# 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 JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of eCommerce sites.**
2. How many websites are compromised each month with formjacking code?   
   **4,818 websites were compromised each month in 2018.**
3. What is Powershell?

**PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS.**

**In the Symantec report it is referred to as ‘off-the-shelf tools and operating system features’ used to conduct attacks by way of ‘living off the land’.**

1. What was the annual percentage increase in malicious Powershell scripts?  
   **In 2018 there was a massive 1,000 percent increase in malicious PowerShell scripts blocked on the endpoint.**
2. What is a coinminer?  
   **A program that runs on the victims’ devices without their knowledge and uses their CPU power to mine cryptocurrencies.**
3. How much can data from a single credit card can be sold for?  **Up to $45 on underground markets.**
4. How did Magecart successfully attack Ticketmaster?

**Magecart compromised a 3rd-party chatbot, which loaded malicious code into the web browsers of visitors to Ticketmaster’s website, with the aim of harvesting customers’ payment data.**

1. What is one reason why there has been a growth of formjacking?   
   **By the drop in the value of cryptocurrencies during the year of 2018 as the value of stolen credit card details on the cyber underground is likely more stable then the value of cryptocurrency.**
2. Cryptojacking dropped by what percentage between January and December 2018?  
   **52 percent**
3. If a web page contains a coinmining script, what happens?   
   **A browser-based coinminer takes place inside a web browser and is implemented using scripting languages. A web page that contains a coinminer uses visitors to the web pages computing power to mine for cryptocurrency for as long as the web page is open.**
4. How does an exploit kit work?   
   **It is a type of toolkit cybercriminals use to attack vulnerabilities in systems so that they can distribute malware or perform other malicious activities. Often used to target commonly installed software such as Flash and Java.**
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?   
   **Consumers were no longer the hardest hit by ransomware. Majority of infections were now occurring in businesses where they now accounted for 81% of all ransomware infections.**
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 computers.**

1. What are “living off the land” attacks? What is the advantage to hackers?  **Using ‘off-the-shelf’ tools and operating system features to conduct attacks.**
2. What is an example of a tool that’s used in “living off the land” attacks?  
   **Malicious PowerShell scripts, malicious XML files, and Office files with DDE payloads.**
3. What are zero-day exploits?  
   **The method hackers use to attack systems with a previously unidentified vulnerability in software or hardware before a manufacturer can provide a patch or a fix.**
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-forcing access to network shares to laterally move across a network.**
6. What are supply chain attacks? By how much did they increase in 2018?  
   **They exploit third-party services and software to compromise a final target. An example is hijacking software updates and injecting malicious code into legitimate software. They increased by 78%**
7. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   **They highlight how attacks are increasingly arriving through trusted channels, using fileless attack methods or legitimate tools for malicious purposes.**
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?   
    **A successful attack on a single physical system could result in data being leaked from several cloud instances.**
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 accounted for 75% of attacks and connected cameras accounted for 15% of attacks.**
14. What is the Mirai worm and what does it do?   
    **Mirai is a DDOS worm and uses up to 16 different exploits to enact distributed denial of service.**
15. Why was Mirai the third most common IoT threat in 2018?   
    **It is constantly evolving and its variants use up to 16 different exploits, persistently adding new exploits to increase the success rate for infection as devices often remain unpatched. Also the worm expanded its target scope by going after unpatched Linux servers.**
16. What was unique about VPNFilter with regards to IoT threats?  
    **It was the first widespread persistent IoT threat, with an ability to survive a reboot making it very difficult to remove.**
17. What type of attack targeted the Democratic National Committee in 2019?   
    **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 at 15.7% and ‘Email delivery failure’ at 13.3%.**
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?  
   **Highest was Sudi Arabia with a rate of 1 in 675. Lowest was Poland with a rate of 1 in 9,653.**
4. What is Emotet and how much did it jump in 2018?   
   **It is a self-propagating malware that accounted for 16% of all financial Trojans in 2018, an increase of 4% of market share from 2017.**
5. What was the top malware threat of the year? How many of those attacks were blocked?  
   **Heur.AdvML.C was the top malware threat of 2018 accounting for 52.1% of attacks. 43,999,373 attacks were blocked.**
6. Malware primarily attacks which type of operating system?   
   **Windows operating systems.**
7. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   **JS.Webcoinminer accounting for 49.7% of attacks with 2,768,721 of attacks blocked.**
8. What were the top three financial Trojans of 2018?   
   **1. Ramnit at 47.4%**

**2. Zbot at 17.6%**

**3. Emotet at 16.0%**

1. What was the most common avenue of attack in 2018?   
   **Spear-phishing emails remained the most popular avenue for attack and were used by 65% of all known groups.**
2. What is destructive malware? By what percent did these attacks increase in 2018?   
   **Malicious software with the capability to render affected systems inoperable and challenge their reconstitution. Most often through the deletion, or wiping, of files that are critical to an operating system’s ability to run. The number of Attack groups using Destructive Malware increased by 25% in 2018 from 6% of known groups to 8%.**
3. What was the top user name used in IoT attacks?   
   **Root at 38.1%**
4. What was the top password used in IoT attacks?   
   **123456 at 24.6%**
5. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
   **Top 3 protocols used were telnet at 90.9%, http at 6.6%, and https at 1.0%. Top 2 ports were the TCP Port numbers 23 from Telnet at 85.0%, and 80 from World Wide Web HTTP at 6.5%.**
6. 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**