Veton Abazovic
NetID: va187
Computer Security

Assignment 6

Question 1

What is the primary disadvantage of signature-based malware detection?

Answer: The primary disadvantage of signature-based malware detection is the fact that there are new strains of strings all the time. Thus, the Av engine would need to have them in order to match the documents.

Question 2

What are three techniques that malware packers use?

Answer: Xoring of the malware, Compression, Encryption

Question 3

How does the use of packers make it more difficult to detect malware?

Answer: The use of packers makes it more difficult to detect malware because packers changes the representation of the malware code. Due to this the Av now has trouble trying to find the malware because it has been changed and thus can not distinguish between malware or non-malware.

Question 4

What technique does the author discuss as a possible mechanism for malware to communicate with a server if it has no direct access to the Internet?

Answer: The possible way malware could communicate with a server if it has no direct access to the internet is by using implementing a covert channel recursive DNS lookups.

Question 5

Anti-malware software and file filters need to be aware of potentially harmful files that can host or conceal malware.

(a) How many forms of compression formats does the paper list?

Answer: There are 25 forms of compression formats ranging from 7zip- zip

(b) How many types of Microsoft Office related file types does the paper list?

Answer: There are 41 related file types of Microsoft Office ranging from csv - xlw

Question 6

Watch/listen to the interview with Amit Serper on OSX.Pirrit malware/adware.

(a) How does the macOS LaunchAgent mechanism help malware?

Answer: A macOS launch Agent helps both Malware and legitimate software to continue to run after a reboot.

(b) List two ways in which users end up using to get Pirrit onto their systems.

Answer: One way to is to use the installer and download a program and with it addons that the program installed like adware or a toolbar.

The other way is from torrent sites that you think you are downloading a crack program but, when you run the installer you are actually downloading malware.