CIS 4367.01 **Brandon Thompson**
Prof. Elibol Due Date: 3/30/2020

Homework 12

PROBLEM #6.2:

The question arises as to whether it is possible to develop a program that can analyze a piece of software to determine if it is a virus. Consider that we have a program D that is supposed to be able to do that. That is, for any program P, if we run $D(P)$, the result returned is TRUE (P is a virus) or FALSE (P is not a virus). Now consider the following program:

```
Program CV :=
     {. . .
     main-program :=
     { if D(CV) then goto next:
else infect-executable;
}
next:
     }
```

In the preceding program, `infect-executable` is a module that scans memory for executable programs and replicates itself in those programs. Determine if D can correctly decide whether CV is a virus.

SOLUTION:
If D returns TRUE (meaning CV is a virus) then the code will continue as normal. If D returns FALSE (meaning CV is not a virus) then the `infect-executable` function is ran, infecting other programs. The function is backwards, this would work if the statement was `if D(CV) then infect-executable:`.

PROBLEM #6.3:

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

SOLUTION:
The metamorphic code has the same functionality as the original code, with the original lines separated by useless lines, but the overall signature of the code has changed. A program might flag the original code as a virus but not the metamorphic code as they will have different signatures.

PROBLEM #6.5:

Consider the following fragment:

```
legitamate code
if data is Friday the 13th;
    crash_computer();
legitamate code
```

what type of malware is this?

SOLUTION:

This is a logic bomb, logic bombs will wait to execute malicious code until a condition is met, in this case if `data = Friday the 13th`.

PROBLEM #6.6:

Consider the following fragment in an authenticated program:

```
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
```

What type of malicious software is this?

SOLUTION:
This is a backdoor, backdoors bypass the common security protocols to allow access. In this case the user with the username `133t h4ck0r` does not have to have a valid password to gain access to the system.

PROBLEM #6.7:

Assume you have found a USB memory stick in your work parking area. What threats might this pose to your work computer should you 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?

SOLUTION:
USB sticks can house many different threats like an executable or macro virus, a worm, or a Trojan horse. To mitigate these threats the user could scan the USB with an anti-virus program (preferably the latest version), or put the USB into a controlled environment to check the contents.

PROBLEM #6.8:

Suppose you observe that your home PC is responding very slowly to information requests from the net. And then you further observe that your network gateway shows high levels of network activity, even though you have closed your e-mail client, Web browser, and other programs that access the net. What types of malware could cause these symptoms? Discuss how the malware might have gained access to your system. What steps can you take to check whether this has occurred? If you do identify malware on your PC, how can you restore it to safe operation?

SOLUTION:

Attacks that are designed to slow down a users PC are denial of service attacks to acquire all of the network bandwidth so none is left for the user, or the system might be part of a botnet.

To make sure that the system is not infected you should scan it with an up to date anti-virus software and check network logs to see which programs are creating the most traffic.

If a virus is identified on the system an anti-virus software should be able to remove the virus from the system. If this fails, the worse option is to remove the storage from the computer and re-image the system.

PROBLEM #6.9:

Suppose that while trying to access a collection of videos on some Web site, you see a pop-up window stating that you need to install this custom codec in order to view the videos. What threat might this pose to your computer system if you approve this installation request?

SOLUTION:
The codec software could contain a Trojan virus that could have numerous confidentiality, integrity and availability threats.

PROBLEM #6.10:

Suppose you have a new smartphone and are excited about the range of apps available for it. You read about a really interesting new game that is available for your phone. You do a quick Web search for it, and see that a version is available from one of the free marketplaces. When you download and start to install this app, you are asked to approve the access permissions granted to it. You see that it wants permission to ”Send SMS messages” and to ”Access your address-book.” Should you be suspicious that a game wants these types of permissions? What threat might the app pose to your smartphone, should you grant these permissions and proceed to install it? What types of malware might it be?

SOLUTION:
This is fairly common, to find friends that also play the game and to send validation codes for logins, however because of the shady nature of the install accepting these permissions is not advisable. Permissions to view contacts and send SMS messages could potentially be to gather information about a users contacts and send it through SMS to the attacker, or send messages to the contacts directly through the users phone. This type of virus is called a Trojan.

PROBLEM #6.11:

Assume you receive an e-mail, which appears to come from a senior manager in your company, with a subject indicating that it concerns a project that you are currently working on. When you view the e-mail, you see that it asks you to review the attached revised press release, supplied as a PDF document, to check that all details are correct before management release it. When you attempt to open the PDF, the viewer pops up a dialog labeled ”Launch File” indicating that ”the file and its viewer application are set to be launched by this PDF file.” In the section of this dialog labeled ”File,” there are a number of blank lines, and finally the text ”Click the ’Open’ button to view this document.” You also note that there is a vertical scroll-bar visible for this region. What type of threat might this pose to your computer system should you indeed select the ”Open” button? How could you check your suspicions without threatening your system? What type of attack is this type of message associated with? How many people are likely to have received this particular e-mail?

SOLUTION:
If the user opens the attached PDF, then the malicious scripting code will run on the computer. If the open button is selected, it could put a Trojan or a worm on the system without the users knowledge. To check if there is a threat, the user could scroll through all of the code to verify there is nothing malicious. The message is a spear-phishing attack against the user. Because the attack is considered a spear phishing attack, it is only viable to a small number of people.

PROBLEM #6.12:

Assume you receive an e-mail, which appears to come from your bank, includes your bank logo in it, and with the following contents: ”Dear Customer, Our records show that your Internet Banking access has been blocked due to too many login attempts with invalid information such as incorrect access number, password, or security number. We urge you to restore your account access immediately, and avoid permanent closure of your account, by clicking on this link to restore your account. Thank you from your customer service team.” What form of attack is this e-mail attempting? What is the most likely mechanism used to distribute this e-mail? How should you respond to such e-mails?

SOLUTION:
This attack is a generic phishing attack sent to many users to trick them into disclosing bank information. This email is most likely distributed via a botnet to be able to send to many accounts. You should not click on the link given in the email, and only log into the bank by a known URL. You could also forward the email to a bank representative to notify them, otherwise just delete the email.

PROBLEM #6.13:

Suppose you receive a letter from a finance company stating that your loan payments are in arrears, 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?

SOLUTION:
The letter entails that an attacker has gathered enough information about the user to take out a loan in the name of the user and leave the after effect for the user to deal with. Types of malware that could disclose this information are Trojan horse malware or spyware.

PROBLEM #6.14:

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

SOLUTION:
Firewalls defend against attacks from outside the network attacking the host system or specific connections from leaving the system. Anti-virus software scans the system, downloaded files and suspicious activity within system to make sure there is no malicious activity going on. Anti-virus would help defend against email attachments, where firewalls would defend against backdoors within the system.