# 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 where hackers inject JavaScript code into a webpage in order to siphon confidential information from said webpage**
2. How many websites are compromised each month with formjacking code?   
    **4,800**
3. What is Powershell? **Powershell is a programming language primarily used for writing scripts to automate tasks and manage frameworks**
4. What was the annual percentage increase in malicious Powershell scripts?  
    **1000%**
5. What is a coinminer?  
    A coinminer is a program that uses your computer as a proxy to generate **cryptocurrency.**
6. How much can data from a single credit card can be sold for?  **Up to $45**
7. How did Magecart successfully attack Ticketmaster?

**Magecart took over a third-party chatbot and used it to load malicious code into the browsers of people that went to the Ticketmaster website.**

1. What is one reason why there has been a growth of formjacking?   
    **The growth in formjacking is because of the decline in value of cryptocurrencies. This is because stolen credit cards have a much more stable value in the “Cyber Underground”**
2. Cryptojacking dropped by what percentage between January and December 2018?  
    **52%**
3. If a web page contains a coinmining script, what happens?   
    **If a web page is corrupted with a coinmining script, then whenever a user is on the corrupted web page, that script will be using their computers as coinminers as long as they are on the web page.**
4. How does an exploit kit work?   
    **An exploit kit will look for vulnerabilities and inject/download an exploit onto your computer determined by the type of vulnerability that it found.**
5. What does the criminal group SamSam specialize in?   
    **Targeted 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?   
    **Enterprises and businesses became more infected with ransomware than consumers**
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**

1. What are “living off the land” attacks? What is the advantage to hackers?  **Living off the land is a type of attack that utilizes the tools and resources that are already on their victims computer. This is advantageous because detecting a threat such as this one is incredibly difficult as they generally hide deep within the computers files to the point where anti-malware programs will not look for it. Also, these attacks allow the hacker to use the tools already on the targeted system making the execution of the attack incredibly easy.**
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?  
    **A zero-day exploit is an exploit that is inside of a software that is unknown to the developer and causes vulnerabilities within the software.**
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 and brute-forcing access to network shares**
6. What are supply chain attacks? By how much did they increase in 2018?  
    **Supply chain attacks are a type of cyber-attack that look for less secure parts of a network in order to damage or exploit its target. Supply chain attacks increased by 78% in 2018.**
7. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
    **The challenge is that these attacks are difficult to detect or stop from happening, are coming from “trusted channels”, and are continuing to increase year after year.**
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?   
    **There were 49 individuals or organizations indicted for cyber criminal activities in 2018 coming from 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?   
     **It is implying that they are using the exploits in the hardware chips in order to access “memory locations” that they aren’t meant to have access to.**
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?   
     **Connected cameras and routers were the most infected with 75% of IoT attacks on Routers and 15% on connected cameras.**
14. What is the Mirai worm and what does it do?   
     **The Mirai worm is a type of worm that uses its evolving nature to continuously create new exploits in order to DDoS its targets.**
15. Why was Mirai the third most common IoT threat in 2018?   
     **Mirai is the third most common IoT threat because its constantly creating new exploits in order to have a high success rate and because its targeting “unpatched Linux Servers”**
16. What was unique about VPNFilter with regards to IoT threats?  
     **VPNFilter is unique because its vast collection of attacks that it uses, such as, “man in the middle attacks, data exfiltration, credential theft, and interception of SCADA communications”. It is also able to “survive a reboot” which makes the removal of VPNFilter incredibly complex.**
17. What type of attack targeted the Democratic National Committee in 2019?   
     **A spear-phishing attack**
18. What were 48% of malicious email attachments in 2018?

**Office Files**

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 email phishing rate while Canada was the lowest**
4. What is Emotet and how much did it jump in 2018?   
    **Emotet is a malware that primarily focuses on the theft of financial information. The use of Emotet jumped by 12% in 2018, going from 4% in 2017 to 16% in 2018.**
5. What was the top malware threat of the year? How many of those attacks were blocked?  
    **The top malware threat of the year was Heur.AdvML.C and had 43,999,373 attacks blocked.**
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 was the top coinminer of 2018 and had 2,768,721 attacks 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?   
     **Destructive malware is a malicious software that has the ability to wipe files that a computer needs to be able to function. The use of destructive malware increased 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?   
     **The top three protocols used in IoT attackers were telnet, http, and https.**

**The top two ports used in IoT attacks were 23 (Telnet) and 80 (World Wide Web HTTP).**

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**