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 cyber criminals load malicious code onto retailers' websites to steal shoppers' credit card details.
2. How many websites are compromised each month with formjacking code?
   4,800+ unique websites are compromised on average every month.

3. What is Powershell?

   Powershell is the command line scripting language on windows system that is designed for system administration.

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

5. What is a coinminer?
   Coinminer is a malware and software that uses the device that uses their central processing unit (CPU) power to mine cryptocurrencies—

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

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?
   Due to the drop of cryptocurrencies during the year: cyber criminals who may have used websites for crypto jacking may now be opting for formjacking

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

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?
    They exploit software applications's security holes

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

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?
    The number of Dharma/Crysis infection attempts seen by Symantec more than tripled during 2018, from an average of 1,473 per month in 2017 to 4,900 per month in 2018

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?
    trend of attackers opting for off-the-shelf tools and operating system features to conduct attacks.
    it is harder to attribute and identify the specific attacks and attackers.

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

19. What are zero-day exploits?
    These are exploits that happen on the same day that the vulnerability was found.

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 network shares to laterally move across a network.

22. What are supply chain attacks? By how much did they increase in 2018?
    They exploit third-party services and software to compromise a final target, it increased by 78%

23. What challenges do supply chain attacks and living off the land attacks highlight for organizations?
    The attacks increasingly arrive 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 individuals and organization were indicted.North korea, Iran and China

26. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?
    Cloud resources that are misconfigured and poorly secured cloud databases

27. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?
    This is particularly problematic for cloud services because while cloud instances have their own virtual processors, they share pools of memory meaning that a successful attack on a single physical system could result in data being leaked

from several cloud instances.

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

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?
    This self-propagating worm exploits weak security on many IoT devices. It infects devices with malware that forces them to report to a central control server, turning them into a bot that can be used in DDoS attacks.
31. Why was Mirai the third most common IoT threat in 2018?
    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. The worm also expanded its target scope by going after unpatched Linux servers.

32. What was unique about VPNFilter with regards to IoT threats?
    VPNFilter was the first widespread persistent IoT threat, with its ability to survive a reboot making it very difficult to remove. With an array of potent payloads at its disposal, such as man in the middle (MitM) attacks, data exfiltration, credential theft, and interception of SCADA communications, VPNFilter was a departure from traditional IoT threat activity such as DDoS and coin mining.

33. What type of attack targeted the Democratic National Committee in 2019?
    It was targeted by an unsuccessful spear-phishing attack s

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 failures

36. What was the top malicious email attachment type in 2018?
    .doc or .dot files

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

    Poland had the lowest and Saudi arabia had the highest.

38. What is Emotet and how much did it jump in 2018?
    It is a type of banking Trojan which gains access to financial information by injecting computer code into the networking stack of an infected Microsoft Windows computer, allowing sensitive data to be stolen via transmission. It jumped from 4% to 16%.

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

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

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

    JS.Webcoinminer with 2,768,721 blocked attacks.

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

43. What was the most common avenue of attack in 2018?
    Spear-phishing email attacks.

44. What is destructive malware? By what percent did these attacks increase in 2018?
    They make the systems infected inoperable and non-functioning making the resolution of it hard. By 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

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:**$1-45**
    e. 500 social media followers:**$2-6**