Introduction to Computer Security Module – G6077

Malwares

Learning objectives:

- Understand malware behavior/actions from pseudo codes
- Relate malware types to our daily life security incidents

Task 1

A computer virus places a copy of itself into other programs, and arranges for that code to be run when the program executes. The "simple" approach just appends the code after the existing code, and changes the address where code execution starts. This will clearly increase the size of the program, which is easily observed. Investigate and briefly list some other approaches that do not change the size of the program.

Answer:

Search it yourself.

Task 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.

Answer:

D is supposed to examine a program P and return TRUE if P is a computer virus and FALSE if it is not. But CV calls D. If D says that CV is a virus, then CV will

not infect an executable. But if D says that CV is not a virus, it infects an executable. D always returns the wrong answer.

Task 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 eax, eax`
	`call [eax]`
	`nop`

Answer:

The original code has been altered to disrupt the signature without affecting the semantics of the code. The ineffective instructions in the metamorphic code are the second, third, fifth, sixth, and eighth.

Task 4

Consider the following fragment:

```
legitimate code
 if an infected document is opened;
  trigger_code_to_infect_other_documents();
 legitimate code
```

What type of malware is this and Why?

Answer:

Macro code. It works on document by using macro feature of the documents.

Task 5

Consider the following fragment embedded in a webpage:

```
username = read_username();
password = read_password();
if username and password are valid
  return ALLOW_LOGIN;
  executable_start_download();
else return DENY_LOGIN
  executable_start_download();
```


What type of malware is this and why?

Answer:

Drive-by-downloads.

Task 6

Suppose that while working on a course assignment you come across a software that seems efficient to complete the assignment. When you run the software, however, you observe it keeps redirecting you to a different website and does not do the desired task. Is there a threat to your computer system?

Answer:

Yes, there can be a threat to the computer system. It may happen that while installing that software, the system became vulnerable to Adware and hence, instead of completing the desired task, the software keeps pointing to a different website, probably an ecommerce website. Such software should be removed from the system at the earliest because it may also steal other personal information from the system and pass on to the attacker.

Task 7

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?

Answer:

If when you download and start to install some game app, you are asked to approve the access permissions "Send SMS messages" and to "Access your address-book" you should indeed be suspicious that a game wants these types of permissions, as it would not seem needed just for a game. Rather it could be malware that wants to collect details of all your contacts, and either return them to the attacker via SMS, or allow the code to send SMS messages to your contacts, perhaps enticing them to also download and install this malware. Such code is a trojan horse, since it contains covert functions as well as the advertised functionality.

Task 8

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 releases 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?

Answer:

If you should open the PDF attachment, then it could contain malicious scripting code that could run should you indeed select the 'Open' button. This may be either worm (specifically exploiting a client-side vulnerability), or trojan horse code. You could you check your suspicions without threatening your system by using the scroll bar to examine all the code about to be executed should you select the 'Open' button, and see if it looks suspicious. You could also scan the PDF document with suitable, up-to-date anti-virus software for any signs of malware – though this will not detect unknown, zero-day exploits. This type of message is associated with a spear-phishing attack, given that the email was clearly crafted to suit the recipient. That particular e-mail would only have been sent to one or a few people for whom the details would seem plausible.

Task 9

Assume you receive an e-mail, which appears to come from an online air ticket reservation system, includes original logo and has following contents: "Dear Customer, Thank you for booking your air ticket through our online reservation system. The PNR for your journey from City1 to City2 is JADSA and for your return journey is EWTEQ. You can download your tickets by logging in through this link." Assume you are a frequent visitor of City1 and City2 is another city you visit very frequently. 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?

Answer:

This email is attempting a general phishing attack, being sent to very large numbers of people, in the hope that a sufficient number of passengers use the named online air ticket reservation, and are fooled into divulging their sensitive login credentials to the attacker. Once the attacker gains login credentials from the passenger, he/she can misuse the account by booking tickets through stored credit card numbers, if any. The most likely mechanism used to distribute this e-mail is

via a botnet using large numbers of compromised systems to generate the necessary high volumes of spam emails. You should never ever follow such a link in an email and supply the requested details. You should only ever access sensitive sites (probably the ones that involve financial transactions) by directly entering their known URL into your browser. It may be appropriate to forward a copy of such emails to a relevant contact at the online air ticket reservation system if they ask for this. Otherwise it should just be deleted.

Task 10

Suppose you receive a letter, which appears to come from your company's mail server stating that the password for your account has been changed, and that an action is required to confirm this. However, as far as you know, you have not changed the password! What may have occurred that led to the password being changed? What type of malware, and on which computer systems might have provided the necessary information to an attacker that enabled them to successfully change the password?

Answer:

Such a letter strongly suggests that an attacker has collected sufficient personal details about you, including your old password, in order to create a new password. This was most likely done using either a phishing attack, perhaps persuading you to complete and return some form with the needed personal details such as password; or answer to a secret question through which password can be guessed; or by using spyware installed on your personal computer system by a worm or trojan horse malware, that then collected the necessary details from files on the system, or by monitoring your access to sensitive sites.