Sasha Shahidi

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?
   4,800

3. What is Powershell?
   Powershell is a task automation programming language that cyber criminals use to create malicious scripts in targeted attacks.

4. What was the annual percentage increase in malicious Powershell scripts?
   1000%

5. What is a coinminer?
   A coinminer is a web browser that a user has scripted language onto, where the computing power will be used to mine for cryptocurrency for as long as the webpage is open, all without being noticed.

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

7. How did Magecart successfully attack Ticketmaster?
   Magecart successfully attacked Ticketmaster by compromising 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?
   One reason formjacking has grown is because of the high monetary gain that it can yield, with information being sold in underground markets.

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

10. If a web page contains a coinmining script, what happens?
    If a webpage contains a coinmining script, the web page 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?
    An exploit kit works by finding vulnerabilities in a machine and exploits them, delivering malicious content such as ransomware and malware.

12. What does the criminal group SamSam specialize in?
    SamSam specializes in targeted ransomware attacks against organizations in the U.S.

13. How many SamSam attacks did Symantec find evidence of in 2018?
    67

14. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?
    One dramatic change in ransomware attacks was that the hardest hit victims of ransomware attacks went from consumers to enterprises and businesses.

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

17. What are “living off the land” attacks? What is the advantage to hackers?
    Living off the land attacks are attacks where the attacking group delivers a malicious document to the victim, such as a spear-phishing email. These documents are made to look applicable to the targeted victim. These documents exploit protocol to gain access to the victims machine. The advantage to hackers is that these attacks don’t use any malicious code and the tools used are generally available.

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

19. What are zero-day exploits?
    Zero-day exploits are attacks that a cyber criminal uses to exploit a vulnerability in a system that the victim did not know about.

20. By what percentage did zero-day exploits decline in 2018?
    27%

21. What are two techniques that worms such as Emotet and Qakbot use?
    Two techniques that these 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 attacks that exploit third-party services and software to compromise a final target, and take many forms, such as hijacking software updates and injecting malicious code in legitimate software. They increased by 78% in 2018.

23. What challenge do supply chain attacks and living off the land attacks highlight for organizations?
    The challenge these attacks highlight is that attacks increasingly arrive through trusted channels, using fileless attack methods or legitimate tools for malicious purposes. Effectively identifying and blocking these attacks requires advanced detection methods such as analytics and machine learning.

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?
    There were 49 indicted for cyber criminal activities in 2018, coming from countries such as 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 in cloud databases

27. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?
    Since 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?
    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?
    Regarding IoT attacks, the two most common infected devices were routers and connected cameras, with 75% and 15% of attacks attributed to them respectively.

30. What is the Mirai worm and what does it do?
    The Mirai worm is a distributed denial of service (DDoS) worm and an Internet of Things (IoT) threat that uses various exploits to infect devices, servers, and control systems.

31. Why was Mirai the third most common IoT threat in 2018?
    Mirai is constantly evolving and variants use up to 16 different exploits, and is persistently adding new exploits to increase the success rate of infection. It also expanded its target to unpatched Linux servers and industrial control systems (ICS).

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

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 and email delivery failure

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

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

38. What is Emotet and how much did it jump in 2018?
    Emotet is a worm that uses simple techniques including dumping passwords from memory or brute-forcing access to network shares to laterally move across a network. It jumped 12% in 2018.

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

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

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

The top coinminer of 2018 was JS.Webcoinminer, with 2,768,721 of those attacks blocked.

42. What were the top three financial Trojans of 2018?
    Ramnit, Zbot, and 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 a malicious software that is designed to make a system not work anymore, effectively destroying it. It increased by 25% in 2018.

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?
    The top three protocols used in IoT attacks were Telnet, http, and https. The top two ports were 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