Chapter 2 Review Questions

1. Which of the following is not a primary trait of malware?
2. diffusion
3. circulation
4. infection
5. concealment
6. Which type of malware requires a user to transport it from one computer to another?
7. worm
8. rootkit
9. adware
10. virus
11. Which type of mutation completely changes a virus from its original form by rewriting its own code whenever it is executed?
12. betamorphic
13. oligomorphic
14. polymorphic
15. metamorphic
16. Ebba received a message from one of her tech support employees. In violation of company policy, a user had downloaded a free program to receive weather reports, but the program had also installed malware on the computer that gave the threat actor unrestricted access to the computer. What type of malware had been downloaded?
17. virus
18. ransomware
19. RAT
20. Trojan
21. Linnea’s father called her to say that a message suddenly appeared on his screen that says his software license has expired and he must immediately pay $500 to have it renewed before control of the computer will be returned to him. What type of malware is this?
22. persistent virusware
23. Trojanware
24. blocking ransomware
25. lockoutware
26. Astrid’s computer screen suddenly says that all files are now locked until money is transferred to a specific account, at which time she will receive a means to unlock the files. What type of malware has infected her computer?
27. Bitcoin malware
28. Crypto-malware
29. Blocking virus
30. Networked worm
31. What is the name of the threat actor’s computer that gives instructions to an infected computer?
32. Command and control (C&C) server
33. Resource server
34. Regulating Net Server (RNS)
35. Monitoring and Infecting (M&I) server
36. Which of these could NOT be defined as a logic bomb?
37. If the company’s stock price drops below $100, then credit Juni’s account with 10 additional years of retirement credit.
38. Erase all data if Matilda’s name is removed from the list of employees.
39. Reformat the hard drive three months after Sigrid left the company.
40. Send spam email to Moa’s inbox on Tuesday.
41. Which of the following is NOT correct about a rootkit?
42. A rootkit is able to hide its presence or the presence of other malware.
43. A rootkit accesses “lower layers” of the operating system.
44. A rootkit is always the payload of a Trojan.
45. The risk of a rootkit is less today than previously.
46. Which of these is a general term used for describing software that gathers information without the user’s consent?
47. gatherware
48. adware
49. spyware
50. scrapeware
51. Which statement regarding a keylogger is NOT true?
52. Keyloggers can be used to capture passwords, credit card numbers, or personal information.
53. Software keyloggers are generally easy to detect.
54. Hardware keyloggers are installed between the keyboard connector and computer keyboard USB port.
55. Software keyloggers can be designed to send captured information automatically back to the attacker through the Internet.
56. A watering hole attack is directed against \_\_\_\_\_.
57. wealthy individuals
58. a smaller group of specific users
59. all users of a large corporation
60. attackers who send spam
61. \_\_\_\_\_ sends phishing messages only to wealthy individuals.
62. Whaling
63. Spear phishing
64. Target phishing
65. Microing
66. Lykke receives a call while working at the helpdesk from someone who needs his account reset immediately. When Lykke questions the caller, he says, “If you don’t reset my account immediately, I will call your supervisor!” What psychological approach is the caller attempting to use on Lykke?
67. Familiarity
68. Scarcity
69. Intimidation
70. Consensus
71. Hedda pretends to be the help desk manager and calls Steve to trick him into giving her his password. What social engineering attack has Hedda performed?
72. aliasing
73. duplicity
74. impersonation
75. luring
76. How can an attacker use a hoax?
77. A hoax could convince a user that a bad Trojan is circulating and that he should change his security settings.
78. By sending out a hoax, an attacker can convince a user to read his email more often.
79. A user who receives multiple hoaxes could contact his supervisor for help.
80. Hoaxes are not used by attackers today.
81. Which of these items retrieved through dumpster diving would NOT provide useful information?
82. calendars
83. organizational charts
84. memos
85. books
86. \_\_\_\_\_ is following an authorized person through a secure door.
87. Tagging
88. Tailgating
89. Backpacking
90. Caboosing
91. Each of these is a reason why adware is scorned EXCEPT \_\_\_\_\_.
92. it displays objectionable content
93. it displays the attacker’s programming skills
94. it can interfere with a user’s productivity
95. it can cause a computer to crash or slow down
96. What is the term used for a threat actor who controls multiple bots in a botnet?
97. bot herder
98. zombie shepherd
99. rogue IRC
100. cyber-robot