FIT3031 TUTORIAL 10

MALICIOUS SOFTWARE

Review

Q1. What is the role of encryption in the operation of a virus?

Q2. What are the typical phases of operation of a virus?

Q3. In general terms, how does a worm propagate?

Q4. What is a digital immune system?

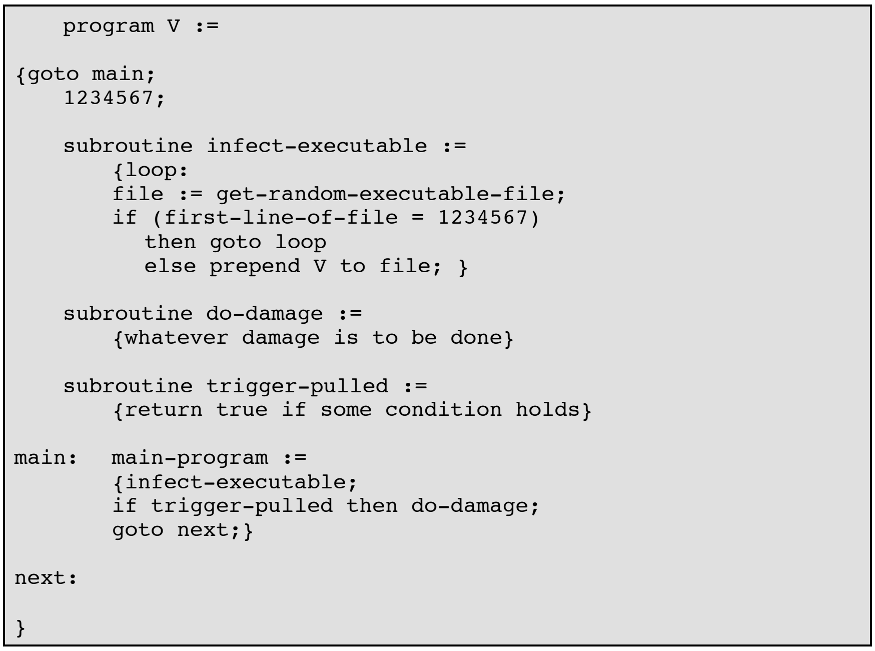
Q5. How does behavior-blocking software work?

Q6. Describe some worm countermeasures.

Q7. What is a DDos?

Problems:

1. There is a flaw in the virus program shown in Figure 1 below. What is it?



```
    program V :=

{goto main;
    1234567;

    subroutine infect-executable :=
        {loop:
        file := get-random-executable-file;
        if (first-line-of-file = 1234567)
           then goto loop
           else prepend V to file; }

    subroutine do-damage :=
        {whatever damage is to be done}

    subroutine trigger-pulled :=
        {return true if some condition holds}

main:   main-program :=
        {infect-executable;
        if trigger-pulled then do-damage;
        goto next;}

next:

}
```

Figure 1: A Simple Virus

2. Consider the following code fragment:

```
Legitimate code
If date is Friday the 13th;
        Crash_computer();
Legitimate code
```

What type of malicious software is this?

3. Consider the following code fragment in an authentication 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?