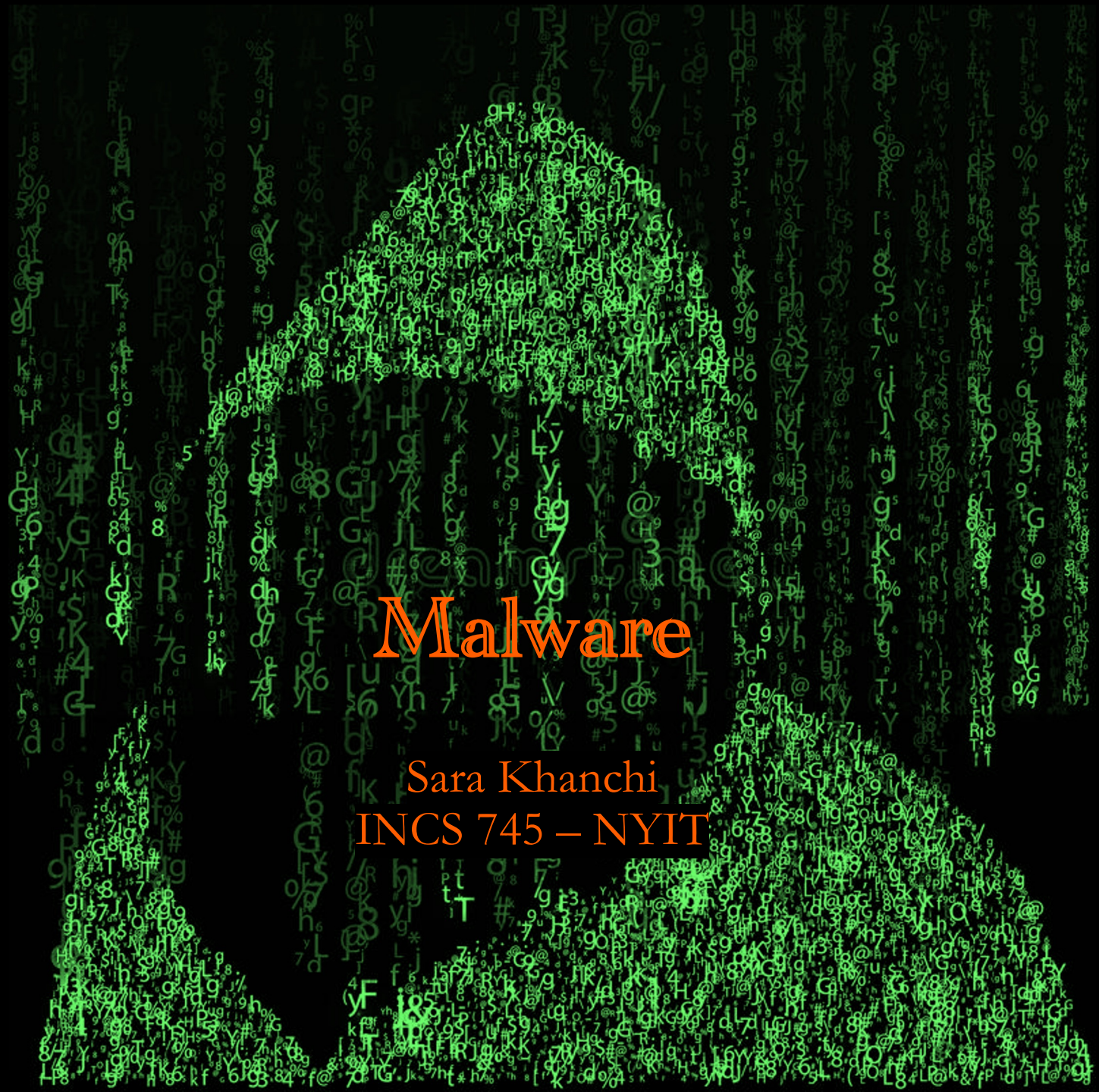


Malware

Sara Khanchi
INCS 745 – NYIT

Outline

- Definition
- Classification
- Detection
- Tools

Malware

- Where the name (Malware) come from?
- What is it?
  - Any software that does something that causes detriment to the user, computer, or network - such as viruses, trojan horses, worms, rootkits, scareware, and spyware - can be considered malware.
  - Based on NIST.SP.800 definition
    - Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system.
    - "Software or code" can be executable programs, or even files that cause controlled code execution to occur.

Malware classification

- Why is it important?
- Malware Taxonomy
- Based on what characteristics we are going to group them?

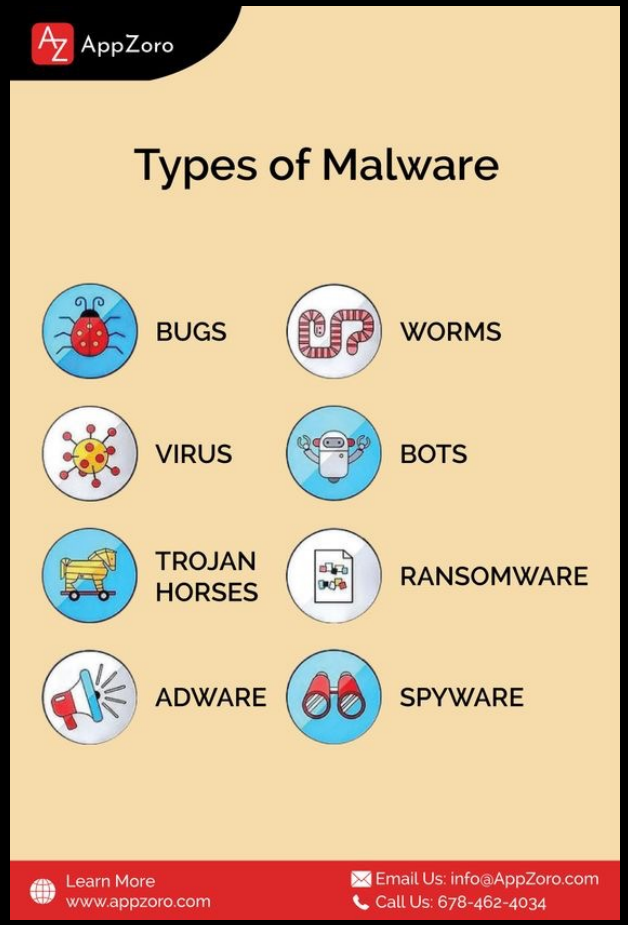
Malware classification

- Classification types
  - Based on the end goals, there are several types of classification
- Functional Classification
  - About the features of the malware
  - Malware names such as ransomware, backdoor,…
- Familial, Lineage Classification
  - The focus is on the authorship and the lineage of the malware tool.
- Behavioral
  - Focuses on the behaviors exhibited by the malware
  - Similar to functional classification, but more focused on the behaviors rather than the features

Functional Classification

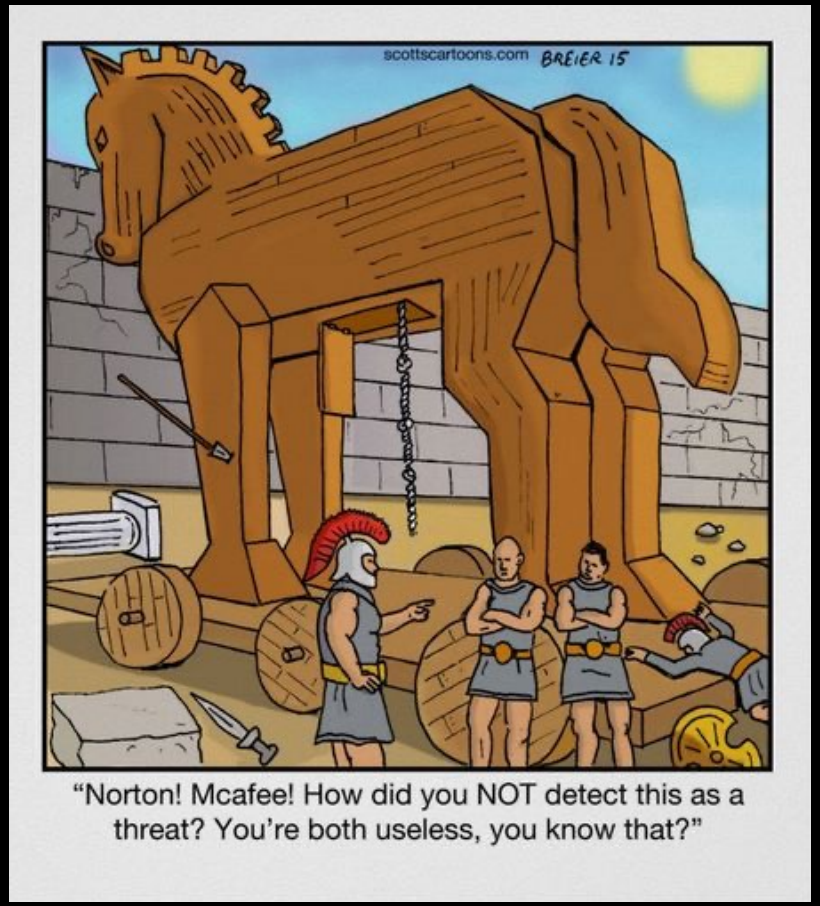
- The first category of the malware uses terminologies like
  - Trojan Horse
  - Backdoor
  - Remote Access Tool
  - Downloader
  - Dropper
  - Botnet
  - Monitor
  - Scareware
  - Ransomware
  - Information Stealer
  - Rootkit
  - Worm
  - Virus

- A malware could have several features



Trojan Horse

- Have you heard the story of Greeks entering the city of Troy?
- How this translate in to the malware?



Trojan Horse

- A Trojan horse, or Trojan in short, is a self-contained, nonreplicating program that, while appearing to be benign, actually has a hidden malicious purpose.
- Trojan horses either replace existing files with malicious versions or add new malicious files to hosts.
- They often deliver other attacker tools to hosts.
- Examples:
  - A free Anti-virus you have downloaded
  - A legit software that you downloaded from untrusted website

Backdoors & Remote Access Tools

- Used by attackers to continue their communication with the compromised system to enhance their malicious activity
- A backdoor is a malicious program that listens for commands on a certain TCP or UDP port.
  - Most backdoors allow an attacker to perform a certain set of actions on a host, such as acquiring passwords or executing arbitrary commands.

- Remote access tool (RAT) is a fancy version of Backdoor with more functionality options

Downloader

- Downloader, provide the capability for the attacker to download other tools on the machine it is running on.
- Mostly, the initial malware is a lightweight tool which is delivered using attack vectors like spear-phishing or malicious Java applet buried in a advertisement.
- The tool is pre-configured to download the more complicated malware from Internet.
- This makes detection of the attack harder.

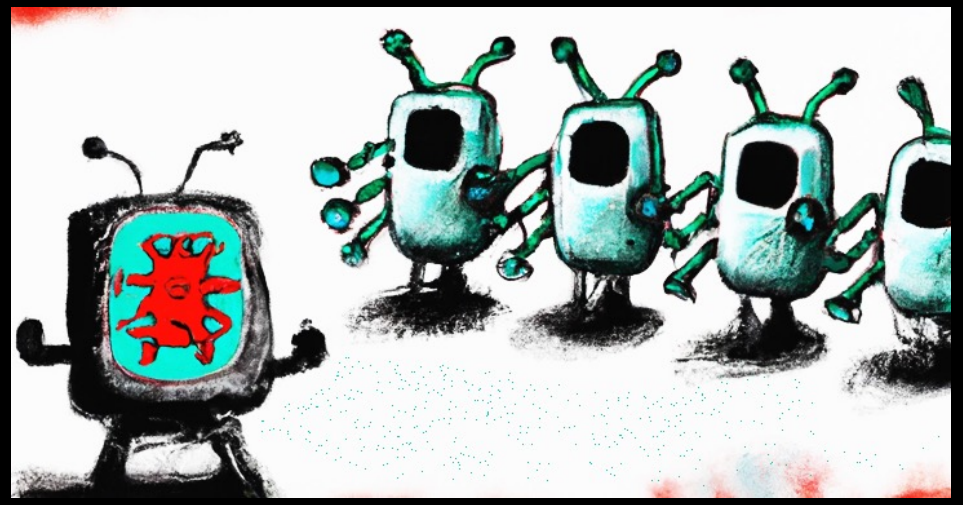
Dropper

- This type of malware, contains other malware code inside, which needs to create them on disk first and then execute them.
- This is a typical case with the Trojan horses.
- The action of writing the malware to the disk to be executed or get ready for execution is called dropper functionality.
  - The Dropper malware, drops an executable malware to the disk.

Botnet

- What the word stands for?
- Similar to the backdoor functionality, but it is described as a malware with 1-n relationship.
  - Bot (robot), zombie, drone
  - Secretly takes over another Internet-attached computer and then uses that computer to launch or manage attacks that are difficult to trace to the bot's creator
- A botnet is a collection of bots often capable of acting in a coordinated manner

- Well-known for what type of attack?



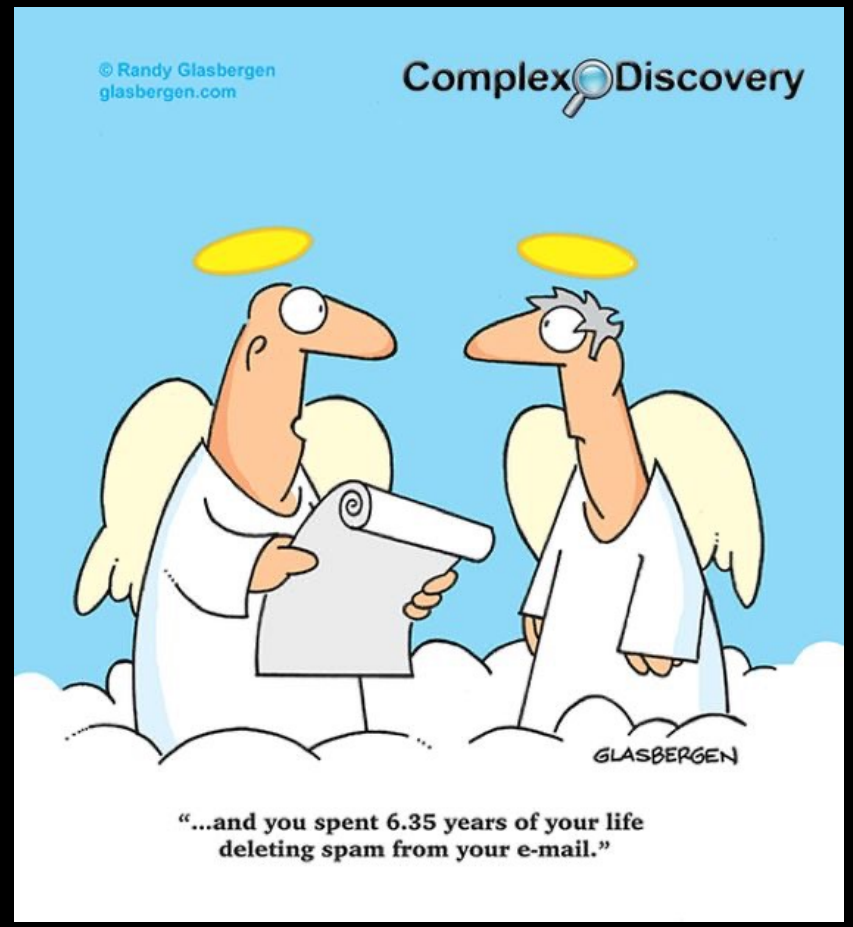
Monitor

- Malware employs Monitor functionality to record user's activity and/or environment.
- The recorded data will be send back to the attacker (Called?).
- Sources for monitoring :
  - Webcam
  - Microphone
  - Desktop recording
  - Password prompts
  - Common data
  - folders (like "My Documents")
  - Keyboard (keylogging)
  - Web browser traffic
  - Network traffic

Mailer

- Also called spammer or spambot.
- Due to the profitable nature of bulk advertising, and bult malware phishing, one technique is to use the compromised systems as sources of the new unsolicited emails.

- Send SMTP emails from the systems
- More complicated: distribute emails using the web-based mail account owned by the target
  - The source is authentic



Scareware/Adware

- It is mostly employed to achieve a social engineering outcome.
- Scares the user to take action immediately, such as paying money to not losing their immigration status
- A common type: Fake Anti-Virus
  - Annoying
  - Pay to remove it

Ransomware

- Similar to scareware
- Tries the social engineering to get the money
- Typically, encrypts the data, or transfer them to a remote server and deletes the local version
- To get the data back, the victim needs to pay the ransom
- Does it guarantee the retrieval of their data?

Information Stealer

- Stealing personal, private, and/or confidential information from the target in an efficient way.
- As soon as connected, the data is gathered based on the hard-coded or network based collection plan to a remote system.
- Common types of information:
  - Contacts list theft
  - Crypto-currency wallets
  - Browser cookies/history/saved credentials
  - Documents theft
  - OS passwords and other keystore data

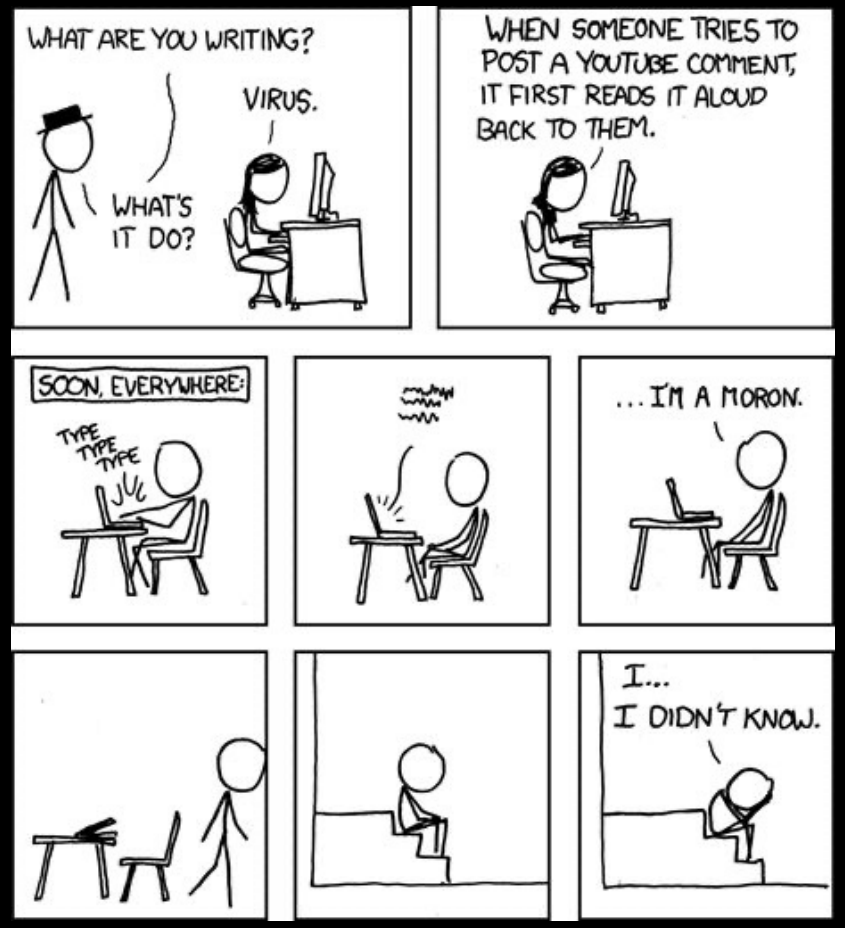
Rootkit

- A set of programs installed on a system to maintain covert access to that system with administrator (or root) privileges, while hiding evidence of its presence to the greatest extent possible
- A common way to do stealth operation
  - Write a driver to get installed with super-user privileges
  - The driver overrides directory traversal, file operations, and process inspection to make sure malware files and processes are hidden when active

Virus and Worm

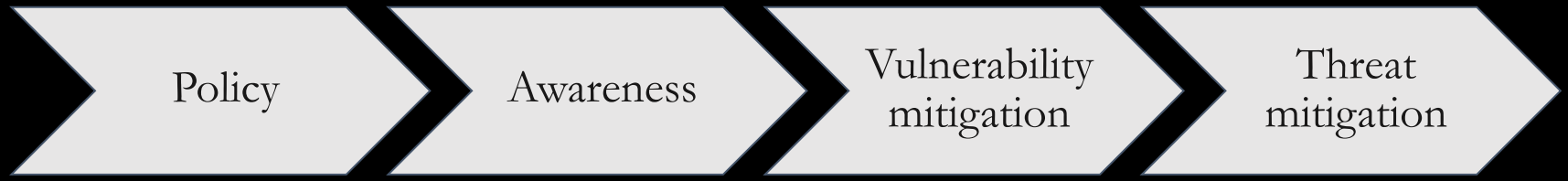
- Both virus and worm functionality describe the self-propagation mechanisms for malware.
- Worm
  - Independent
  - Fully propagate itself across system and networks.
- Virus
  - Parasite
  - Needs a host to replicate
- Can a document be infected by a virus?

Virus


WHAT ARE YOU WRITING?
VIRUS.
WHAT'S IT DO?
WHEN SOMEONE TRIES TO POST A YOUTUBE COMMENT, IT FIRST READS IT ALOUD BACK TO THEM.
SOON, EVERYWHERE:
TYPE TYPE TYPE
...I'M A MORON.
I...
I DIDN'T KNOW.

Countermeasures

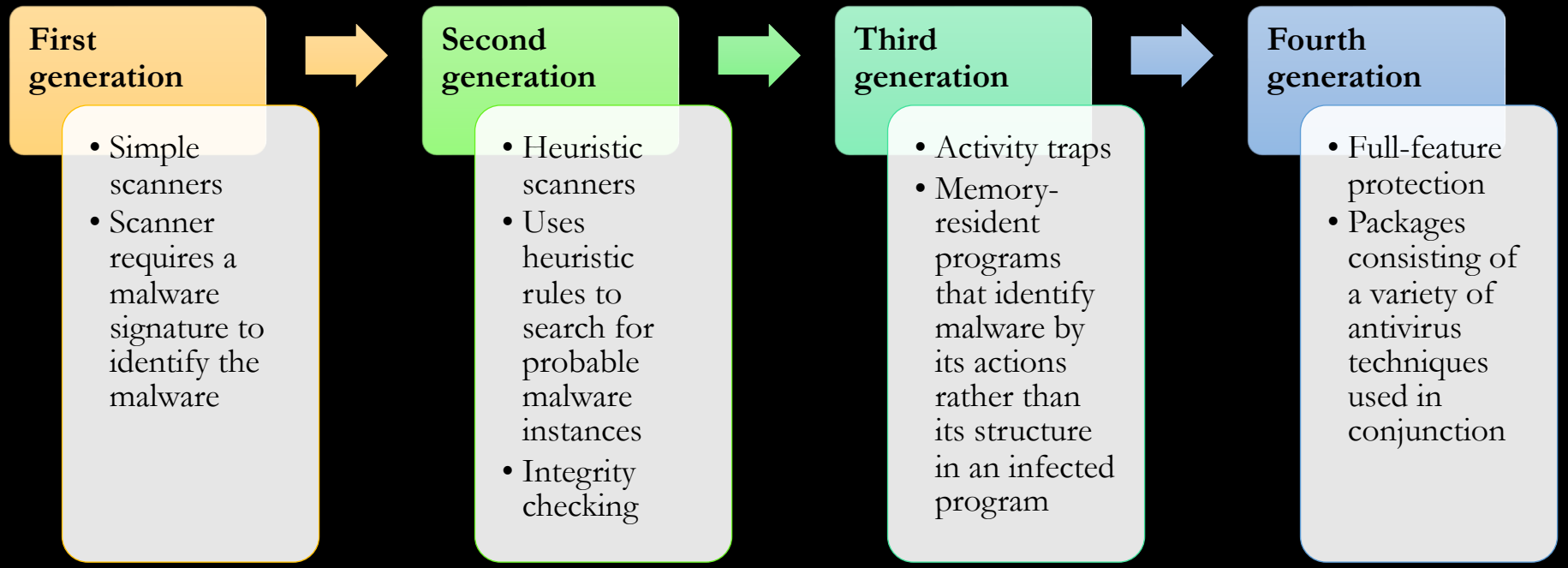
- Elements of prevention:



- Systems are current: all patches are applied
  - Reduces the number of vulnerabilities
- Set proper access controls on application and data stored
- User awareness for social engineering attacks

Host-Based Scanners

- Four generations of antivirus software:



Host-Based Behavior-Blocking Software

- Integrates with the operating system of a host computer
- Monitors program behavior in real time for malicious actions
- Block malicious actions
- All good! Then what is the limitation?

Malware Analysis

- Why analyzing malware?

- Two types of malware analysis:
  - Static Analysis
  - Dynamic Analysis

Static Analysis vs Dynamic Analysis

- The process of documenting your observations about what identifying characteristics a malware sample exhibits.
- Use the information to get more samples of the malware

- Static analysis doesn't activate the malware
  - The focus is on how the malware "looks"

- Dynamic analysis explore the behavior of the malware (the actions)
  - Should be done in a sandbox to prevent the spread of the malware

Tools

- Static Analysis
  - Awk | sed |grep
  - Strings
  - Yara
  - Readelf
  - Exiftool
  - File
  - Hex reader: hxd, xxd
  - File Analyzer: PEView, PE Studio
  - Wireshark, Tshark, Tcpdump
- Debugger:
  - X64dbg, x32dbg
  - ollydbg
- Disassembler:
  - Ida Pro
  - Objdump
  - Radar2
- Decompilers:
  - Cutter: C/C++
  - .NET: DnSpy
  - Java: Jad
  - Flash action script: Jpexs
  - Ghidra: reverse engineering
- Dynamic Analysis
  - Process Monitor
  - Sandboxes
  - Decompiler

Helpfull Websites

- virustotal.com - free service that analyzes suspicious files and URLs
- any.run – Check malware behavior
- malwr.com - Malwr is a free malware analysis service
- hyrbid-analysis - free malware analysis service
- whois.domaintools.com - look up domains
- robtex.com - free DNS lookup tool
- regex101.com - Online Visual Regex Tester

Summary

- Malware definition
- Malware classification
  - Functional Classification
  - Familial, Lineage Classification
  - Behavioral
- Functional Classification: Malware features
  - Trojan Horse
  - Backdoor
  - Remote Access Tool
  - Downloader
  - Dropper
  - Etc.
- Scanner Types
- Malware analysis
  - Static
  - Dynamic