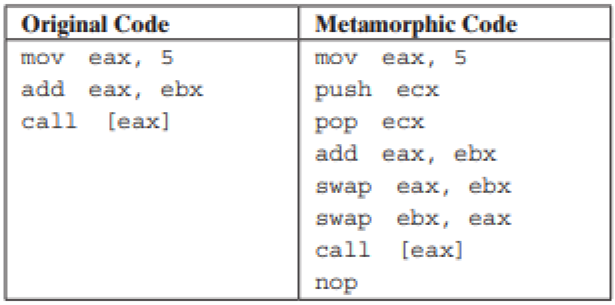
Tutorial Session - 8

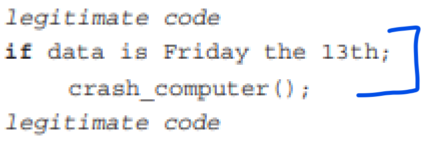
1. What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware?
2. Give practical examples for each of the following:
   i. Backdoor
   ii. Bot
   iii. Keylogger
   iv. Phishing
   v. Spear Phishing
   vi. Worm

3. List three places malware mitigation mechanisms may be located.
4. Briefly describe the four generations of anti-virus software.
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`	`mov  eax, 5`
`add  eax, ebx`	`push  ecx`
`call  [eax]`	`pop  ecx`
	`add  eax, ebx`
	`swap  eax, ebx`
	`swap  ebx, eax`
	`call  [eax]`
	`nop`

6. Consider the following fragment:

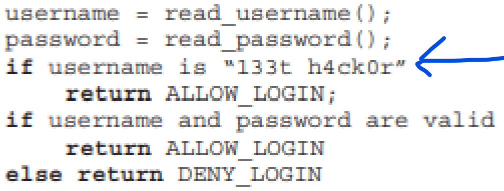


```
legitimate code
if data is Friday the 13th;
    crash_computer();
legitimate code
```

What type of malware is this?

Logic bomb

7. Consider the following 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
```

loop hole

What type of malicious software is this?

Backdoor