# 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?  
   **An attack that involves malicious JavaScript code to payment information on the checkout web pages of eCommerce sites.**
2. How many websites are compromised each month with formjacking code?   
   **Symantec data showed that 4,818 unique websites were compromised with formjacking code every month**
3. What is Powershell? **IT is a object based programming language. Microsoft defines it as a cross-platform automation and configuration management framework, consisting of a command-line shell and script language.**
4. What was the annual percentage increase in malicious Powershell scripts?  
   **1000%(998.9%) increase in 2018**
5. What is a coinminer?  
   **A program/script that utilizes computing power to mine for cryptocurrency.**
6. How much can data from a single credit card can be sold for?  **$0.50 to $20**
7. How did Magecart successfully attack Ticketmaster?   
   **By compromising a third-party chatbot, they loaded malicious code into the web browsers of visitors to Ticketmaster's website, with the aim of harvesting customers payment data.**
8. What is one reason why there has been a growth of formjacking?   
   **General growth in supply chain attacks**
9. Cryptojacking dropped by what percentage between January and December 2018?  
   **52%**
10. If a web page contains a coinmining script, what happens?   
    **The visitor's computer power will be used to mine cryptocurrencies.**
11. How does an exploit kit work?   
    **Users visit an infected site that has been compromised and be diverted to another page. Exploit kits scans visitors browser and/or other software to see if the vulnerability it is designed to exploit is present. If there are vulnerabilities, then network traffic will be diverted to exploit.**
12. What does the criminal group SamSam specialize in?   
    **Targeted Ransomware attacks, breaking into networks and encrypting multiple computers across an organization before issuing a high volume ransom demand.**
13. How many SamSam attacks did Symantec find evidence of in 2018?   
    **65 SamSam attacks**
14. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
    **Consumer attacks reduced and enterprise attacks increased 12%.**
15. In 2018, what was the primary ransomware distribution method?   
    **email campaigns**
16. 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?  **Attackers using off-the-shelf tools and operating system features to as means to perform attacks. It can help maintain low profile by hiding their activity in a mass of legitimate processes.**
2. What is an example of a tool that’s used in “living off the land” attacks?  
   **WindowsRoamingToolsTask**

**WinZip  
Rex PowerShell Library**

1. What are zero-day exploits?  
   **Vulnerability that is unknown to software vendor and as a result remains unpatched. Such a vulnerability can be exploited by a threat actor to exploit a network.**
2. By what percentage did zero-day exploits decline in 2018?   
   **27% reduction**
3. What are two techniques that worms such as Emotet and Qakbot use?  
   **Dumping passwords from memory or brute-forcing access to network shares to laterally move across a network**
4. What are supply chain attacks? By how much did they increase in 2018?  
   **Exploiting third party services and software to compromise a target. It can be done by hijacking software updates and injecting malicious code into legitimate software. This sort of attacks increased by 78%.**
5. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   **Identifying and blocking such attacks require advance detection methods. For example analytics and machine learning.**
6. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
   **55 organizations**
7. 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 or organizations were indicted. These included groups being from Russia, China and North Korea.**
8. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
   **Poor configuration is a common theme and here are tools available for attackers to identify misconfigured cloud resources.**
9. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?   
   **Cloud instances share pools of memory. By attackers being able to successfully attack a single physical system they also can retrieve data from several cloud instances.**
10. What are two examples of the above cloud attack?   
    **Meltdown and Spectre exploit**

**Speculative Store Bypass and Foreshadow**

**L1 Terminal Fault.**

1. 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. Such devices account for 75 and 15% of attacks.**
2. What is the Mirai worm and what does it do?   
   **DDoS worm that constantly evolving and variants use up to 16 different exploits. It infects smart devices and then attacks the servers of internet infrastructure company with malicious traffic.**
3. Why was Mirai the third most common IoT threat in 2018?   
   **It is a worm that is always adding new exploits to itself increase success rate for infection.**
4. What was unique about VPNFilter with regards to IoT threats?  
   **It can survive a reboot and also has destructive capabilities which can "brick," or wipe evidence.**
5. What type of attack targeted the Democratic National Committee in 2019?   
   **Spear-phishing attack**
6. What were 48% of malicious email attachments in 2018?

**Office files**

1. What were the top two malicious email themes in 2018?   
   **Subject topics such as 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 was the highest and Poland the lowest**
4. What is Emotet and how much did it jump in 2018?   
   **Trojan worm that uses simple techniques including dumping passwords from memory or brute-force access to network shares to laterally move a network. It jumped 4% from 2017 to 2018 (92,039).**
5. What was the top malware threat of the year? How many of those attacks were blocked?  
   **Heur.AdvML.C was the top malware of the year 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 it had 2,768,721 attacks blocked.**
8. What were the top three financial Trojans of 2018?   
   **Ramnit, Zbot, Emotet**
9. What was the most common avenue of attack in 2018?   
   **Spear-phishing emails is the most popular avenue for attack and was made use of by 65 percent of all known groups.**
10. What is destructive malware? By what percent did these attacks increase in 2018?   
    **Malware that enters a system and downloads a payload that has abilities to "brick" or wipe a device at the attackers command. Destructive malware attacks increased by 8% 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?   
    **Telnet, http, and https were the top three protocols attacked. TCP port number 23 and 80 were top ports used.**
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: **$15-$20**
    3. Hacker for hire: **$100+**
    4. Single credit card with full details: **$1-$45**
    5. 500 social media followers: **$2-$6**