# 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 uses javascript code to steal information such as credit card details

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

**4818** websites are compromised each month using formjacking

1. What is Powershell?

Powershell is a command shell/language used to give directions directly to the windows operating system

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

There is a **1000%** increase of malicious PS scripts per year

1. What is a coinminer?

Coinminers are malicious bits of code found on websites that utilize visitor’s hardware to mine cryptocurrency as long as the page is open

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

Credit card data can be sold for around **$45** on the underground market

1. How did Magecart successfully attack Ticketmaster?

Magecart attacked Ticketmaster using a **formjacker**. It used a chatbot to load the malicious code into browsers that were using Ticketmasters’ website trying to collect payment data

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

The value of cryptocurrency has dropped, and the income guaranteed by selling stolen credit card information makes formjacking more profitable than cryptohacking

1. Cryptojacking dropped by what percentage between January and December 2018?  
    Cryptojacking rates dropped by **52%** between January and December 2018
2. If a web page contains a coinmining script, what happens?

If a web page contains a coinmining script the visitor’s hardware will be utilized to mine cryptocurrency as long as the web page is open

1. How does an exploit kit work?

An exploit kit works by getting information on the victims machine and delivering an exploit that will work with the hardware/software it detects

1. What does the criminal group SamSam specialize in?

SamSam Specalizes in **ransomware** attacks

1. How many SamSam attacks did Symantec find evidence of in 2018?

Symantic found evidence of **67** ransomware attacks by SamSam in 2018

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

While ransomware attacks in general declined in 2017-2018 **there was a large increase in business/enterprise infections**

1. In 2018, what was the primary ransomware distribution method?

In 2018 the main distribution method for ransomware was **Email campaigns**

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

The **Windows** operating system is still the most common ransomware target

1. What are “living off the land” attacks? What is the advantage to hackers?

Living off the land attacks use system tools/resources that are already present on the victim’s machine. This is useful to hackers because it means they do not have to worry about compatibility and dependencies. This means that everything they need is there and they just need to inject malicious code or commands, which can be difficult to detect by administrators

1. What is an example of a tool that’s used in “living off the land” attacks?

Some tools that use “living off the land” attacks include **Powershell, or the task scheduler**

1. What are zero-day exploits?

Zero-day exploits are attacks using vulnerabilities that are unknown to software developers

1. By what percentage did zero-day exploits decline in 2018?

Zero-day exploits went from 27% (2017) to 23% (2018) meaning there was a total decrease by **4%**

1. What are two techniques that worms such as Emotet and Qakbot use?

Emotet and Quakbot both use malicious “living off the land” techniques to self-propagate and also brute-force passwords to gain administrative privileges. They may also use supply chain attacks to offload their malicious code onto their target systems

1. What are supply chain attacks? By how much did they increase in 2018?

Supply chain attacks increased by **78%** in 2018. These attacks use third party services/software to inject malicious code into their final target

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 are difficult to mitigate because they use software that is often essential and powerful (meaning it has the ability to bypass administrative privileges). They are also difficult to detect because they utilize systems that are already making changes to your system so you need to monitor core system actions to ensure malicious processes are not being run

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

About **55** organizations were targeted by attack groups tracked by Symantec between the years of 2016 and 2018

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?

About **49** individuals or organizations were indicted for cyber criminal activities from countries such as **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** is the most common theme when it comes to the increased number of cloud cybersecurity attacks

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

**Speculative execution** targets cloud services because they tend to use virtual processors with a **shared pool of memory**, which means that an attack on one physical system could quickly spread to other instance/servers through the shared memory

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

**Meltdown and Spectre** are both examples of cloud attacks

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** are the two most commonly infected IoT devices accounting for **90%** (75% routers, 15% cameras) of all IoT attacks

1. What is the Mirai worm and what does it do?

The Mirai worm uses a DDos attacks using learned exploits to specifically target at IoT devices

1. Why was Mirai the third most common IoT threat in 2018?

Mirai was the third most common IoT threat in 2018 because it constantly updated its many exploits and expanded its target scope to include linux based servers

1. What was unique about VPNFilter with regards to IoT threats?

VPNFilter was unique in regards to IoT threats because it was persistent and could **survive reboots** and had several attack types and targets (MitM, credential theft, communication interception).

1. What type of attack targeted the Democratic National Committee in 2019?

In 2019 the Democratic National Committee was targeted by a **Spear-phishing attack**

1. What were 48% of malicious email attachments in 2018?

48% of malicious email attachments in 2018 were **Office Files**

1. What were the top two malicious email themes in 2018?

The most common theme of malicious emails in 2018 were **Bills and Email Delivery Failure** (15.5% and 13.3% respectively)

1. What was the top malicious email attachment type in 2018?

The most malicious email attachment type in 2018 were **.doc, .dot**

1. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?

**Saudia Arabia** had the highest phishing rate of 1 in 675. **Poland** had the lowest phishing rate of 1 in 9,653

1. What is Emotet and how much did it jump in 2018?

Emotet is a **Financial Trojan** and jumped **12%** up to 16% of financial Trojans in 2018 from 4% in 2017.

1. 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 (52.1%)

1. Malware primarily attacks which type of operating system?

Malware primarily attacks the **Windows** operating system

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

The top Coinminer of 2018 was **JS.Webcoinminer** with **2,768,721** attacks blocked (49.7%)

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

**Ramnit, Zbot, and Emotet** were the top the financial trojans of 2018

1. What was the most common avenue of attack in 2018?

The most common avenue of attack in 2018 was **Spear-Phishing emails**

1. What is destructive malware? By what percent did these attacks increase in 2018?

Destructive malware is capable of standard malware attack tactics but also includes the ability to **wipe or brick** devices if the attacker chooses to do so. These type of attacks increased by **25%** in 2018

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

The top user name used in IoT attacks is **“root”** (not surprising since root is the default administrator user name for linux systems)

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

The top password used in IoT attacks is **“123456”**

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

The top three protocols for IoT attacks were **telnet, http, and https** using ports **23 and 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**