# 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 payment card details and other information from payment forms on the checkout web pages of eCommerce sites,

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

4800

1. What is Powershell?

PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS.

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

1000

1. What is a coinminer?  
   Coinminer is an unwanted malicious software which uses the victim's computational power (CPU and RAM mostly) to mine for coins (for example Monero or Zcash). ... Most sophisticated coin miners use timer settings or cap the CPU usage in order to remain stealthy**.**
2. How much can data from a single credit card can be sold for?

45 dollars in underground marker

1. How did Magecart successfully attack Ticketmaster?

Magecart compromised a third-party chatbot, which loaded malicious code into the web browsers of visitors to Ticketmaster’s website, with the aim of harvesting customers’ payment data.

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

Since the drop in value of crpto currency that is what why formjacking has increased

1. Cryptojacking dropped by what percentage between January and December 2018?  
   90%
2. If a web page contains a coinmining script, what happens?

If a web page contains a coinmining script, the web page visitors’ computing power will be used to mine for cryptocurrency for as long as the web page is open

1. How does an exploit kit work?

Exploit kits start with a website that has been compromised. The compromised page will discreetly divert web traffic to another landing page. Within the landing page is code that will profile the victim's device for any vulnerable browser-based applications.

1. What does the criminal group SamSam specialize in?   
    ransomware attacks
2. How many SamSam attacks did Symantec find evidence of in 2018?

67

1. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?

Up until 2017, consumers were the hardest hit by ransomware, accounting for the majority of infections. In 2017, the balance tipped towards enterprises, with the majority of infections occurring in businesses. In 2018, that shift accelerated and enterprises accounted for 81 percent of all ransomware infections. While overall ransomware infections were down, enterprise infections were up by 12 percent in 2018. This shift in victim profile was likely due to a decline in exploit kit activity, which was previously an important channel for ransomware delivery

1. In 2018, what was the primary ransomware distribution method?   
   Email campaigns
2. What operating systems do most types of ransomware attacks still target?

Windows based system

1. What are “living off the land” attacks? What is the advantage to hackers? The trend of attackers opting for off-the-shelf tools and operating system features to conduct attacks

it can help 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?  
   A zero day exploit is a cyber attack that occurs on the same day a weakness is discovered in software
3. By what percentage did zero-day exploits decline in 2018?

23 %

1. What are two techniques that worms such as Emotet and Qakbot use?  
   use simple techniques including dumping passwords from memory or brute-forcing access to network shares to laterally move across a network.
2. What are supply chain attacks? By how much did they increase in 2018?  
   Supply chain attacks, which exploit third-party services and software to compromise a final target, take many forms, including hijacking software updates and injecting malicious code into legitimate software. Developers continued to be exploited as a source of supply chain attacks, either through attackers stealing credentials for version control tools, or by attackers compromising third-party libraries that are integrated into larger software projects.

78 %

1. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   That the attacks increasingly arriving through trusted channels, using fileless attack methods or legitimate tools for malicious purposes.
2. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?

The 20 most active groups tracked by Symantec targeted an average of 55 organizations over the past three years, up from 42 between 2015 and 2017.

1. 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 , China , Russia, North Korea, Iran

1. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?

Poorly secured cloud databases and poor configuration

1. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?

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.

1. What are two examples of the above cloud attack? ‘

Store Bypass and Foreshadow

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 Cameras , 75 and 15
2. What is the Mirai worm and what does it do?   
   Mirai worm is DDOS attack and It basically exploits unpatched devices
3. Why was Mirai the third most common IoT threat in 2018?

Mirai is constantly evolving and variants use up to 16 different exploits, persistently adding new exploits to increase the success rate for infection, as devices often remain unpatched. The worm also expanded its target scope by going after unpatched Linux servers. Another noticeable trend was the increase in attacks against industrial control systems (ICS). The Thrip group went after satellites, and Triton attacked industrial safety systems, leaving them vulnerable to sabotage or extortion attacks

1. What was unique about VPNFilter with regards to IoT threats?  
   Its ability to survive a reboot making it very difficult to remove
2. What type of attack targeted the Democratic National Committee in 2019?   
   Cyber attack
3. What were 48% of malicious email attachments in 2018?

Microsoft office files

1. What were the top two malicious email themes in 2018?   
   Bills
2. What was the top malicious email attachment type in 2018?

Macros , malicious XML files and Office files with DDE payloads

1. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   Saudi Arabia and Poland
2. What is Emotet and how much did it jump in 2018?

Emotet is a Trojan which uses simple techniques of dumping passwords from memory or brute-forcing access to network shares to laterally move across a network.   
16%

1. What was the top malware threat of the year? How many of those attacks were blocked?

Banking trojans and information stealers and 25%

1. Malware primarily attacks which type of operating system?

Windows

1. What was the top coinminer of 2018 and how many of those attacks were blocked?

JS.Webcoinminer and 2,768,721

1. What were the top three financial Trojans of 2018?   
   Ramnit

Zbot

Emotet

1. What was the most common avenue of attack in 2018?   
   Zero Day Vulnerabilities
2. What is destructive malware? By what percent did these attacks increase in 2018?   
   Spear Fishing and 65%

1. What was the top user name used in IoT attacks?

oot

1. What was the top password used in IoT attacks?

123456

1. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?

Telnet, http and https

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: $15–20
   3. Hacker for hire: $100+
   4. Single credit card with full details: $1–45
   5. 500 social media followers: $2–6