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? - a type of cyber attack where hackers inject malicious JavaScript code into a webpage form, most often a payment page form.

2. How many websites are compromised each month with formjacking code? - 4800

3. What is Powershell? - Consists of a command-line shell and associated scripting language. It's from Microsoft

4. What was the annual percentage increase in malicious Powershell scripts? 100%

5. What is a coinminer? - AKA cryptocurrency miners. Programs that generate cryptocurrencies.

6. How much can data from a single credit card can be sold for? $45 (underground markets)

7. How did Magecart successfully attack Ticketmaster? - Magecart compromised a 3rd party chatbot, which loaded malicious code into the web browsers of visitors to Tickemaster's website, with the aim of harvesting customers' payment data.

8. What is one reason why there has been a growth of formjacking? -there was a drop in the value of crytpocurrencies during the year

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

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

11. How does an exploit kit work? - automated threats that utilize compromised websites to divert web traffic, scan for vulnerable browser-base applications, and run malware.

12. What does the criminal group SamSam specialize in? - ransomware attacks

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 majority of infections occurred in businesses, and not with customers

15. In 2018, what was the primary ransomware distribution method? - email 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 choosing off-the-shelf tools and operating system features to conduct attacks. Advantage: They help the attacker maintain a low profile by hiding their

activity in a mass of legitimate processes.

18. What is an example of a tool that's used in "living off the land" attacks? - PowerShell

19. What are zero-day exploits? - Cyber attacks that occur on the same day a weakness is discovered in software.

20. By what percentage did zero-day exploits decline in 2018? - 23%

21. What are two techniques that worms such as Emotet and Qakbot use?
    a. Dumping passwords from memory
    b. 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? - Supply chain attacks aim to damage an organization by targeting less secure elements in its supply network. They increased by 78% in 2018.

23. What challenge do supply chain attacks and living off the land attacks highlight for organizations? - The challenge is attacks are arriving through trusted channels, using fileless attack method 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? An average of 55 organizations

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. Russia, China, Iran, North Korea

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? - A successful attack on a single physical system could result in data being leaked from.

28. What are two examples of the above cloud attack? - Meltdown and Spectre exploits

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 (75%) and connected camera (15%)

30. What is the Mirai worm and what does it do? - A distributed denial of service worm. (A malicious attempt to disrupt normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic.) An IoT threat. Also targets unpatched Linux servers.

    Source:

https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

31. Why was Mirai the third most common IoT threat in 2018? - Because Mirai is constantly evolving and variants use up to 16 different exploits, persistently adding new exploits to increase the success rate for infection, as devices often remain unpatched

32. What was unique about VPNFilter with regards to IoT threats? - It was the first widespread presistent IoT threat, with its ability ti survive a reboot making it very difficult to remove. It also has an array of potent payloads.

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

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

35. What were the top two malicious email themes in 2018? - Attachments and URLs.

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

37. Which country had the highest email phishing rate? Which country had the lowest email phishing rate? Highest rate: Saudi Arabia. Lowest rate: Poland

38. What is Emotet and how much did it jump in 2018? A kind of malware originally designed as a banking Trojan aimed at stealing financial data. It jumped up to 16% in 2018, from 4% in 2017
    Source:

https://www.malwarebytes.com/emotet/

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

40. Malware primarily attacks which type of operating system? - Windows -> 92% per year

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

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

43. What was the most common avenue of attack in 2018? - Malicious Powershell script

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. Source:

www.ibm.com/downloads/cas/XZGZL
RVD

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, https. Top 2 ports: 23(telnet) and 80 (World Wide Web HTTP)

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

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