Kieren Ng

3/7/18

Homework 7

6.1

“Infection of existing executable or interpreted content by viruses”

“Exploit of software vulnerabilities either locally or over a network by worms or drive-by downloads”

“Social engineering attacks that convince users to bypass security to install Trojans or respond to phishing attacks” (186)

6.11

A backdoor is a “secret entry point into a program that allows someone who is aware of the backdoor to gain access without going through the usual security access procedures”

A bot can eat network or computational resources

A keylogger records all the keystrokes on the machine it’s on, so an attacker could read the information.

Spyware allows monitoring of a wide range of activity on the infected machine.

Rootkit is implemented on a system to get access on a system with admin rights, whilst being hidden

6.3

The metamorphic code gives the same overall final effect, however it uses different registers that essentially do nothing, that change and change back for no net change. It does this to give the impression of being different, despite not being ultimately.

6.5

This code could be parasitic malware, it requires some other code to exist, and it takes the date from other legitimate code, using a ‘logic bomb’

6.6

This software has a backdoor, I’m assuming since the question says it’s malicious that the backdoor was not an intentional thing by the original programmer.

6.10

Yes, you absolutely should be suspicious of a game that wants those permissions, because there’s really no reason for a game to have those things (or very many other apps in general, to be honest). If you give the game those permissions, they can send text messages to every contact without your knowledge. This type of software might be a Trojan, due to the fact that it may look legitimate at first glance but in reality it isn’t. Another thing it might do is it may cause your phone to collect data charges due to messages being sent out

6.11

If you decide to run the Launch the file, you could just be executing a virus which obviously would be pretty bad. An easy way to check whether the file is legit or not is to simply ask the manager who sent it whether it’s legit. If you received it, other people in the company probably also received it as well, and it’s probably a macro virus.