Comptia Security + SY0-601 2023/ 2024 Exam| Questions and Verified Answers with Rationales| 100% Correct| Grade A

Q: You have heard about a new malware program that presents itself to users as a virus scanner. When users run the software, it installs itself as a hidden program that has administrator access to various operating system components. The program then tracks system activity and allows an attacker to remotely gain administrator access to the computer.
Which of the following terms best describes this software?

A. Privilege escalation
B. Trojan horse
C. Rootkit
D. Spyware
E. Botnet

Answer:
C. Rootkit

This program is an example of a rootkit. A rootkit is a set of programs that allow attackers to maintain permanent, administrator-level, and hidden access to a computer. Rootkits require administrator access for installation and typically gain this access using a Trojan horse approach--masquerading as a legitimate program to entice users to install the software.
While this program is an example of a Trojan horse that also performs spying activities (spyware), the ability to hide itself and maintain administrator access makes rootkit a better description for the software. A botnet is a group of zombie computers that are commanded from a central control infrastructure.

Q: While browsing the internet, you notice that the browser displays ads that are targeted towards recent keyword searches you have performed.
What is this an example of?

A. Zombie
B. Worm
C. Adware
D.Logic bomb

Answer:
C. Adware

Adware monitors actions that denote personal preferences, then sends pop-ups and ads that match those preferences. Adware:
• Is usually passive
• Is privacy-invasive software
• Is installed on your machine by visiting a particular website or running an application
• Is usually more annoying than harmful

A logic bomb is designed to execute only under predefined conditions and lays dormant until the predefined condition is met. A worm is a self-replicating virus. A zombie is a computer that is infected with malware that allows remote software updates and control by a command and control center called a zombie master.

Q: Which of the following best describes spyware?

A. It monitors the actions you take on your machine and sends the information back to its originating source.
B. It is a malicious program disguised as legitimate software.
C. It is a program that attempts to damage a computer system and replicate itself to other computer systems.
D. It monitors user actions that denote personal preferences, then sends pop-ups and ads to the user that match their tastes.

Answer:
A. It monitors the actions you take on your machine and sends the information back to its originating source.

Spyware monitors the actions you take on your machine and sends the information back to its originating source.
Adware monitors the actions of the user that denote their personal preferences, then sends pop-ups and ads to the user that match their tastes. A virus is a program that attempts to damage a computer system and replicate itself to other computer systems. A Trojan horse is a malicious program disguised as legitimate software.

Q: What is the common name for a program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the systems where it is found?

A. Virus
B. Trojan horse

C. Java applet
D. Windows Messenger

Answer:
A. Virus

A virus is the common name for a program that has no useful purpose, but attempts to spread itself to other systems and often damages resources on the systems where it is found. Viruses are a serious threat to computer systems, especially if they are connected to the internet. It is often a minimal requirement to have an antivirus scanner installed on every machine of a secured network to protect against viruses.
Trojan horses are programs that claim to serve a useful purpose but hide a malicious purpose or activity. Windows Messenger is an instant message chat utility. Java applets are web applications that operate within a security sandbox.

Q: What is the primary distinguishing characteristic between a worm and a logic bomb?

A. Masquerades as a useful program
B. Self-replication
C. Spreads via email
D. Incidental damage to resources

Answer:
B. Self-replication

The primary distinguishing characteristic between a worm and a logic bomb is self-replication. Worms are designed to replicate and spread as quickly and as broadly as possible. Logic bombs do not self-replicate. They are designed for a specific single system or type of system. Once planted on a system, it remains there until it is triggered.
Both worms and logic bombs can be spread via email, and both may cause incidental damage to resources. While either may be brought into a system as a parasite on a legitimate program or file or as the payload of a Trojan horse, the worm or logic bomb itself does not masquerade as a useful program.

Q: What is another name for a logic bomb?

A. Asynchronous attack
B. Trojan horse
C. DNS poisoning
D. Pseudo flaw

Answer:
A. Asynchronous attack

A logic bomb is a specific example of an asynchronous attack. An asynchronous attack is a form of malicious attack where actions taken at one time do not cause their intended, albeit negative, action until a later time.
A pseudo flaw is a form of IDS that detects when an intruder attempts to perform a common but potentially dangerous administrative task. DNS poisoning is the act of inserting incorrect domain name or IP address mapping information into a DNS server or a client's cache. A Trojan horse is any malicious code embedded inside of a seemingly benign carrier. None of these three terms is a synonym for logic bomb.

Q: You have installed anti-malware software that checks for viruses in email attachments. You configure the software to quarantine any files with problems.
You receive an email with an important attachment, but the attachment is not there. Instead, you see a message that the file has been quarantined by the anti-malware software
What has happened to the file?

A. The file extension has been changed to prevent it from running.
B. The infection has been removed, and the file has been saved to a different location.
C. It has been moved to a secure folder on your computer.
D. It has been deleted from your system.

Answer:
C. It has been moved to a secure folder on your computer.

Quarantine moves the infected file to a secure folder where it cannot be opened or run normally. By configuring the software to quarantine any problem files, you can view, scan, and possibly repair those files.
Quarantine does not automatically repair files. Deleting a file is one possible action to take, but this action removes the file from your system.

Q: Which of the following measures are you most likely to implement to protect against a worm or Trojan horse?

A. IPsec
B. Password policy
C. Anti-virus software
D. Firewall