Research Week 06

Chaz Davis

February 12, 2020

1 Briefly describe the four generations of anti-virus software

Anti-virus: The computer software that is used to avoid, catch, and eliminate malicious software is known as anti-virus

- **Four generations:**

  first generation avs is required to have "simple scanners" to determine the malware

  second gen avs is required to have "heuristic scanners" to search for possible malware occassion using heuristic rules or needs an "integrity checking" to determine changed files

  third gen avs is required to have "activity traps" in an infected program to determine malware by its measures rather than its structure.

  fourth gen avs is required to have "Full Featured Protection" This full featured protection uses a collection of anti-virus techniques packages used in conjunction with activity trap components and scanning.

2 Describe some malware countermeasure elements.

- **Prevention** this measure prevents Mal ware from getting into the system or blocking its capability to change the system through policy, awareness, susceptibility, mitigation, and threat detection
- **Detection** the measure determines the positions of the Mal ware
- **Identification** detects the specific malware that has infected the system
- **Removal** removes all elements of malware virus from every infected system so it cannot propagate further.

3 What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware?

- **Backdoor** it is a secret admission point into a system or program that permits an important person who is concious of the backdoor to get access without going through the common security access procedures
- **Rootkit** collection of programs implemented on a system to sustain secret access to that system with administrator rights, while hiding proof of its presence to the most extent possible
- **Bot** a threat to the network resources and computational of the infected system for use and it is done by the attacker
- **Keylogger** software which records every keystroke on the infected machine to permit an attacker to observe responsive information especially the information that contains the login and password credentials
- **Spyware** an attack that causes the machine to permit observing of the range of action on the system, observing the history and content of browsing action, dynamically changes the data exchange between the browser and websites

Yes, all can be present within the same malware.

4 What is "Ransomware"?

A type of malicious software designed to block access to a computer system until a sum of money is paid. Files are encrypted. Like an RSA encryption, where the attacker has the unencryption key and until paid you are locked out.

5 What means can a worm use to access remote systems to propagate?

The mechanisms that worm can use to spread:

- Email or instant messenger
- File sharing
- Remote execution capability
- Remote file access or transfer capability
- Remote login capability

6 Assume you have found a USB memory stick in your work parking area.

What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms we discuss could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?

When a memory stick is plugged into the computer which was found in the parking area may create a variety of threats to the confidentiality, integrity, and availability of the system

*The memory stick may transmit an "executable virus" or "macro virus" on to the system**

Executable virus - Executable program files are affected by machine executable virus and these program files work with specific operating system and in some cases it is based upon the hardware platform.

Macro virus - Files with macro or scripting code are affected by macro viruses and its support effective content in a field of user document types and is translated by an application

*The memory stick may transmit a "malicious worm"**

Worm - While viewing the memory stick, worm runs automatically and infects other appropriate files as a virus on the system

*The memory stick may contain a trojan horse**

Trojan horse - malicious piece of code that is delivered through the mail or web page or through the USB drives that causes damage to the data or system

Steps to mitigate the problem:

- the user should scan the memory stick with appropriate up-to-date avs
- the user could check the memory stick in a controlled environment.

  for example a live boot linux or emulation environment

7 Consider the following fragment:

```
legitimate code
if data is Friday the 13th;
crash_computer();
legitimate code
```

What type of malware is this?
The type of malware being used is a logic bomb, which is a key part of data corrupting malware.

- It is code inserted in malware that is placed to "explode" when certain actions are met
- The actions take place in the given fragment, it checks the data with appropriate day and date that is Friday the 13th
- If the condition is met it calls the function crash_computer()
- For a logic bomb, the example conditions hat can be used as triggers are as follows
- The presence or absence of devices or files on the system
- An appropriate date or day of the week
- Software with appropriate version or configuration
- The application executed by the appropriate user
- Once activated, a bomb may change or delete data or complete files, or other damage