# 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 a term used to describe the use of a malicious javascript code so that the person using this code can steal credit card information as well as other payment information. This is used during the payment screen or on e-commerce sites.**
2. How many websites are compromised each month with formjacking code?   
   **4,800**
3. What is Powershell? **A management framework that can be used cross-platformed containing a command line shell or scripting language**
4. What was the annual percentage increase in malicious Powershell scripts?  
   **1,000% increase**
5. What is a coinminer?  
   **This is a program that can generate in bitcoin, monero, ethereum or other forms of cryptocurrency while it’s at the peak of popularity to financially benefit. These can also be known as cryptocurrency miners**
6. How much can data from a single credit card can be sold for?  **$45+**
7. How did Magecart successfully attack Ticketmaster?

**They created a third party chat bot which loaded malicious code onto the browsers of the visitors who went onto the ticketmaster site to get customer payment information**

1. What is one reason why there has been a growth of formjacking?   
   **There has been a drop in the value of crypto currencies making it more difficult for cybercriminals to make money**
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 website contains a coinmining script, once the visitor logs onto the website it will collect cryptocurrency for however long the visitor stays on that site**
4. How does an exploit kit work?   
   **An expliot kit is a package that delivers malware through common targets such as java or internet explorer**
5. What does the criminal group SamSam 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?   
   **Although the attacks declined, they found that the cybersecurity measures put in place were stopping more attacks**
8. In 2018, what was the primary ransomware distribution method?   
   **Through cloud services**
9. What operating systems do most types of ransomware attacks still target?

**Windows OS**

1. What are “living off the land” attacks? What is the advantage to hackers?  **They are attackers who use tools already installed on targeted systems to run scripts and shell code directly into memory. The advantage to these hackers are half their work is already done and since they target well used programs the odds of their attacks going through are higher.**
2. What is an example of a tool that’s used in “living off the land” attacks?  
   **Microsoft office files from malicious email file attachments in 2018**
3. What are zero-day exploits?  
   **This is a cyber attack that occurs the same day a weakness is discovered within the system**
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?  
   **They perform password dumping from memory or use brute force to access network shares**
6. What are supply chain attacks? By how much did they increase in 2018?  
   **This is an attack used through a business partner or supplier to get into an organizations network through authorized access. This increased by 78% in 2018**
7. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   **The challenge they pose is that an organization can be breach through alternative means rather than just through that specific company themselves. For supply chain attacks it’s through using suppliers to get into the organization. For living off the land the organization has to make sure it’s products aren’t tampered with to have cybercrime linked to their organization. Attacks come from all sides**
8. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
   **An average of 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 indicted in 2018. Some of the countries listed are Russia, China, Iran and North Korea**
10. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
    **Poorly secured cloud databases and poor configuration**
11. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?   
    **Hardware chip vulnerabilities**
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 (75%) and connected cameras (15%)**
14. What is the Mirai worm and what does it do?   
    **This is a worm that turns devices running on Linux into bots remotely controlled so they can be used in large scaled network attacks persistently making an increased success rate of infection**
15. Why was Mirai the third most common IoT threat in 2018?   
    **Because it’s constantly evolving, and variants can use up to 16 exploits at a time increase rate of infection**
16. What was unique about VPNFilter with regards to IoT threats?  
    **It was the first widespread persistent IoT threat and also included a destructive capacity to brick**
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?

**spam**

1. What were the top two malicious email themes in 2018?   
   **Spam & Phishing**
2. What was the top malicious email attachment type in 2018?   
   **malware**
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   **Brazil- Highest**

**Israel-Lowest**

1. What is Emotet and how much did it jump in 2018?

**Emotet is a trojan primarily sent through spam emails, 16% jump in 2018**

1. What was the top malware threat of the year? How many of those attacks were blocked?  
   **Heur.AdvML.C. 43,999,373 attacks blocked**
2. Malware primarily attacks which type of operating system?   
   **Windows**
3. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   **JS.Webcoinminer. 2,768,721 attacks blocked**
4. What were the top three financial Trojans of 2018?   
   **Ramnit, Zbot, Emotet**
5. What was the most common avenue of attack in 2018?   
   **Powershell scripts**
6. What is destructive malware? By what percent did these attacks increase in 2018?   
   **Destructive malware is a malicious software capable of rendering the system under attack inoperable and can challenge reconstitution of that system. AN increase of 78%**
7. What was the top user name used in IoT attacks?   
   **root**
8. What was the top password used in IoT attacks?   
   **123456**
9. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
   **Protocols: telnet, http. https**

**Ports: 23, 80**

1. In the underground economy, how much can someone get for the following?
   1. Stolen or fake identity: **$25- $5,000**
   2. Stolen medical records: **$50-$220**
   3. Hacker for hire: **$100+**
   4. Single credit card with full details: **$1-$45**
   5. 500 social media followers**:$2-$6**