February 22, 2021
Malware

- Today
  - Malware
  - Lab 1 Network Simulations
  - Paper Presentation
- Assignments
  - Lab 2 (Assignment will be posted later this week):
    - Due Monday, Mar 22
  - Project
    - Outline: Due Monday, Mar 29

Malware Discussion

- Goals
- Types
- Stages

Strategies

- Baselining
- Detection Strategies
- Context Available

Examining malware

- **Trace system calls:**
  - most OSes support method to trace sequence of
  - system calls e.g., ptrace, strace, etc.
  - all “interesting” behavior (e.g., networking, file I/O, etc.) must go through system calls
  - capturing sequence of system calls (plus their arguments) reveals useful info about malware’s behavior

Examining malware

- **Observe filesystem changes and network IO:**
  - “diff” the filesystem before and after
    - which files are the malware reading/ writing?
  - capture network packets
    - to whom is the malware communicating
- **Utilize hidden kernel module:**
  - capture all activity
  - challenge: encryption

Worms

A worm is a self-propagating program that:

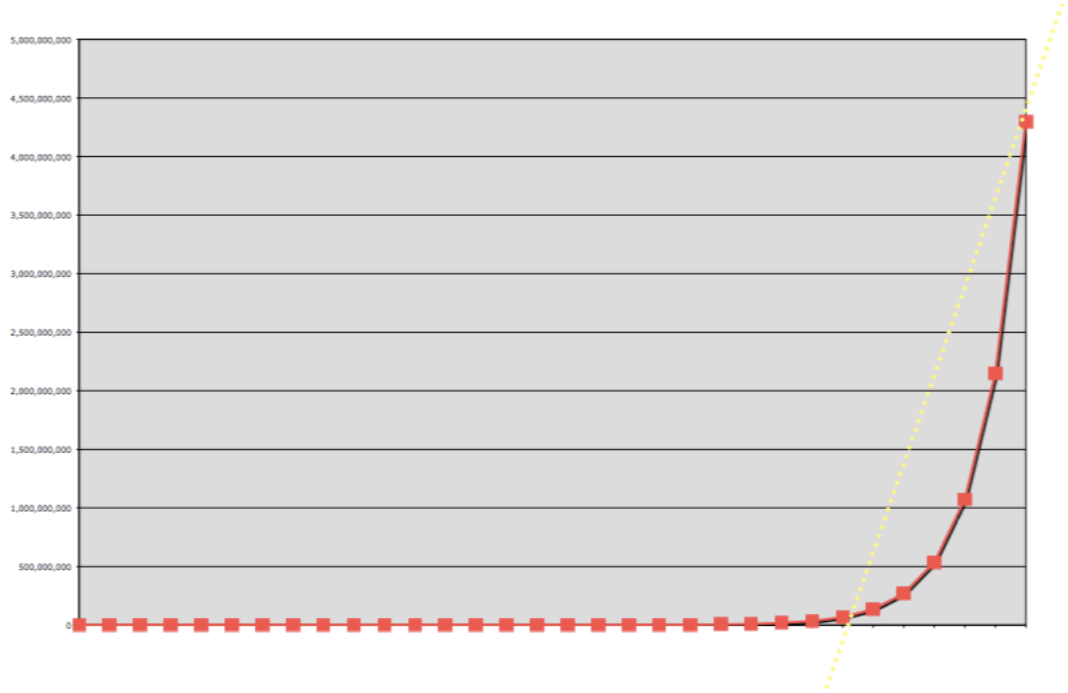
1. Exploits some vulnerability on a target host
2. (often) imbeds itself into a host ...
3. Searches for other vulnerable hosts ...
4. Goto step 1

The Danger

- What makes worms so dangerous is that infection grows at an exponential rate
- A simple model:
  - *s* (search) is the time it takes to find vulnerable host
  - *i* (infect) is the time is take to infect a host
  - Assume that t=0 is the *worm outbreak*, the number of hosts at t=j is

$$2^{\left(\frac{j}{(s+i)}\right)}$$

The result


5,000,000,000
4,500,000,000
4,000,000,000
3,500,000,000
3,000,000,000
2,500,000,000
2,000,000,000
1,500,000,000
1,000,000,000
500,000,000
0

Morris Worm – Nov. 2nd 1988

- 6pm: someone ran a program at a computer at MIT
- The program collected host, network, and user info...
- ... and then spread to other machines running Sun 3, VAX, and some BSD variants
- ... rinse and repeat

Worms and infection

- **The effectiveness of a worm is determined by how good it is at identifying vulnerable machines**
- Multi-vector worms use lots of ways to infect: e.g., network, email, drive by downloads, etc.
- Example scanning strategies:
  - **Random IP:** select random IPs; wastes a lot of time scanning "dark" or unreachable addresses (e.g., Code Red)
  - **Signpost scanning:** use info on local host to find new targets (e.g., Morris)
  - **Local scanning:** biased randomness
  - **Permutation scanning:** "hitlist" based on shared pseudorandom sequence; when victim is already infected, infected node chooses new random position within sequence

Worms Defense Strategies

- (Auto) **patch** your systems: most large worm outbreaks have exploited known vulnerabilities (Stuxnet is an exception)
- **Heterogeneity**: use more than one vendor for your networks
- **IDS**: provides filtering for known vulnerabilities, such that they are protected immediately (analog to virus scanning)
- **Filtering**: look for unnecessary or unusual communication patterns, then drop them on the floor

Morris Worm

- Computers became multiply infected
- Systems became overloaded with processes
- Swap space became exhausted, and machines failed
- Wednesday night: UC Berkeley captures copy of program
- 5AM Thursday: UC Berkeley builds *sendmail* patch to stop spread of worm
- Difficult to spread knowledge of fix
  - Not coincidentally, the Internet was running slow
- Around 6,000 machines (~10% of Internet) infected at cost of $10M-$100M

Morris Worm Attack Vectors

- rsh: terminal client with network(IP)-based authentication
- fingerd: used *gets* call without bounds checking
- sendmail: DEBUG mode allows remoteuser to run commands
- lots of sendmail daemons running in DEBUG mode

Stuxnet

- First reported June 2010
  - Exploited **unknown vulnerabilities**
- Not one zero-day
- Not two zero-days
- Not three zero-days
- But four zero-days!
  - print spooler bug
  - handful of escalation-of-privilege vulnerabilities

Stuxnet

- Spread through infected USB drives
  - bypasses "***air gaps***"
- Worm actively targeted SCADA systems (i.e., industrial control systems)
  - attempted 0-day exploit
  - also tried using default passwords
- apparently, specifically targeted Iran's nuclear architecture
- Once SCADA system compromised, worm attempts to reprogram Programmable Logic Controllers (PLCs)
- Forensics aggravated by lack of logging in SCADA systems

Agent Examples

- SolarWinds
- https://arstechnica.com/information-technology/2021/02/new-malware-found-on-30000-macs-has-security-pros-stumped/