Notes

Malicious Software

- Programs exploiting system vulnerabilities
- AKA Malware (attack vector)
  - Program fragments that need a host program
    - Viruses, logic bombs, backdoors
  - Independent self-contained programs
    - Worms, Bots
  - Can be replicating
- Sophisticated threat to computer systems
- History:
- Can be used to help or harm
  - First PC Virus, Brain, infected Microsoft DOS systems to protect medical software from piracy. (Targeted copyright infringers only).
  - The Vienna virus – the first virus made to destroy data
    - One of Viennas alleged authors creates a program to neutralize the virus (The first known antivirus).
- 1989 – IBM introduces Viruscan for MS-DOS to combat the growing array of malware
- 1991 – Virus Construction set (vsc) released a simple toolkit to help create customized malware
- 1994 – Goodtime Virus Hoax – scared people about a code scam that didn’t happen
- 1995 – First Macro Virus – These were implemented in Microsoft Word macro languages, infecting document files. These techniques spread to other macro languages in other programs (Documents are shared more than programs)
- 1996 – Netcat in released for UNIX. The most popular backdoor for UNIX although it has significant legitimate use.
- 1998 – StrangeBrew (the pun is appreciated), the first Java virus released
  - Back Orifice tool released
- 1999 – Melissa virus/worm – Microsoft macro virus/worm infected document files -> spread via emails
  - First malware identified as having spread around the globe
- 1999 – Knark – First kernel level root kit for unix
• 2001 – Code Red Worm – First case of a very rapid spreading worm
  250,000+ machines in less than 8 hours
• 2003 – Sapphire/Slammer worm (not malicious) – infected population
doubled every 8.5 sec.
  ○ Achieved full scanning rate (55+ mil. scans/sec.) after 3 minutes.
    Slowed down because many portions of the internet did not have
    enough bandwidth to grow
• Concept of a worm: affects a machine once as to not infect a machine where
damage has already been done (similar to the human body: get sick from 1
strain of virus once (but difference is because we gain immunity from that
strain))
• 2005 – Sony BGM Rootkit scandal (Good intentions, bad outcomes
  ○ Introduced as a copy protection mechanism in music CDs
  ○ Auto installed on Windows desktop comp. when users tried to play
    the CDs (Before EULA could be acknowledged by user)
  ○ Interfered with normal operation of Windows OS playing CDs by
    installing a rootkit that created vulnerabilities for other malware to
    exploit

**Terminology**

*Virus* – program that attaches itself to a host program and propagates copies of itself to other programs

*Worm* – program that propagates copies of itself to other computers

*Polymorphic Virus* – a virus that morphs (changes its signature) when it gets transferred

*Logic bomb* – program that triggers action when a particular condition occurs

*Trojan horse* – program that hides itself in a host program and contains unexpected additional functionality

*Script Kitties* – NOT REAL HACKERS, wannabee scrubs that use other people’s code to do things like DoS or launch malware, etc

*Backdoor* – program modification that allows unauthorized access to functionality

*Mobile code* – software that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics

*Auto-rooter* – malicious hacker tools used to break into new machines remotely

*Kit (virus generator)* – set of tools for generating new viruses automatically

*Spammer and Flooder* – programs that are used to send large volumes of unwanted e-mail, or to attack systems with a large volumes of traffic to carry out a DoS attack

*Keyloggers* – programs that capture keystrokes on a compromised system

*Rootkit* – set of hacker tools used after attacker has broken into a computer system and gained root-level access
Zombie – program on infected machine activated to launch attacks on other machines

**Viruses**
- Piece of software that infects programs
  - Modifying them to include a copy of the virus
  - It executes secretly when host program is run
- Specific to operating system and hardware
  - Taking advantage of their details and weaknesses

**4 Phases**
Dormant phase: The virus is idle. The virus will eventually be activated by some event,
- A date – The presence of another program or file
- Or the capacity of the disk exceeding some limit.
- Not all viruses have this stage.
Propagation phase: The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- A virus will typically not propagate to another infected program
Triggering phase: The virus is activated to perform the function for which it was intended.
- As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself
Execution phase: The function is performed, which may be
- harmless, e.g. a message on the screen, or
- damaging, e.g. the destruction of programs and data files

**Virus Structure**
- Components:
  - Infection (propagation) mechanism - enables replication AKA *Infection vector*
  - Trigger – handler for event that activates payload AKA *logic bomb*
  - Payload – what it does, malicious or benign
- When infected program invoked, executes virus code then original program code
- Can block initial infection (difficult)
- Or propagation (with access controls)

**Socrative Questions**
• What do we do if team members are not contributing anything to projects?
  ○ Talk to the teacher about this
• How do polymorphic viruses alter their signature?
  ○ They alter their signatures via hashes functions
• [https://www.youtube.com/user/danoct1](https://www.youtube.com/user/danoct1) has videos about vintage viruses
• Do you believe that malware or anti-malware has the upper hand in terms of development and effectiveness?
  ○ Depends
  ○ malware only needs to find 1 weak spot
  ○ If an entity (company, individual) has good anti-malware it could be difficult for an attacker who’s not experienced to compromise the system; Or the other way around.
• What does a payload look like?
  ○ Google it
• What is the difference between a virus and a worm?
  ○ Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage
• Are there any malware examples that use machine learning?
  ○ There are some machine learning models out there that are exploited to create malware
• How do modern virus scanners work? do they look for footprints of specific viruses or are there more generic traits they look for in files?
  ○ Sophisticated
  ○ A virus scanner operates by searching for the signatures of known viruses. Antivirus software does “heuristic” checking