# 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?  
   **Answer: -** Formjacking is a type of digital information cyber-attack where cybercriminals inject malicious JavaScript code on the forms available on the website and especially eCommerce sites to steal credit card details and payment information, personal information and majority hackers get these details from the checkout or payment forms web pages. This is also sometimes referred to as virtual credit card skimming when a consumer enters their payment card information and hit submit then the malicious code collects the payment card information and any additional information the consumer may have entered such as Name, Address, Mobile Numbers then the code sends this information to the hackers or a location where hackers want it and the stolen data is sent on the form usually as fake image in the nomenclature of basically fake domain forward slash image and it can be very hard to see inject code due to there are so many images tags everywhere on a checkout webpages.
2. How many websites are compromised each month with formjacking code?   
   **Answer: -** As per Symantec reported that on average, 4,181 unique websites are compromised with formjacking code each month.
3. What is Powershell? **Answer: -** PowerShell is an open-source shell and scripting language built on top of Microsoft .NET technology. There are two things, PowerShell is an easy-to-use command-line shell that allows users to run commands at a command-line similar to the legacy command prompt (cmd.exe), and PowerShell is also a robust scripting environment language that can build tools and automating administrative tasks of systems and PowerShell can be used in a form of using malicious script used for cyber-attacks.

I want to mention that PowerShell, also known as Windows PowerShell, but with the 2016 introduction of PowerShell Core, it is no longer officially called Windows PowerShell. It is just called PowerShell, and Microsoft has opened the source to .NET Core, a cross platform, general purpose development framework, upon which PowerShell Core is coded and now PowerShell compiles, runs on UNIX based systems including Mac OS X and Linux. All of the built-in command line tools you expect from those operating systems are fully supported.

1. What was the annual percentage increase in malicious Powershell scripts?  
   **Answer: -** Use of malicious PowerShell scripts increased by 1,000 percent in 2018
2. What is a coinminer?  
   **Answer: -** Coinminer is a program that generates any given form of crypto-currency like Bitcoin, Monero.Coinminers are also called as cryptocurrency miners, and there is mainly Browser-based Cryptocurrency Miners. Coinminers run on victim’s devices without their knowledge use their central processing unit (CPU) power to mine cryptocurrencies, during this activity it consumes a lot of processing power and makes the computer slower than usual.
3. How much can data from a single credit card can be sold for?

**Answer: -** The data from a single credit card can be sold for up to $45 on underground markets.

1. How did Magecart successfully attack Ticketmaster?

**Answer: -** Magecart compromised a third-party chatbot, which loaded malicious code in to web browsers of visitors to Ticketmaster’s website, with the aim of harvesting customers payment data.

1. What is one reason why there has been a growth of formjacking?   
   **Answer: -** Drop in the value of crypto currencies is one of the reasons for the growth in formjacking.
2. Cryptojacking dropped by what percentage between January and December 2018?  
   **Answer: -** Cryptojacking dropped by around 52% percent between January and December 2018.
3. If a web page contains a coinmining script, what happens?   
   **Answer: -** If a web page contains a coinmining script, the web page visitor’s computing power will be used to mine for cryptocurrency for as long as the web page is open or active. 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.
4. How does an exploit kit work?   
   **Answer: -** Exploit kit gathers information on the victim machine, finds vulnerabilities and deciphers which exploit to use then determines the appropriate exploit, and delivers the exploit. Exploit kits are known by a number of other names, including infection kit, crimeware kit, DIY attack kit and malware toolkit.
5. What does the criminal group SamSam specialize in?   
   **Answer: -** SamSam specializes in targeted ransomware attacks, and they mostly targeted against organizations in the US, their first initial target to break into networks and encrypting multiple computers across an organization before issuing a high-value ransom demand.
6. How many SamSam attacks did Symantec find evidence of in 2018?   
   **Answer: -** During 2018, Symantec found evidence of 67 SamSam attacks, mostly against organizations in the U.S.
7. Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
   **Answer: -** The one dramatic change occurred that attacks tipped towards enterprises. 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.

1. In 2018, what was the primary ransomware distribution method?   
   **Answer: -** During 2018, the chief ransomware distribution method was email campaigns.
2. What operating systems do most types of ransomware attacks still target?

**Answer: -** Most major ransomware families still target Windows-based computers.

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

**A)** The world of cybercrime, the trend of attackers opting for off-the-shelf tools and operating system features to conduct attacks. That means those attacks that make use of tools already installed on targeted computers or attacks that run simple scripts and shellcode directly in memory.

**B)** Other advantage is the attackers don’t require malicious code and It can help attackers maintain a low profile by hiding their activity in a mass of legitimate processes.

1. What is an example of a tool that’s used in “living off the land” attacks?  
   **Answer: -** The example of a tool that’s used "living off the land" refers to fileless, malware less attacks that turn a system's own native tools against them, there are some tools commonly exploited for living off the land attacks include PowerShell scripts, VB scripts, Windows Management Instrumentation (WMI), Mimikatz, and PsExec.
2. What are zero-day exploits?  
   **Answer: -** Zero-day exploit is a cyberattack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator and Zero-day exploit is an unknown security vulnerability or software flaw that a hacker can target with malicious code and it can be referred to as zero-day vulnerability.
3. By what percentage did zero-day exploits decline in 2018?   
   **Answer: -** Zero-day exploits declined in 2018 by 4 percent, only 23 percent of attack groups were known to use zero-days, down from 27 percent in 2017.
4. What are two techniques that worms such as Emotet and Qakbot use?  
   **Answer: -** 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.
5. What are supply chain attacks? By how much did they increase in 2018?  
   **Answer: -**

**A)** Supply chain attacks are adding backdoors to legitimate and certified software or compromising systems used by third-party providers, which exploit third-party services and software to compromise a final target, and take many forms, including hijacking software updates and injecting malicious code into legitimate software.

**B)** It increased by 78 percent in 2018.

1. What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
   **Answer: -** 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.
2. The 20 most active groups tracked by Symantec targeted an average of how manyorganizations between 2016 and 2018?   
   **Answer: -** They attacked an average of 55 organizations over the past three years.
3. How many individuals or organizations were indicted for cyber criminal activities in 2018? What are some of the countries that these entities were from?   
   **Answer: -** 49 organizations were indicted by USA authorities. They were from China, Russia, Iran and North Korea.
4. When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
   **Answer: -** The common theme across these cloud cybersecurity attacks - Poor Configuration.
5. What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?   
   **Answer: -** Successful exploitation provides access to memory locations that are normally forbidden, 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.
6. What are two examples of the above cloud attack?   
   **Answer: -** Meltdown and Spectre, They were also followed up by similar chip-level vulnerabilities such as Speculative Store Bypass and Foreshadow, or L1 Terminal Fault.
7. Regarding Internet of Things (IoT) attacks, what were the two most common infected devices and what percentage of IoT attacks were attributed to them?   
   **Answer: -**
8. Routers and connected cameras were the most infected devices.
9. and accounted for 75 and 15 percent of the attacks respectively.
10. What is the Mirai worm and what does it do?   
    **Answer: -** Mirai is a distributed denial of service (DDoS) worm and Mirai malware infects smart devices that run on ARC processors, turning them into a network of remotely controlled bots, and as devices often remain unpatched, the worm also expanded its target scope by going after unpatched Linux servers.
11. Why was Mirai the third most common IoT threat in 2018?   
    **Answer: -** Mirai is constantly evolving and variants use up to 16 different exploits, persistently adding new exploits to increase the success rate for infection, that’s why Mirai was the third most common loT threat in 2018.
12. What was unique about VPNFilter with regards to IoT threats?  
    **Answer: -** Unique aboutVPNFilter was the first widespread persistent IoT threat, with its ability to survive a reboot making it very difficult to remove.
13. What type of attack targeted the Democratic National Committee in 2019?   
    **Answer: -** The Democratic National Committee revealed in January 2019, it was targeted by an unsuccessful spear-phishing attack.
14. What were 48% of malicious email attachments in 2018?

**Answer: -** They were email-based malware, with Office files.

1. What were the top two malicious email themes in 2018?   
   **Answer: -** The top two malicious email themes in 2018 were **Bill and Email delivery failure.**
2. What was the top malicious email attachment type in 2018?   
   **Answer: -** The top malicious email attachment type were .doc, .dot.
3. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
   **Answer: -**

Highest: - The country with the highest email phishing rate is Poland.

Lowest: - The country with the lowest email phishing rate is Suidi Arabia**.**

1. What is Emotet and how much did it jump in 2018?   
   **Answer: -**

**A)** Emotet is a computer malware program that was originally developed in the form of a banking Trojan, which obtains financial information by injecting computer code into the networking stack of an infected Microsoft Windows computer, allowing sensitive data to be stolen via transmission.

**B)** Emotet jumps up to 16%, from 4% in 2017.

1. What was the top malware threat of the year? How many of those attacks were blocked?  
   **Answer: -** The top malware threat was Heur.AdvML.C, and 43,999,373 attacks were blocked.
2. Malware primarily attacks which type of operating system?   
   **Answer: -** The malware primarily attacks on **Windows** operating system in the year of 2017, 2018, and 2018.
3. What was the top coinminer of 2018 and how many of those attacks were blocked?   
   **Answer: -** The top coinminer of 2018 was JS.Webcoinminer, and 2,768,721 were blocked.
4. What were the top three financial Trojans of 2018?   
   **Answer: -** 1)Ramnit, 2) Zbot, 3) Emote.
5. What was the most common avenue of attack in 2018?   
   **Answer: -** Spear-phishing emails remained the most popular avenue for attack and were used by 65 percent of all known groups.
6. What is destructive malware? By what percent did these attacks increase in 2018?   
   **Answer: -**
7. Destructive malware is malicious software with the capability to render affected systems inoperable and challenge reconstitution, most destructive malware variants cause destruction through the deletion, or wiping, of files that are critical to the operating system's ability to run.
8. Destructive malware attacks increase by 25 percent in 2018.
9. What was the top user name used in IoT attacks?   
   **Answer: -** The top user name used in IoT is Root.
10. What was the top password used in IoT attacks?   
    **Answer: -** The top password used in loT attacks were 123456.
11. What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
    **Answer: -**
12. The top three protocols were telnet, http, and https**.**
13. The top two ports were 23 and 80**.**
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.**