# 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 using malicious Javascript code on a websites checkout page to steal payment information, such as credit card information.
2. How many websites are compromised each month with formjacking code?   
   4818 unique websites were compromised each month in 2018.
3. What is Powershell?Powershell is a task automation & configuration management system from Microsoft. It consists of a command-line shell, and its associated script language.
4. What was the annual percentage increase in malicious Powershell scripts?  
   Malicious Powershell scripts increased 1000% between 2017 and 2018.
5. What is a coinminer?  
   A coinminer is malicious code that targets a victims’ CPU to mine for Cryptocurrencies.
6. How much can data from a single credit card can be sold for? The data from a single credit card can be sold for $45.
7. How did Magecart successfully attack Ticketmaster?

Magecart attacked Ticketmaster by compromising a 34d-party chat-bot, using formjacking. Their end goal was the harvesting of payment data.

1. What is one reason why there has been a growth of formjacking?   
   There was a large growth in formjacking partly because there has been a drop in the value of cryptocurrencies.
2. Cryptojacking dropped by what percentage between January and December 2018?  
   Cryptojacking dropped 52% between January and December of 2018.
3. If a web page contains a coinmining script, what happens?

The visitors’ computing power will be used to mine the cryptocurrencies for as long as the webpage is open. Typically, the user doesn’t even realize this is happening.

1. How does an exploit kit work?

They use compromised sites to divert web traffic, scan for vulnerable browser-based applications, and run malware.

1. What does the criminal group SamSam specialize in?   
   SamSam specializes in Ransomware.
2. How many SamSam attacks did Symantec find evidence of in 2018?   
   Systemic found evidence of 67 SamSam attacks in 2018.
3. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
   In 2017, more businesses began to be targets of ransomware, rather than consumers. This trend accelerated in 2018, up 12% from the previous year.
4. In 2018, what was the primary ransomware distribution method?   
   The primary distribution method of ransomware was email campaigns.
5. What operating systems do most types of ransomware attacks still target?

Most ransomware attacks target Windows-based computers.

1. What are “living off the land” attacks? What is the advantage to hackers? Living off the Land Attacks feature the use of “off-the-shelf” tools and operating features to conduct an attack and don’t use any malicious code.
2. What is an example of a tool that’s used in “living off the land” attacks?  
   PowerShell is frequently used in Living Off the Land Attacks. There was an increase of 1,000% of malicious PowerShell scripts that were blocked in 2018.
3. What are zero-day exploits?  
   A Zero-Day exploit, is a cyber-attack that occurs on the same day a weakness is discovered in the software so there hasn’t been time to fix or adjust for the weakness.
4. By what percentage did zero-day exploits decline in 2018?   
   Zero-Day exploits were down 4%, decreasing from 27% down to 23% in 2018.
5. What are two techniques that worms such as Emotet and Qakbot use?  
   Both Emotet and Qakbot dump passwords from the memory and use Brute Force attacks.
6. What are supply chain attacks? By how much did they increase in 2018?  
   Supply Chain attacks exploit 3rd-party services and software to compromise a target. This includes hijacking software updates and injecting malicious code into legitimate software. Supply Chain attacks were up 78% in 2018.
7. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   Supply chain attacks use legitimate tools, fileless attack methods, and arrive through trusted channels. This means that advanced detection methods are needed to combat Supply Chain attacks.
8. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
   They targeted an average of 55 groups over the past three years, up from 42 between 2015 and 2017.
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 individuals were indicted in 2018, up from just 4 in 2017. Of the 49 people facing criminal charges, 18 were from Russia, 19 were from China, 11 were from Iran, and one was from North Korea.
10. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
    The common theme is poor configuration.
11. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?

This kind of attack could give the Bad Actor access to data from several cloud instances, even if only one physical system is attacked.

1. What are two examples of the above cloud attack?   
   Meltdown and Spectre both exploit vulnerabilities through speculative execution.
2. 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 connected cameras were the two most common infected devices. Routers accounted for 75% and connected cameras for 15%.
3. What is the Mirai worm and what does it do?   
   Mirai is a malware that turns devices running Linux into remotely controlled bots that can be used in large-scale network attacks. It primarily targets online consumer devices such as IP cameras and home routers.
4. Why was Mirai the third most common IoT threat in 2018?   
   The devices that are targeted are often unpatched, so this increases the rate of success.
5. What was unique about VPNFilter with regards to IoT threats?  
   It was the 1st widespread, persistent IoT threat. It has the ability to survive even after a reboot so it is very difficult to remove.
6. What type of attack targeted the Democratic National Committee in 2019?   
   The DNC was targeted by an unsuccessful spear-phishing attack.
7. What were 48% of malicious email attachments in 2018?

Microsoft Office Files.

1. What were the top two malicious email themes in 2018?   
   The top two malicious email themes were bill and email delivery failures.
2. What was the top malicious email attachment type in 2018?   
   The top malicious email attachment types were .doc/.dot
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   Saudi Arabia and Norway had the highest email phishing rate, while South Korea and Poland had the lowest.
4. What is Emotet and how much did it jump in 2018?   
   Emotet is a worm and it jumped 12% in 2018, accounting for 16% of financial Trojans in 2018.
5. What was the top malware threat of the year? How many of those attacks were blocked?  
   The top malware threat was Heur.AdvML.C. 43, 999, 373 of these attacks were blocked.
6. Malware primarily attacks which type of operating system?   
   Malware primarily attacks Windows, accounting for 97.2% of all attacks in 2018.
7. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   The top coinminer was js.webcoinminer. 2,768,721attacks were blocked in 2018.
8. What were the top three financial Trojans of 2018?   
   The top 3 financial Trojans were Ramnit, Emotet, and Zbot.
9. What was the most common avenue of attack in 2018?   
   Spear-phishing was the most common avenue of attack in 2018.
10. What is destructive malware? By what percent did these attacks increase in 2018?   
    Destructive malware is malicious software with the ability to render the affected systems inoperable. These attacks increased 25% in 2018.
11. What was the top user name used in IoT attacks?   
    The top username was “root”.
12. What was the top password used in IoT attacks?   
    The top password was “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 that were attacked were telnel, http, and https
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: $0.10-$35.00
    3. Hacker for hire: $100.00+
    4. Single credit card with full details: $1.00-$45.00
    5. 500 social media followers: $2.00-$6.00