# 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?  
   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
3. What is Powershell?Powershell is a scripting and shell language developed by Microsoft
4. What was the annual percentage increase in malicious Powershell scripts?  
   100%
5. What is a coinminer?  
   A coinminer mines for crypto currency
6. How much can data from a single credit card can be sold for? $45
7. How did Magecart successfully attack Ticketmaster?

Compromised a third part chat bot, infecting users visiting their site

1. What is one reason why there has been a growth of formjacking?   
   The drop in value of crypto currency
2. Cryptojacking dropped by what percentage between January and December 2018?  
   52%
3. If a web page contains a coinmining script, what happens?   
   The web page visitors’ computing power will be used to mine for cryptocurrency for as long as the web page is open.
4. How does an exploit kit work?

An exploit kit exposes flaws in an application or operating system

1. What does the criminal group SamSam specialize in?

Ransomware attacks

1. How many SamSam attacks did Symantec find evidence of in 2018?   
   67
2. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?

Enterprises were hit more often by ransomware attacks

1. In 2018, what was the primary ransomware distribution method?   
   e-mail
2. 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? Using off the shelf tools to attack systems. Hackers do not need to build custom tools.
2. What is an example of a tool that’s used in “living off the land” attacks?  
   Powershell
3. What are zero-day exploits?  
   threat of an unknown security vulnerability
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?  
   Password dumps and brute force attacks.
6. What are supply chain attacks? By how much did they increase in 2018?  
   A supply chain attack is a cyberattack that attempts to inflict damage to a company by exploiting vulnerabilities in its supply chain network.
7. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   Highlights the challenges facing organizations and individuals, with attacks increasingly arriving through trusted channels
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, & North Korea
10. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
    Poor or mis configuration of environments
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 Specter

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 Connected Cameras, 75% and 15%
2. What is the Mirai worm and what does it do?   
   It is a command and control worm, that does ddos attacks
3. Why was Mirai the third most common IoT threat in 2018?   
   It is consistently evolving.
4. What was unique about VPNFilter with regards to IoT threats?  
   It can survive a reboot
5. What type of attack targeted the Democratic National Committee in 2019?   
   A spear-fishing attack
6. What were 48% of malicious email attachments in 2018?

Office Files

1. What were the top two malicious email themes in 2018?   
   phishing rates declinedand mail attachments increased
2. What was the top malicious email attachment type in 2018?   
   doc and dot attachments
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   Saudi Arabia had the highest and Poland had the lowest
4. What is Emotet and how much did it jump in 2018?   
   A financial trojan, it jumped 150% to 16% of all infections
5. What was the top malware threat of the year? How many of those attacks were blocked?  
   Heur.AdvML.C, 43,999,373
6. Malware primarily attacks which type of operating system?   
   Windows **OS**
7. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   JS.Webcoinminer, 2,768,721
8. What were the top three financial Trojans of 2018?   
   Ramnit, Zbot, Emotet
9. What was the most common avenue of attack in 2018?   
   Malicious E-mail
10. What is destructive malware? By what percent did these attacks increase in 2018? Malware that destroys the target, 25%
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,https 23,80
14. In the underground economy, how much can someone get for the following?
    1. Stolen or fake identity: $1.50
    2. Stolen medical records: $20
    3. Hacker for hire: $100+
    4. Single credit card with full details: $45
    5. 500 social media followers: $2-$6