COM-301 Computer Security
Exercise 11: Malware

Malware

1. Are the following statements True or False:

   (a) Eliminating buffer overflows would completely prevent the problem of Internet worms

   (b) Some viruses add their code to that of existing executables residing on disk.

   (c) Having a centralized botnet with one command & control (C&C) is a good idea. You do not need to manage many computers since all report to the same C&C.

   (d) We cannot trust that executing a program will not do damage just by inspecting the program's source code

   (e) Trojans are self-contained programs that replicate themselves to infect other machines

   (f) Ransomware is a type of malware focused on network denial of service

   (g) Signature-based antiviruses are very effective against known viruses but not new

2. You got access to an encrypted version of the final exam of COM-301 which is a file of 100KB encrypted with AES-128 (symmetric encryption with a key length of 128 bits). You really want to decrypt the file to get a very good score. It turns out that you have become a millionaire. For some reason instead of going to Hawaii, you decide that you are going to finish your degree and need to pass this course. Therefore, you really, really want to decrypt the exam. Assume you have three options:

   (a) Buy a botnet that costs you 100 CHF for every 2^{10} bots. Each bot can brute force 2^{40} keys a day (fictitious number!). You can buy at most 2^{24} bots.

   (b) Pay one of the assistants to leak you the key using a covert channel so that the professor does not realize. The covert channel leaks 4 bits of the key per day. The assistant does want to go to Hawaii for vacation every summer of his life, and since he has learned that you have became a millionaire, asks you for 25,000 CHF per bit.

(c) Buy the latest coolest ever technology by Dr Nefario that can use a side channel attack from your seat in the classroom to get the cleartext version of the exam from the professor computer that can extract 1KB of the file every week. This coolest tech costs 1M CHF, but you are a millionaire and you do not care.

Which option is the fastest? And which is the cheapest? Justify.

3. Malware can use different approaches to choose to which machines in the network to spread. Compare each of the following approaches for the following points: i) how well they work to spread faster, ii) how effective they are if the malware has a pre-defined target, iii) how well they work for remaining undetected, iv) how well they work to obtain the widest coverage.

   (a) Random (i.e., try random nodes in the network) vs Targeted (i.e., select new targets from a pre-define set)

   (b) Full (send to every reachable node every time it spreads) vs Limited (restrict the number of nodes in each spreading step)

4. Explain what type of Intrusion Detection System (IDS) would you choose for (justify your answer):

   (a) Detecting a well-known worm that rarely mutates

   (b) Detecting unknown worm

   (c) Detecting a known worm that randomizes its operation all the time (i.e., it never repeats the same pattern).

   (d) Detecting this particular worm that acts by sending 5 SYN-ACK at the beginning of the attack