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?

   Formjacking is when cybercriminals inject malicious JavaScript code to hack a website and take over the functionality of the site's form page to collect sensitive user information.

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

   On average 4800 websites are compromised.

3. What is Powershell?

   It's a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting language.

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

   An increase in 1000 percent in malicious Powershell scripts.

5. What is a coinminer?

   Its other name is a cryptocurrency miner, which are programs that generate Bitcoin and other cryptocurrencies that are the future of money.

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

   Anywhere from $1 to more than $45, depending on the information available.

7. How did Magecart successfully attack Ticketmaster?

   By manipulating the Inbenta JavaScript code on Ticketmaster's webpages, Magecart could exfiltrate payment information from every single Ticketmaster customer who was served the Inbenta code. The client-side browser is the primary environment wherein websites display and capture critical customer and payment data.

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

   Attackers/Hackers are using to steal credit card data and other personal information.

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

   by around 52 percent

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

    As long as the web page is open, the visitors' computing power can be used to mine for cryptocurrency.

11. How does an exploit kit work?

    The exploit kit gathers information on the victim machine, finds vulnerabilities and determines the appropriate exploit, and delivers the exploit, which typically silently drive-by downloads and executes malware, and further running post-exploitation modules to maintain further remote access to the compromised system.

12. What does the criminal group SamSam specialize in?

    ransomware attacks mostly against organizations in the U.S.

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

    67 attacks

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

    Symantec's increased efficiency of catching the ransomware.

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

    Spear phishing through emails

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

    Windows OS

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

    It allows hackers to take full control of your computers and other connected devices. Antivirus software cannot detect such attacks from hackers.

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

    PowerShell scripts, or VB scripts.

19. What are zero-day exploits?

    A zero-day exploit is a cyber attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator.

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?

    Dumping passwords from memory or brute-forcing access to the network shares.

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

    Exploits third-party services and software to compromise a final target data. It increased by 78 percent.

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

    Attacks are increasingly arriving through trusted channels, using fileless attack methods.

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 over the past three years.

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?

    Forty-nine individuals or organizations were indicted in 2018. Russia, China, and Iran are the countries that had their agents indicted.

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

    Poor configurations.

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

    Hardware chip vulnerabilities could lead to a leak of data from several cloud instances as attackers exploit such vulnerabilities to access memory locations that are normally forbidden.

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

    Meltdown and Spectre

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 were the most infected devices and accounted for 75 and 15 percent of the attacks respectively.

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

    It's distributed denial of service (DDoS) worm (malware) that controls consumer devices such as IP cameras and home routers.

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

    It is constantly evolving and variants use up to 16 different exploits

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

    Its ability to survive a reboot making it very difficult to remove.

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

    Spear-phishing attacks.

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

    Spam emails

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

    Invoices, and payment notifications.

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

    .DOC. .XLS, .PDF, .ZIP

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

    Poland with the highest, and Greece with the lowest.

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

    It's malware and it jumped 16 percentage.

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

    Ramnit was the top, and 271,930 were blocked.

40. Malware primarily attacks which type of operating system?

    Windows OS

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

    JS. Webcoinminer and 2,768,721 were blocked42.

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

    Trickbot, Gozi, Ramnit

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

    Malware – 49% of Attacks. …
    Social Engineering – 25% of Attacks. ...
    Hacking – 21% of Attacks. ...
    Credential Compromise – 19% ...
    Web Attacks – 18% of Attacks. ...
    DDoS – 5% of Attacks.

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

    It causes destruction through the deletion or wiping, of files that are critical to the operating system's ability to run. It increased by 25 percentages.

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

    Root, followed by admin.

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?

    Telenet, http, and https were the top three. Telenet and WWW HTTP were the top two ports.

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**