# 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 a form of digital information theft when cybercriminals inject malicious JavaScript code to hack a website and hijack the functionality of forms on the page. If these forms are login forms or Payment forms, they can collect sensitive user information like login credentials, credit card numbers, SSN among other PII.
2. How many websites are compromised each month with formjacking code?   
   4,818 unique websites were compromised with FormJacking code every month in 2018
3. What is Powershell?According to Microsoft website, PowerShell is a task automcation and configuration management framework, consisting of a command-line shell and scripting language. It is an equivalent of Linux Bash but for Windows operating system.
4. What was the annual percentage increase in malicious Powershell scripts?  
   Malicious Powershell scripts increased by 1,000 percent in 2018
5. What is a coinminer?  
   Coinminer is a program that generates cryptocurrencies like Bitcoin, Monero, Ethereum among others.
6. How much can data from a single credit card can be sold for? Data from a single credit card can be sold on underground markets for up to $45. However, Cyber criminals can sell this data to multiple actors and earn much more.
7. How did Magecart successfully attack Ticketmaster?

Magecart compromised a third-party chatbot hosted on Ticketmaster and loaded malicious code into the web browsers of visitors to Ticketmaster’s website. This attack aimed at harvesting customers’ payment data.

1. What is one reason why there has been a growth of formjacking?   
   The growth in formjacking can be attributed to the general growth in supply chain attacks. With the reliance of online businesses on third-party services like chatbots and customer reviews, the attackers target these third-party services with formjacking and thus affect bigger online retailers.
2. Cryptojacking dropped by what percentage between January and December 2018?  
   Cryptojacking events dropped by 52% between January and December 2018.
3. If a web page contains a coinmining script, what happens?   
   A coinmining script on a web page can use the web page visitors’ computing power to mine for cryptocurrency for as long as the web page is open.
4. How does an exploit kit work?   
   An exploit kit is a tool that comes with a collection of exploits from multiple exploit authors but packed into one tool. An exploit kit works in the following stages:
5. Victim lands on a compromised website
6. Victim is redirected to the exploit kit’s landing page
7. Exploits are served ( exploit uses a vulnerable application to secretly run malware)
8. Malicious payload is served ( when an exploit is successful, the exploit kit sends a payload to infect the host which can be ransomware, keylogger, banking trojan among many)
9. What does the criminal group SamSam specialize in?   
   Targeted Ransomware attacks
10. How many SamSam attacks did Symantec find evidence of in 2018?   
    67 SamSam attacks mostly against organizations in the U.S.
11. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
    Balance of attack pattern changed from consumers to enterprises with majority of infections occurring in businesses
12. In 2018, what was the primary ransomware distribution method?   
    Email campaigns
13. 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? “Living off the land” attacks make use of what already exists in the environment. They rely on exploiting points of entry that already exist in IT systems by injecting malicious code in trusted programs.

This type of attack helps attackers maintain a low profile by hiding their activity in a mass of legitimate processes.

1. What is an example of a tool that’s used in “living off the land” attacks?  
   PowerShell
2. What are zero-day exploits?  
   Zero-day exploits are cyber attacks that occur on the same day a weakness is discovered in software.
3. By what percentage did zero-day exploits decline in 2018?   
   4 percent (from 27 in 2017 to 23 in 2018)
4. What are two techniques that worms such as Emotet and Qakbot use?  
   Dumping Passwords from Memory

Brute-force access to network shares

1. What are supply chain attacks? By how much did they increase in 2018?  
   Supply chain attacks exploit third-party services or software to compromise a final target. They can take many forms including hijacking software updates and injecting malicious code into legitimate software. Supply chain attacks increased by 78 percent in 2018.
2. What challenge do supply chain attacks and living off the land attacks highlight for organizations?

Both supply chain and living off the land attacks come from trusted channels, using fileless attack methods or legitimate tools for malicious purposes, this is a challenge for organizations which rely heavily on supply chain for their business operation.

1. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
   55
2. 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 and North Korea

1. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
   Poor configuration
2. 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
3. What are two examples of the above cloud attack?   
   Meltdown and Spectre
4. 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 of IoT with 75 percent of attacks on Routers and 15 percent of attacks on connected Cameras
5. What is the Mirai worm and what does it do?   
   Mirai is a [malware](https://en.wikipedia.org/wiki/Malware) that turns networked devices running [Linux](https://en.wikipedia.org/wiki/Linux) into remotely controlled [bots](https://en.wikipedia.org/wiki/Internet_bot) that can be used as part of a [botnet](https://en.wikipedia.org/wiki/Botnet) in large-scale network attacks. Mirai distributed denial of service worm is the third most common IoT threat in 2018. Devices infected by Mirai continuously scan the internet for the [IP address](https://en.wikipedia.org/wiki/IP_address) of [Internet of things](https://en.wikipedia.org/wiki/Internet_of_things) (IoT) devices and try brute-force login attacks using default usernames and passwords from IoT vendors.
6. Why was Mirai the third most common IoT threat in 2018?   
    Mirai was the third most common IoT threat in 2018 because IoT devices often remain unpatched.
7. What was unique about VPNFilter with regards to IoT threats?  
   VPNFilter was the first widespread IoT threat that was able to survive a reboot making it difficult to remove.
8. What type of attack targeted the Democratic National Committee in 2019?   
   Spear-phishing attack
9. What were 48% of malicious email attachments in 2018?

Microsoft Office Files

1. What were the top two malicious email themes in 2018?   
   Bill and Email delivery failure
2. What was the top malicious email attachment type in 2018?   
   .doc, .dot
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   Highest was Saudi Arabia (1 in 675)

Lowest was Poland (1 in 9,653)

1. What is Emotet and how much did it jump in 2018?   
   Emotet is a self propagating banking trojan malware program which obtains financial information by injecting computer code into the networking stack of an infected Microsoft Windows computer, allowing sensitive data to be stolen via transmission. It jumped to account for 16 percent of financial Trojans in 2018 up from 4 percent in 2017.
2. What was the top malware threat of the year? How many of those attacks were blocked?  
   Top malware threat of 2018 was Heur.AdvML.C

43,999,373 attacks were blocked

1. Malware primarily attacks which type of operating system?   
   Windows
2. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   JS.Webcoinminer

2,768,721 attacks were blocked

1. What were the top three financial Trojans of 2018?   
   Ramnit, Zbot and Emotet
2. What was the most common avenue of attack in 2018?   
   Spear-phishing emails
3. What is destructive malware? By what percent did these attacks increase in 2018?

Destructive malware is malicious software with the capability to render affected systems inoperable and challenge reconstitution.  
25 percent increase over 2017 in destructive malware attack

1. What was the top user name used in IoT attacks?   
   root
2. What was the top password used in IoT attacks?   
   123456
3. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
   Telnet, http and https

23, 80

1. 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