CS808: Computer Security Fundamentals

5.3 Malware Questions

Complete the following questions.

1. What is the difference between a virus and a worm?
2. Why are worms potentially more dangerous than viruses?
3. Certain worms propagate on the internet do not cause any damage on the computers they hit, so why are they considered malware? Provide an example of such a worm
4. How could an attacker install a backdoor?
5. What is a Trojan horse?
6. Think of a scenario of how an attacker could deploy a Trojan horse.
7. Describe two techniques which could be used to help disguise a virus from antivirus software
8. A dictionary based antivirus can recognise the signatures of all known viruses. Why might the computer still be prone to infection?

Scenario-based Questions

Scenario 1

John discovered a virus in his office computer. The virus expert was called and took half a day to clean the computer and recover the data. The following day, the same virus came back. After spending several days fighting this virus, it was discovered that John himself unknowingly infected his computer immediately after each cleaning.

He had a game that he liked to play during his lunch break. His wife, a student, brought the game from college on an infected USB. Every time John inserted the USB into his office computer, the virus installed itself afresh.

Question

Given the above scenario, what actions do you think the company should take to prevent this happening again?

Scenario 2

You have discovered malware on your system. After analysing it, you notice its behaviour is as follows. After infecting your machine by attaching itself to a file, every Monday a message appears on your screen at 9am with a picture of a cat called Garfield saying ‘I hate Mondays’. It sends itself out to all your mail contacts.

Question

a) What type of malware is this and why?

b) What could the impact of this malware be if it were on an organisation’s network?

c) What is the trigger for this malware and how would you classify it?

d) What is an alternative trigger type? Provide an example