPS: block and report detected malicious packets
  - Inspection based on signatures or abnormal behaviors
    - Signatures are useful to detect known attacks
    - Learning is used to establish the rules for distinguishing between normal and abnormal behaviors
    - Behavior-based IDS/IPS may detect zero-day attacks