Computer Security (COM-301)

Malware

Malware

Which of these malware types is self-spreading and does not require a host program?

a) Worm
b) Trojan
c) Virus
d) Keylogger

A) Only worms and viruses are self-spreading. A virus needs a host program
See slide 7 of the slides.

Malware

Which of the following statements are correct?

a) Eliminating buffer overflows would completely prevent the problem of viruses.
b) Only expert hackers can use malware.
c) Viruses can spread to systems even if they have no Internet connectivity.
d) A honeypot is useful to understand how malwares work.

A) False, it might prevent some viruses from spreading but a virus might still exploit other classes of vulnerabilities
B) False, even hackers with little technical knowledge can use malwares to cause harm
C) True, viruses can spread in other ways. Think, for instance, about USB keys
D) True, honeypot could be useful for other things such as deflecting malware, but it does not make the statement false

Thesis Theft

Ariel has been working hard on her bachelor's project report, due in a few days. Her report contains valuable and sensitive information. One morning, when she turns on her laptop, she realizes that the Microsoft Word document that contains her entire report is missing. Furthermore, she notices a pop-up that says "Want your report back? It'll cost you $1000 ". Given the situation, Ariel starts worrying and asks you for help.

Part 1: What **kind** of malware is Ariel's laptop infected with?

Part 2: How can the thief **convince** Ariel to pay, i.e., show that they have not just destroyed the document from Ariel's laptop but hold a copy of it?

Part 1: This is ransomware: Ransomware is a particular type of malware that threatens with destroying a computer's content unless the owner pays an economical compensation.

Part 2: The thief could show a part of the document as a proof of ownership, e.g. show the one page of choice to Alice. Sending a copy to Alice is not a good choice: Alice would not have incentives to pay the adversary.

The start-up 2.0

Alice listened to the advice received during the monday live exercises and changes her antivirus to be anomaly-based instead of her former choice: checking for match of hash with a known virus (signature-based).

Describe a drawback of an anomaly-based antivirus that her former choice did not have.

Possible answers:
False Positives are possible with anomaly based antiviruses: anomalies may be challenging to distinguish from intentional or benign deviations and trigger. Distinguishing “normal” from “malicious” is not trivial, while for signatures, malicious signatures are hashes of known viruses.