# 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 the use of malicious JS code to steal credit card details and other information from payment forms off the checkout pages on websites.**

1. How many websites are compromised each month with formjacking code?

**According to the symantec report, and based off the data in 2018 - “4818 unique websites were compromised with formjacking code every month”**

1. What is Powershell?

**Powershell is a command-line shell and scripting language for windows**

1. What was the annual percentage increase in malicious Powershell scripts?

**The annual percentage increase of malicious powershell scripts between 2017 and 2018 was 1000% increase.**

1. What is a coinminer?

**When cyber criminals embed malicious scripts on websites that run coinminers on victim’s computers and use the processing power of their GPU and CPU to mine Cryptocurrencies.**

1. How much can data from a single credit card can be sold for?

**Credit card data can be sold for approximately $45 in underground markets**

1. How did Magecart successfully attack Ticketmaster?

**Magecart compromised a third party chatbot that loaded malicious code into the web browsers of the visitors to the website with the motive of saving customers’ payment details.**

1. What is one reason why there has been a growth of formjacking?

**Due to the drop in price of cryptocurrencies.**

1. Cryptojacking dropped by what percentage between January and December 2018?  
   **Cryptojacking dropped 52% between january and december**
2. If a web page contains a coinmining script, what happens?

**It uses the processing power of the visitor’s GPU and CPU to mine cryptocurrencies.**

1. How does an exploit kit work?

**It gathers information on the visitors computer and finds vulnerabilities within the system to determine what exploit to use. Once the vulnerability is found, the kit will deliver the exploit and silently downloads and executes the malware.**

1. What does the criminal group SamSam specialize in?   
   **Ransomware attacks against organizations**
2. How many SamSam attacks did Symantec find evidence of in 2018?   
   **67 attacks**
3. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
   **Ransomware attacks shifted from consumers to enterprises and businesses**
4. In 2018, what was the primary ransomware distribution method?

**Email Campaigns was the primary ransomware distribution method.**

1. What operating systems do most types of ransomware attacks still target?

**Windows, primarily**

1. What are “living off the land” attacks? What is the advantage to hackers?  **When a user’s machine is compromised by an email or malicious website, a kit scans the machine for any vulnerabilities to find places where it can hide. The kit then uses fileless malware into legitimate software already on the machine.  
     
   This allows the user remote access, and data stealing while hiding in plain site. Thus coined, “living off the land”**
2. What is an example of a tool that’s used in “living off the land” attacks?  
     
   **An exploit kit.**
3. What are zero-day exploits?  
   **It is cyber attack that occurs on the same day a vulnerability is found in the** software.
4. By what percentage did zero-day exploits decline in 2018?   
   23% decline in 2018
5. What are two techniques that worms such as Emotet and Qakbot use?  
   **Financial trojans, brute force attacks and password dumping from memory**

1. What are supply chain attacks? By how much did they increase in 2018?  
   **Is a cyber attack that targets organizations through weaknesses in its supply chain. They increased by 78% in 2018**
2. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
     
   **Organizations are faced with the challenge of trying to secure their network and data from cyber criminals. They would need to be able to find if their is any malware hiding in any of their software that may be living off the land and stealing their data.**
3. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
     
   **They targeted an average of 55 organizations**
4. 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 individuals were indicted in 2018 from countries ranging from russia, china, iranians and 1 north korean**
5. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
     
   **Poor configuration**
6. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?   
     
   **While the cloud may have their own virtual processors, they share pools of memory, meaning a successful attack on the system would result in data leakage from several cloud instances**
7. What are two examples of the above cloud attack?   
   **Cryptojacking, cloud snooper attack**
8. 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 were the most infected devices for 75 and 15 percent of attacks**
9. What is the Mirai worm and what does it do?

**The Mirai is a DDos worm. It takes control of several machines. This network is called a “botnet” and is often used to launch ddos attacks**

1. Why was Mirai the third most common IoT threat in 2018?  
      
   **New exploits were constantly being added to the kit to increase the success of infection. It would go for unpatched linux servers and industrial control systems**
2. What was unique about VPNFilter with regards to IoT threats?  
     
   **It had destructive capabilities to brick the computer at the attackers command to destroy any evidence**
3. What type of attack targeted the Democratic National Committee in 2019?   
     
   **They were targeted by a spear-phishing attack**
4. 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**

1. What was the top malicious email attachment type in 2018?   
   .doc , .dot
2. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
     
   **Saudi arabia**
3. What is Emotet and how much did it jump in 2018?   
     
   **Emotet is financial trojan and it jumped to 16% from 4%in 2018**

1. What was the top malware threat of the year? How many of those attacks were blocked?  
     
   **Heur.adv.ML.C and roughly 44mil attacks were 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.Webcoinminers and 2.76mil attacks were blocked in 2018**
4. What were the top three financial Trojans of 2018?   
    **Ramnit, Zbot, Emotet**
5. What was the most common avenue of attack in 2018?   
   **Mobile malware**
6. What is destructive malware? By what percent did these attacks increase in 2018?   
   **Living off the land malware that allows the attack to brick the machine. It was up 25% in 2018**
7. What was the top user name used in IoT attacks?   
   **The top usernames name used in IoT attacks is “root”**
8. What was the top password used in IoT attacks?   
    **Top password used was 123456**
9. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
    **The top three protocols were telnet,http,https and the top two ports used were port 23 and port 80.**
10. In the underground economy, how much can someone get for the following?
    1. Stolen or fake identity: **$.10-$1.50**
    2. Stolen medical records: **$10-$35**
    3. Hacker for hire: **$100+**
    4. Single credit card with full details: **$1-$45**
    5. 500 social media followers: **$2-$6**