# 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 credit card details and other information from payment forms in the checkout webpages of eCommerce sites …” (Symantec Corporation, 2019)**
2. How many websites are compromised each month with formjacking code?   
   **About 4,800**
3. What is Powershell? **“Powershell is a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting language.” (Microsoft, 2020)**
4. What was the annual percentage increase in malicious Powershell scripts?  
   **In 2018, the increase in malicious Powershell scripts was noted to be by 1,000 percent, according to the Symantec Report.**
5. What is a coinminer?  
   **“Coinminers (also called cryptocurrency miners) are programs that generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity. When intentionally run for one’s own benefit, they may prove a valuable source of income.” (NortonLifeLock, 2019)**
6. How much can data from a single credit card can be sold for?

**Up to $45.**

1. How did Magecart successfully attack Ticketmaster?

**“Megacart 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.” (Symantec Corporation, 2019)**

1. What is one reason why there has been a growth of formjacking?   
   **“The growth in formjacking in 2018 may be partially explained by the drop in the value of cryptocurrencies during the year: cyber criminals who may have used websites for cryptojacking may now be opting for formjacking.”** (**Symantec** **Corporation**, **2019**)
2. Cryptojacking dropped by what percentage between January and December 2018?  
   **Dropped by 52%**
3. 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.” (Symantec Corporation, 2019)**
4. How does an exploit kit work?   
   **“Exploits are often the first part of a larger attack. Hackers scan for outdated systems that contain critical vulnerabilities, which they then exploit by deploying targeted malware.” (Microsoft, 2020)**

**“Exploit kits are more comprehensive tools that contain a collection of exploits. These kits scan devices for different kinds of software vulnerabilities and, if any are detected, deploy additional malware to further infect a device. Kits can use exploits targeting a variety of software …”** (**Microsoft**, **2020**)

1. What does the criminal group SamSam specialize in?   
   **The criminal group “SamSam specializes in targeted ransomware attacks, breaking into networks and ecrypting multiple computers across an organization before issuing a high-value ransom demand.” (Threat Hunter Team, 2018)**
2. How many SamSam attacks did Symantec find evidence of in 2018?   
   **“During 2018, Symantec has to date found evidence of attacks against 67 different organizations. SamSam targeted organizations in a wide range of sectore, but healthcare was by far the most affected sector, accounting for 24 percent of the attacks in 2018.” (Threat Hunter Team, 2018)**
3. 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.” (Symantec Corporation, 2019)**
4. In 2018, what was the primary ransomware distribution method?   
   **In 2018 the primary ransomware distribution method was email campaigns.** (**Symantec** **Corporation**, **2019**)
5. What operating systems do most types of ransomware attacks still target?

**Windows-based systems.**

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

**“Attackers are increasingly making use of tools already installed on targeted computers or are running simple scripts and shellcode directly in memory.”**

**(Wueest & Anand, 2017)**

**There are multiple advantages to hackers using this type of attack including less chance of being discovered by creating less new files.**

1. What is an example of a tool that’s used in “living off the land” attacks?  
   **sc.exe, WMI, VNC, RDP, PsExec, Mimkatz, Powershell (Wueest & Anand, 2017)**
2. What are zero-day exploits?  
   **“The term ‘zero-day’ refers to a newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn’t been released.” (Chivers, 2019)**
3. By what percentage did zero-day exploits decline in 2018?   
   **23%**
4. What are two techniques that worms such as Emotet and Qakbot use?  
   **Dumping passwords or brute-forcing.**
5. What are supply chain attacks? By how much did they increase in 2018?  
   **“Supply chain attacks continued to be a feature of the threat landscape, with attacks increasing by 78% 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 legitmate softward.” (Symantec Corporation, 2019)**
6. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   **Both attacks are able to disguise themselves well.**
7. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
   **55**
8. 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, Iran and North Korea**
9. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
   **Poor configuration.**
10. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?   
    **“Successful exploitation provides access to memory locations that are normally forbidden. This is particularly problematic for cloud services because while cloud instances have thir 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.” (Symantec Corporation, 2019)**
11. What are two examples of the above cloud attack?   
    **Meltdown and Spectre**
12. 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 at 75% and connected cameras at 15%**
13. What is the Mirai worm and what does it do?   
    **Mirai worm is a distributed denial of service (DDoS) that is constantly evolving by using up to 16 different exploits.**

**“Mirai can launch both HTTP flood and network-level attacks, there are certain IP address ranges that Mirai is hard-wired to avoid, including those owned by GE, Hewlett-Packard, and the U.S. Department of Defense and upon infecting a device, Mirai looks for *other* malware on that device and wipes it out, in order to claim the gadget as its own.” (Fruhlinger, 2018)**

1. Why was Mirai the third most common IoT threat in 2018?   
   **“The notorious Mirai distributed denial of service (DDoS) worm remained an active threat and, with 16 percent of the attacks, was 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 remain unpatched.” (Symantec Corporation, 2019)**
2. What was unique about VPNFilter with regards to IoT threats?  
   **“VPNFilter was the first widespread persistent IoT threat, with its ability to survive a reboot making it very difficult to remove.” (Symantec Corporation, 2019)**
3. What type of attack targeted the Democratic National Committee in 2019?   
   **An unsuccessful spear-phishing attack targeted the DNC in 2019.**
4. What were 48% of malicious email attachments in 2018?

**The 48% of malicious email attachments in 2018 were Office Files, which were up 5% from 2017.**

1. What were the top two malicious email themes in 2018?   
   **The top two malicious email theme were Bill and Email delivery failure with 15.7 and 13.3, respectively.**
2. What was the top malicious email attachment type in 2018?   
   **The top malicious email attachment with 37% was .doc and .dot.**
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?

**The country with the highest email phishing rate with 1 in 118 was Saudi Arabia and the country with the lowest with 1 in 905 was Japan.**

1. What is Emotet and how much did it jump in 2018?   
   **Emotet is ‘… a sophisticated Trojan commonly functioning as a downloader or dropper of other malware …” (Cybersecurity & Infrastructure Security Agency, 2020) The Emotet jumped to 16 percent from 4 percent in 2017.**
2. 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.Adv.ML.C and 43,999,373 attacks were blocked.**
3. Malware primarily attacks which type of operating system?   
   **The malware primarily attacked Windows operating system from2016-2018.**
4. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   **The top coimminer of 2018 was JS.Webcoinminer with 2,768,721 attacks blocked.**
5. What were the top three financial Trojans of 2018?   
   **The top three financial Trojans of 2018 were Ramnit, Zbot, and Emotet.**
6. What was the most common avenue of attack in 2018?   
   **The most common avenue of attack in 2018 was spear phishing.**
7. 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 reconstruction**.**”** **(IBM, 2020)**

**“IBM’s X-Force Incident Response and Intelligence Services team released the report … which outlines a 200 percent increase in the number of destructive attacks it’s responded to since the second half of 2018.” (Uria, 2019)**

1. What was the top user name used in IoT attacks?   
   **The top user name used in IoT attacks was root.**
2. What was the top password used in IoT attacks?   
   **Top password used in IoT attacks was 123456.**
3. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
   **The top three protocols were telnet, http, and https while the top two ports were 23 and 80.**
4. 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**