# 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?  
   **A malicious Javascript code used to steal sensitive user info.**
2. How many websites are compromised each month with formjacking code?

**4,818 websites were compromised with the formjacking code every month in 2018.**

1. What is Powershell? **Powershell is a framework created by Microsoft that consist of a command-line shell and scripting language.**
2. What was the annual percentage increase in malicious Powershell scripts?  
   **A 1000% increase in malicious Powershell scripts.**
3. What is a coinminer?  
   **Programs that generate cryptocurrencies.**
4. How much can data from a single credit card can be sold for?  **In 2018, credit cards were being sold for up to $45 on the black market.**
5. How did Magecart successfully attack Ticketmaster?

**Magecart compromised a 3rd party chatbot that loaded the malicious code into the web browser of viewers on Ticketmaster’s site.**

1. What is one reason why there has been a growth of formjacking?   
   **The growth of formjacking came from the drop of value in cryptocurrencies. Credit card information are more lucrative.**
2. Cryptojacking dropped by what percentage between January and December 2018?  
   **Cryptojacking dropped by 52 percent**
3. If a web page contains a coinmining script, what happens?   
   **The visitors computing power will be used to mine for cryptocurrency.**
4. How does an exploit kit work?   
   **They attack vulnerabilities in systems so they can distribute malware or other malicious attacks.**
5. What does the criminal group SamSam specialize in?   
   **Highly damaging ransomware attacks.**
6. How many SamSam attacks did Symantec find evidence of in 2018?   
   **67 SamSam attacks**
7. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
   **Businesses became the bigger target.**
8. In 2018, what was the primary ransomware distribution method?   
   **Email based attacks because emails remained the primary communication tool for organizations.**
9. What operating systems do most types of ransomware attacks still target?

**Window based computers**

1. What are “living off the land” attacks? What is the advantage to hackers?  **It’s a fileless malware attack so cant be detected**
2. What is an example of a tool that’s used in “living off the land” attacks?  
   **PowerShell Scripts**
3. What are zero-day exploits?  
   **An exploit for a vulnerability that can be use to attack a system before anyone is ever aware.**
4. By what percentage did zero-day exploits decline in 2018?   
   **Zero-day exploits declined by 23%**
5. What are two techniques that worms such as Emotet and Qakbot use?  
   **Dumping passwords from memory & BruteForce**
6. What are supply chain attacks? By how much did they increase in 2018?  
   **Attacks that will exploit a 3rd party software to reach the target. They increased by 78%**
7. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   **Organizations need advance detections such as machine learning to avoid these attacks.**
8. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
   **55 organization**
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 were indicted. Are from Russia, China, Iran, & North Korea**
10. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
    **Poor configurations**
11. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?
12. What are two examples of the above cloud attack?   
    **Meltdown and Spectre**
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 are commonly infected.**
14. What is the Mirai worm and what does it do?   
    **A malicous program that replicates itself by finding, attacking, and infecting unprotected IoT devices**
15. Why was Mirai the third most common IoT threat in 2018?   
    **Its constantly evolving and variants use up to 16 different exploits.**
16. What was unique about VPNFilter with regards to IoT threats?
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?

**Microsoft Office Files**

1. What were the top two malicious email themes in 2018?   
   **Bills and email delivery failures**
2. What was the top malicious email attachment type in 2018?   
   .**doc and .dot**
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   **Saudia Arabia has the highest and Poland has the lowest.**
4. What is Emotet and how much did it jump in 2018?   
   **Emotet is a malware that originally aimed to steal financial data but evolved to attack everyone. It jumped up to 16% in 2018.**
5. What was the top malware threat of the year? How many of those attacks were blocked?  
   **Heur.AdvML.C and 43,999,373 attacks were blocked**
6. Malware primarily attacks which type of operating system?   
   **Windows OS**
7. What was the top coinminer of 2018 and how many of those attacks were blocked? **JS.Webcoinminer and 2,768,721 attacks were blocked**
8. What were the top three financial Trojans of 2018?   
   **Ramnit, 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?   
    **A malware used to destroy a computer system. Use of destructive malware went up by 25% in 2018**
11. What was the top user name used in IoT attacks?   
    **Root**
12. What was the top password used in IoT attacks?   
    **123456**
13. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?
14. In the underground economy, how much can someone get for the following?
    1. Stolen or fake identity: $.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