CprE 431
Homework 4

Sean Gordon

Oct 4, 2020

1. Machine-executable viruses attach themselves to a program that can be executed, while a macro virus embeds itself in popular applications. Because of the way they embed themselves, macro viruses tend to be platform independent.

2. (a) Infection of existing files on a computer that is then spread to other computers.
   (b) Software vulnerabilities that allow the malware to spread.
   (c) Social engineering to obtain access for the malware to spread.

3. This is an example of a logic bomb.

4. The memory stick could contain malware that would execute upon plugging the stick into a computer. This could infect all the computers on your work network and do serious damage to the company. To mitigate the threat, you could plug the threat into a test computer to check for malware, or just not plug it in at all.

5. This custom codec might actually help view the videos, but it is likely to be some other software package with malicious intent. This would be installed willingly on your computer if approved.

6. There is little reason for a smartphone game to need access to messages or your adress book, so the app is very suspicious. This app is likely setting itself up to send messages containing itself or some other malware to all contacts. This is an example of trojan horse malware.

7. A spoofed source address stops the attack from being traced back to its correct origin, and stops response packets from being received and potentially DOSsing the attacking computer.

8. The main defense lies in the routers that the attacks will run through. As an ISP knows all the IPs of its customers, it can ensure the source IP is valid, stopping the attacks from the spoofed source.

9. $9.5\text{mb} \rightarrow \dfrac{9.5}{.0005} = 19000$ packets/sec

   $2\text{mb} \rightarrow \dfrac{2}{.0005} = 4000$ packets/sec

   $10\text{mb} \rightarrow \dfrac{10}{.0005} = 20000$ packets/sec