# 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” (pg14)**
2. How many websites are compromised each month with formjacking code?   
   **- 4,818 unique websites (pg14)**
3. What is Powershell? **- “The trend of attackers opting for off-the-shelf tools and operating system features to conduct attacks. This trend of “living off the land” shows no sign of abating—in fact, there was a significant increase in certain activity in 2018. PowerShell usage is now a staple of both cybercrime and targeted attacks” (pg17)**
4. What was the annual percentage increase in malicious Powershell scripts?  
   **-1,000% increase ( pg 17)**
5. What is a coinminer?  
   **- a coinminer allows for a device to be used to mine crypto on the users device using CPU power to mine. This is used in Cyrptojacking, where criminals surreptitiously run coinminers on victims’ devices without their knowledge and use. (pg 15)**
6. How much can data from a single credit card can be sold for?  **-$45 on underground markets (pg 14)**
7. 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.” (pg14)**

1. What is one reason why there has been a growth of formjacking?   
   **- Much of this formjacking activity has been blamed on actors dubbed Magecart, which is believed to be several groups, with some operating in competition with one another. (pg 14)**
2. Cryptojacking dropped by what percentage between January and December 2018?  
   **- Cryptojacking activity fell by 52% between January and December**
3. If a web page contains a coinmining script, what happens?   
   **-“Browser-based coin mining takes place inside a web browser and is implemented using scripting languages. 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. Browser-based miners allow cyber criminals to target even fully patched devices and can also allow them to operate stealthily without the activity being noticed by victims.” (pg 15)**
4. How does an exploit kit work?   
   **- “exploit kit activity, which was previously an important channel for ransomware delivery.” (pg 16)**
5. What does the criminal group SamSam specialize in?   
   **- Ransomware attacks (pg 16)**
6. How many SamSam attacks did Symantec find evidence of in 2018?   
   **-“During 2018, Symantec found evidence of 67 SamSam attacks, mostly against organizations in the U.S.” (pg 16)**
7. 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.” (pg 16)**
8. In 2018, what was the primary ransomware distribution method?   
   **-During 2018, the chief ransomware distribution method was email campaigns. (pg 16)**
9. What operating systems do most types of ransomware attacks still target?

**-Windows based operating systems (pg 16)**

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.” (pg 17)**
2. What is an example of a tool that’s used in “living off the land” attacks?  
   **- “The use of macros in Office files as their preferred method to propagate malicious payloads in 2018, but also experimented with malicious XML files and Office files with DDE payloads.” (pg 17)**
3. What are zero-day exploits?  
   **-A zero-day is a computer-software vulnerability unknown to those who should be interested in its mitigation. Until the vulnerability is mitigated, hackers can exploit it to adversely affect programs, data, additional computers or a network.**
4. By what percentage did zero-day exploits decline in 2018?   
   **-27%**
5. What are two techniques that worms such as Emotet and Qakbot use?  
   **- “Instead, worms such as Emotet (Trojan.Emotet) and Qakbot (W32. Qakbot) use simple techniques including dumping passwords from memory or brute-forcing access to network shares to laterally move across a network.” (pg 17)**
6. 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 percent 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.” (pg 17)**
7. What challenge 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. While we block on average 115,000 malicious PowerShell scripts each month, this only accounts for less than 1 percent of overall PowerShell usage. Effectively identifying and blocking these attacks requires the use of advanced detection methods such as analytics and machine learning.” (pg 17)**
8. 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.” (pg 18)**
9. How many individuals or organizations were indicted for cyber criminal activities in 2018? What are some of the countries that these entities were from?   
   **- “One of the most dramatic developments during 2018 was the significant increase in indictments in the United States against people alleged to be involved in state-sponsored espionage. Forty-nine individuals or organizations were indicted during 2018, up from four in 2017 and five in 2016. While most of the headlines were devoted to the indictment of 18 alleged Russian agents, most of whom were charged with involvement in attacks relating to the 2016 presidential election, the indictments were far more wide ranging. Alongside Russian nationals, 19 Chinese individuals or organizations were charged, along with 11 Iranians, and one North Korean.” (pg 18)**
10. 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. In 2018, S3 buckets emerged as an Achilles heel for organizations, with more than 70 million records stolen or leaked as a result of poor configuration.” (pg 19)**
11. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?   
    **- “Meltdown and Spectre exploit vulnerabilities in a process known as speculative execution. Successful exploitation provides access to memory locations that are normally forbidden. This is particularly problematic for cloud services because while 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.” (pg 19)**
12. What are two examples of the above cloud attack?   
    **- “They were also followed up by similar chip-level vulnerabilities such as Speculative Store Bypass and Foreshadow, or L1 Terminal Fault” (pg 19)**
13. 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 connected cameras were the most infected devices and accounted for 75 and 15 percent of the attacks respectively.” (pg 20)**
14. What is the Mirai worm and what does it do?   
    **- “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.” (pg 20)**
15. 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.” (pg 20)**
16. 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. With an array of potent payloads at its disposal, such as man in the middle (MitM) attacks, data exfiltration, credential theft, and interception of SCADA communications, VPNFilter was a departure from traditional IoT threat activity such as DDoS and coin mining. It also includes a destructive capability which can “brick,” or wipe a device at the attackers’ command, should they wish to destroy evidence. VPNFilter is the work of a skilled and well-resourced threat actor and demonstrates how IoT devices are now facing attack from many fronts.” (Pg 20)**
17. What type of attack targeted the Democratic National Committee in 2019?   
    **- “Unsuccessful spear-phising attack” (pg 21)**
18. What were 48% of malicious email attachments in 2018?

* **“48% of malicious email attachments are office files up from 5% in 2017” (pg 23)**

1. What were the top two malicious email themes in 2018?   
   **- Bill; Email Delivery Failure (pg 27)**
2. What was the top malicious email attachment type in 2018?   
   **- .doc, .dot; .exe (pg 27)**
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   **- Saudi Arabia (1 in 675)**  
   **Canada (1 in 4,308) (pg 29)**
4. What is Emotet and how much did it jump in 2018?   
   **- 16% jump (pg 31)**
5. What was the top malware threat of the year? How many of those attacks were blocked?  
   **-Heur.AdvML.C; 43,999,373; 52.1% (pg 23)**
6. Malware primarily attacks which type of operating system?   
   **- 2016 Windows; 161,708,289; 98.5% (pg 35)**
7. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   **- JS.Webcoinminer; 2,768,721 attacks blocked; 49.7% (pg 39)**
8. What were the top three financial Trojans of 2018?   
   **-Ramnit; Zbot; Emotet (pg 40)**
9. What was the most common avenue of attack in 2018?   
   **- Spear-phising emails remained the most popular avenue for attack and were used by 65% of all known groups. (pg 51)**
10. What is destructive malware? By what percent did these attacks increase in 2018?   
    **-While still a niche area, the use of destructive malware continued to grow. Eight percent of groups were known to use destructive tools, up from 6 percent at the end of 2017. (pg 52)**
11. What was the top user name used in IoT attacks?   
    **- root; 38.1% (pg 54)**
12. What was the top password used in IoT attacks?   
    **- 123456; 24.6% (pg 54)**
13. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
    **- Protocols: Telnet (90.9%); http (6.6%); https (1.0%)**

**-Ports: 23 Telnet (85.0%); 80 World Wide Web HTTP (6.5%) (pg 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: $15-20
   3. Hacker for hire: $100+
   4. Single credit card with full details: $1-45
   5. 500 social media followers: $2-6