# Intro to Security Attacks

## Malware

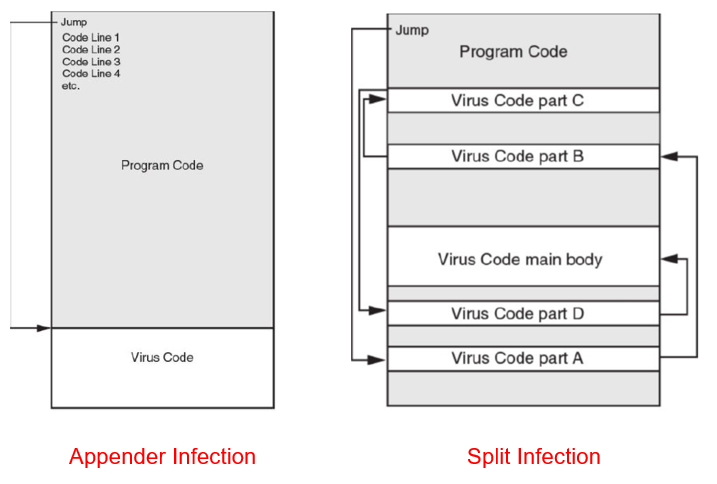
* Malware is short for "malicious software," aka malicious code or "malcode".
* Designed to damage, disrupt, or gain unauthorized access to a computer system.
* Includes viruses, trojans, ransomware etc.,
* Can be distinguished from each other in terms of how they propagate and operate
* Most popular attacking tool (APWG, 2017)

## Computer Viruses

* Propagates by inserting a copy of itself into and becoming part of another program, (i.e., reproduce by infecting other files)
  + Insertion Phase is inserting itself into file
  + Execution phase is performing some (possibly null) action
* Almost all viruses are attached to an executable file (and macros)
* Insertion phase must be present but does not need to be always executed
* Require a host program for spreading
* Viruses may display an annoying message or be much more harmful…
  + Cause a computer to repeatedly crash
  + Erase files from or reformat hard drive
  + Turn off computer’s security settings
* Virus cannot automatically spread to another computer
  + needs user action to spread
  + spread by sharing infecting files

## Types of Virus Infection

* Appender infection:
  + Virus appends itself to the end of the file
  + Moves first three bytes of original file and places them in virus code
  + Replaces them with a jump instruction that redirects control to virus
* Swiss cheese infection:
  + Viruses inject themselves into executable code
  + Original code transferred and stored inside virus code
  + Host code executes properly after the infection
* Split infection:
  + Viruses split the malicious code itself into several parts:
    - Parts placed at random positions in host program
    - Head of virus code starts at beginning of file
    - Once executed, gives control to next piece of virus code
  + To make detection even more difficult these parts may contain unnecessary “garbage” code to mask their true purpose



## 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
* Worms may:
  + Consume resources or
  + Leave behind a payload to harm infected systems
* Examples of worm actions
  + Deleting computer files
  + Allowing remote control of a computer by an attacker



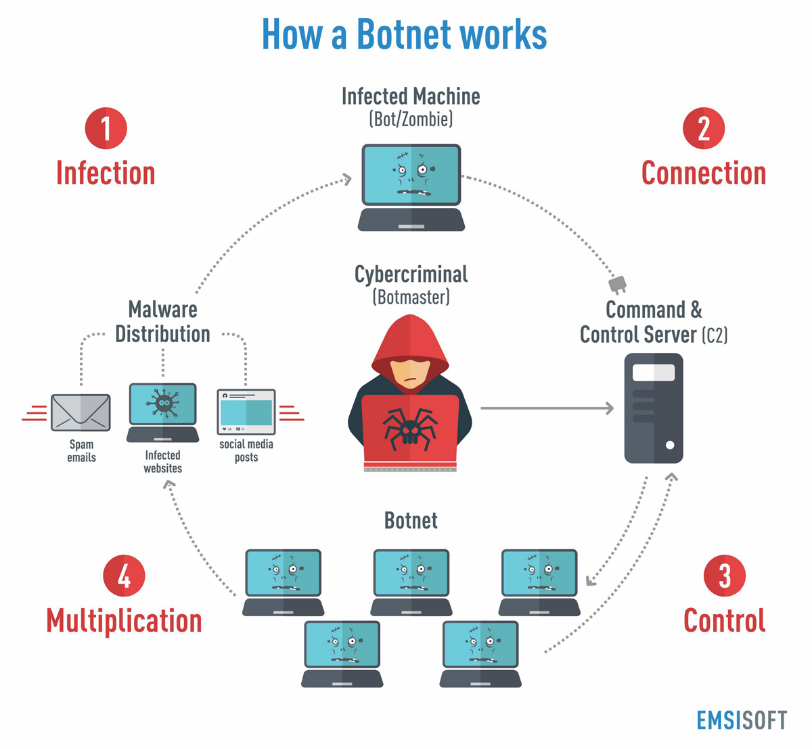
## Trojans

* Harmful program that looks legitimate but does something other than advertised
  + Sometimes made to appear as data file
* Users are typically tricked into loading and executing it on their systems (e.g., video/audio files online)
* Typically executable programs
  + Contain hidden code that launches an attack
* Example:
  + User downloads “free calendar program”
  + Program scans system for credit card numbers and passwords
  + Transmits information to attacker through network



## Bots and Botnets

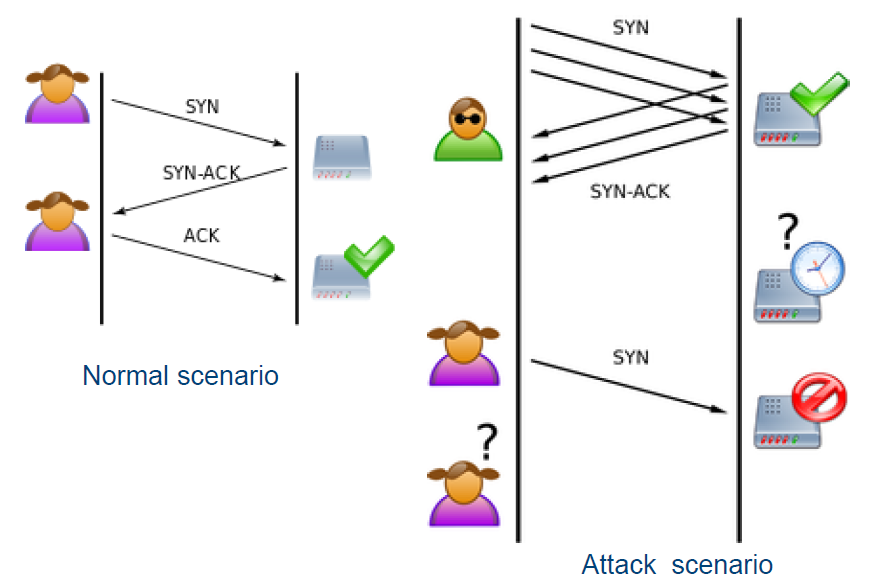
* Bot is derived from the word "robot" and is an automated process that interacts with other network services
  + self-propagating malware designed to infect a host, contains payload of trojans, worms, and viruses
  + connects infected computer, known as a **zombie**, to a central server or servers that act as the command and control center.
  + The entire network of zombie computers together called **botnet**
* With a botnet, attackers can launch broad-based, "remote-control," flood type attacks against their target(s).



## Distributed Denial of Service (DDoS)

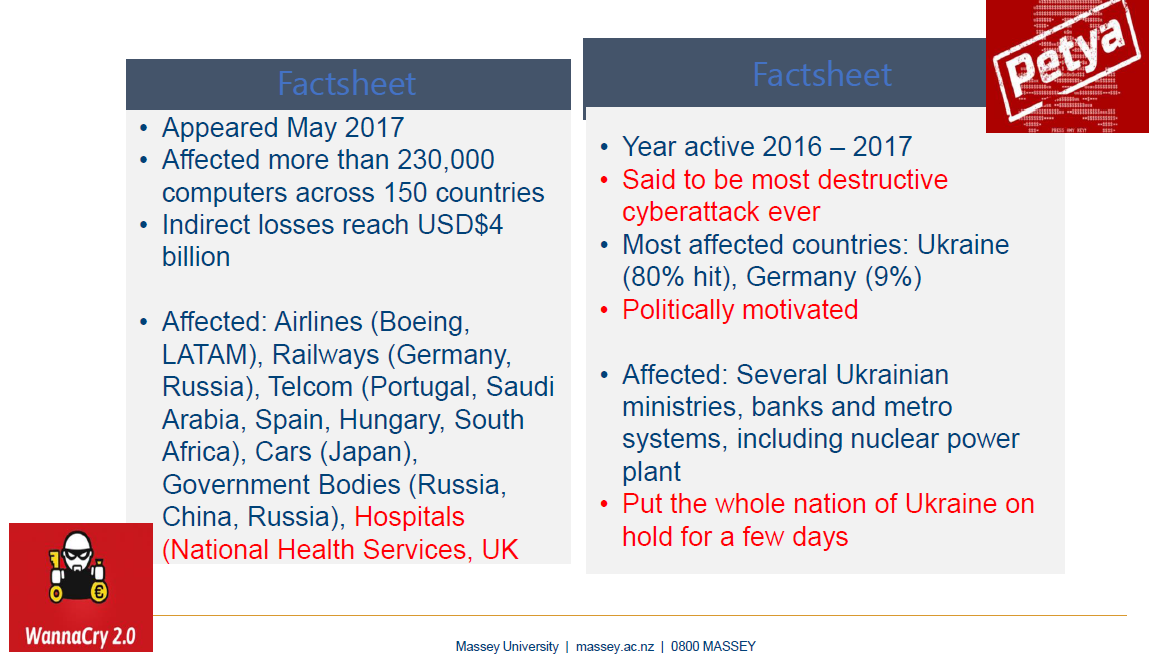


* These multi-person, multi-device barrages are generally harder to deflect, mostly due to the sheer volume of devices involved.
* launched from multiple connected devices that are distributed across the Internet.
  + Command zombies to stage a coordinated attack on the victim
  + Overwhelm victim with traffic arriving from thousands of different sources
* DDoS often exploits networking protocols
  + SYN flood: send lots of “open TCP connection” requests with spoofed source addresses
  + UDP flood: exhaust bandwidth by sending thousands of bogus UDP packets
  + Smurf: ICMP echo request to broadcast address with spoofed victim’s address as source
  + HTTP request flood: flood server with legitimate looking requests for Web content

  
*Example of SYN Flood*

## Ransomware

* A type of malicious software designed to block access to a computer system until a sum of money is paid.
* Has a number of phases:
  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
     + Confidential files (business documents, operational data, etc)
  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
* Examples include WannaCry and Petya…



## 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 + Ransomware
  + Petya targeting Ukrainian organizations (banks, ministries, newspapers, and electricity firms etc.,)