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?
   Using malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce sites.

2. How many websites are compromised each month with formjacking code?
   4,818 in 2018.

3. What is Powershell?
   A task-based command-line shell and scripting language built on . NET. Powershell helps system administrators and power-users rapidly automate tasks that manage operating systems and processes. PowerShell commands let you manage computers from the command line.

4. What was the annual percentage increase in malicious Powershell scripts?
   1,000%

5. What is a coinminer?
   Something used by cyber criminals that runs on victims' devices without their knowledge. Uses their CPU power to mine cryptocurrencies.

6. How much can data from a single credit card can be sold for?
   Up to $45 on the underground market.

7. How did Magecart successfully attack Ticketmaster?
   Magecart compromised a third-party chatbot, which loaded malicious code into the web browsers of visitors to Ticketmaster's website, with the aim of harvesting customers' payment data.

8. What is one reason why there has been a growth of formjacking?
   There has been a drop in value of cryptocurrencies, so those who cryptojack have turned to formjacking because the value of stolen credit card details is more assured.

9. Cryptojacking dropped by what percentage between January and December 2018?
   52%.

10. If a web page contains a coinmining script, what happens?
    Visitors' computing power will be used to mine for cryptocurrency as long as the page is open.

11. How does an exploit kit work?
    They are automated threats that utilize compromised websites to divert web traffic, scan for vulnerable browser-based applications, and run malware. They were developed as a way to silently and automatically expliot vulnerabilities on victims' machines while browsing the web.

12. What does the criminal group SamSam specialize in?
    Ransomware.

13. How many SamSam attacks did Symantec find evidence of in 2018?
    67.

14. Even though ransomware attacks declined in 2019, what was one dramatic change that occurred?
    The amount of attacks on consumers decreased and the amount on enterprises and businesses increased.

15. In 2018, what was the primary ransomware distribution method?
    E-mail campaigns.

16. What operating systems do most types of ransomware attacks still target?
    Windows-based computers

17. What are "living off the land" attacks? What is the advantage to hackers?
    Attackers using off-the-shelf tools and operating system features to

conduct attacks. It makes it convenient for them to compromise software updates because they're easier than zero-day vulnerability exploitation.

18. What is an example of a tool that's used in "living off the land" attacks?
    Using Microsoft Office files with malicious email attachments, PowerShell to write code.

19. What are zero-day exploits?
    Cyber attack that occurs on the same day a weakness is discovered in software. Exploiting before a fix comes from the editor.

20. By what percentage did zero-day exploits decline in 2018?
    They went down to 23%, down from 27% at the end of 2017.

21. What are two techniques that worms such as Emotet and Qakbot use?
    Dumping passwords from memory or brute-forcing access to network shares to laterally move across a network.

22. What are supply chain attacks? By how much did they increase in 2018?
    Attacks, which exploit third-party services and software to compromise a final target, take many forms, including hijacking software updates and injecting malicious code into legitimate software. 78%

23. What challenge do supply chain attacks and living off the land attacks highlight for organizations?
    Attacks are increasingly arriving through trusted channels, using fileless attack methods or legitimate tools for malicious purposes.

24. The 20 most active groups tracked by Symantec targeted an average of how many organizations between 2016 and 2018?
    55.

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?
    49. Russian, Chinese, Iranian and North Korean.

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

27. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?
    Data being leaked from several cloud instances.

28. What are two examples of the above cloud attack?
    Chip-level attacks and speculative execution.

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?
    Routers and connected cameras. 75% and 15%.

30. What is the Mirai worm and what does it do?
    DdoS worm, turns networked devices running Linux into remotely controlled bots that can be used in a botnet for large-scale network-attacks.

31. Why was Mirai the third most common IoT threat in 2018?
    Persistently adding new exploits increasing success rate for infection.

32. What was unique about VPNFilter with regards to IoT threats?
    It was the first widespread persistent IoT threat, with it's ability to survive a reboot, making it very hard to remove.

33. What type of attack targeted the Democratic National Committee in 2019?
    Unsuccessful spear-fishing attack

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

35. What were the top two malicious email themes in 2018?
    Bill and email delivery failure.

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

37. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?
    Poland had most, Saudi Arabia had least.

38. What is Emotet and how much did it jump in 2018?
    A worm that use simple techniques including dumping passwords from memory or brute-forcing access to network shares to laterally move across a network. 16%.

39. What was the top malware threat of the year? How many of those attacks were blocked?
    Heur.AdvML.C. 43,999,373.

40. Malware primarily attacks which type of operating system?
    Windows.

41. What was the top coinminer of 2018 and how many of those attacks were blocked?
    JS.Webcoinminer. 2,768,721.

42. What were the top three financial Trojans of 2018?
    Ramnit, Zbot and Emotet.

43. What was the most common avenue of attack in 2018?
    Spear-fishing emails.

44. What is destructive malware? By what percent did these attacks increase in 2018?
    Malicious software with the capability to render affected systems inoperable and challenge reconstitution. 25%.

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

46. What was the top password used in IoT attacks?
    123456

47. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?
    Telnet, http and https. 23 and 80.

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

    a. Stolen or fake identity: **$0.10-1.50**
    b. Stolen medical records: **$0.10-35**
    c. Hacker for hire: **$100+**
    d. Single credit card with full details: **$1-45**
    e. 500 social media followers: **$2-6**