# 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 hacking a website by javascript injection and thereby stealing user information, especially identity or payment information submitted through the forms on that website.
2. How many websites are compromised each month with formjacking code?   
   4,800 websites were compromised each month with formjacking code.
3. What is Powershell?Powershell is a modern command shell with the ability to script and automate management tasks. It is a cross platform tool that could be used to manage Windows, Linux & OSx. Unlike many other shells, instead of just returning text output, powershell can return .NET objects which makes it an advanced tool.
4. What was the annual percentage increase in malicious Powershell scripts?  
   It was observed that there was a 1,000% increase in malicious Powershell scripts.
5. What is a coinminer?  
   Coinminer also known as crypto miner is a program that is used to mine/generate crypto currency like Bitcoin, Ethereum etc.. A coinminer attack is also known as cryptojacking, where hacking for compute resources thereby to mine the crypto currency using coinminer programs.
6. How much can data from a single credit card can be sold for? $0.50 - $20 is the value of a single credit card in the underground economy.
7. How did Magecart successfully attack Ticketmaster?

By using a formjacking Magecart compromised a third-party chatbot, which injected javascript code onto the TicketMaster website visitor's browser and thereby harvesting the payment data.

1. What is one reason why there has been a growth of formjacking?   
   In 2018, the fall of cryptocurrency value is considered as a trigger for the growth of formjacking.
2. Cryptojacking dropped by what percentage between January and December 2018?  
   52% is the drop in cryptojacking between January - December 2018.
3. If a web page contains a coinmining script, what happens?   
   As long as the visitor has the web page open, Coinminer will keep using the compute power for crypto mining.
4. How does an exploit kit work?   
   Exploit kit looks for vulnerabilities in a system to deliver the malware payloads by exploiting those vulnerabilities.
5. What does the criminal group SamSam specialize in?   
   SamSam group is specialised in ransomware attacks.
6. How many SamSam attacks did Symantec find evidence of in 2018?   
   Symantec found 67 SamSam attacks, most of them against the U.S Organisations.
7. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
   Even though the overall ransomware attacks declined in 2017-2018, there was a 12% raise in enterprise infections.
8. In 2018, what was the primary ransomware distribution method?   
   Exploit kit was the primary ransomware distribution method until the start of 2018 and then it shifted to email campaigns.
9. What operating systems do most types of ransomware attacks still target?

While WIndows & Mac operating systems are the most targeted OSs, Linux based IoT are also high on the list.

1. What are “living off the land” attacks? What is the advantage to hackers? “Living off the land” attack is fileless malware attack that uses the readily available tools such as Powershell, WMI, Office etc. The advantage is that the activity is hard to locate in the mass amount of legitimate process logs. Also as these tools are already whitelisted on the systems, in most instances there would be very minimal logging enabled on the process by these tools.
2. What is an example of a tool that’s used in “living off the land” attacks?  
   Office macros, Powershell scripts are the tools used in “living off the land” attacks.
3. What are zero-day exploits?  
   Zero-day exploits are the attacks based on the vulnerability that is known to the software/hardware vendor but yet the patch is not available to fix it. Usually these attacks happen on the same day that they are discovered.
4. By what percentage did zero-day exploits decline in 2018?   
   Zero-day exploits decreased by 4% in 2018 to 23% compared to 27% in 2017.
5. What are two techniques that worms such as Emotet and Qakbot use?  
   Dumping passwords from system memory & brute-force techniques are used to access the available network shares.
6. What are supply chain attacks? By how much did they increase in 2018?  
   Supply Chain attacks are more of exploiting the 3rd party software and services like software updates or injecting malicious code into a legitimate code by different means. These attacks have gone up by 78% in 2018.
7. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   As both supply chain and living off the land attacks use the genuine software and tools installed on the machines, it is very hard to isolate and identify the activity. These attacks would prove to be most effective and destructive in nature.
8. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
   The average is about 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 individuals or organisations from different countries including Russia, China, Iran & North Korea.
10. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
    Poor configuration is the most common theme in the cloud cybersecurity attacks.
11. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?   
    As memory is a shared resource, a successful cloud exploitation could result in data breach on multiple server instances.
12. What are two examples of the above cloud attack?   
    Emotet & Qakbot are good examples that exploit memory access by dumping data, mainly passwords to propagate laterally from server to server.
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 are the two most common devices with 75% and 15% IoT attacks attributed to them respectively.
14. What is the Mirai worm and what does it do?   
    Mirai worm is a DDos attacker mainly infecting the routers and they by attacking the networks.
15. Why was Mirai the third most common IoT threat in 2018?   
    It accounted for 16% of the attacks in 2018.
16. What was unique about VPNFilter with regards to IoT threats?  
    VPNFilter is a persistent IoT threat that could survive a restart unlike Mirai.
17. What type of attack targeted the Democratic National Committee in 2019?   
    DNC was unsuccessfully targeted by spear-phishing attack in 2019.
18. What were 48% of malicious email attachments in 2018?

In 2018, 48% of malicious email attachments are office files.

1. What were the top two malicious email themes in 2018?   
   Spam and email malware were the top two malicious email themes in 2018.
2. What was the top malicious email attachment type in 2018?   
   Malicious Office files are sent as email attachments which accounted for 48% of malicious email attachments.
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   Poland had the highest email phishing rate with 1 in 9653 while Saudi Arabia had lowest with 1 in 675 emails.
4. What is Emotet and how much did it jump in 2018?   
   Emotet is a banking trojan, a self-propagating worm that spreads through known remotely exploitable vulnerabilities. There was an increase in these supply chain attacks in 2018 by 78%.
5. What was the top malware threat of the year? How many of those attacks were blocked?  
   Heur.AdvML.C is the top malware threat for the year 2018 accounting to 52.1% of the total Malware threats. 43,999,373 Heur.AdvML.C attacks were blocked in 2018.
6. Malware primarily attacks which type of operating system?   
   Windows is the primary target for the Malware attacks.
7. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   JS.Webcoinminer is the top coinminer of 2018 and 2,768,721 of JS.Webcoinminer attacks were blocked in 2018.
8. What were the top three financial Trojans of 2018?   
   Ramnit, Zbot & Emotet are the top three financial Trojans of 2018. Just these three account for 81% of the total Financial trojan attacks in 2018.
9. What was the most common avenue of attack in 2018?   
   Spear Phishing is the most common avenue of attack in 2018 accounting for 65% of attack groups using this as their primary infection vector.
10. What is destructive malware? By what percent did these attacks increase in 2018?   
    Destructive malware is malicious software used to deem the infected systems inoperable [Gathered from infographic published by IBM]. There is a 25% increase in groups using these tools.
11. What was the top user name used in IoT attacks?   
    “root” is the top username used in the IoT attacks.
12. What was the top password used in IoT attacks?   
    “123456” is the top password used in IoT attacks.
13. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
    Telnet, http & https are the top three protocols used in IoT attacks. 23 & 80 are the top two ports used in the IoT attacks.
14. 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