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.

Notes on my answers: sometimes I included sources of my research as well as other thoughts and observations. I did this as I realized I could use this document later on for research.

---

1. What is formjacking?
   Used the following source article:
   https://us.norton.com/internetsecurity-emerging-threats-what-is-formjacking.html
   "Formjacking is when cybercriminals inject malicious JavaScript code to hack a website and take over the functionality of the site's form page to collect sensitive user information."
   My thoughts:
   - The usual target is payment form where money source information and access is entered.
   - Reading this article -- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/formjacking-attacks-retailers -- I found a great graphic (please see the article for the graphic). The graphic outlines how the attacker compromised the server which is actually hosting the website. The attack seems like just one of many issues you'd have as a result of a server compromise.
   - This is a complicated attack. The attackers need to compromise the network of the company that hosts the website and then inject the malicious code.

2. How many websites are compromised each month with formjacking code?
   From the report: an average of 4800 each month

3. What is Powershell?
   Used the following source article:
   https://docs.microsoft.com/en-us/powershell/scripting/overview?view=powersh

ell-7.1
"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."
My thoughts:
- I never knew that PowerShell could run on Linux and Mac.

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

5. What is a coinminer?
   Used the following source article:
   https://support.norton.com/sp/en/us/home/current/solutions/v125881893
   "Coinminers (also called cryptocurrency miners) are programs that generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity."
   My thoughts:
   - These programs run on a host PC's. While some people use their own PC's to do this, attackers use Malware to get these to run on a PC without the owner's consent.
   - The above Norton article outlines three different ways a coinminer can run: executables, browser-based, and through PowerShell.

6. How much can data from a single credit card can be sold for?
   The report says that data from a single card can be sold for $45. This seems odd given it also says, "just 10 credit cards stolen from compromised websites could result in a yield of up to $2.2 million for cyber criminals each month." I'm guessing this means they can sell multiple pieces of data from each credit card.

7. How did Magecart successfully attack Ticketmaster?
   From the report: "Magecart compromised a third-party chatbot, which loaded malicious code into the web browsers of visitors to Ticketmaster's website."
   My thoughts:
   - This is an interesting instance of formjacking as it attacked the users' browsers and not the website's server. I would be interested to see that code that got into the browser.

8. What is one reason why there has been a growth of formjacking?
   From the report: "The growth in formjacking in 2018 may be partially explained by

the drop in the value of cryptocurrencies during the year: cyber criminals who may have used websites for cryptojacking may now be opting for formjacking."

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

10. If a web page contains a coinmining script, what happens?
    For as long as the web page remains open, the script will use the visitor's computing power to mine for cryptocurrency.

11. How does an exploit kit work?
    I think this website provided an effective explanation as well as diagram:
    https://www.trendmicro.com/vinfo/us/security/definition/exploit-kit
    Step by step In my words:
    - The user clicks on a link they see in an email, a malicious advertisement, or a compromised website.
    - The link brings them to the server that contains the exploit kit.
    - The server determines which vulnerability to exploit.
    - The attacker infects the visitor's computer with the "appropriate" malware.

12. What does the criminal group SamSam specialize in?
    They specialize in ransomware attacks.
    Observations:
    - This group is nasty. They are mostly a mystery while the ransomware they distribute isn't. The fact that they can remain unknown while their "product" is well known is scary.
    - See this article:
    https://www.csoonline.com/article/3263777/samsam-explained-everything-you-need-to-know-about-this-opportunistic-group-of-threat-actors.html

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?
    Historically ransomware has targeted consumers. However, in 2017, this shifted and enterprises accounted for a slight majority of ransomware attacks. In 2018

ransomware attacks against enterprises surged to 81%.

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?
    From the following website article, https://logrhythm.com/blog/what-are-living-off-the-land-attacks/: “In the technology world, “living off the land” (LotL) refers to attacker behavior that uses tools or features that already exist in the target environment.”
    Some advantages LofL attacks:
    - The attacker doesn’t need to develop, test, and QA their own exploit tools.
    - Using existing tools makes the defenders job more difficult as they have to try to detect malicious activity disguised inside of what looks like authorized behavior.

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

19. What are zero-day exploits?
    From the website, https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html: “A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong.”

20. By what percentage did zero-day exploits decline in 2018?
    23% in 2018 from 27% in 2017

21. What are two techniques that worms such as Emotet and Qakbot use?
    From the report: “...dumping passwords from memory or brute-forcing access to network shares...“
    My thoughts:
    - The above techniques are used by the worms to move laterally across the network.
    - Password dumping is the act of getting a hashed or plain text file containing the username and password of a user or users.

22. What are supply chain attacks? By how much did they increase in 2018?
    From the report: “Supply chain attacks, which exploit third-party services and software to compromise a final target, take many forms, including hijacking software updates and injecting malicious code into legitimate software.”
    These attacks increased by 78% in 2018.

23. What challenges do supply chain attacks and living off the land attacks highlight for organizations?
    From the report: “Both supply chain and living off the land attacks highlight the challenges facing organizations and individuals, with attacks increasingly arriving through trusted channels, using fileless attack methods or legitimate tools for malicious purposes.”
    My thoughts:
    - The time and money to investigate potential breaches in a source already vetted must be significant.
    - From a troubleshooting perspective, these attacks must present a significant challenge to simply see the trusted source as a possible source of the attack.

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 or organizations were indicted in 2018. They came from Russia, China, North Korea, and Iran.

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?
    From the report: “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.”
    My thoughts:

- When the report says “several cloud instances” I wonder if that means an attacker could gain information from multiple customers’ data in the case the attacker compromised a cloud vendor. I suppose it would depend on the compromised cloud system.

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?
    Routers and Cameras at 75% and 15% respectively

30. What is the Mirai worm and what does it do?
    From the website, https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/: “Mirai is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots or ‘zombies’. This network of bots, called a botnet, is often used to launch DDoS attacks.”

31. Why was Mirai the third most common IoT threat in 2018?
    From the report: “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.”
    My thoughts:
    - The report doesn’t explicitly state the above as the reason for its frequency but I think it’s a pretty good reason.

32. What was unique about VPNFilter with regards to IoT threats?
    From the report: “VPNFilter was the first widespread persistent IoT threat, with its ability to survive a reboot making it very difficult to remove.”
    My thoughts:
    - A future area of research would be to see why IoT threats previous to VPNFilter could be neutralized by a reboot.

33. What type of attack targeted the Democratic National Committee in 2019?
    Spear-Phishing
    My thoughts:
    - Here’s a site that provides a good definition of spear-phishing:

https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing
- I was surprised at how targeted it actually is and given the effort -- gleaning personal information coupled with posing as a trusted entity -- I can see why it's so successful.

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 (#1) and Email Delivery Failure (#2)

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

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

38. What is Emotet and how much did it jump in 2018?
    From the website, https://www.malwarebytes.com/emotet: "Emotet is a Trojan that is primarily spread through spam emails (malspam)." It's "market share" rose 4% (to 16%) from 2017.
    My thoughts:
    - My research other than the above site found that Emotet was originally used primarily for financial crimes.

39. What was the top malware threat of the year? How many of those attacks were blocked?
    Heur.AdvML.C → 43,999,373 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?
    JS.Webcoinminer → 2,768,721 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?
    From the document, https://www.ibm.com/downloads/cas/XZGZLRVD:
    "Destructive malware is malicious software with the capability to render affected systems inoperable and challenge reconstitution. Most destructive malware variants cause destruction through the deletion, or wiping, of files that are critical to the operating system's ability to run."
    The report doesn't state the number of attacks in 2018 that used destructive malware. It only states the percentage of groups that use destructive malware: 8%. That's up from 6% in 2017.

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
    22 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 - $35.00
    c. Hacker for hire: $100+
    d. Single credit card with full details: $1.00 - $45.00
    e. 500 social media followers: $2.00 - $6.00