Breesy Reyes
Sam Chen

Assignment 3 - Malicious Software

1. **What mechanisms can a virus use to conceal itself?**
   - Encrypted Virus:
     Uses encryption to obscure it's content. A portion creates a random encryption key and encrypts the remainder of the virus. When an infected program is invoked, it uses the stored key to decrypt itself.
   - Stealth Virus:
     Is designed to hide itself from anti-virus software detection.
   - Polymorphic Virus:
     It creates copies during replication making detection by the "signature" of the virus impossible.
   - Metamorphic Virus:
     Mutates with every infection and re-writes itself after each iteration making it difficult to detect. May change their behaviour as well as their appearance.

2. **What is a logic bomb?**
   It is code embedded in the malware that is set to "explode" when certain conditions are met. Once triggered, it may alter or delete data or entire files, causes a machine to halt, or do some other damage. Triggers could include the presence or absence of devices or files on a system, a date or time, a software with an appropriate version or configuration, or an application being executed.

3. **How does a Trojan enable malware to propagate? How common are Trojans on computer systems? Or on mobile platforms?**
   A trojan virus sneaks into your files, for example, whenever you download something off the internet. Once it is inside your computer, it will inject its code into any executable file causing it to spread. They are common when you visit an unfamiliar website or download a game or useful utility program. Another example would be spam emails where Trojan horses can be hidden under advertisement links if you open the email. As smartphones are getting more popular these days, make for an easy target for criminals. A recent situation was a phishing Trojan that tricks the user to enter their bank details, and ransomware that mimicked Google's design to appear more real and legitimate. Trojans on mobile platforms usually are most common in app marketplaces. Sometimes the Trojan can be found in an application store.

4. **What is the difference between machine executable and macro viruses?**
   Machine executable viruses affect executable programs if the infected program is executed, these program files work with specific operating systems. Macro viruses only affect the documents on a system if they have macro or scripting code such as Microsoft office and PDF documents.

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

The effect produced by the metamorphic code is that it changes the original code's signature without affecting the logic behind the original code. This is done by adding the highlighted lines of code.

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

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

This type of malware is logic bomb because it has a condition that triggers the payload which is hidden in legitimate code. In this case the malware crashes the computer if the date is Friday the 13th. Logic bombs are data corrupting malware so it can change or delete data or crash a computer at a given date or time.

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?**

Plugging in a suspicious usb into your pc could compromise its confidentiality, integrity, and availability. There is a possibility of a trojan virus being inside the USB, once plugged into your pc it will infect your files after opening the contents. It's possible an executable virus may be transmitted and attack your operating system. A worm can appear on the usb because it runs automatically and infects other files on the system.

Macro viruses can definitely be a possibility to infect your user documents because it's near a work area. To mitigate these threats the user can scan the memory stick with an anti-virus software. Another way would be to open the usb in a controlled environment such as a virtual machine so that your real system won't be attacked. You can also plug it into an old computer that is not connected to the internet and has an updated antivirus program.

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

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

The type of malware used here in this fragment is called the Back door. This code checks the username "133 t h4ck0r " and returns allow login when conditions are satisfied. It does the same for username and password. Else it denies the login. This authentication program gives secret access to the username "133 t h4ck0r" into a system. The backdoor malware allows secret admission for the user.

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?**

Since applying for loans requires private information we know that a hacker was able to gather the user's private information. They then used the information to get the loan and left the user with responsibility of making the repayments. The type of malware that could be used to gain information are phishing attacks, keyloggers, spyware, trojan horse, or rootkit. Phishing attacks can be sent by emails and are used to obtain usernames, passwords, credit card information. Keyloggers can be used to capture keystrokes and allow the attacker to monitor the sensitive information a user puts in. Spyware allows the attacker to monitor a wide range of activity on the system. Trojan horse can be set by email or webpage to allow the attacker to gain access to sensitive and private information stored in files. Rootkit allows the attacker to gain admin level access to the computer.

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?**
    The type of attacks can be Trojan, Viruses, Worms, Spyware, Keylogger, DDoS, Phishing, Backdoor. Checking your updates often can prevent the spread of macro viruses, such as making sure your security programs are up to date. Another way to prevent the spread is to not start it at all by not opening suspicious emails and having zip/exe files extracted. A decent firewall can block backdoor programs. An anti malware program or an antivirus program can help monitor the networks of your system.