# 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 a cyber attack that involves hackers inserting malicious Javascript code into the webpage, most often a payment form. Once the code is in operation and a consumer enters their details it is sent to the hacker including but not limited to name, address and credit card details.  
   (Gupta, 2021)
2. **How many websites are compromised each month with formjacking code?**According to the data provided by Symantec(Internet security threat report, 2019, pg.14) 4818 unique websites were compromised each month in 2018.
3. **What is Powershell?**Powershell is a cross-platform task automation solution made up of a command-line shell, a scripting language and a configuration management framework that runs on windows, linux and macOS.  
   (What is PowerShell? - PowerShell, 2021)
4. **What was the annual percentage increase in malicious Powershell scripts?**According to Symantec(Internet security threat report, 2019, pg.17) there has been a 1000% increase in malicious Powershell scripts in 2018.
5. **What is a coinminer?**A coinminer is a program that performs complex mathematical calculations to maintain the blockchain ledger; this process uses significant resources on a computer. While they aren’t inherently malicious, cybercriminals use malware to install trojanized miners on peoples computers without their knowledge to use their resources.  
   (Coin miners - Windows security, 2021)
6. **How much can data from a single credit card can be sold for?**According to Symantec(Internet security threat report, 2019, pg.14) the data from 1 credit card can be sold for up to $45 on underground markets.
7. **How did Magecart successfully attack Ticketmaster?** According to Symantec(Internet security threat report, 2019, pg.14) Magecart did this by compromising a third-party chatbot which then loaded malicious code into the web browsers of customers with the aim of stealing their payment data.
8. **What is one reason why there has been a growth of formjacking?**According to Symantec(Internet security threat report, 2019, pg.14) Magecart, several groups of actors, some of which are competitors, are responsible for the growth in forjacking attacks.
9. **Cryptojacking dropped by what percentage between January and December 2018?**According to Symantec(Internet security threat report, 2019, pg.15) Cryptojacking dropped by 52% between January and December 2018.
10. **If a web page contains a coinmining script, what happens?**According to Symantec(Internet security threat report, 2019, pg.15) when a web page contains a coinmining script the visitor's computing power will be used to mine for cryptocurrency without the visitor knowing for as long as the web page remains open. Miners like this allow cyber criminals to operate stealthily.
11. **How does an exploit kit work?**Exploit kits are comprehensive tools that contain a collection of exploits, these kits scan devices for different vulnerabilities in several kinds of software and when a vulnerability is detected it will deploy further malware to infect a device.  
    (Exploits and exploit kits - Windows security, 2021)
12. **What does the criminal group SamSam specialize in?**According to Symantec(Internet security threat report, 2019, pg.16) SamSam is an organization that specializes in Ransomware attacks.

1. **How many SamSam attacks did Symantec find evidence of in 2018?**According to Symantec(Internet security threat report, 2019, pg.16) SamSam was responsible for 67 attacks, mostly against organizations in the US.
2. **Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?**According to Symantec(Internet security threat report, 2019, pg.16) A dramatic change that occurred was the primary target shifted from consumers to businesses and in 2018 shifted to enterprises.
3. **In 2018, what was the primary ransomware distribution method?**According to Symantec(Internet security threat report, 2019, pg.16) the primary distribution method was through email.
4. **What operating systems do most types of ransomware attacks still target?**

85% of managed service providers say that the most common OS to be infected by Ransomware is Windows, for the simple fact that they are more affordable therefore more widespread.  
(Ransomware Facts, Trends & Statistics for 2021, 2021)

1. **What are “living off the land” attacks? What is the advantage to hackers?**Living off the land refers to attackers using tools or features that already exist in the target environment, the benefit for hackers to do this is they do not need a file to infect the target device which makes it easier to remain undetected and don’t need to worry about developing a compatible tool for the job.  
   (What Are Living Off the Land Attacks? | LogRhythm, 2021)
2. **What is an example of a tool that’s used in “living off the land” attacks?**According to Symantec(Internet security threat report, 2019, pg.17) a common tool used for LOTL attacks is Powershell.
3. **What are zero-day exploits?**A Zero-day exploit is an attack that involves an actor exploiting a vulnerability that the developer has only just learned of and has not yet had time to fix the problem.  
   (What is a Zero-day Attack? - Definition and Explanation, 2021)
4. **By what percentage did zero-day exploits decline in 2018?**According to Symantec(Internet security threat report, 2019, pg.17) only 23% of attack groups were known to use Zero-day exploits.
5. **What are two techniques that worms such as Emotet and Qakbot use?**According to Symantec(Internet security threat report, 2019, pg.17) Two techniques that worms use are; Dumping passwords from memory or brute forcing access to move laterally across a network.
6. **What are supply chain attacks? By how much did they increase in 2018?**Supply chain attacks are when a trusted piece of software had been compromised by a supplier.  
   (Greenberg, 2021)
7. **What challenge do supply chain attacks and living off the land attacks highlight for organizations?**According to Symantec(Internet security threat report, 2019, pg.17) the challenge highlighted for organizations is that these attacks come through trusted channels and are difficult to defend against.
8. **The 20 most active groups tracked by Symantec targeted an average of how many organizations between 2016 and 2018?**According to Symantec(Internet security threat report, 2019, pg.18) the 20 most active groups tracked by Symantec targeted an average of 55 organizations.
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?**According to Symantec(Internet security threat report, 2019, pg.18) 49 individuals or organizations were indicted, most of which headlined from Russia, 19 Chinese individuals or organizations, 11 Iranians and 1 North Korean.
10. **When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?**According to Symantec(Internet security threat report, 2019, pg.19) the common theme for cloud cybersecurity attacks is poor configuration. There are numerous tools that allow an actor to identify misconfigured cloud resources.
11. **What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?**According to Symantec(Internet security threat report, 2019, pg.19) The implication of successful cloud exploitation is that cloud systems share pools of memory which means a single physical system being breached will result in multiple systems worth of memory being leaked.
12. **What are two examples of the above cloud attack?**According to Symantec(Internet security threat report, 2019, pg.19) examples would be Meltdown and Spectre, the former breaks the fundamental isolation between applications and an OS which allows access to the memory, the latter breaks down the isolation between different applications which tricks error-free programs into leaking information.  
    (Meltdown and Spectre, 2021)
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 Symantec(Internet security threat report, 2019, pg.20) the two most infected devices are Routers and Connected Cameras accounting for 75% and 15% respectively.
14. **What is the Mirai worm and what does it do?**The Mirai worm is a malware that infects smart devices that run specifically on ARC processors turning them into a network of remotely controlled bots which then can effectively launch DDoS attacks on a large scale.  
    (What is the Mirai botnet?, 2021)
15. **Why was Mirai the third most common IoT threat in 2018?**According to Symantec(Internet security threat report, 2019, pg.20) Mirai was the third most common IoT threat because it can use up to 16 existing exploits and is constantly evolving, persistently adding new exploits to increase the success rate because devices often remain unpatched.
16. **What was unique about VPNFilter with regards to IoT threats?**According to Symantec(Internet security threat report, 2019, pg.20) it’s ability to survive a reboot, making it hard to remove, it’s many potent payloads and the ability to ‘Brick’ a device at the attackers command, is what makes it unique.
17. **What type of attack targeted the Democratic National Committee in 2019?**According to Symantec(Internet security threat report, 2019, pg.21) the DNC was targeted (unsuccessfully) by a Spear Phishing attack, the cyber espionage group APT29 which can be attributed to Russia by many sources is thought to be responsible.
18. **What were 48% of malicious email attachments in 2018?**According to Symantec(Internet security threat report, 2019, pg.17) Microsoft office files account for 48% of malicious email attachments which is a 5% increase from the previous year.

1. **What were the top two malicious email themes in 2018?**According to Symantec(Internet security threat report, 2019, pg.27) the top 2 themes are Bills (15.7%) and email delivery failure (13.3%).
2. **What was the top malicious email attachment type in 2018?**According to Symantec(Internet security threat report, 2019, pg.27) the top malicious email attachment type is the .doc/.dot file type (37%).
3. **Which country had the highest email phishing rate? Which country had the lowest email phishing rate?**According to Symantec(Internet security threat report, 2019, pg.29) the country that had the highest phishing rate is Poland (9653) and the country with the lowest is Saudi Arabia (641).
4. **What is Emotet and how much did it jump in 2018?**According to Symantec(Internet security threat report, 2019, pg.31) Emotet jumped up 12% between 2017 - 2018 from 4% to 16%. Emotet is a malware program that was originally a banking trojan, it’s goal is to access devices and take private data from it.  
   (Emotet: How to best protect yourself from the Trojan, 2021)
5. **What was the top malware threat of the year? How many of those attacks were blocked?**According to Symantec(Internet security threat report, 2019, pg.33) the top malware threat of the year is Heur.AdvML.C with a total of 43,999,373 attacks blocked (52.1%).
6. **Malware primarily attacks which type of operating system?**According to Symantec(Internet security threat report, 2019, pg.35) Malware primarily attacks the Windows operating system (98.5% from 2016, 97.6% from 2017 and 97.2% from 2018).
7. **What was the top coinminer of 2018 and how many of those attacks were blocked?**According to Symantec(Internet security threat report, 2019, pg.39) the top coinminer blocked in 2018 is the JS.Webcoinminer with a total of 2,768,721 attacks blocked (49.7%).
8. **What were the top three financial Trojans of 2018?**According to Symantec(Internet security threat report, 2019, pg.40) the top 3 finacial trojans of 2018 are; Ramnit at 271,930 attacks blocked (47.4%), Zbot at 100,821 attacks blocked (17.6%) and Emotet at 92,039 attacks blocked (16%).
9. **What was the most common avenue of attack in 2018?**According to Symantec(Internet security threat report, 2019, pg.49) the most common avenue of attack in 2018 remains Spear-phishing emails, used by 65% of all known groups.
10. **What is destructive malware? By what percent did these attacks increase in 2018?**According to Symantec(Internet security threat report, 2019, pg.49) Destructive malware is present within 8% of groups and has grown by 25% since 2017. Destructive Malware is malicious software with the capability to render affected systems inoperable. Most destructive malware causes destruction through deletion or wiping of files that are critical for operating systems.  
    (What is Destructive Malware?, 2021)
11. **What was the top user name used in IoT attacks?**According to Symantec(Internet security threat report, 2019, pg.54) the top username used in IoT attacks is root (38.1%).
12. **What was the top password used in IoT attacks?**According to Symantec(Internet security threat report, 2019, pg.54) the top password used in IoT attacks is 123456 (24.6%).
13. **What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?**According to Symantec(Internet security threat report, 2019, pg.55) the top 3 protocols used in IoT attacks are; telnet (90.9%), http (6.6%) and https (1%).
14. **In the underground economy, how much can someone get for the following?**According to Symantec(Internet security threat report, 2019, pg.54) In the Underground economy the amount you could get for each are as follows;
    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

**Bibliography**

Docs.microsoft.com. 2021. *Coin miners - Windows security*. [online] Available at: <<https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/coinminer-malware>>.

www.kaspersky.com. 2021. *Emotet: How to best protect yourself from the Trojan*. [online] Available at: <<https://www.kaspersky.com/resource-center/threats/emotet>>.

Docs.microsoft.com. 2021. *Exploits and exploit kits - Windows security*. [online] Available at: <<https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/exploits-malware>>.

Greenberg, A., 2021. *What Is a Supply Chain Attack?*. [online] Wired. Available at: <<https://www.wired.com/story/hacker-lexicon-what-is-a-supply-chain-attack/>>

.  
Gupta, D., 2021. *What is a Formjacking attack?*. [online] Loginradius.com. Available at: <<https://www.loginradius.com/blog/start-with-identity/2021/01/what-is-formjacking/>>.

2019. *Internet security threat report*. Symantec, pg.14-21,27,29,33,35,39,40,49,54,55.

Meltdownattack.com. 2021. *Meltdown and Spectre*. [online] Available at: <<https://meltdownattack.com/>>.

SafetyDetectives. 2021. *Ransomware Facts, Trends & Statistics for 2021*. [online] Available at: <<https://www.safetydetectives.com/blog/ransomware-statistics/#:~:text=Eighty%2Dfive%20percent%20of%20managed,therefore%20more%20people%20use%20them>.>.

LogRhythm. 2021. *What Are Living Off the Land Attacks? | LogRhythm*. [online] Available at: <https://logrhythm.com/blog/what-are-living-off-the-land-attacks/>.

www.kaspersky.com. 2021. *What is a Zero-day Attack? - Definition and Explanation*. [online] Available at: <<https://www.kaspersky.com/resource-center/definitions/zero-day-exploit>>.