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 using malicious JavaScript to steal details like credit card information from web pages of eCommerce sites.

2. How many websites are compromised each month with formjacking code? 4,818 websites were compromised in 2018.

3. What is Powershell? PowerShell is a command shell that runs on Windows, Linux and macOS. A common use for PowerShell is to automate the management of systems.

4. What was the annual percentage increase in malicious Powershell scripts? 1,000%

5. What is a coinminer? A coinminer is a program that mines or generates cryptocurrencies using the power of an unsuspecting victim's CPU.

6. How much can data from a single credit card can be sold for? A single credit card can be sold for up to $45 on underground markets.

7. How did Magecart successfully attack Ticketmaster? Magecart compromised a chatbot and uploaded malicious code on customers that visited Ticketmaster’s website. Their endgame was to collect payment data.

8. What is one reason why there has been a growth of formjacking? The drop in value for cryptocurrencies in 2018 could be a reason for the growth of formjacking, because the data from a stolen credit card can generate a lot of money in the 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? When someone visits a webpage, their own CPU will start to mine for cryptocurrency for as long as the webpage is open.

11. How does an exploit kit work? Exploit kits contain a collection of exploits which can be distributed through webpages or even emails. For example, when a web page is visited, it contacts an exploit kit page and then it figures out what your PC is vulnerable to and then chooses an exploit to infect your PC.

12. What does the criminal group SamSam specialize in? Ransomware

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? There was a shift in targets. The targeted victims shifted from consumers to enterprises.

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? They are attacks that use tools that already exist in their target’s environment. Using this approach, hackers are able to fly under the radar.

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

19. What are zero-day exploits? A zero-day exploit is an exploit that was essentially just discovered or exposed and is typically not protected against. Basically, the vulnerability has zero days of history.

20. By what percentage did zero-day exploits decline in 2018? 4%

21. What are two techniques that worms such as Emotet and Qakbot use? Dumping passwords from memory or brute-forcing access to network shares

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. This can be done by injecting code into software after hijacking the software updates. 78%

23. What challenge do supply chain attacks and living off the land attacks highlight for organizations? They are increasingly coming through trusted channels by using legitimate tools for malicious intent.

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/organizations. Russia, China, Iran, North Korea.

26. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme? Poor configuration such as not setting up password protection.

27. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden? A successful attack can result in data being leaked from multiple cloud instances.

28. What are two examples of the above cloud attack? Meltdown and Spectre. Meltdown "melts" the security boundaries while Spectre is a flaw that attackers can exploit to force a program to reveal its data.

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 (75%) and connected cameras (15%).

30. What is the Mirai worm and what does it do? Mirai infects smart devices and turns them into a network or remotely controlled bots or "zombies". This botnet is often used to launch DDoS attacks.

31. Why was Mirai the third most common IoT threat in 2018? Mirai is constantly evolving which increases the rate for infection. It also expanded its target by going after unpatched linux servers.

32. What was unique about VPNFilter with regards to IoT threats? It is able to survive a reboot and also contains a variety of attacks rather than just a DDoS or coinming.

33. What type of attack targeted the Democratic National Committee in 2019? Spear-phishing attack which is a very targeted phishing attack.

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

37. Which country had the highest email phishing rate? Which country had the lowest email phishing rate? Highest - Canada / Lowest - Saudi Arabia

38. What is Emotet and how much did it jump in 2018? Malware (trojan) and it jumped 12% in a year to a total of 16%

39. What was the top malware threat of the year? How many of those attacks were blocked? Heur.AdvML.C and 43,999,373 were 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? JS.Webcoinminer and 2,768,721 were blocked

42. What were the top three financial Trojans of 2018? 1. Ramnit / 2. Zbot / 3. 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? It is malicious software that has the capability to cause a system to become inoperable and make it difficult to rebuild. Increased by 25%

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?
Protocols were 1. Telnet / 2. Http / 3. Https
Ports were 23, 80, 2323

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 - $35.00
c. Hacker for hire: $100.00 +
d. Single credit card with full details: $1.00 - $45.00
e. 500 social media followers: $2.00 - $6.00