# 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 foam jacking?

* 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.

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

* 4,818 unique websites were compromised with foam jacking code every month in 2018.

1. What is Powershell?

* Is a task automation and configuration management program from Microsoft, consisting of a command-line shell and the associated scripting language.

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

* Reflected by a massive 1,000 percent increase in malicious PowerShell scripts blocked in 2018 on the endpoint.

1. What is a coinminer?

* Devices used without their knowledge use their central processing unit (CPU) power to mine cryptocurrencies.

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

* The data from a single credit card can be sold for more than $45.

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 foam jacking?

* The growth in foam jacking in 2018 may be partially explained by the drop in the value of cryptocurrencies during the year.

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

* Dropping by 52 percent between January and December 2018.

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

* The web page visitors’ computing power will be used to mine cryptocurrency for as long as the web page is open.

1. How does an exploit kit work?

* The exploit kit gathers information on the victim machine, finds vulnerabilities, and determines the appropriate exploit.

1. What does the criminal group SamSam specialize in?

* Modus Operandi is to gain access to an organization’s network, spend time performing reconnaissance by mapping out the network, before encrypting as many computers as possible, and presenting the organization with a single ransom demand

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

* 4,900 per month in 2018 or 59000 in total.

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

* email protection and using technologies such as behavioral analysis or machine learning increased efficiency at blocking ransomware earlier in the infection process.

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

* During 2018, the chief ransomware distribution method was email campaigns.

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

* Windows-based computers.

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

* Using malicious PowerShell scripts that allow hackers to take control of your computers and other connected devices. The advantages are they don't have to download files to your computer all the time.

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

* PowerShell

1. What are zero-day exploits?

* Is a vulnerability that is either known to the developers of the program or unknown that is exploited before a patch can be done.

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

* Only 23 percent of attack groups were known to use zero-days in 2018, down from 27 percent in 2017.

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

* Dumping passwords from memory or brute-forcing access to network shares.

1. 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; these attacks increased by 78 percent in 2018.

1. What challenges do supply chain attacks and living off the land attacks highlight for organizations?

* Increase attack from trusted channels

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

* 55 organizations

1. How many individuals or organizations were indicted for cybercriminal activities in 2018? What are some of the countries that these entities were from?

* Forty-nine individuals or organizations were indicted during 2018. There were 18 alleged Russian agents, along with19 Chinese individuals or organizations were charged, along with 11 Iranians, and one North Korean.

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

* Poorly secured cloud databases continued to be a weak point for organizations

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

* Cloud instances have their own 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?

* 1) S3 buckets emerged as an Achilles heel for organizations, with more than 70 million records stolen or leaked as a result of poor configuration. 2) This was on the heels of a spate of ransomware attacks against open databases such as MongoDB in 2017, which saw attackers wipe their contents and seek payment in order to restore them.

1. Regarding the 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 and accounted for 75 and 15 percent of the attacks respectively.

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

* Malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots.

1. 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.

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

* Its ability to survive a reboot makes it very difficult to remove.

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

* The DNC revealed it was targeted by an unsuccessful spear-phishing attack shortly after the midterms had ended.

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

* Office Files

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

* Bill and Email delivery failure

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

* doc, .dot

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

* Saudi Arabia 675 and Poland 9,653

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

* Type of Worm and it jumped to 16% in 2018

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 and 43,999,373 attacks were blocked or 52.1% of attacks

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?

* The top coinminer of 2018 was JS.Webcoinminer and 2,768,721 attacks were blocked or 49.7% of attacks

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

* 1) Ramnit (2) Zbot (3) Emotet

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

* Spear-phishing emails remained the most popular avenue for attack and were used by 65 percent of all known groups.

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

* Malicious software with the capability to render affected systems inoperable and challenge reconstitution. Had 25 percent increase over 2017.

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

* Root

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?

* The top three protocols used in IoT attacks (1)telnet, (2)http, (3)https. The top two ports used in IoT attacks were (1)Telnet and (2)World Wide Web HTTP.

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: $0.50–20
   5. 500 social media followers: $2–6