# 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?  
   **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?   
   **4818**
3. What is Powershell? **Task automation and configuration management framework from Microsoft**
4. What was the annual percentage increase in malicious Powershell scripts?  
   **1000 percent increase**
5. What is a coinminer?  
   **Programs that usually generate cryptocurrency like Bitcoin, etc.**
6. How much can data from a single credit card can be sold for?  **$45**
7. How did Magecart successfully attack Ticketmaster?

**formjacking**

1. What is one reason why there has been a growth of formjacking?   
   **Because of the drop in value of Cryptocurrencies during that time. Cyber Criminals who cryptojacked might have instead started to formjack.**
2. Cryptojacking dropped by what percentage between January and December 2018? **52%**
3. If a web page contains a coinmining script, what happens?   
   **The web page visitor’s computing power will be used to start mining cryptocurrency for as long as the web page is open**
4. How does an exploit kit work?   
   **Gathers info on the victim machine, finds vulnerabilities and determines the appropriate exploit, and delivers the exploit**
5. What does the criminal group SamSam specialize in?   
   **Ransomware attacks**
6. How many SamSam attacks did Symantec find evidence of in 2018?   
   **67 attacks**
7. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
   **Consumers were the hardest hit by ransomware but in 2017 it was the enterprises with the most infections**
8. In 2018, what was the primary ransomware distribution method?   
   **Email campaigns - emailed based attacks towards business since it was their form of communication**
9. What operating systems do most types of ransomware attacks still target?

**Windows**

1. What are “living off the land” attacks? What is the advantage to hackers?  **A track scenario uses office macros to call a PowerShell script, which in turn downloads the malicious payload.**
2. What is an example of a tool that’s used in “living off the land” attacks?  
   **Mimikatz, Microsoft PS Exec tool**
3. What are zero-day exploits?  
   **A flaw that exposes a vulnerability in software or the hardware. The attack happens before a developer has an opportunity to fix the flaw.**
4. By what percentage did zero-day exploits decline in 2018?   
   **23%**
5. What are two techniques that worms such as Emotet and Qakbot use?  
   **Dumping passwords from memory or brute-forcing access to networks shares to laterally move across a network**
6. What are supply chain attacks? By how much did they increase in 2018?  
   **Exploit third-party services and software to compromise a final target. Includes hijacking software updates and injecting malicious code into legitimate software. This increased by 78%**
7. What challenge do supply chain attacks and living off the land attacks highlight for organizations? **Effectively identifying and blocking these attacks requires the use of advanced detection methods such as analytics and machine learning**
8. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
   **55 organizations**
9. 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; Iran, russia, china and North korea.**
10. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
    **Poor Configuration**
11. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?   
    **Data could be leaked from several cloud instances.**
12. What are two examples of the above cloud attack?   
    **phishing, malware**
13. 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. 75 and 15 precent**
14. What is the Mirai worm and what does it do?   
    **Is an infection that is constantly evolving and uses up to 16 different exploits, and adding new ones to increase the success rate for infection. Worm also goes after unpatched Linux servers.**
15. Why was Mirai the third most common IoT threat in 2018?   
    **Because it remained an active threat and with 16 percent of the attacks.**
16. What was unique about VPNFilter with regards to IoT threats?  
    **It was able to survive a reboot making it very difficult to remove. It is also able to brick or whip a device at the attackers’ command.**
17. What type of attack targeted the Democratic National Committee in 2019?   
    **Spear-phishing attack**
18. What were 48% of malicious email attachments in 2018?

**Office files accounted with 48%**

1. What were the top two malicious email themes in 2018?   
    **Bill and email delivery failure**
2. What was the top malicious email attachment type in 2018?   
   **.doc, .dot**
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   **Saudi Arabia had the highest, and Poland had the lowest**
4. What is Emotet and how much did it jump in 2018?   
   **It’s a trojan that primarily spread through spam emails, and it jumped 16%**
5. What was the top malware threat of the year? How many of those attacks were blocked?  
   **Heur.AdvML.C, attacks that were blocked is 43,999,373**
6. Malware primarily attacks which type of operating system?   
   **Windows**
7. What was the top coinminer of 2018 and how many of those attacks were blocked? **JS.Webcoinminer and 2,768,721 were blocked**
8. What were the top three financial Trojans of 2018?   
   **RAMMIT, ZBOT AND EMOTET**
9. What was the most common avenue of attack in 2018?   
   **Spear-phishing emails**
10. What is destructive malware? By what percent did these attacks increase in 2018?

**Malicious software that is able to render affected systems inoperable. It increased by 25% in 2018**

1. What was the top user name used in IoT attacks?   
   **Root**
2. What was the top password used in IoT attacks?   
   **123456**
3. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
   **Telnet, http and https**

**Ports used 23 and 80**

1. In the underground economy, how much can someone get for the following?
   1. Stolen or fake identity: **$0.10-1.50**
   2. Stolen medical records: **$0.10-35**
   3. Hacker for hire: **$100+**
   4. Single credit card with full details:**$1-45**
   5. 500 social media followers:**$2-6**