# 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?

“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 - trended upwards in 2018.” **(Symantec Report Pg. 14)**

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

“Symantec data shows that 4,818 unique websites were compromised with formjacking code every month in 2018.” **(Symantec Report Pg. 14)**

1. What is Powershell?

“Powershell is a task automation and configuration management framework from Microsoft, Consisting of a command - line shell and the associated scripting language.” (<https://en.wikipedia.org/wiki/PowerShell>)

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

The annual percentage of Powershell scripts has gone up 1000%. (<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/formjacking-attacks-retailers>)

1. What is a coinminer?

Coinminer is a program to mine different cryptocurrencies. Here are a few cryptocurrencies; DogeCoin, Ethereum, or Bitcoin; ext.

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

“The data from a single credit card can be sold for more than $45, data security provider Symantec reports.” (<https://www.cnbc.com/2019/09/26/heres-everything-cyber-criminals-can-do-if-they-steal-your-credit-card.html#:~:text=The%20data%20from%20a%20single,information%20for%20383%20million%20people.>)

1. How did Magecart successfully attack Ticketmaster?

“Magecart attackers injected malicious JavaScript code onto Ticketmaster’s website after they compromised a chatbot from tech firm Inbenta that was used for customer support on Ticketmaster’s websites. Magecart was then able to alter the JavaScript code on Ticketmaster’s website to capture payment card data from customers and send it to their servers.” (<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/formjacking-attacks-retailers>)

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

“Hackers and cybercriminals look for the most efficient way to do their jobs. That’s one of the reasons for the recent increase in formjacking, in which credit card data and other personal information is stolen via illicit JavaScript from the forms on e-commerce sites.” (<https://biztechmagazine.com/article/2019/04/formjacking-attacks-rise-retail-sector#:~:text=Just%20like%20any%20worker%2C%20hackers,forms%20on%20e%2Dcommerce%20sites.>)

1. Cryptojacking dropped by what percentage between January and December 2018?  
   Cyrptojacking activity “dropped by 52% between January and December 2018” **(Symantec Report Pg. 15)**
2. If a web page contains a coinmining script, what happens?

“The web page visitor’s computing power will be used to mine for cryptocurrency for as long as the web page is open.” **(Symantec Report Pg. 15)**

1. How does an exploit kit work?

“An exploit kit gathers information on the victim machine, finds vulnerabilities and determines the appropriate exploit, and delivers the exploit, which typically silently drive-by downloads and executes malware, and further running post-exploitation modules to maintain further remote access to the compromised system.” (<https://en.wikipedia.org/wiki/Exploit_kit#:~:text=The%20exploit%20kit%20gathers%20information,access%20to%20the%20compromised%20system.>)

1. What does the criminal group SamSam specialize in?

“Samsam specializes in target ransomware attacks, breaking into networks, and encrypting multiple computers across an organization before issuing a high-value ransom demand.” (<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks>)

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

Samsam was found to be “seen in 67 different targets” in 2018. (<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/samsam-targeted-ransomware-attacks>)

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

“Initial adopters of cryptojacking turned to other ways to make money, such as formjacking.” **(Symantec Report Pg. 15)**

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

During 2018, the chief ransomware distribution method was email campaigns.” **(Symantec Report Pg. 16)**

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

“Windows Computers” **(Symantec Report Pg. 15)**

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

“A Living off the Land (LotL) attack describes a cyberattack in which intruders use legitimate software and functions available in the system to perform malicious actions on it.”

“Attackers do not leave traces in the form of malicious fil;es on device hard drives, so Living off the Land attacks cannot be detected by comparing signatures. Additionally, operating system tools, such as Powershell and WMI, may appear in the security software’s allowlist, which also impededes detection of their anomalous activity. Finally, adversaries' use of legitimate tools also complicates the investigation and attribution of cyberattacks.”

<https://encyclopedia.kaspersky.com/glossary/lotl-living-off-the-land/#:~:text=A%20Living%20off%20the%20Land%20(LotL)%20attack%20describes%20a%20cyberattack,perform%20malicious%20actions%20on%20it.&text=LotL%20attacks%20are%20often%20classified,not%20leave%20any%20artifacts%20behind.>

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

An example of “Living off the Land (LotL) tools; Powershell, WMI (Windows Management Instrumentation), PsExec, and Mimikatz.” (<https://encyclopedia.kaspersky.com/glossary/lotl-living-off-the-land/#:~:text=A%20Living%20off%20the%20Land%20(LotL)%20attack%20describes%20a%20cyberattack,perform%20malicious%20actions%20on%20it.&text=LotL%20attacks%20are%20often%20classified,not%20leave%20any%20artifacts%20behind.>)

1. What are zero-day exploits?

“A zero-day exploit is the method hackers use to attack systems with a previously unidentified vulnerability.” (<https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit>)

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

Zero-day exploits “declined in 2018 by 23% from 27% in 2017%” **(Symantec Report Pg. 17)**

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

Emote and Qakbot both “use simple techniques including dumping passwords from memory or brute-forcing access to network shares laterally move across a network.” **(Symantec Report Pg. 17)**

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.” **(Symantec Report Pg. 17)**

1. What challenges do supply chain attacks and living off the land attacks highlight for organizations?   
   “Both supply chain and Living off the Land attacks highlight the challenges facing organizations and individuals, with attacks increasingly arriving through trusted channels, using fileless attack methods or legitimate tools for malicious purposes.” **(Symantec Report Pg. 17)**
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 2025 and 2017.” **(Symantec Report Pg. 18)**

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?

“Forty-nine individuals or organizations were indicted in 2018. Some of the countries these entities were from are Russia, China, Iran, and North Korea.” **(Symantec Report Pg. 18)**

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.” **(Symantec Report Pg. 19)**

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

Depends on who the manufacturer is. Chip makers are now becoming more popular for attack due to chip exploits. “Cloud services not only have their own virtual processors, they also share pools of memory.” **(Symantec Report Pg. 19)**

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

In 2018, there were two exploit attacks; Meltdown and Spectre.

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?

The two most common IoT attacks were both “routers and connected cameras,” accounting for “75 and 15 percent of the attacks.” **(Symantec Report Pg. 20)**

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

“Miarai worm is malware that infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots or zombies.” (<https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/#:~:text=What%20is%20Mirai%3F,used%20to%20launch%20DDoS%20attacks.>) Miarai distributes a denial of service (DDoS).

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

Just about everything we ran back then and now is connected to the internet. It is easy to exploit since everything is talking to each other.

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

A VPNFilter has an ability to survive a reboot making it very difficult to remove. It can attack as “a man in the middle (MitM), data exfiltration, credential theft, and interception of SCADA communications.” **(Symantec Report Pg. 19)** Not to mention it could completely brick the IoT device and or even wipe itself if not wanting to be detected.

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

Malicious spear-phishing attacks were used in 2019.

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

“ 48% Malicious email attachments are office files.” **(Symantec Report Pg. 19)**

1. What were the top two malicious email themes in 2018?   
   The top two malicious emails were both, “spam and email malware.”
2. What was the top malicious email attachment type in 2018?

The top malicious email in 2018 were, “email attachments.”

1. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   Poland has the highest email phishing rate of 9,653. Suadi Arabia has the lowest at 675. **(Symantec Report Facts and Figures 29)**
2. What is Emotet and how much did it jump in 2018?

Emot is a Trojan that is primarily spread through spam emails (malspam). (<https://www.malwarebytes.com/emotet>) It has grown from “4% to 16%.” **(Symantec Report Facts and Figures 29)**

1. What was the top malware threat of the year? How many of those attacks were blocked?  
     
   Heur.AdvML.C is the top malware of 2018. There were 43,999,373 blocked in that time. **(Symantec Report Facts and Figures 33)**
2. Malware primarily attacks which type of operating system?

Windows OS is the operating of choice for most malware.

1. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   The top coinminer 0f 2018 was “JS.Webcoinminer.” It was blocked “2,768,721” times. **(Symantec Report Facts and Figures 39)**
2. What were the top three financial Trojans of 2018?   
   The top three financial Trojans of 2018 are, “Ramnit, Zbot, and Emotet.” **(Symantec Report Facts and Figures 40)**
3. What was the most common avenue of attack in 2018?

The most common avenue of attack in 2018 is “Spear-phishing emails.” **(Symantec Report Facts and Figures 50)**

1. 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. Destructive malware went up “8%” in 2018. (<https://www.ibm.com/downloads/cas/XZGZLRVD#:~:text=Destructive%20malware%20is%20malicious%20software,operating%20system's%20ability%20to%20run.>) / **(Symantec Report Facts and Figures 50)**

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

“Root,” is the top user name in IoT attacks in 2018 **(Symantec Report Facts and Figures 54)**

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

“123456,” is the top password used in IoT attacks in 2018. **(Symantec Report Facts and Figures 54)**

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 are, “telnet, http, and https.” The top two ports used were, “Telnet and World Wide Web HTTP.” **(Symantec Report Facts and Figures 55)**

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 - $35.00
   3. Hacker for hire: $100
   4. Single credit card with full details: $1.00 - $45.00
   5. 500 social media followers: $2.00 - $6.00

**(Symantec Report Facts and Figures 40)**