Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 1/30/2022 10:35:01 am • Time spent: 03:42

Score: 100% Passing Score: 80%

Question 1: ✔ Correct

A collection of zombie computers have been set up to collect personal information. Which type of malware do the zombie computers represent?

- Trojan horse
- ➡ Botnet
- Logic bomb
- Spyware

EXPLANATION

A botnet is a collection of zombie computers that are controlled from a central control infrastructure to propagate spam or to collect usernames and passwords to access secure information.

A logic bomb is malware that lies dormant until triggered.

A Trojan horse is a malicious program that is disguised as legitimate software.

Spyware monitors the actions performed on a machine and then sends the information back to its originating source.

Question 2: ✔ Correct

Which kind of virus operates only in memory and usually exploits a trusted application like PowerShell to circumvent traditional endpoint security solutions?

- Fileless virus
- Ransomware
- Remote Access Trojan (RAT)
- Worm

EXPLANATION

Fileless viruses operate only in memory to avoid detection by traditional endpoint security solutions that are focused on matching signatures to files that have been written to the hard drive.

A worm is a self-replicating program.

Ransomware denies access to a computer system until the user pays a ransom.

A Remote Access Trojan (RAT) is a malware program that includes a backdoor that allows administrative control over the target computer.

Question 3: ✔ Correct

Which of the following describes a logic bomb?

- 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 type of malicious code similar to a virus whose primary purpose is to duplicate itself and spread while not necessarily intentionally damaging or destroying resources.
- A program that appears to be a legitimate application, utility, game, or screensaver that performs malicious activities surreptitiously.
- ➡ A program that performs a malicious activity at a specific time or after a triggering event.

EXPLANATION

A logic bomb is a program that performs a malicious activity at a specific time or after a triggering event. Logic bombs can be planted by a virus, a Trojan horse, or an intruder. Logic bombs may perform their malicious activity at a specific time and date or when a specific event occurs on the system, such as logging in, accessing an online bank account, or encrypting a file.

A type of malicious code similar to a virus whose primary purpose is to duplicate itself and spread, while not necessarily intentionally damaging or destroying resources, is a worm.

A program that appears to be a legitimate application, utility, game, or screensaver that performs malicious activities surreptitiously is a Trojan horse.

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 is a virus.

Question 4: ✔ Correct

A type of malware that prevents the system from being used until the victim pays the attacker money is known as what?

- Fileless virus
- Remote Access Trojan (RAT)
- Denial-of-service attack (DoS attack)
- ➡ Ransomware

EXPLANATION

A type of malware used to prevent the system from being used until a ransom is paid by the victim is known as ransomware.

While it does perform a denial of service, a DoS attack doesn't necessarily demand payment.

A Remote Access Trojan (RAT) is a malware program that includes a backdoor that allows administrative control over the target computer.

A fileless virus uses legitimate programs to infect a computer.

Question 5: ✔ Correct

Which kind of malware provides an attacker with administrative control over a target computer through a backdoor?

- ➡ Remote Access Trojan (RAT)
- Crypto-malware
- Potentially Unwanted Program (PUP)
- Trojan horse

EXPLANATION

A Remote Access Trojan (RAT) provides a backdoor for an attacker to remotely control a computer with administrative control. The other types of malware could be used in conjunction with a RAT, but they do not provide the remote control access.

PUP is software that contains adware, installs toolbars, or has other unclear objectives.

Crypto-malware is ransomware that encrypts files until a ransom is paid.

A Trojan horse is a malicious program that is disguised as legitimate or desirable software.

Question 6: ✔ Correct

Which of the following are characteristics of a rootkit? (Select two.)

- [ ] Uses cookies saved on the hard drive to track user preferences.
- [x] Resides below regular antivirus software detection.
- [ ] Collects various types of personal information.
- [ ] Monitors user actions and opens pop-ups based on user preferences.
- [x] Requires administrator-level privileges for installation.

EXPLANATION

A rootkit is a set of programs that allow attackers to maintain hidden, permanent, administrator-level access to a computer. A rootkit:

- Is almost invisible software.
- Resides below regular antivirus software detection.
- Requires administrator privileges for installation and then maintains those privileges to allow subsequent access.
- Might not be malicious.
- Often replaces operating system files with alternate versions that allow hidden access.

Spyware collects various types of personal information, such as internet surfing habits and passwords, and sends the information back to its originating source.

Adware monitors actions that denote personal preferences and then sends pop-ups and ads that match those preferences.

Both spyware and adware can use cookies to collect and report a user's activities.

Question 7: ✔ Correct

Which of the following best describes spyware?

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

EXPLANATION

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 and 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.

Question 8: ✔ Correct

Which of the following is a program that appears to be a legitimate application, utility, game, or screensaver, but performs malicious activities surreptitiously?

- ActiveX control
- Worm
- Outlook Express
- ➡ Trojan horse

EXPLANATION

A Trojan horse is a program that appears to be a legitimate application, utility, game, or screensaver, but performs malicious activities surreptitiously. Trojan horses are very common on the internet. To keep your systems secure and free from such malicious code, you need to take extreme caution when downloading any type of file from just about any site on the internet. If you don't fully trust the site or service that is offering a file, don't download it.

Outlook Express is an email client found on Windows.

A worm is a type of malicious code similar to a virus. A worm's primary purpose is to duplicate itself and spread while not necessarily intentionally damaging or destroying resources.

ActiveX controls are web applications written in the ActiveX framework.

Question 9: ✔ Correct

In 2001, a worm exploited vulnerabilities in Microsoft Internet Information Services (IIS) to infect over 250,000 systems in under nine hours. What was this worm called?

- Code Red
- Melissa
- Nimda
- Michelangelo

EXPLANATION

The worm known as Code Red replicated across the internet with incredible speed using a vulnerability in Microsoft IIS.

In 1991, the Michelangelo virus was designed to infect MS-DOS systems and remain dormant until March 6, the birthday of Renaissance artist Michelangelo.

In 1999, the Melissa worm was the first widely distributed macrovirus that was propagated in the form of an email message containing an infected Word document as an attachment.

In 2001, the Nimda worm took advantage of weaknesses found in the Windows platform and propagated itself in several ways, including email, infected websites, and network shares.

Question 10: ✔ Correct

You have installed antivirus software on the computers on your network. You update the definition and engine files and configure the software to update those files every day.

What else should you do to protect your systems from malware? (Select two.)

- [ ] Enable chassis intrusion detection.
- [ ] Enable account lockout.
- [x] Educate users about malware.
- [x] Schedule regular full-system scans.
- [ ] Disable UAC.

EXPLANATION

You should schedule regular full-system scans to look for any malware. In addition, educate users about the dangers of downloading software and the importance of anti-malware protections.

You should enable User Account Control (UAC) to prevent unauthorized administrative changes to your system.

Use account lockout to help protect your system from hackers trying to guess passwords.

Use chassis intrusion detection to identify when the system case has been opened.