Implementation and Management of Systems Security
158.738

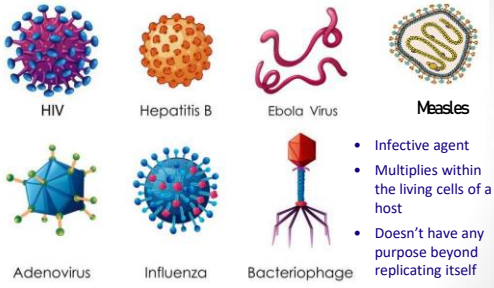
A/Prof. Julian Jang-Jaccard
Massey University

COMPUTER SECURITY

Malware

- Malware is short for "malicious software," also known as malicious code or "malcode."
- Specifically designed to damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or networks.
- Often used as a general term refers to a wide variety of damaging software programs
- Most used attacking tool (APWG, 2015)

Viruses

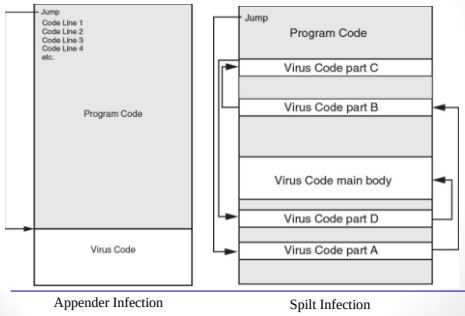


- Infective agent
- Multiplies within the living cells of a host
- Doesn't have any purpose beyond replicating itself

Viruses

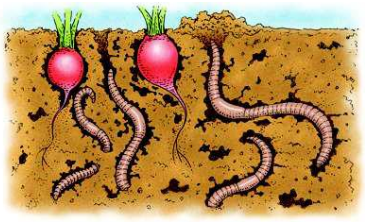
- Propagates by inserting a copy of itself into and becoming part of another program, (i.e., reproduce by infecting other files)
- Almost all viruses are attached to an executable file (and macros)
- Viruses spread when the software or document they are attached to is transferred from one computer to another using the network, a disk, file sharing, or infected email attachments.
- Require a host program or a human to help spreading

How a virus works?



Appender Infection Spilt Infection

Worms



- Worms follow tunnels
- Find vulnerable vegetables

Worms

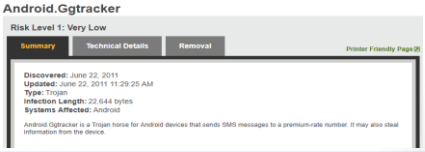
- worms are standalone software and do not require a host program or human help to propagate
- worms either exploit a vulnerability on the target system or use some kind of social engineering to trick users into executing them
- A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided

Trojan Horse

- Trojan war - 10 years of fighting.
- Impregnable city walls.
- Greeks tricked the trojans into letting them inside their city.

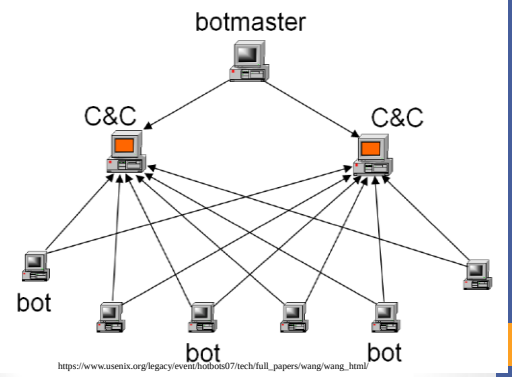
Trojans

- It is a harmful piece of software that looks legitimate
- Program with an overt purpose (known to user) and a covert purpose (unknown to user)
- Users are typically tricked into loading and executing it on their systems (e.g, video/audio files online)
- Example: Android malware (tracker for Starcraft 2 game)



Bots

- "Bot" is derived from the word "robot" and is an automated process that interacts with other network services.
- A malicious bot is self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices, or "botnet."
- With a botnet, attackers can launch broad-based, "remote-control," flood-type attacks against their target(s).



https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/wang/wang_html/

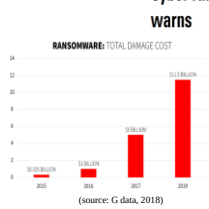
Distributed DOS (DDOS)

- DDoS attack
  - launched from multiple connected devices that are distributed across the Internet.
  - These multi-person, multi-device barrages are generally harder to deflect, mostly due to the sheer volume of devices involved.
- Command zombies to stage a coordinated attack on the victim
- Overwhelm victim with traffic arriving from thousands of different sources (人海戰術?)

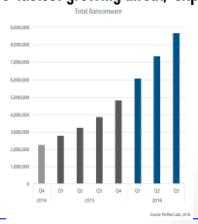
Ransomware

Ransomware damage costs predicted to hit $11.5B by 2019

Cyber ransoms are 'fastest-growing threat,' expert warns



(source: G data, 2018)



Ransomware Factsheets

Factsheet

- Appeared May 2017
- **Affected more than 230,000 computers across 150 countries**
- Indirect losses reach USD$4 billion
- Affected: Airlines (Boeing, LATAM), Railways (Germany, Russia), Telcom (Portugal, Saudi Arabia, Spain, Hungary, South Africa), Cars (Japan), Government Bodies (Russia, hina, Russia), Hospitals National Health Services, UK)

WannaCry 2.0

Factsheet

Petya

- Year active 2016 – 2017
- **Said to be most destructive cyberattack ever**
- Most affected countries: Ukraine (80% hit), Germany (9%)
- **Politically motivated**
- Affected: Several Ukrainian ministries, banks and metro systems, including nuclear power plant
- Put the whole nation of Ukraine on hold for a few days

Phases of Ransomware

1. Infection and installation
   - 97% of phishing emails deliver ransomware
2. Command and control
   - Often utilizes botnet to infect as many computers as possible
3. Selection of file targets
   - Family photos, business documents
4. Encryption
   - Difficult to decrypt without super (or quantum) computer
5. Extortion
   - 70% of infected businesses have paid the ransom, range from $200 – 10,000

Cyber Warfare

- May 2007: DDoS attacks on Estonia after government relocated Soviet-era war monument
- Aug 2008: similar attack on Georgia during the war between Russia and Georgia
- June 2017: DDoS + Ransomeware Petya targeting Ukrainian organizations (banks, ministries, newspapers, and electricity firms etc.,)

Malware Propagation

- Spam
- Phishing
- Social Media (Internet and Social Networking Sites)

Spam

- Act of sending irrelevant, inappropriate and unsolicited messages
- Prolific due to low barrier to entry
- Between 88–92% of email messages carried spam*
- Unsolicited Electronic Messages Act 2007 (NZ)
  - IMG ordered to pay $120 000 for sending spam via email and text messages to half million new Zealander

Phishing

- Act of attempting to acquire sensitive information by masquerading as a trustworthy entity
- deceives users into visiting a malicious web site claiming to be from legitimate businesses and agencies
- Unsuspecting user enters private information in the malicious web site which is then subsequently used by malicious criminals.

Phishing sample (email)

Phishing sample (Internet)

Phishing Variations

- Spear Phishing
  - Targets only specific users
  - Customized to the recipients including their names and perfonal info to make it appear legitimate
- Whaling
  - Going after “big fish” e.g., wealthy individuals or senior executives
  - Highly tuned message
- Vishing (also known as voice phishing)
  - Attacker calls a victim masquerading to be from a trusted third party e.g., bank manager

Social Media

- Fastest Growing medium to spread malware
- Internet
  - Drive-by download—Unintended download of computer software from the Internet
- Social Networking Sites (SNS)
  - Tricks the user into “voluntarily” installing a malicious binary
  - Fake video players and video codecs
  - Facebook Trojan attack (2015)
    - Pornography site + flash player

Vulnerability Repository

- Common Vulnerabilities and Exposures (CVE)
  - Reference list of standard names for vulnerabilities and exposures
  - Developed by MITRE corporation
- National Vulnerability Database (NVD)
  - NVD is a cybersecurity vulnerability database
  - Managed by National Institute of Standards and Technology (NIST)
  - Stores CVE info + additional Information (such as fix data, severity scores or impact ratings)
- Common Vulnerability Scoring System (CVSS)
  - Also maintained by NIST as part of CVD
  - facilitate an open and standardized method for rating vulnerabilities

Computer defenses

- Managing Patches
- Installing Antivirus Software
- Examining Firewalls
- Monitoring User Account Privilege
- Creating Data Backups

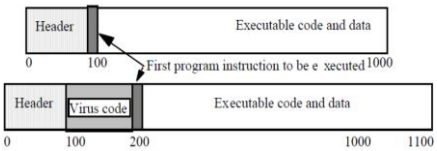
Defense: Patches

- Increase of unintentional vulnerabilities due to increased complexity of software
  - MS-DOS v1.0 : 4,000 lines of code vs. Windows 10: 80 million lines
- Patches are deployable software fixes to address the vulnerabilities uncovered after software release
  - Forced updates, continual updates, choose when to reboot etc.,
- A service pack : cumulative package of all patches and feature updates

Defense: Antivirus

- Used to be considered to be the primary defense against attackers
- Antivirus Functions;
  - Monitor computer activity
  - Examines a computer for any infections
  - Scan new documents for potential malware
  - Clean, quarantine, delete the file

Antivirus Technique – Integrity Check



- Viruses make size of file grow
- Computer keeps a list of the lengths
- Periodically checks against the list
- Any unexpected change indicates a problem

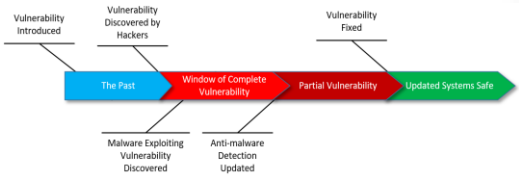
Antivirus Technique -Signature Detection

```
0002E950  6D 65 6D 6F 72 79 20 66 6F 72 20 6E 65 77 20 6C  memory for new l
0002E960  69 73 74 21 0A 00 00 00 55 73 65 20 2D 68 20 66  ist!....Use -h f
0002E970  6F 72 20 68 65 6C 70 2E 0A 00 00 00 00 00 00 00  or help.........
0002E980  77 63 65 20 25 73 20 28 77 49 4E 44 4F 57 53 20  wce %s (WINDOWS
0002E990  63 52 45 44 45 4E 54 49 41 4C 53 20 65 44 49 54  cREDENTIALS eDIT
0002E9A0  4F 52 29 20 2D 20 28 43 29 20 32 30 31 30 2D 32  OR) - (C) 2010-2
0002E9B0  30 31 33 20 61 4D 50 4C 49 41 20 73 45 43 55 52  013 aMPLIA sECUR
0002E9C0  49 54 59 20 2D 20 42 59 20 68 45 52 4E 41 4E 20  ITY - BY hERNAN
0002E9D0  6F 43 48 4F 41 20 28 48 45 52 4E 41 4E 40 41 4D  oCHOA (HERNAN@AM
0002E9E0  50 4C 49 41 53 45 43 55 52 49 54 59 2E 43 4F 4D  PLIASECURITY.COM
0002E9F0  29 0A 00 00 5C 00 00 00 4F 70 74 69 6F 6E 73 3A  )...\...Options:
0002EA00  20 20 0A 00 0A 00 00 00 09 2D 6C 09 09 4C 69 73    .......-l..Lis
0002EA10  74 20 6C 6F 67 6F 6E 20 73 65 73 73 69 6F 6E 73  t logon sessions
```

- Database of malware signatures (sometimes called DAT files).
- Search for bit pattern or a hash.
- Requires regular updates.
- Limited to detection of known malware.

Zero Day Exploits

- A zero-day exploit is an attack that exploits a previously unknown security vulnerability

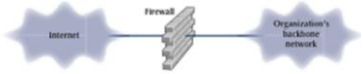


Zero Day Exploits

- Especially vulnerable to Encrypted and Polymorphic Viruses
- These both change their code as they spread.
- This means our signature no longer will work.
- For example, every file with “BAD” in it is a virus.
- Virus mutates and changes this to “ADB”, it will no longer be detected.

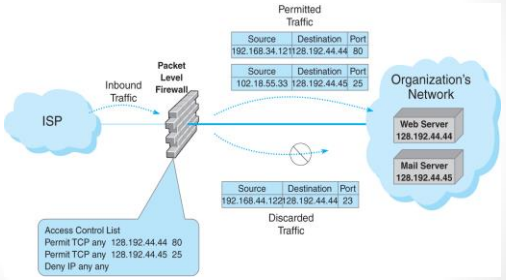
Defense: Firewalls

- Firewalls restrict access to the network



- Examines the source and destination address of every packet passing through
  - Allows only packets that have acceptable IP addresses (protocols and ports) to pass
  - Based on the Access Control Lists
    - permit packets into a network
    - deny packets entry
  - Blacklist, whitelist

Packet Level Firewalls



Defense: User Privilege

- A User Account indicates the privilege level of a user
  - Tells the computer which files and folders to access
  - Who can modify configuration changes
- Different Privileges
  - Guest accounts
  - Standard accounts
  - Administrator accounts

Creating Data Backups

- Copying files from a computer’s hard drive onto other digital media in a secure location
  - backup server, external hard drive, Cloud
- Questions?
  - What data to back up?
  - What media to use to store backups?
  - Where to store?
- Backup strategies;
  - Scheduled Backups
  - Continuous Backups

END