Malicious Code

Dr. Amit Praseed

WannaCry

- The WannaCry attack targetted computers running Windows by encrypting data and demanding ransom
    - “Ransomware” attack
    - NHS and FedEx servers were affected
- WannaCry propagates using a buffer overflow vulnerability in the SMB protocol
- Once the ransomware infects a system, it tries to contact an obscure server and proceeds to encrypt the system if the server was not reachable
    - This acted as a killswitch to stop the spread of the ransomware
- Once it infects a system, it searches for other systems on the network and spreads using the SMB protocol

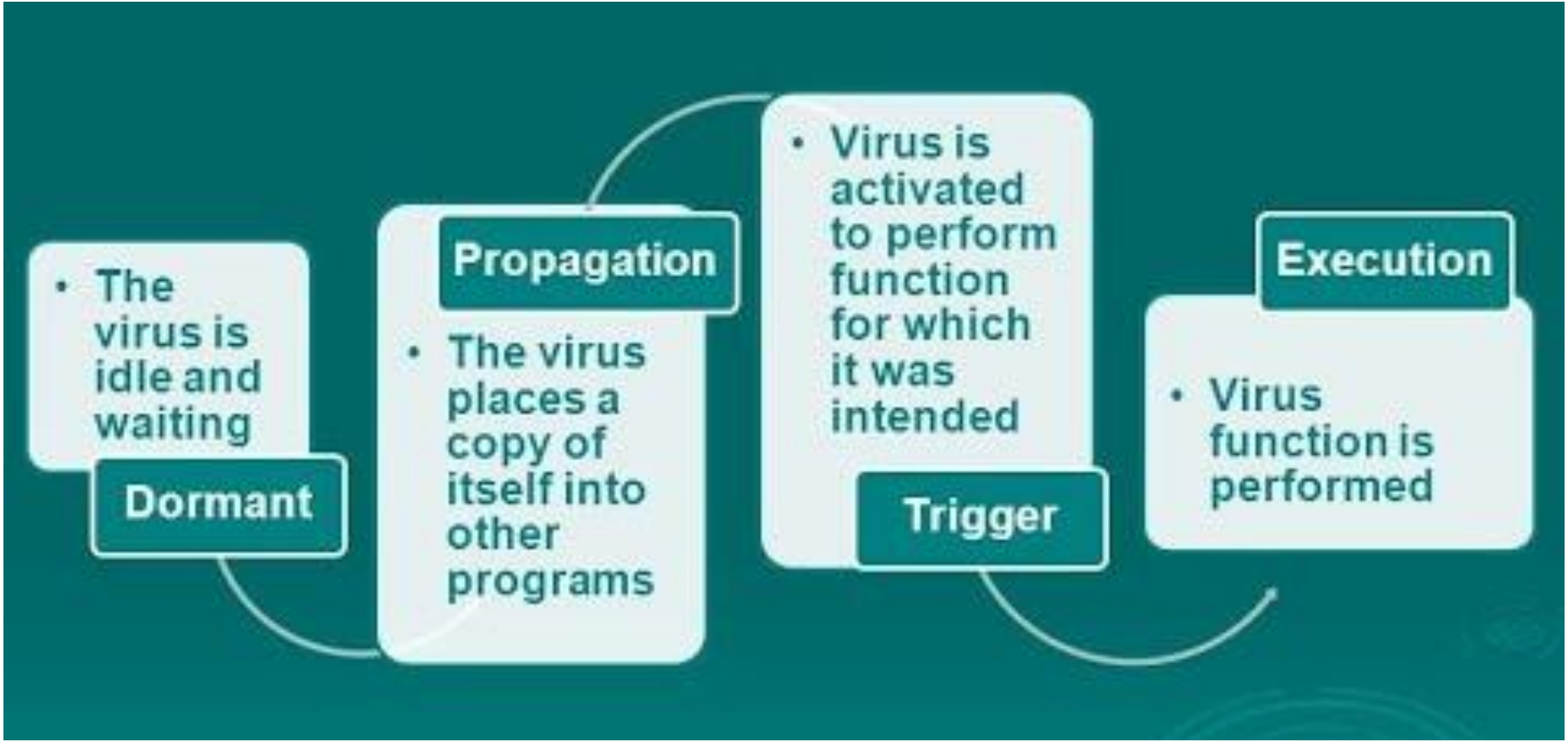
Malicious Code

- Malicious code or rogue programs or malware is the general name for programs or program parts planted by an agent with malicious intent to cause unanticipated or undesired effects
    - Distinguishes this type of code from unintentional errors, even though both kinds can certainly have similar and serious negative effects.
- Malware is an umbrella term for a wide variety of software
    - Virus
    - Worms
    - Adware
    - Spyware
    - Trojan Horses etc...

Virus

- A virus is a program that can replicate itself and pass on malicious code to other nonmalicious programs by modifying them.
- A good program can be modified to include a copy of the virus program, so the infected good program itself begins to act as a virus
- There are two broad categories of virus
    - A **transient virus** has a life span that depends on the life of its host; the virus runs when the program to which it is attached executes, and it terminates when the attached program ends.
    - A **resident virus** locates itself in memory; it can then remain active or be activated as a stand-alone program, even after its attached program ends.

Virus Life Cycle



Dormant

- The virus is idle and waiting

Propagation

- The virus places a copy of itself into other programs

Trigger

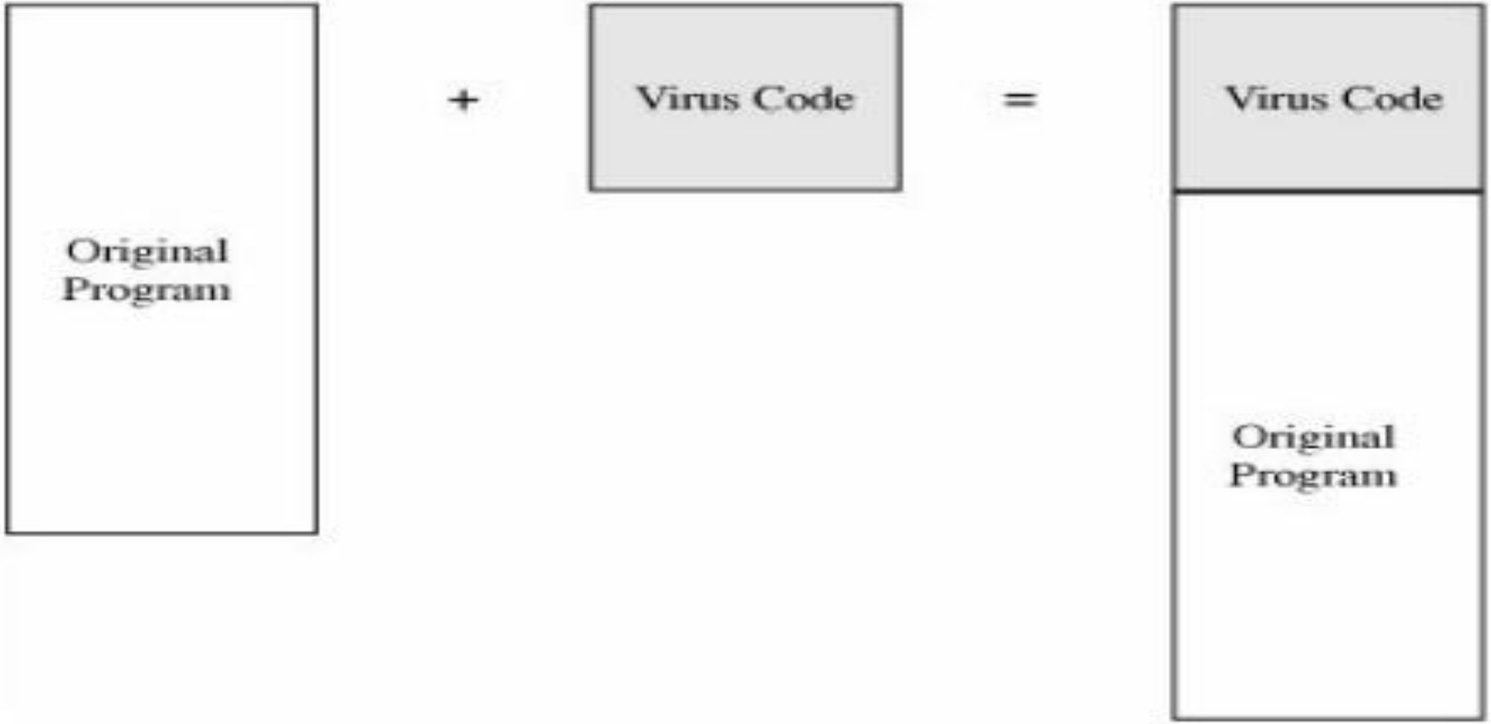
- Virus is activated to perform function for which it was intended

Execution

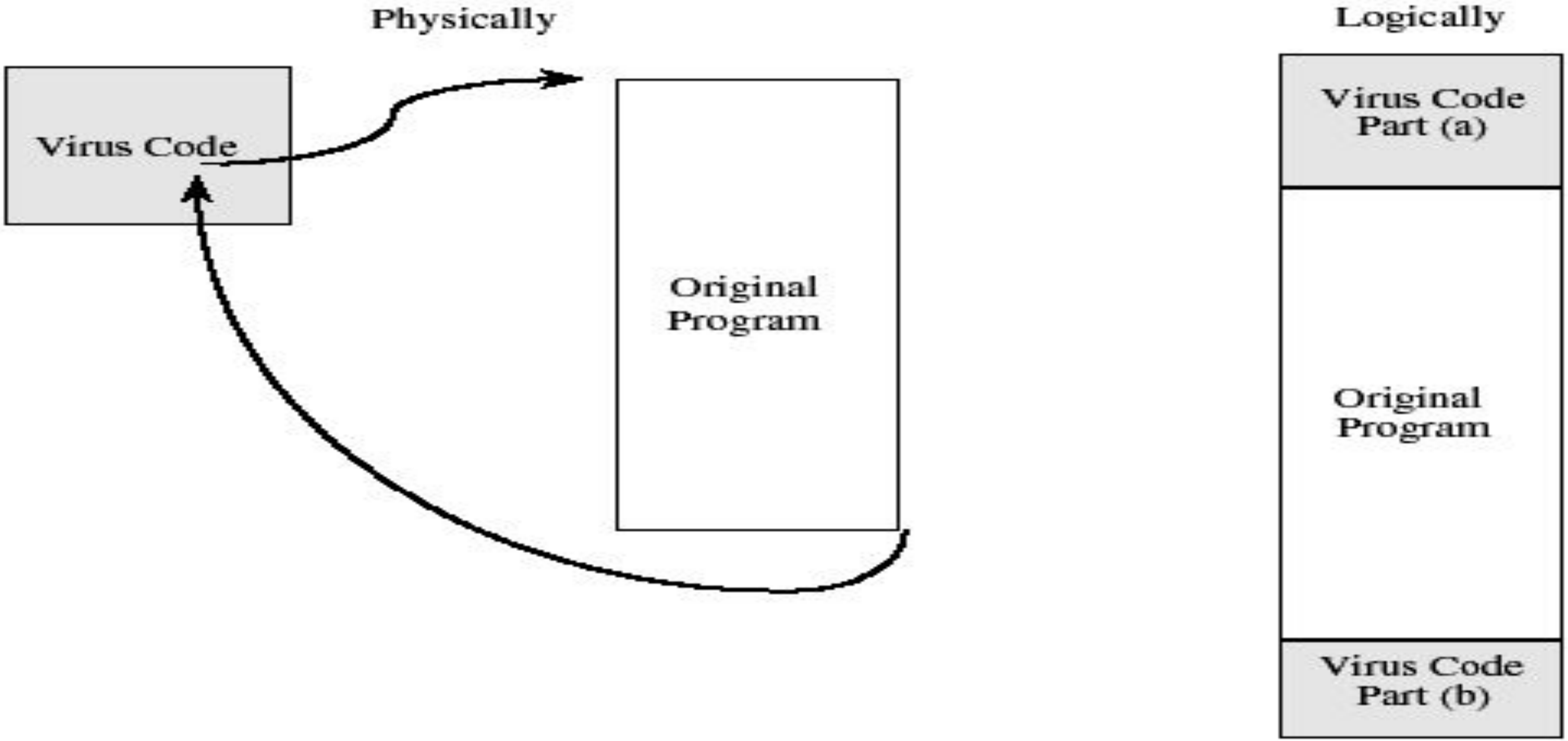
- Virus function is performed

Attached Virus

Figure 3-4. Virus Appended to a Program.

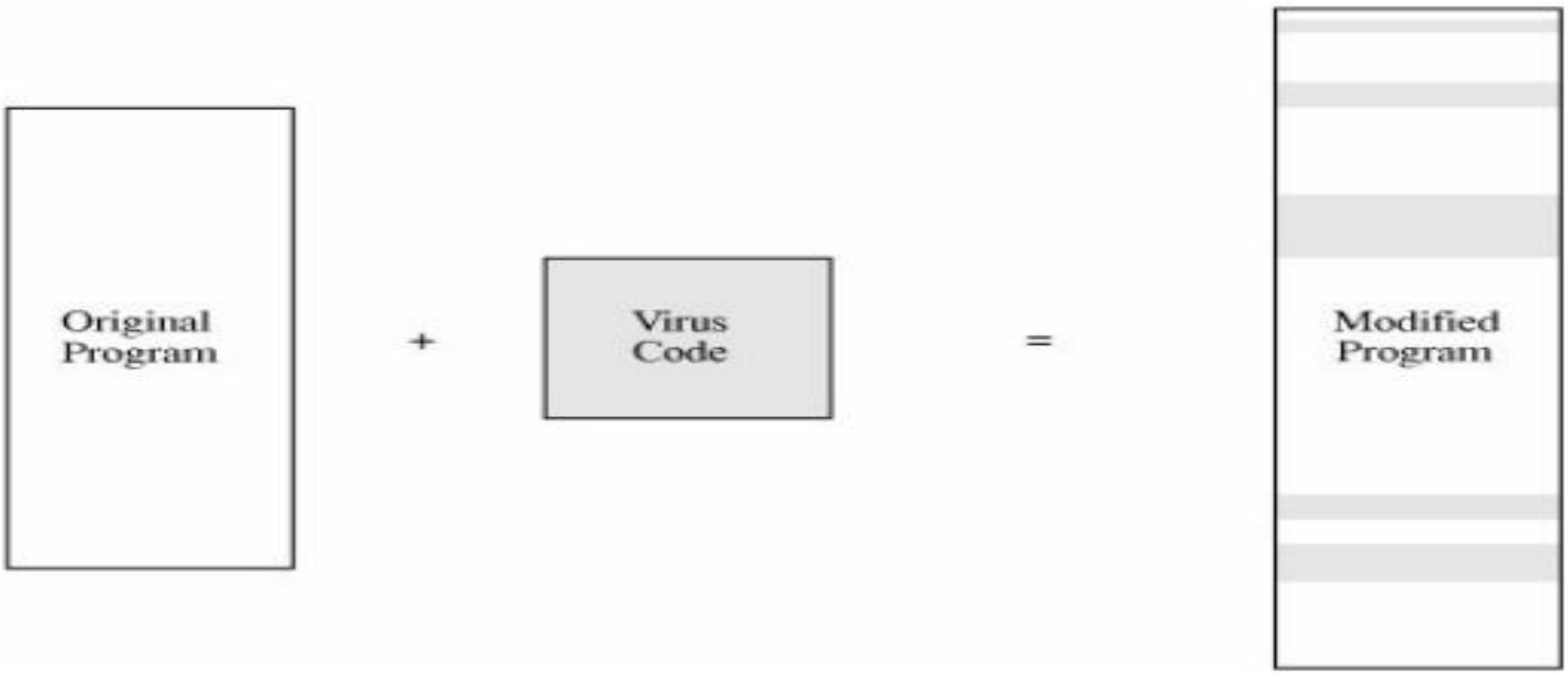


Virus surrounding a Program



Integrated Virus

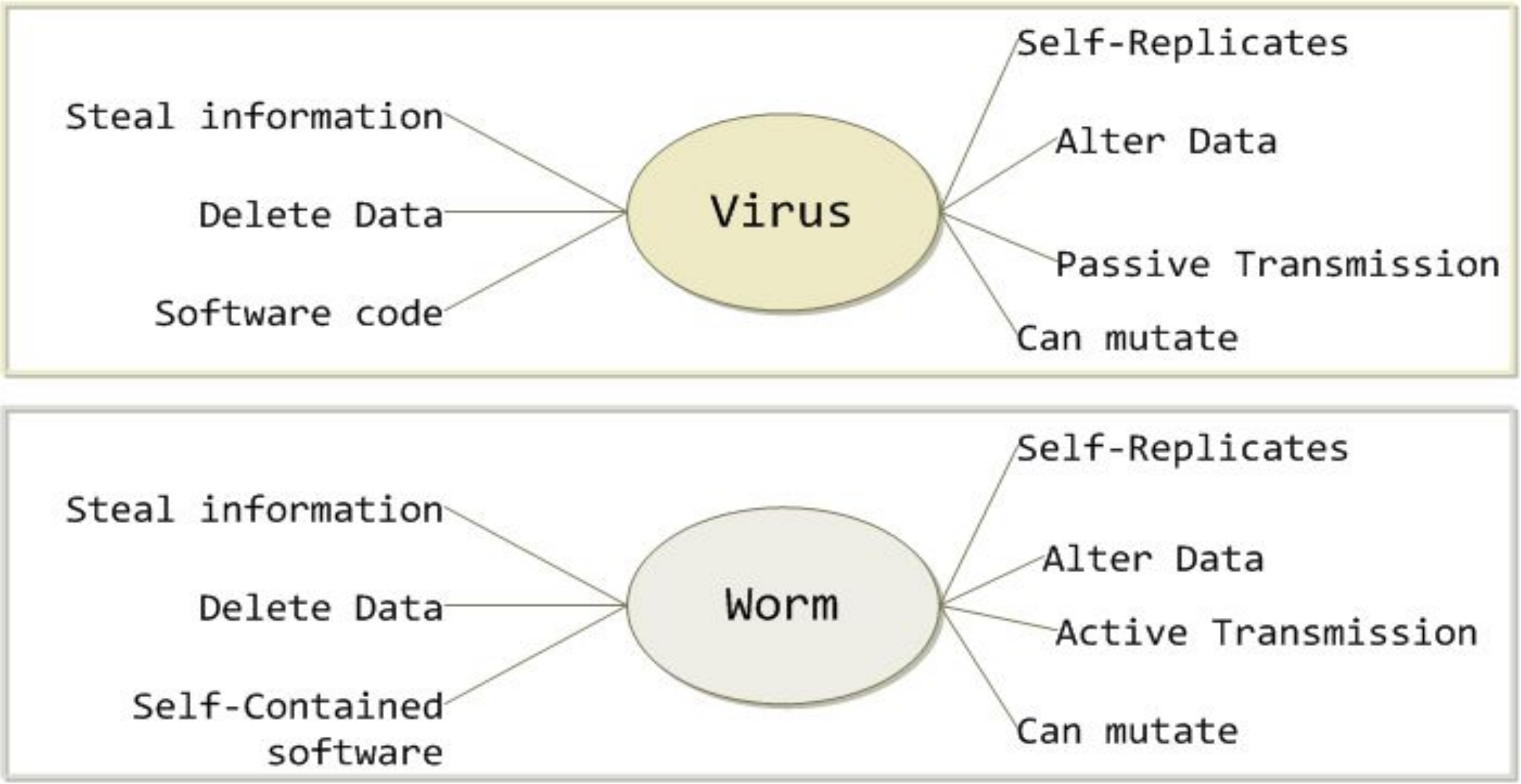
Figure 3-6. Virus Integrated into a Program.



Worm

- A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers
- Computer worms use recursive methods to copy themselves without host programs and distribute themselves based on the law of exponential growth, thus controlling and infecting more and more computers in a short time
- Many worms are designed only to spread, and do not attempt to change the systems they pass through. However, side effects of worm infestation can be damaging by themselves
- Eg: Morris Worm spread using a buffer overflow vulnerability in the UNIX fingerd utility. Morris' coding mistake, in instructing the worm to replicate itself regardless of a computer's reported infection status, transformed the worm from a potentially harmless intellectual and computing exercise into a viral denial of service attack

Virus vs Worm



Steal information

Delete Data

Software code

Virus

Self-Replicates

Alter Data

Passive Transmission

Can mutate

Steal information

Delete Data

Self-Contained software

Worm

Self-Replicates

Alter Data

Active Transmission

Can mutate

Trojan Horse

- A Trojan horse is any malware that misleads users of its true intent
- Trojans generally do not attempt to inject themselves into other files or otherwise propagate themselves
- Once installed, trojans may perform a range of malicious actions
  - Many tend to contact one or more Command and Control (C2) servers across the Internet and await instruction.
  - Can be used to launch attacks discreetly
  - Since individual trojans typically use a specific set of ports for this communication, it can be relatively simple to detect them.
- Eg: Storm Worm was a trojan horse worm that spread through emails with catchy titles. The infected systems were turned into a botnet