Security 101 Homework: Security Reporting

Part I: Symantec

For Part 1 of your homework assignment, you should primarily use the *Symantec Internet Security Threat Report* along with independent research to answer the following questions.

---

1. What is formjacking?

2. How many websites are compromised each month with formjacking code?

3. What is Powershell?

4. What was the annual percentage increase in malicious Powershell scripts?

5. What is a coinminer?

6. How much can data from a single credit card can be sold for?

7. How did Magecart successfully attack Ticketmaster?

8. What is one reason why there has been a growth of formjacking?

9. Cryptojacking dropped by what percentage between January and December 2018?

10. If a web page contains a coinmining script, what happens?

11. How does an exploit kit work?

12. What does the criminal group SamSam specialize in?

13. How many SamSam attacks did Symantec find evidence of in 2018?

14. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?

15. In 2018, what was the primary ransomware distribution method?

16. What operating systems do most types of ransomware attacks still target?

17. What are “living off the land” attacks? What is the advantage to hackers?

18. What is an example of a tool that’s used in “living off the land” attacks?

19. What are zero-day exploits?

20. By what percentage did zero-day exploits decline in 2018?

21. What are two techniques that worms such as Emotet and Qakbot use?

22. What are supply chain attacks? By how much did they increase in 2018?

23. What challenge do supply chain attacks and living off the land attacks highlight for organizations?

24. The 20 most active groups tracked by Symantec targeted an average of how many organizations between 2016 and 2018?

25. How many individuals or organizations were indicted for cyber criminal activities in 2018? What are some of the countries that these entities were from?

26. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?

27. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?

28. What are two examples of the above cloud attack?

29. Regarding Internet of Things (IoT) attacks, what were the two most common infected devices and what percentage of IoT attacks were attributed to them?

30. What is the Mirai worm and what does it do?

31. Why was Mirai the third most common IoT threat in 2018?

32. What was unique about VPNFilter with regards to IoT threats?

33. What type of attack targeted the Democratic National Committee in 2019?

34. What were 48% of malicious email attachments in 2018?

35. What were the top two malicious email themes in 2018?

36. What was the top malicious email attachment type in 2018?

37. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?

38. What is Emotet and how much did it jump in 2018?

39. What was the top malware threat of the year? How many of those attacks were blocked?

40. Malware primarily attacks which type of operating system?

41. What was the top coinminer of 2018 and how many of those attacks were blocked?

42. What were the top three financial Trojans of 2018?

43. What was the most common avenue of attack in 2018?

44. What is destructive malware? By what percent did these attacks increase in 2018?

45. What was the top user name used in IoT attacks?

46. What was the top password used in IoT attacks?

47. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?

48. In the underground economy, how much can someone get for the following?

    a. Stolen or fake identity:
    b. Stolen medical records:
    c. Hacker for hire:
    d. Single credit card with full details:
    e. 500 social media followers: