# 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 injecting malicious javascript code. Most commonly payment page forms, to obtain credit card information.**
2. How many websites are compromised each month with formjacking code?   
   **According to lifelockbuissnesssolutions.com, there were 4,818 uniqe formjacing attacks per month in 2018, another site experian.com there were 3.7 million in 2018 and 4,800 per month.**
3. What is Powershell? **Developed by Microsoft, Powershell is a tool used for task automation and configuration management. It consists of a command-line shell and associated scripting language.**
4. What was the annual percentage increase in malicious Powershell scripts?  
   **McAfee reported an increase of 432% of malicious powershell scripts in 2016-2017**.
5. What is a coinminer?  
   **A coinminer is a cryptocurrency miner that generates digital currency like bitcoin or Monero, crypto currency is (if used correctly) untraceable.**
6. How much data from a single credit card can be sold for?  **According to experian.com a single credit card can be sold on the black market anywhere between $5-$110.**
7. How did Magecart successfully attack Ticketmaster?

**They used digital credit card skimmers made of javascript and injected it with a specialized URL**

1. What is one reason why there has been a growth of foam jacking?   
   **Because ransomware and crypto jacking are becoming less lucrative**
2. Cryptojacking dropped by what percentage between January and December 2018? **According to symantec it dropped by 52%**
3. If a web page contains a coinmining script, what happens?   
   **It infects your computer and your machine begins mining cryptocurrency and running your cpu at 100%**
4. How does an exploit kit work?   
   **It gathers information on a victim's machine, finds vulnerabilities and determines an exploit to use**
5. What does the criminal group SamSam specialize in?   
   **Targeted Ransomware attacks**
6. How many SamSam attacks did Symantec find evidence of in 2018?   
   **It was found that they mounted attacks against 67 diffrent targets mostly in the U.S.**
7. Even though ransomware attacks declined in 2019, what was one dramatic change that occurred? **Attackers moved to coin mining and phishing schemes.**
8. In 2018, what was the primary ransomware distribution method?   
   **According to systematic email campaigns that use spear phishing were the primary distribution methods of ransomware in 2018**
9. What operating systems do most types of ransomware attacks still target? **Windows operating systems are still the most popular still so most attacks still target them**
10. What are “living off the land” attacks? What is the advantage to hackers?  **A “living off the land” attack uses tools and/or shell scripts already on the targets machine leading to little too no new files on the hard disk, with less chance of being detected by security tools and less risk of being detected**
11. What is an example of a tool that’s used in “living off the land” attacks?  
    **OS features legitimate tools and cloud services**
12. What are zero-day exploits?  
    **Bugs and exploits discovered on the day something is released that the developers missed**
13. By what percentage did zero-day exploits decline in 2018?   
    **25%**
14. What are two techniques that worms such as Emotet and Qakbot use?  
    **They both have keyloggers and can communicate with its command and control sever, they both also “sleep” for 10-15 minuts to avoid sandboxing.**
15. What are supply chain attacks? By how much did they increase in 2018?  
    **Supply chain attacks are an attack to a target through a third-party, via compromised website or legitimate downloadable software. These attacks increased by 78% between 2017-2018.**
16. What challenge do supply chain attacks and living off the land attacks highlight for organizations? **Being secure with these attacks is much more difficult then patching a bug,it calls for the company, the individual and the developers of software to be more cautious of what they code, the software they download and to keep in mind the vulnerabilities they themselves are taking on to their hardware.**
17. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018? **55 organizations**
18. How many individuals or organizations were indicted for cyber criminal activities in 2018? What are some of the countries that these entities were from? **18 allegide Russians, 19 Chinese, 11 Iranians and one North Korian. All are individuals or organizations**
19. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?  **Poor configuration**
20. What is the implication for successful cloud exploitation that provides access speculative executions to memory locations that are normally forbidden?   
    **Vulnerabilities in hardware chips**.
21. What are two examples of the above cloud attack?   
    **mongoDB and Apache struts**
22. 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 most common infected devices. 75 and 15 percent respectively were IoT attacks on these devices.**
23. What is the Mirai worm and what does it do?   
    M**irai is a DDoS worm that uses thousands of compromised IoT devices.**
24. Why was Mirai the third most common IoT threat in 2018?   
    **Its constantly evolving and variants sixteen different exploits, and persistently adding new exploits to increase the success rate for infection.**
25. What was unique about VPNFilter with regards to IoT threats?  
    **Its ability to survive a reboot making it difficult to remove along with an array of potent payloads at its disposal such as MitM attacks,data exfiltration, credential theft, and interception of SCADA communication. It's also capable of destructive things such as “Brick” or wipe a device at the will of the attacker.**
26. What type of attack targeted the Democratic National Committee in 2019? *2016?***A spear phishing campaign**
27. What were 48% of malicious email attachments in 2018?

**Office files**

1. What were the top two malicious email themes in 2018?   
   **Bills, email delivery failure**
2. What was the top malicious email attachment type in 2018?   
   **.doc.dot, .exe files**
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate? **Highest: Japan Lowest: Saudi Arabia**
4. What is Emotet and how much did it jump in 2018?   
   **Jumped to 16%**
5. What was the top malware threat of the year? How many of those attacks were blocked? **Heur.AdvML.C, 43,999,373 of this attack were 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, 2,768,721 were 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?   
   **Living off the land**
10. What is destructive malware? By what percent did these attacks increase in 2018? **Destructive malware is malicious software with the ability to render affected systems inoperable usually through wiping the drives of the system or deleting files. Fell by more the 20%**
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? **Protocols: telnet,http,https Ports:23,80**
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**
    3. Hacker for hire:**$100+**
    4. Single credit card with full details:**$1-45**
    5. 500 social media followers:**$2-6**