# 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 attack consists of using malicious JavaScript code to steal credit card details and other information from payment forms on websites.
2. How many websites are compromised each month with formjacking code?   
   Symantec report shows that 4,818 unique websites were compromised with formjacking code every month in 2018.
3. What is Powershell?Powershell is a task automation solution made up of a command-line shell, a scripting language, and a configuration management framework.
4. What was the annual percentage increase in malicious Powershell scripts?  
   Symantec report is showing us a massive 1,000 percent increase in malicious PowerShell scripts blocked in 2018.
5. What is a coinminer?  
   Coinminer is a program that mines/generates cryptocurrency like Bitcoin, Ethereum, etc.
6. How much can data from a single credit card can be sold for? Data from a single credit card can be sold for up to $45 on underground markets.
7. How did Magecart successfully attack Ticketmaster?

They did it by using formjacking attack (defined in question 1).

1. What is one reason why there has been a growth of formjacking?   
   According to the Symantec report, the gronth in formjacking my be partially explained by the drop in the value of cryptocurrencies.
2. Cryptojacking dropped by what percentage between January and December 2018?  
   Between January and December 2018 cryptojacking dropped by 52%.
3. If a web page contains a coinmining script, what happens?   
   It will use the web page visitors’ computing power as long as the visitor keep the web page open.
4. How does an exploit kit work?   
   Exploit kit is simply a collection of tools and exploits that cyber criminals use to exploit vulnerabilities in systems/devices. It works by gathering information on victim computers and then choosing the appropriate exploit to take advantage of the victim computers’ vulnerabilities.
5. What does the criminal group SamSam specialize in?   
   Ransomware attacks.
6. How many SamSam attacks did Symantec find evidence of in 2018?   
   According to the Symantec report, Symantec found evidence of 67 attacks during 2018.
7. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
   Ransomware infections were declining but enterprise infections were up by 12% in 2018.
8. In 2018, what was the primary ransomware distribution method?   
   Email. Enterprises tend to be more affected by email-based attacks since email is still the primary communication tool for organizations.
9. What operating systems do most types of ransomware attacks still target?

Most types of ransomware attacks are mostly targeting Windows-based systems.

1. What are “living off the land” attacks? What is the advantage to hackers? Living of the land attack can be described as gaining more access using the tools that already exist in the computing environment. The benefit for the attacker is that the process/attack using pre-existing software/tools avoids being flagged as suspicious.
2. What is an example of a tool that’s used in “living off the land” attacks?  
   One of the most commonly used tools is Powershell.
3. What are zero-day exploits?  
   Zero-day exploit is an exploit for a vulnerability only the attacker is aware of and it is used to exploit a vulnerability in system/software before the developer is even aware of it. Sometimes it can take up to several years for the developer to find the vulnerability that was present since day one or, for the sake of the argument, day-zero. Once a patch has been issued it is no longer called a day-zero exploit.
4. By what percentage did zero-day exploits decline in 2018?   
   According to the Symantec report the zero-dat exploit usage by targeted attack groups declined to 23% in 2018, down from 27% in 2017.
5. What are two techniques that worms such as Emotet and Qakbot use?  
   Worms such as Emotet and Quakbot use techniques such as dumpling passwords from memory and brute-forcing access to network shares to laterally move across a network, according to the Symantec report.
6. What are supply chain attacks? By how much did they increase in 2018?  
   A supply chain attack is an attack that seeks to infiltrate and disrupt the computer systems of a company's supply chain in order to harm that target company. They increased by 78% in 2018, according to the Symantec report.
7. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   The problem are the attacks that 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?   
   According to the Symantec report they targeted an average of 55 organizations between 2016 and 2018.
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?   
   There were 49 individuals or organizations that were indicted for cyber criminal activities in 2018. Some of the countries these entities were from were Russia, China, Iran and North Korea.
10. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
    The common theme was poor configuration.
11. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?   
    Cloud instances have their own virtual processors, they share pools of memory - meaning that 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. Meltdown breaks the isolation between user applications and the operating system. Spectre breaks the isolation between different applications.
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?   
    The two most commonly infected devices are routers and connected cameras and accounted for 75% ad 15% of the attacks respectively.
14. What is the Mirai worm and what does it do?   
    According to an article from Wikipedia, Mirai worm is a malware that turns networked devices running Linux into remotely controlled bots that can be used as part of botnet in large-scale network attacks.
15. Why was Mirai the third most common IoT threat in 2018?   
    It was because it was responsible for 16% of the attacks in 2018.
16. What was unique about VPNFilter with regards to IoT threats?  
    Unique thing about VPNFilter is its ability to survive a reboot which makes it very difficult to remove.
17. What type of attack targeted the Democratic National Committee in 2019?   
    The DNC was targeted by an unsuccessful spear-phishing attack. Note: The attack happened in 2018, November 14 2018 to be specific, the DNC revealed the fact in 2019. The question suggests that the said attack occurred in 2019 which, I believe, was a typo.
18. What were 48% of malicious email attachments in 2018?

48% of malicious email attachments were Office files.

1. What were the top two malicious email themes in 2018?   
   Top two malicious email themes were “Bill” (15.7%) and “Email delivery failure” (13.3%).
2. What was the top malicious email attachment type in 2018?   
   Top malicious email attachment type was .doc, .dot (37%).
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   The country with the highest email phishing rate was Saudi Arabia (1 in 675) and the country with the lowest email phishing rate was Poland (1 in 9,653).
4. What is Emotet and how much did it jump in 2018?   
   Emotet is a Trojan and it had a big jump in 2018, accounting for 16% of financial Trojans, up from 4% in 2017.
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”. The number of blocked attacks is 43,999,373.
6. Malware primarily attacks which type of operating system?   
   Malware primarily attacks the Windows operating system.
7. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   The top coinminer of 2018 was “JS.Webcoinminer” with 2,768,721 attack blocked.
8. What were the top three financial Trojans of 2018?   
   Top three financial Trojans of 2018 were “Ramnit”, “Zbot” and “Emotet”.
9. What was the most common avenue of attack in 2018?   
   The most common avenue of attack in 2018 were spear-phishing emails.

1. What is destructive malware? By what percent did these attacks increase in 2018?   
   Destructive malware is a type of malware with ability to render affected systems inoperable by deleting/wiping system critical files necessary for the operating system to run. The use of destructive malware increased by 25% in 2018.
2. What was the top user name used in IoT attacks?   
   Top user name used in IoT attacks was “root” (38.1%)
3. What was the top password used in IoT attacks?   
   Top password used in IoT attacks was “123456” (24,6%)
4. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
   Top protocols used in IoT attacks were “telnet” (90.9%), “http” (6.6%) and “https” (1%).
5. 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