# 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 stealing someone's personal information, mainly payment information, while checking out on a website through using JavaScript.
2. How many websites are compromised each month with formjacking code?   
   About 4,818 each month in 2018
3. What is Powershell?Powershell is a more powerful command prompt that was created by Microsoft to simplify task automation and configuration management.
4. What was the annual percentage increase in malicious Powershell scripts?  
   Over 1000%
5. What is a coinminer?  
   A coinminer is someone who mines cryptocurrency through solving complex math problems. This takes a lot of CPU so sometime miners will create trojan horse virus’ that infect others systems and use their CPU’s without permission.
6. How much can data from a single credit card can be sold for? Up to $45
7. How did Magecart successfully attack Ticketmaster?

They were able to manipulate the code using a chatbot and take payment information from all of the users who used ticketmaster.

1. What is one reason why there has been a growth of formjacking?   
   There was a drop in price of Cryptocurrencies leading criminals to move from coinmining attacks to formjacking.
2. Cryptojacking dropped by what percentage between January and December 2018?  
   52%
3. If a web page contains a coinmining script, what happens?   
   The victims computing power will be used to mine cryptocurrency while the website is open.
4. How does an exploit kit work?   
   An exploit kit looks at a victims machine looking for a vulnerability and then attacking that vulnerability .
5. What does the criminal group SamSam specialize in?   
   They specialize in Ransomware attacks
6. How many SamSam attacks did Symantec find evidence of in 2018?   
   67
7. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
   Attackers switched from consumers to businesses for their attacks.
8. In 2018, what was the primary ransomware distribution method?   
   Email campaigns
9. What operating systems do most types of ransomware attacks still target?

Windows based

1. What are “living off the land” attacks? What is the advantage to hackers? They are attacks that exploit features that are already on a system. The advantage to them are that they dont always set off red flags.
2. What is an example of a tool that’s used in “living off the land” attacks?  
   Microsoft Office was commonly used in 2018
3. What are zero-day exploits?  
   Zero-day exploits are unknown vulnerabilities that attackers can exploit until they are found and fixed.
4. By what percentage did zero-day exploits decline in 2018?   
   4%
5. What are two techniques that worms such as Emotet and Qakbot use?  
   Dumping passwords from memory or brute force attacks
6. What are supply chain attacks? By how much did they increase in 2018?  
   They take advantage of third party software and do things like inject malicious code to get to the end user. They increased by 78% in 2018.
7. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   They point out that attacks can be fileless and can come from trusted sources.
8. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
   55
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. Russia, China, Iran, 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?   
    Once you get into one system you can have access to the data of many other networks.
12. What are two examples of the above cloud attack?   
    L1 terminal fault and Speculative Store Bypass
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 Cameras. They account for 75% and 15%
14. What is the Mirai worm and what does it do?   
    Its a Distributed Denial of Service worm and it targets unpatched systems like unpatched linux servers.
15. Why was Mirai the third most common IoT threat in 2018?   
    Because it was constantly evolving and coming up with new variants.
16. What was unique about VPNFilter with regards to IoT threats?  
    It was able to survive reboots so it was harder to get rid of and it could brick the victims system to cover its tracks.
17. What type of attack targeted the Democratic National Committee in 2019?   
    A spear-phishing attack that was unsuccessful.
18. What were 48% of malicious email attachments in 2018?

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, .dot
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   Poland had the highest and Saudia Arabia had the lowest.
4. What is Emotet and how much did it jump in 2018?   
   A self-propagating worm that attacked by dumping passwords or brute force attacks. It jumped by 12% in 2018
5. What was the top malware threat of the year? How many of those attacks were blocked?  
   Heur.AdvML.C, 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, 2,768,721
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
10. What is destructive malware? By what percent did these attacks increase in 2018?   
    Software that can render a system inoperable or wipe it. 25%
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?   
    Telnet, http, and https. 23 Telnet, 80 Worldwide Web Http.
14. 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