CECS 378 Assignment 3 - Malicious Software

20 points

Assignment Description. Answer the following questions from the Chapter 6 reading from your textbook. Be through and complete with your answers. You *may* work on these questions with a partner (no more than two working together), but **both** students must submit the document individually on Beachboard Dropbox along with both of your names on each submission.

1. What mechanisms can a virus use to conceal itself?

2. What is a *logic bomb*?

3. How does a Trojan enable malware to propagate? How common are Trojans on computer systems? Or on mobile platforms?

4. What is the difference between machine executable and macro viruses?

5. The following code fragments show a sequence of virus instructions and a metamorphic version of the virus. Describe the effect produced by the metamorphic code.

Original Code	Metamorphic Code

`mov eax, 5`
`add eax, ebx`
`call [ebx]`
	`mov eax, 5`
	`push ecx`
	`pop ecx`
	`add eax, ebx`
	`swap eax, ebx`
	`swap ebx, eax`
	`call [eax]`
	`nop`

6. Consider the following fragment. What type of malware is this?

```
[legitimate code]
if data is Friday the 13th;
  crash_computer();
[legitimate code]
```

7. Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms we discuss could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?

8. Consider the following fragment in an authentication program. What type of malware is this?:

```
username = read_username();
password = read_password();
if username is ”133t h4ck0r”
   return ALLOW_LOGIN;
if username and password are valid
   return ALLOW_LOGIN
else return DENY_LOGIN
```

9. Suppose you receive a letter from a finance company stating that your loan payments are in arrears (in default), and that action is required to correct this. However, as far as you know, you have never applied for, or received, a loan from this company! What may have occurred that led to this loan being created? What type of malware, and on which computer systems, might have provided the necessary information to an attacker that enabled them to successfully obtain this loan?

10. List the types of attacks on a personal computer that each of a (host-based) personal firewall, and anti-virus software, can help you protect against. Which of these counter- measures would help block the spread of macro viruses spread using email attachments? Which would block the use of backdoors on the system?

Deliverables. Submit the answers to the questions on **Beachboard Dropbox** by the indicated due date and time. Acceptable file submission formats are: .txt, .rtf, .odt, .doc, .docx, or .pdf.