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 the use of 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?

   On average 4800 websites are being compromised each month.

3. What is Powershell?

   PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS.

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

   1000%

5. What is a coinminer?

   Coinminers (also called cryptocurrency miners) are programs that use the central processing unit (CPU) power of victims to mine cryptocurrencies and generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity

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

   Data from a single credit card can be sold for up to $45 on the underground market.

7. How did Magecart successfully attack Ticketmaster?

Ticketmasters payment data was compromised because its website was running code from Inbenta, a customer support software company, which hackers (Magecart) had altered.

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

   Growth in supply chain attacks and drop in the value of cryptocurrencies

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

   Cryptojacking dropped by 52% between January and December 2018

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

    The web page visitors' computing power will be used to mine for cryptocurrency for as long as the web page is open.

11. How does an exploit kit work?

    Exploit kits work by exploiting vulnerabilities in software in order to install malware.

12. What does the criminal group SamSam specialize in?

    SamSam specializes in targeted ransomware attacks, breaking into networks and encrypting multiple computers across an organization

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

    67 SamSam attacks were found by Symantec

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

    Symantec's increased efficiency at blocking ransomware earlier in the infection process, either via email protection or using technologies such as behavioral analysis or machine learning.
    Decline in exploit kit activity

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

    Ransomware distribution method was 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?

    A common attack scenario uses Office macros to call a PowerShell script, which in turn downloads the malicious payload. It can help attackers 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?

    WindowsRoamingToolsTask

19. What are zero-day exploits?

    A zero day exploit is a cyber attack that happens on the same day a vulnerability is discovered in software. It is exploited before a fix becomes available.

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

    Down by 4%, in 2017 it was at 27% and fell down to 23% in 2018.

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

    Dumping passwords from memory and 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, exploit third-party services and software to compromise a final target, including hijacking software updates and injecting malicious code into legitimate software.
    Supply chain attacks increased by 78 percent in 2018.

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

They are facing the challenge that trusted channels and legitimate tools are being used for their attacks.

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

    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 inducements in 2018, Russia, China, Iran and 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?

    Vulnerabilities in hardware chips.

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

    Speculative Store Bypass and Foreshadow

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 with 75.2% and Connected Cameras with 15.2%

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

    It is a distributed denial of service (DDoS) worm.

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

    Because Mirai keeps evolving and adds different types of exploits currently sitting at 16 and it keeps adding exploits to maximise its penetration rate.

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

    It can not be deactivated or disabeled by rebooting the system.

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?

    Bill with 15.7% and Email delivery failure with 13.3%

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

    .doc, .dot with 37.0%

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

    Saudi Arabia has the highest rate with 1 in 675
    Poland has the lowest rate with 1 in 9,653

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

    Emotet is a financial trojan, it jumped up 12% to the previous year.

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

    Heur.AdvML.C and 43,999,373 attacks 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 was the top coinminer in 2018 and it blocked 2,768,721attacks.

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

    Ramnit, Zbot, Emotet

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

    Spear-phishing emails

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

    Destructive malware is malicious software which causes infected systems to be inoperable through the deletion of files that are critical to the OS to work. Up by 2% from 6% at the end of 2017 to 8%.

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.
    TCP Port Nr. 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**