# 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 information from payment forms on the checkout pages of eCommerce sites.

1. How many websites are compromised each month with formjacking code?

4,818 websites are compromised by formjacking each month during 2018.

1. What is Powershell?

Powershell is an automation framework and associated scripted language developed by Microsoft.

1. What was the annual percentage increase in malicious Powershell scripts?

The annual percentage increase in malicious Powershell scripts is 1,000%.

1. What is a coinminer?

A coinminer is a program that generates cryptocurrency.

1. How much can data from a single credit card be sold for?

Data from a single credit card can be sold for $45.

1. How did Magecart successfully attack Ticketmaster?

Magecart attacked Ticketmaster by compromising a third-party chatbot to load malicious code into the web browsers of Ticketmaster website visitors for the purpose of collecting payment data from customers.

1. What is one reason why there has been a growth of formjacking?

One reason for the increase in formjacking is the decrease in cryptocurrency value; the value of credit card information on the black market is less volatile than that of cryptocurrencies.

1. Cryptojacking dropped by what percentage between January and December 2018?

Cryptojacking decreased by 52% between January and December, 2018.

1. If a web page contains a coinmining script, what happens?

If a web page contains a coinmining script, it auto-executes malicious JavaScript on a user’s computer unknowingly and uses that computer and its processing power to mine cryptocurrency.

1. How does an exploit kit work?  
    An exploit kit works via an infected website to redirect a victim to a rogue server hosting the exploit, gathers information on the victim to determine the proper exploit to deliver, and downloads the malware on the victim's computer. Exploit kits take advantage of security holes in common software applications.
2. What does the criminal group SamSam specialize in?

SamSam specializes in ransomware attacks.

1. How many SamSam attacks did Symantec find evidence of in 2018?  
     
    Symantec found evidence of 67 SamSam attacks in 2018.
2. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?  
     
    Ransomware attacks target at enterprises/businesses increased; accounting for 81% of ransomware attacks.
3. In 2018, what was the primary ransomware distribution method?

The primary ransomware distribution method was email.

1. What operating systems do most types of ransomware attacks still target?

Windows is the most common operating system targeted by ransomware attacks.

1. What are “living off the land” attacks? What is the advantage to hackers?  
     
    “Living off the Land” attacks are attacks which employ tools and features already existing in the target environment. These attacks are advantageous for hackers for these reasons:

* They do not require any code/software development.
* They do not have any dependency issues.
* They are cheap.
* They are difficult to detect.

1. What is an example of a tool that’s used in “living off the land” attacks?  
     
   PowerShell is an example of a tool used in “living off the land” attacks.
2. What are zero-day exploits?  
   Zero-day exploits are exploits that occur the same day a weakness is discovered.
3. By what percentage did zero-day exploits decline in 2018?  
    There was a 4% decline in zero-day exploits in 2018.
4. What are two techniques that worms such as Emotet and Qakbot use?

Two techniques employed by worms such as Emotet and Qakbot are:

1. Dumping passwords from memory
2. Brute force
3. What are supply chain attacks? By how much did they increase in 2018?  
     
   Supply chain attacks exploit third software to compromise a target. This can be done by:

* Hijacking software updates and injecting malicious code into software.
* Stealing credentials for version control tools.
* Compromising third party libraries used in software projects.
* Formjacking

Supply chain attacks increased by 78% in 2018.

1. What challenge do supply chain attacks and living off the land attacks highlight for organizations?  
     
    Supply chain attacks and living off the land attacks occur through trusted channels using legitimate methods and tools to exploit victims. This makes detection challenging and necessitates advanced analytics and machine learning techniques to detect compromises.
2. The 20 most active groups tracked by Symantec targeted an average of how many organizations between 2016 and 2018?  
     
    Fifty-five organizations were targeted, on average, by the twenty most active groups tracked by Symantec.
3. How many individuals or organizations were indicted for cyber criminal activities in 2018? What are some of the countries that these entities were from?  
     
    Forty-nine individuals or organizations were indicted in 2018. The countries these entities were from include Russia, China, Iran, and North Korea.
4. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?  
     
    Poorly secured and poorly configured databases is the most common theme in cloud cybersecurity attacks.
5. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?  
     
    Data can be leaked from several instances through the attack of one physical system because of the sharing of memory pools.
6. What are two examples of the above cloud attack?  
     
    Two examples are Meltdown and Spectre.
7. 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 infected devices. Routers accounted for 75% and connected cameras accounted for 15% of attacks.
8. What is the Mirai worm and what does it do?

The Mirai worm is a distributed denial of service attack that can turn networked devices into remotely controlled bots and can incorporate them into larger botnets for large-scale attacks. Common targets are connected cameras and routers.

1. Why was Mirai the third most common IoT threat in 2018?  
     
    Mirai was the third most common IoT threat because it is constantly evolving into new variants which use up to 16 different exploits.
2. What was unique about VPNFilter with regards to IoT threats?  
     
   VPNFilter was the first widespread persistent IoT threat. It is capable of surviving reboots and is difficult to remove. It has numerous malicious payloads it can use and is capable of wiping data and bricking a device, allowing the destruction of evidence.
3. What type of attack targeted the Democratic National Committee in 2019?  
     
    The DNC was targeted by a spear-phishing attack.
4. What were 48% of malicious email attachments in 2018?  
     
    48% of malicious email attachments were Office files.
5. What were the top two malicious email themes in 2018?  
     
    Decline in phishing and increase in malicious file attachments.
6. What was the top malicious email attachment type in 2018?  
     
    Microsoft Office file attachments were the most common malicious email attachment.
7. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
     
   Saudi Arabia had the highest email phishing rate (1 in 675 emails) and Poland had the lowest email phishing rate (1 in 9,653).
8. What is Emotet and how much did it jump in 2018?  
     
   Emotet is financial trojan malware. It’s prevalence increased by 12% in 2018, up to 16% from 4%.
9. What was the top malware threat of the year? How many of those attacks were blocked?  
   The top malware threat of the year was Heur.AdvML.C with 43,999,373 attacks blocked.
10. Malware primarily attacks which type of operating system?  
      
    Malware primarily attacks the Windows operating system.
11. What was the top coinminer of 2018 and how many of those attacks were blocked?  
      
    The top coinminer of 2018 was JS.Webcoinminer wit 2,768, 721 attacks blocked.
12. What were the top three financial Trojans of 2018?  
      
    The top three financial trojans of 2018 were:  
     - Ramnit  
    - Zbot  
    - Emotet
13. What was the most common avenue of attack in 2018?  
      
    Spear-phishing emails were the most common avenue of attack and were used by 65% of all known groups.
14. What is destructive malware? By what percent did these attacks increase in 2018?  
      
    Destructive malware is a type of malicious software used to make affected systems inoperable and pose challenges to reconstitution by employing the deletion of files critical to operation system function. These attacks increased by 25% in 2018.
15. What was the top user name used in IoT attacks?  
      
    The top user name used in IoT attacks was *root*.
16. What was the top password used in IoT attacks?  
      
    The top password used in IoT attacks was 123456
17. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?  
      
    The top three protocols used in IoT attacks were:  
     - telnet  
     - http  
     - https  
      
    The top two ports used in IoT attacks were:  
     - 23 Telnet  
     - 80 World Wide Web HTTP
18. In the underground economy, how much can someone get for the following?
19. Stolen or fake identity: $0.10 - $1.50
20. Stolen medical records: $15.00 - $25.00
21. Hacker for hire: $100.00+
22. Single credit card with full details: $1.00 - $45.00
23. 500 social media followers: $2.00 - $6.00