COMP3632 Assignment 1

Kyu Doun Sim

kdsim@connect.ust.hk

20306527

1.(a)

i. Integrity of the system is violated. The infected machines no longer work as the user intended. As stated, the malware is mining cryptocurrency in the background while the user did not intend so.

ii. Trojan horse. It is spread through tricking the user into running it and giving it admin privilege. I assume that the tricking part implies that users installed and ran a program that would provide some sort of functionality that they need.

iii. Rootkits. A rootkit is a piece of malware that changes the behavior of system functionalities to hide itself from the system. As Skidmap tricks the user to run the malware and obtain administrator privilege to hide from the user and reinstalls by scheduling by itself, this malware would be a rootkit. Specifically, the malware overwrites the 'rm' binary so that even it was removed by the user, it would re-install itself.

1.(b)

i. Availability is violated. The WannaCry ransomware ultimately blocked the user's access to his or her own machine and the files unless they pay.

ii. Worm. The WannaCry is spread via the internet and took advantage of vulnerable background daemons, such malware would be classified as a worm.

iii. Ransomware. As the payload was to lock the user's machine and files unless the users paid for the attackers, such type of malware would be categorized as ransomware.

1.(c)

i. Confidentiality. The ultimate purpose of the two men was to steal the unlock codes for an AT&T phone. Such codes are a vital piece of confidential information that directly relates to the profit of the company.

ii. Planted malware. Two men bribed AT&T employees to purposefully install a malware so that it could sent out sensitive information. Since the ultimate purpose of the arrested two men was to make employees to install it on the system, the method of spread shows that it is a planted malware.

iii. Spyware. Not only the malware was stealing the unlock codes for AT&T phones, but it was also recording and sending victim employees' actions on AT&T computers to

help the hackers to penetrate its infrastructure. There is a possibility that it could be a keylogger too, but the paragraph did not specify whether it was registering physical keystrokes.

2.

(a) True. Cryptographic protocols are open design, but the keys are secret. The Kerchkhoffs' principle states that a cryptosystem should be secure even if everything about the system, except the key, is public knowledge. If everything is hidden, people will eventually figure out the system and exploit it.

(b) True. The principle of least common mechanism states that mechanisms used to access resources should not be shared. Furthermore, if the common mechanism had a vulnerability, it would make all systems vulnerable. Since the glibc is used by most computers, and buffer overflow could affect any machine because it relies on the same share mechanism.

(c) True. The Heartbleed bug can read sensitive data of the victim, therefore able to expose personal information. This could be a privacy issue, even if the information read does not directly lead to the identity of the victim, any vital information such as username or password could potentially lead to reveal who the victim is. Such would be a privacy issue as well. There is no guarantee that there will be no information related to the victim on the compromised machine.

(d) False. For XSRF, the attacker creates a maliciously forged link, and will trick the victims to make a request through the malicious link to a proper website that would operate a function or request that the attacker wants. The attacker would not fully own the web server but understands its behavior and able to create requests that could take advantage from the victims.

(e) True. The format string vulnerability can not only read memory by not providing the length of the printf statement but combine %d and %n in a printf() statement wherever they want to even write over the memory.