Introduction to Computer Security Module – G6077

Malwares

Learning objectives:

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.

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.

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

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?

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();
```

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?

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?

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?

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?

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?

Task 11

Carry out your own research to write a brief one-line explanation along with pseudo code for the principles listed below.

	Description	Pseudocode representation
Fail-safe defaults		
Complete mediation		
Least privilege		
Separation of privilege		
Isolation		
Encapsulation		

Modularity		