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 a malicious JavaSpript code used to steal payment information details and other payment form information on the checkout web pages of eCommerce sites.

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

   Symantec data shows that 4,818 unique websites were compromised with formjacking code every month in 2018.

3. What is Powershell?

   PowerShell is a task automation and configuration management framework from Microsoft consisting of a command-line shell and the associated scripting language.

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

   Annual percentage increase in malicious Powershell scripts are at a raise of 1000 percent in malicious Powershell scripts blocked in 2018 on the endpoint. Compared to 2017, Microsoft Officer files accounted for 48 percent of all malicious email attachments, increasing 5 percent in 2018.

5. What is a coinminer?

   Coinminers, also called cryptocurrency miners, are the programs that generate cyptocurrcies like Btcoin, Monero, Ethereum.

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

   On the underground markets, a single credit card can be sold for up to $45.

7. How did Magecart successfully attack Ticketmaster?

   Magecart's victory in their assault against Ticketmaster, accomplished by a formjacking supply chain technique, in targeting third-party service in order to get its code onto targeted websites. Magecart loaded malicious code into the web browser 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?

   In 2018, the value of cryptocurrencies had dropped significantly enough to turn cyber criminals who had used crypojacking to formjacking, the value in stolen credit card details was more assured.

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

   In 2018, between the months of January and December, cryptojacking activity fell by 52 percent.

10. If a web page contains a coinmining script, what happens?
    Websites hosting exploit kits that attempt to use weakness in web browsers and other software to install coin miners and are also taking advantage of computers.

processing power by running scripts while users browse the website.

11. How does an exploit kit work?

    Exploit kit work, by attempting to take advantage of weaknesses in web browsers and other softwares to install coin miners.

12. What does the criminal group SamSam specialize in?

    SamSam group specializes in ransomware attacks.

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

    In 2018, Symantec found evidence of 67 ransomware attacks.

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

    The one drastic way ransomware had changed during 2017-2018, was that up until 2017 consumers were the main targets, then a trend onto enterprises that were the most hit.

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

    During 2018, email campaigning was the primary method of distribution.

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

The main operating system still targeted by ransomware are windows-based computers.

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

    “Living off the land” attacks are off-the-shelf and operating system features used in malevolent ways. This is a malevolent exploitation of readily available tools against vulnerabilities and its working for them.

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

    PowerShell would be an example of a tool that is used for “Living off the land” attacks.

19. What are zero-day exploits?

    Zero-day exploits are 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?

    In 2018, the groups known to use zero-day was only 23 percent down from 27 percent.

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

    Two techniques that worms use are, 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?

    Supply chain attacks are third-party services and software that are exploited and compromised, that take many forms to hijack software or inject malicious code into legitimate software.

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

Supply chain attacks and living off the land attacks have brought attention to focus for organizations, that attacks increasingly arriving through trusted channels.

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

    There were 55 organizations that Symantec was actively tracking.

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?

    During 2018, 49 individuals or organizations were indicted, most of these agents from different countries such as Russa, China, Iran and North Korea.

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

    In 2018, the common theme for cloud cybersecurity was that there was a range of security challenges that the cloud presents.

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

    The implication for successful exploitation that provides access to memory location is called Meltdown and spectre exploit.

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

    One example of a Meltdown attack is an exploitation of a race condition vulnerability. Another example would be the exploit provides access to memory locations that are normally forbidden.

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?

    Regarding (IoT) attacks, in 2018, the two most commonly infected devices were routers and connected cameras and they accounted for 70 and 15 of the attacks respectively.

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

    A Mirai worm is a (DDoS) worm and 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.

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

    In 2018, Mirai worm represented 16 percent of IoT attacks making it the third most common.

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

    VPNFiler was the first widespread persistent IoT threat, with its ability to survive a reboot making it very difficult to remove.

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

    In 2019, the DNC was targeted by an unsuccessful spear-phishing attack.

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

    In 2018, Officer files accounted for 48 percent of malicious email attachments.

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

    In 2018, the two top malicious email themes were; Bills and email delivery failure.

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

In 2018, the top malicious email attachment types were; .doc.dot and .exe.

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

    The county that had the highest email phishing rate was Poland. The county with the lowest phishing rate was Saudi Arabia.

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

    Emotet is an aggressive financial Trojan and jumps up 16 persent in 2018.

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

    Heur.AdvML.C was the top malware threat in 2018 and 43,999,373 were blocked.

40. Malware primarily attacks which type of operating system?

    Malware's primary attack on the operating system was 2016 Windows.

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

    JS.Webcoinminer was the top coinminer of 2018 and 2,768,721 was blocked.

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

    The top three financial trojans of 2018 were; Ramnit, Zbot, and Emotet.

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

    Spear-phishing emails remained the most popular avenue for attack and were used by 65 percent of all known groups.

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

    While still a niche area, the use of destructive malware continued to grow. Eight percent of groups were known to use destructive tools, up from 6 percent at the end of 2017.

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

    The top user name used in IoT attack is root.

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

    The top password used in the IoT attack was 123456.

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

    The top three protocols used in IoT attacks were; telnet, http, and https.

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

    a. Stolen or fake identity: $.10-1.50
    b. Stolen medical records: $ .10- 35
    c. Hacker for hire: $100
    d. Single credit card with full details: 41-45
    e. 500 social media followers: $2-6