Content in this lecture is mainly based on Purdue CS 526 Fall 13 by Prof. Ninghui Li.

CS 419: COMPUTER SECURITY

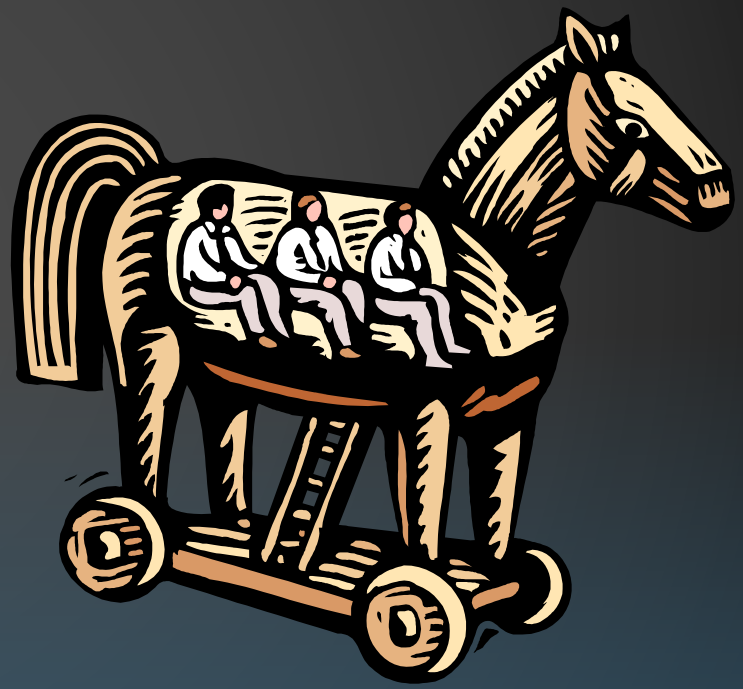
MALWARES

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	

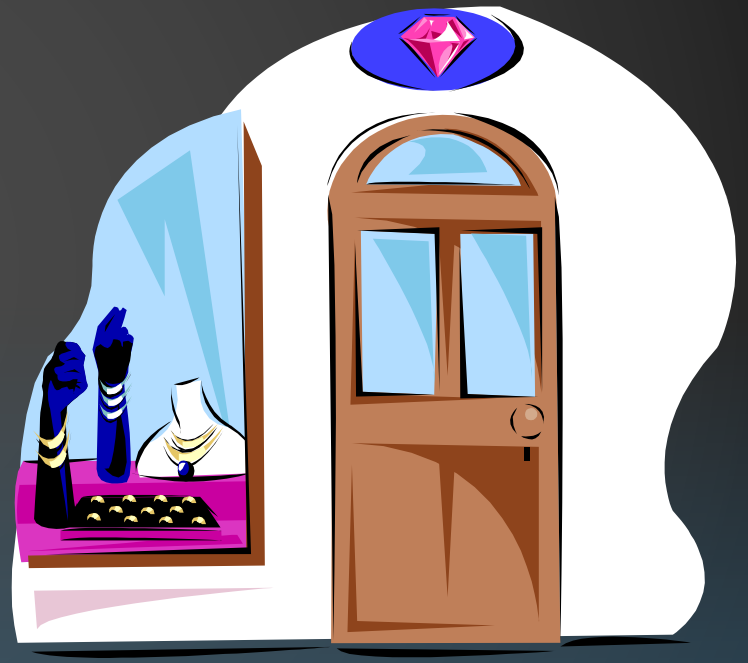
TROJAN HORSE

- 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



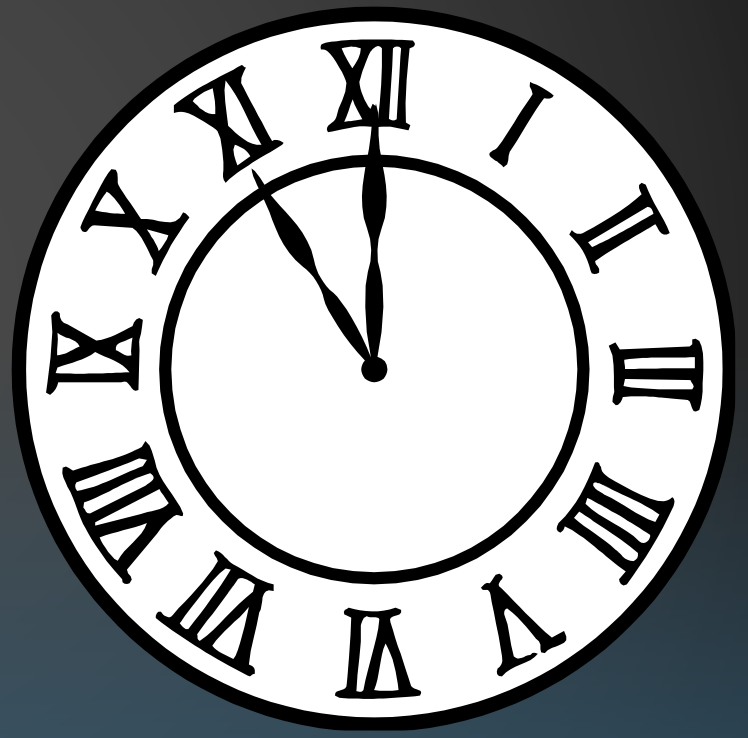
TRAPDOOR OR BACKDOOR

- 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

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

GandCrab Ransomware Crew To Retire After $2 Billion Shakedown Of Victims

A comment made by an FBI agent at a little-noticed cybersecurity conference in Boston last week is all of a sudden making big headlines, many of them suggesting that the FBI is telling victims of ransomware to "just pay" the ransom.

The comments by Joseph Bonavolonta, Assistant Special Agent in Charge of the Cyber and Counterintelligence Program in the FBI's Boston office, were first reported by The Security Ledger.

What Bonavolonta supposedly said is that the encryption used by cybercrooks in the ransomware known as CryptoWall is so good that the FBI "often [advises] people just to pay the ransom."

Here's the exact quote:

> *The ransomware is that good... To be honest, we often advise people just to pay the ransom.*

Bonavolonta was also quoted as saying "the easiest thing may be to just pay the ransom," and the "overwhelming majority of institutions just pay the ransom."

And he said: "You do get your access back" (to your files once you pay).

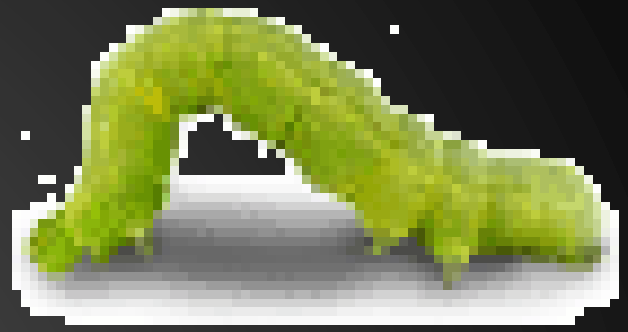
ne flips side, there are bad deeds that get rewarded. So it
ular form of ransomware that was sold to clients on the
h their earnings.

und $2 billion, all extracted from victims who opted to pay
e. Whether that figure is accurate or not is up for debate.
e than $150 million per year" from GandCrab and is now

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

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

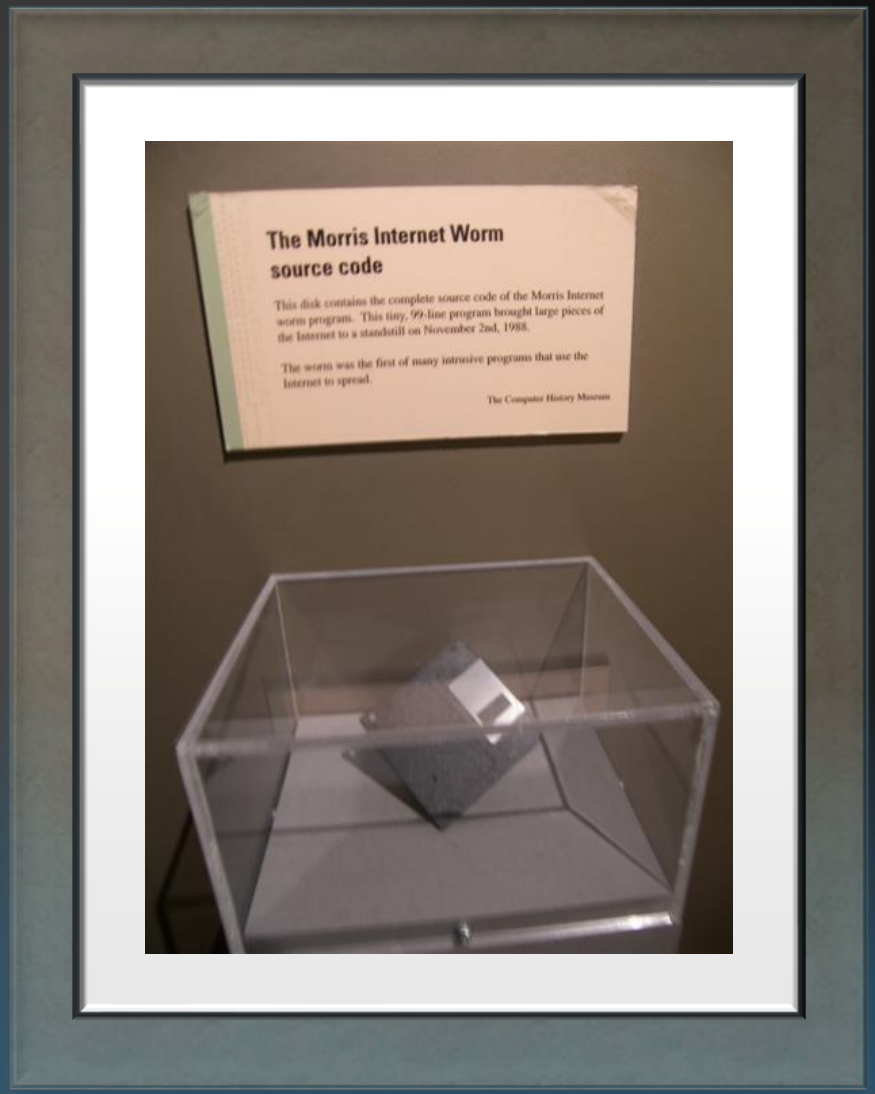
Exploiting software vulnerabilities to exploiting human vulnerabilities

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



MORRIS WORM (NOVEMBER 1988)

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

- Fingerd
  - used to find information about computer users: login name, the full name, login time, idle time, time mail was last read, and the user's plan and project files.
  - Useful tools for social engineering attacks, and gathering information.
  - Often blocked to outside domains.
  - 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

July 2001

Code Red

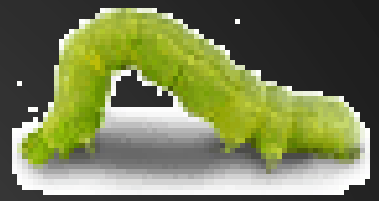
- Affects Microsoft Index Server 2.0,
- Exploits known buffer overflow in Idq.dll
- Vulnerable population (360,000 servers) infected in 14 hours

Jan. 2003

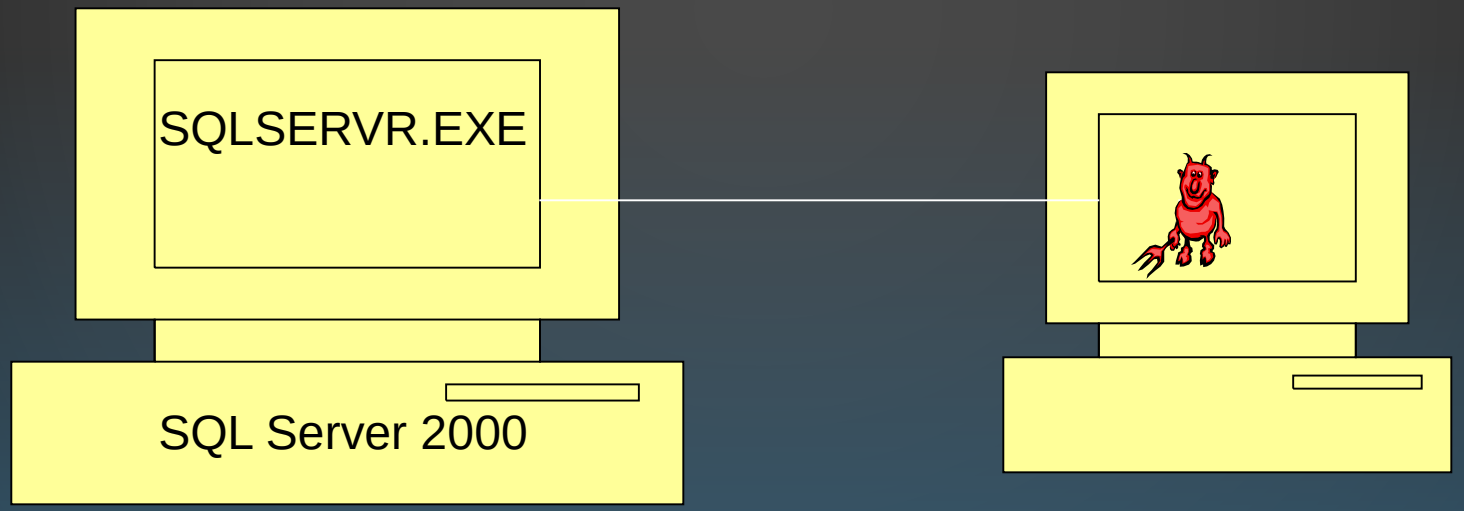
SQL Slammer

- Affects in Microsoft SQL 2000
- Exploits known months ahead of worm outbreak
- Vulnerable population infected in less than 10 minutes

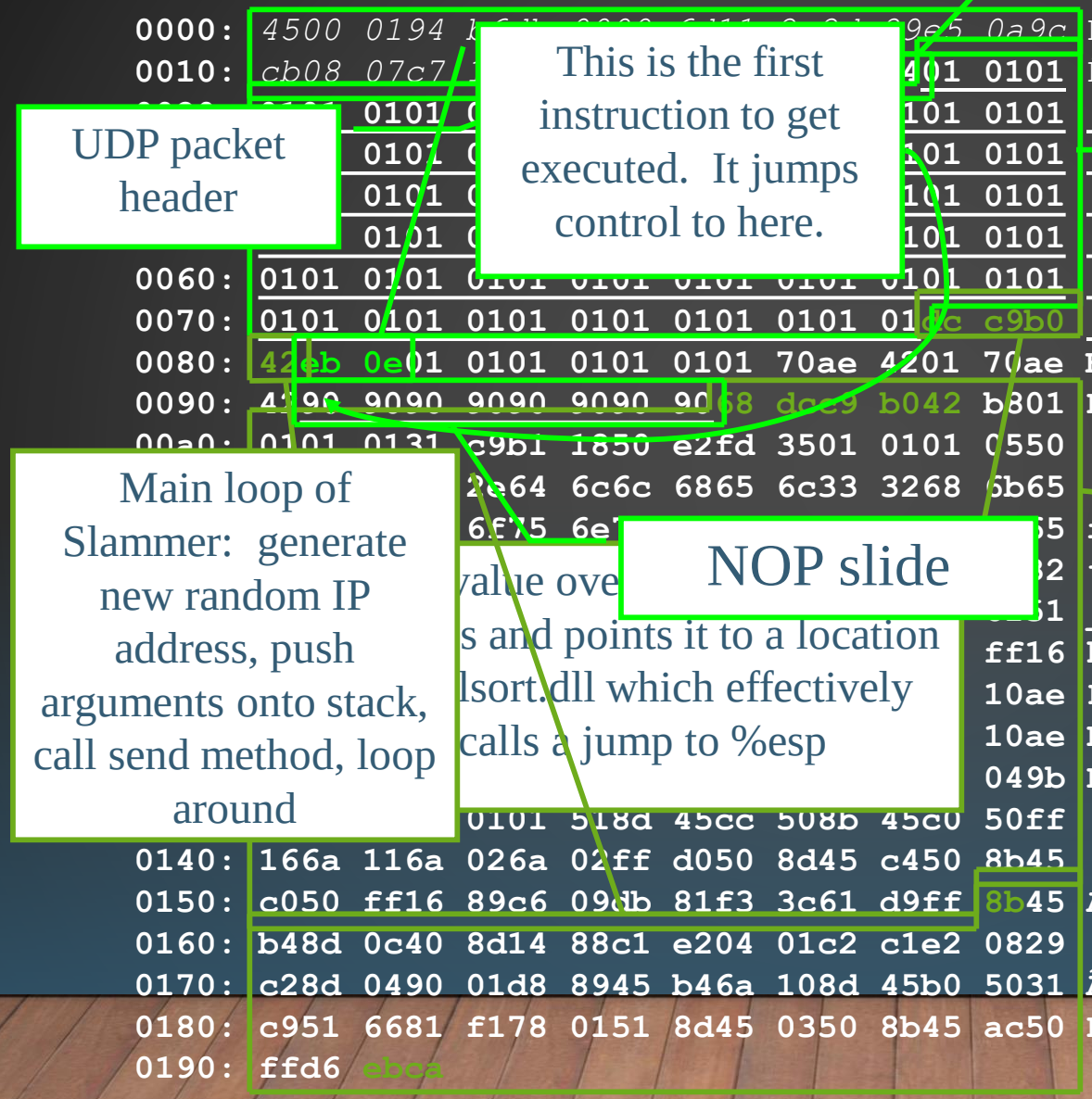
Slammer Worms (Jan., 2003)



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



Slammer's code is 376 bytes!



This byte signals the SQL Server to store the contents of the packet in the buffer

This is the first instruction to get executed. It jumps control to here.

UDP packet header

The 0x01 characters overflow the buffer and spill into the stack right up to the return address

Main loop of Slammer: generate new random IP address, push arguments onto stack, call send method, loop around

NOP slide

[illegible] value ove[illegible]
s and points it to a location
lsort.dll which effectively
calls a jump to %esp

Restore payload, set up socket structure, and get the seed for the random number generator

RESEARCH WORMS

WHAT IS THE KEY CHALLENGES?

Shiqing Ma, Rutgers

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

NIMDA WORM (SEPTEMBER 18, 2001)

- Key Vulnerability to Exploit
  - **Microsoft Security Bulletin (MS01-020):** March 29, 2001
  - A logic bug in IE's rendering of HTML
  - Specially crafted HTML email can cause the launching of an embedded email
- Vector 1: e-mails itself as an attachment (every 10 days)
  - runs once viewed in preview plane
- Vector 2: copies itself to shared disk drives on networked PCs
  - Why this may lead to propagating to other hosts?

NIMDA WORM

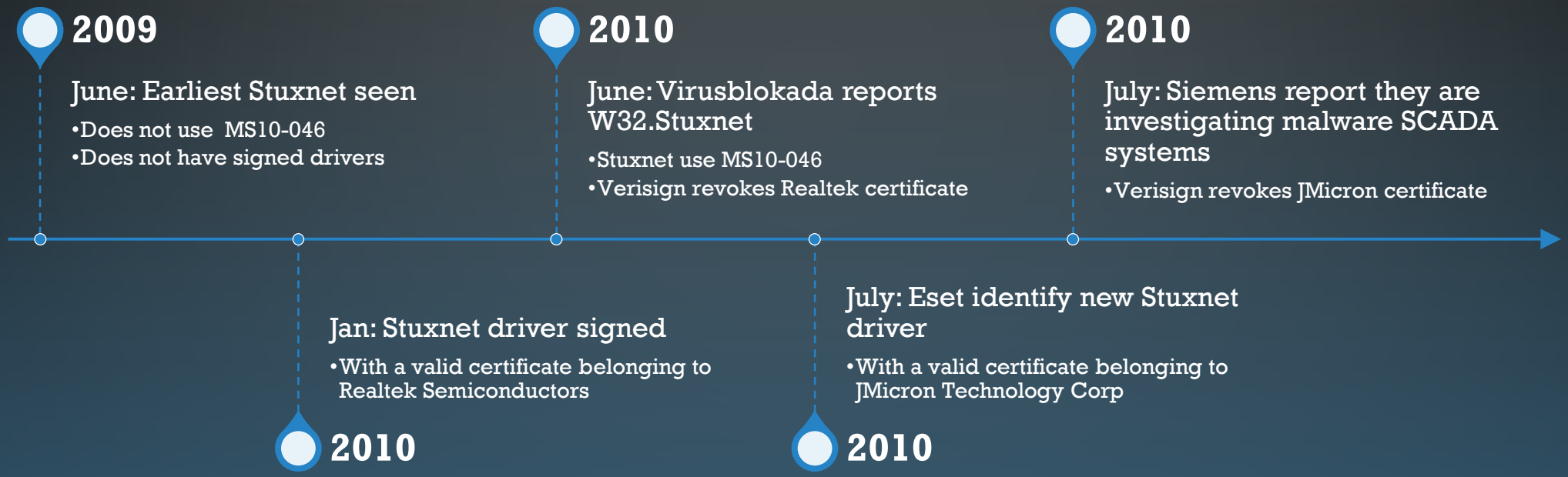
- Vector 3: Exploits various IIS directory traversal vulnerabilities
  - Use crafted URL to cause a command executing at
  - Example of a directory traversal attack:
    - http://address.of.iis5.system/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\
- Vector 4: Exploit backdoors left by earlier worms
- Vector 5: Appends JavaScript code to Web pages

```
<script language="JavaScript">
window.open("readme.eml", null, "resizable=no,top=6000,left=6000")
</script>
```

NIMDA WORM

- 'Nimda fix' Trojan disguised as security bulletin
  - claims to be from SecurityFocus and TrendMicro
  - comes in file named FIX_NIMDA.exe
    - TrendMicro calls their free Nimda removal tool FIX_NIMDA.com

STUXNET: HISTORY (1)



HISTORY (2)

Aug

2010 Aug: Microsoft issues MS10-046

- Patches windows shell shortcut vulnerability

Sept

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

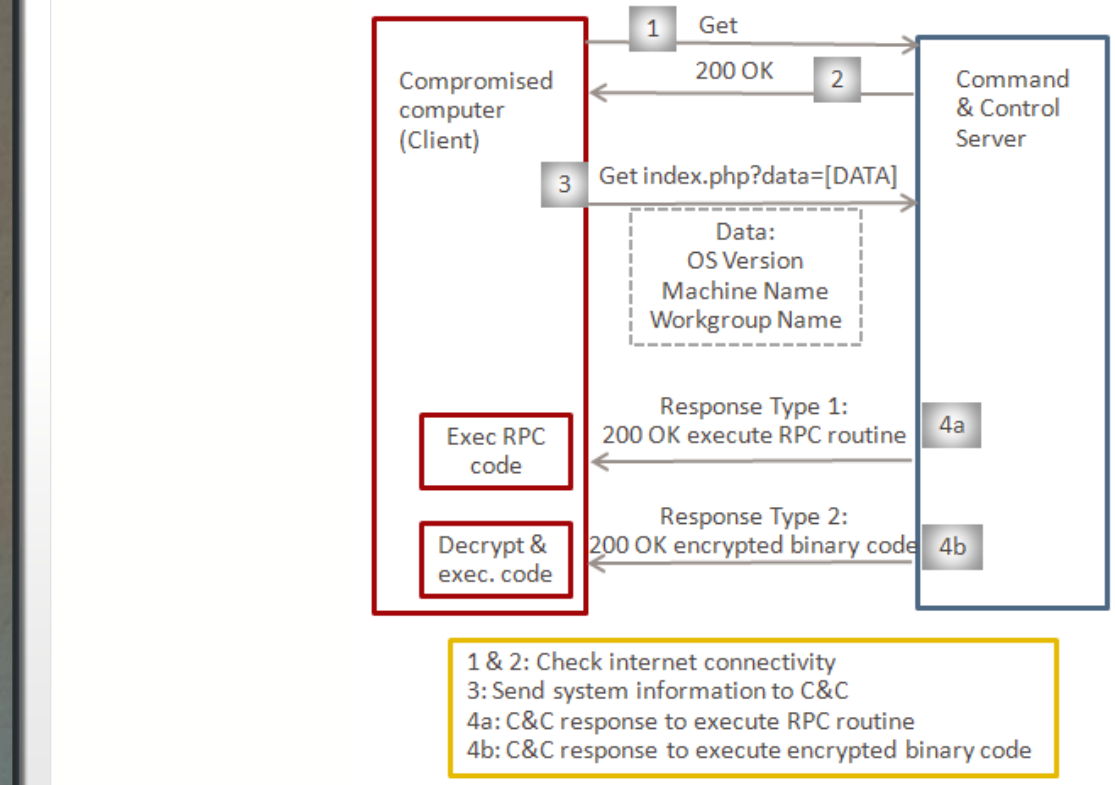
SCENARIO (6)

- 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

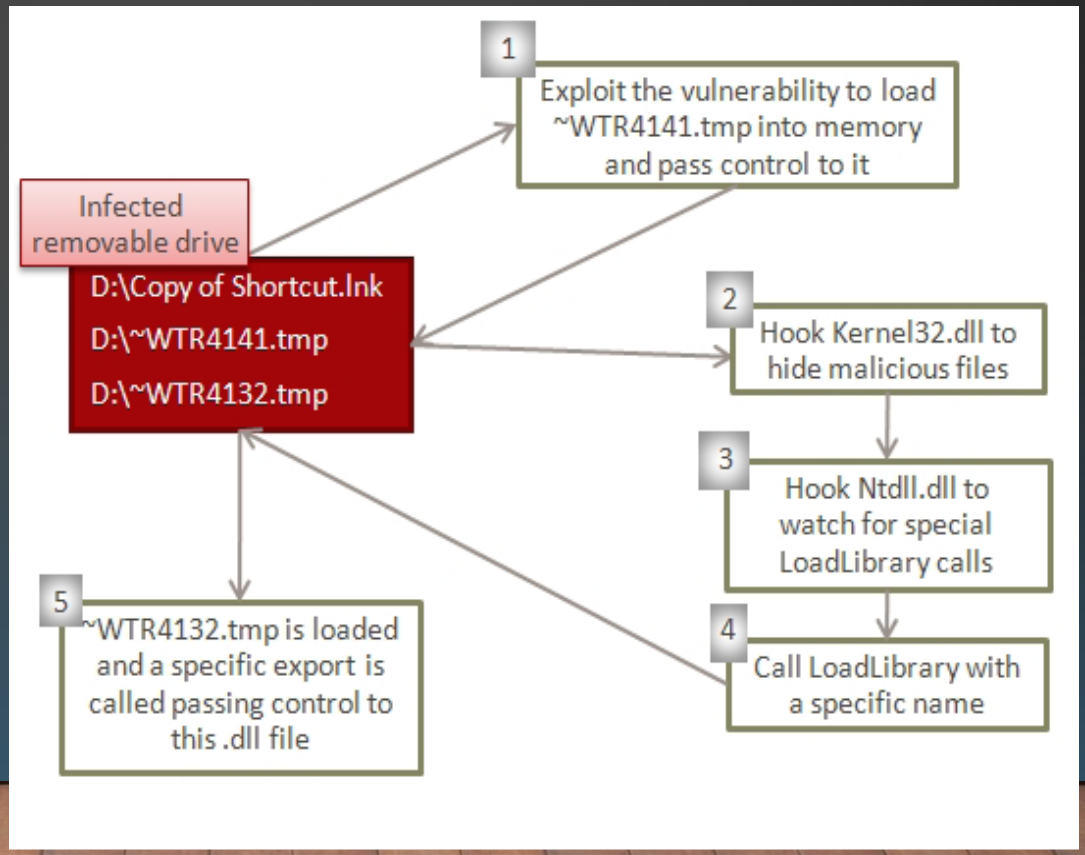
- Peer-to-peer communication and updates
- Infecting WinCC machines via a hardcoded database server password
- Propagating through network shares
- Propagating through the MS10-061 Print Spooler Zero-Day Vulnerability
- Propagating through the MS08-067 Windows Server Service Vulnerability

PROPAGATION METHODS: USB

- LNK Vulnerability (CVE-2010-2568)
- AutoRun.Inf

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

UseAutoPLAY=0
```



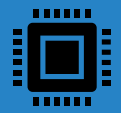
WHAT WAS THE TARGET?

- 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.

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

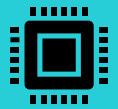
- User-level rootkits
  - Replace utilities such as ps, ls, ifconfig, etc
  - Replace key libraries
  - Detectable by utilities like tripwire
- Kernel-level rootkits
  - Replace or hook key kernel functions
  - Through, e.g., loadable kernel modules or direct kernel memory access
  - A common detection 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)

MORE ROOTKITS

- Bootkit (variant of kernel-level rootkit)
  - Replace the boot loader (master boot record)
  - Used to attack full disk encryption key
  - Malicious boot loader can intercept encryption keys or disable requirement for kernel-driver signing
- Hypervisor-level rootkits
- Hardware/firmware rootkits
- Whoever gets to the lower level has the upper hand.

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

STORM BOTNET

- First detected in Jan 2007
- Vectors (primarily social engineering):
  - Email attachments
  - Download program to show a video
  - Drive-by exploits
- DDoS spam fighting sites, and whichever host discovered to investigate the botnet
- Peer-to-peer communications among bots
  - for asking for C&C server

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

ANTI-VIRUS SOFTWARE

- Goal: Find malware programs on a system, in transmission, etc.
- Main deployed approach: Signature-based detection
  - Uses pattern matching
  - Searches for known patterns of data belonging to malwares in executable programs or other types of files
  - Maintains and updates a blacklist of signatures
- Problems
  - Cannot detect new malwares, variants of malwares, etc.
  - Hard to keep up with new malware
    - More malwares are created each day than benign programs

POLYMORPHIC MALWARES

- Uses a polymorphic engine (a mutation engine or mutating engine) to generate multiple copies of the same malware that look different
  - E.g., serve a different version to each computer subject to a drive-by download attack
- Typically encrypts the majority of the code, each time with a different key is used
- Weakness: decryption code often remains the same, and may be detected and/or used as signatures

METAMORPHIC MALWARE

- A malware automatically changes itself each time it propagates
- Each new version has different code, though the same functionality
- Uses techniques that include
  - Adding varying lengths of NOP instructions, permuting use of registers, add useless instructions, use functional equivalent instructions, reorder functions, reorder data structures, etc.

SEMANTIC, OR HEURISTICS BASED MALWARE DETECTION

- Static approach: Looks for specific code behavior instead of specific strings
- Dynamic approach: Execute the program to identify potentially malicious behavior
- Main limitations
  - Performance overhead
  - Potential of high false positives

APPLICATION WHITELISTING

- Instead of finding malwares and stop then, list all known good/allowed programs and only run them.

- Typically deployed by enterprise, who can afford to maintain a list of allowed programs