# 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?**  
   Essentially the hijacking of a website’s forms. This may include anything from a general contact form to a payment form.
2. **How many websites are compromised each month with formjacking code?**   
   According to the Symantec report - 4800
3. **What is Powershell?**A hybrid solution of shell, language and framework which allows for the control and automation of tasks, native to windows but available for other OS’s.
4. **What was the annual percentage increase in malicious Powershell scripts?**  
   According to the Symantec report - 1000%
5. **What is a coinminer?**  
   Typically a program that ‘mines’ cryptocurrency. In a malicious context, they can be deployed on targets to leverage a large collective computing power, delivering the mined currency to the actors pocket.
6. **How much can data from a single credit card can be sold for?** According to the Symantec report - Data from a single card could be sold for up to $45
7. **How did Magecart successfully attack Ticketmaster?**  
   Magecart managed to exploit a vulnerability in a third party Chat Bot, having it inject malicious code for the site’s visitors to load.
8. **What is one reason why there has been a growth of formjacking?**   
   Due to the immense surface area available, formjacking is fairly easy, efficient and profitable
9. **Cryptojacking dropped by what percentage between January and December 2018?**  
   According to the Symantec report - 52%
10. **If a web page contains a coinmining script, what happens?**   
    This can cause the web page to utilise the visitors hardware resources to mine cryptocurrency, provided the webpage stays open and the script is able to run.
11. **How does an exploit kit work?**   
    Exploit Kits typically provide an automated method to leverage vulnerabilities in systems or applications such as websites and then distribute malware to a victim’s machine.
12. **What does the criminal group SamSam specialize in?**   
    SamSam treats ransomware like a proper business, focussing attacks on competitors and maintaining control over their intellectual property, which in turn restricts defensive tactics.
13. **How many SamSam attacks did Symantec find evidence of in 2018?**According to the Symantec report - 67 SamSam attacks were detected.
14. **Even though ransomware attacks declined in 2017-2018, what was one dramatic** change that occurred?   
    There was an increase in the percentage of ransomware attacks on enterprise businesses.
15. **In 2018, what was the primary ransomware distribution method?**   
    According to the Symantec report - Email campaigns were the chief method.
16. **What operating systems do most types of ransomware attacks still target?**

Windows operating system is generally the most targeted OS for ransomware attacks.

1. **What are “living off the land” attacks? What is the advantage to hackers?**These attacks are usually conducted via tools and features provided by operating systems and software suites
2. **What is an example of a tool that’s used in “living off the land” attacks?**  
   Powershell is a great example. It is now native to the Windows OS and thereby every Windows host potentially carries the associated vulnerabilities.
3. **What are zero-day exploits?**  
   An vulnerability that is considered unknown to parties who would seek to mitigate it, preferably prior to its exploitation.
4. **By what percentage did zero-day exploits decline in 2018?**   
   According to the Symantec report - There was a 4% decline from 27% (2017) to 23% (2018)
5. **What are two techniques that worms such as Emotet and Qakbot use?**  
   Brute forcing network shares and dumping passwords from memory.
6. **What are supply chain attacks? By how much did they increase in 2018?**  
   These attacks are generally via components & services that support the actual target, such as libraries that are integrated into software projects. According to the Symantec report - supply chain attacks increased by 78% in 2018
7. **What challenge do supply chain attacks and living off the land attacks highlight for organizations?**These types of attack are becoming increasingly difficult to detect and defend.
8. **The 20 most active groups tracked by Symantec targeted an average of how many organizations between 2016 and 2018?**   
   According to the Symantec report - 55 organisations between 2016 and 2018
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?**49 organisations or individuals were indicted during 2018, with entities from countries such as Russia, China, Iran and North Korea.
10. **When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?**   
    According to the Symantec report - Poor configuration was the primary vulnerability.
11. **What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?**   
    Cloud based infrastructure typically pools resources, thereby an attack via one instance could innately provide access to other instances sharing the pool.
12. **What are two examples of the above cloud attack?**   
    Spectre and Foreshadow are two example exploitations of the speculative execution vulnerability.
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?**   
    According to the Symantec report - Routers (75%) and Cameras (15%) were the two most common device types.
14. **What is the Mirai worm and what does it do?**   
    This worm performs DDoS attacks upon internet connected devices.
15. **Why was Mirai the third most common IoT threat in 2018?**  
    The constant evolution and updating of this threat gives it a high success rate, especially against poorly patched devices.
16. **What was unique about VPNFilter with regards to IoT threats?**  
    VPNFilter was the first widespread persistent threat, meaning that it could remain active after a reboot and prove to be very difficult to overcome.
17. **What type of attack targeted the Democratic National Committee in 2019?**   
    The DNC was targeted by a spear-phishing attack, supposedly it was unsuccessful.
18. **What were 48% of malicious email attachments in 2018?**   
    According to the Symantec report - In 2018, 48% of malicious email attachments were Office files

1. **What were the top two malicious email themes in 2018?**   
   According to the Symantec report - The top two themes were Bills and Email Delivery Failures.
2. **What was the top malicious email attachment type in 2018?**   
   According to the Symantec report - The top malicious email attachment types were the extensions .doc and .dot
3. **Which country had the highest email phishing rate? Which country had the lowest email phishing rate?**  
   According to the Symantec report - Saudi Arabia had the highest email phishing rate with 1 in 675 emails being malicious. The lowest phishing rate was attributed to Poland with only 1 in 9,653 emails.
4. **What is Emotet and how much did it jump in 2018?**   
   Emotet is a Trojan that also has features similar to a worm, enabling it to spread quickly. It utilises techniques such as brute forcing of network shares to traverse a network. It was attributed to 16% of financial Trojans, jumping 12% from 2017.
5. **What was the top malware threat of the year? How many of those attacks were blocked?**  
   According to the Symantec report - Heur.AdvML.C was the top malware threat for 2018, with 43,999,373 attacks blocked it was attributed to 52.1% of attacks.
6. **Malware primarily attacks which type of operating system?**   
   The Windows OS is the most attacked OS, with over 97% of attacks for 3 years running.
7. **What was the top coinminer of 2018 and how many of those attacks were blocked?**   
   According to the Symantec report - JS.Webcoinminer was the top contender, with 2,768,721 attacks blocked - just under 50%.
8. **What were the top three financial Trojans of 2018?**   
   According to the Symantec report - Ramnit, Zbot and Emotet were the top three, accounting for 81%.
9. **What was the most common avenue of attack in 2018?**   
   According to the Symantec report - Spear-phising emails were most popular with 65% of known groups using them.
10. **What is destructive malware? By what percent did these attacks increase in 2018?**  
    Destructive malware typically ‘bricks’ devices, making them inoperable. The use of destructive malware rose 2% in 2018, with 8% of groups utilising them.
11. **What was the top user name used in IoT attacks?**   
    The top user name used in IoT attacks during 2018 was ‘root’
12. **What was the top password used in IoT attacks?**   
    The top password used in IoT attacks during 2018 was ‘123456’
13. **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 for IoT attacks in 2018 were telnet (90.9%), http (6.6%) and https (1%). The top two ports attacked were the default ports for the top two protocols, TCP 23 (telnet) and TCP 80 (http).
14. **In the underground economy, how much can someone get for the following?** 
    1. Stolen or fake identity: $0.10 to $1.50
    2. Stolen medical records: $0.10 to $35
    3. Hacker for hire: $100+
    4. Single credit card with full details: $1 to $45
    5. 500 social media followers: $2 to $6

Great work Glenn.