**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.

* What is formjacking?  
  When cybercriminals inject malicious JavaScript code to hack a website and take over the functionality of the site's form page to collect sensitive user information. Formjacking is designed to steal credit card details and other information from payment forms that can be captured on the checkout pages of websites.
* How many websites are compromised each month with formjacking code?   
  4800
* 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.
* What was the annual percentage increase in malicious Powershell scripts?  
  1000%
* What is a coinminer?  
  Mining is the process of running complex mathematical calculations necessary to maintain the blockchain ledger. This process generates coins but requires significant computing resources.
* How much can data from a single credit card can be sold for? $45
* 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.

* What is one reason why there has been a growth of formjacking?

The growth in formjacking in 2018 may be partially explained by the drop in the value of cryptocurrencies during the year: cyber criminals who may have used websites for cryptojacking may now be opting for formjacking. The value of stolen credit card details on the cyber underground is probably more assured than the value of cryptocurrencies in the current climate.

* Cryptojacking dropped by what percentage between January and December 2018?

52%

* If a web page contains a coinmining script, what happens?   
  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.
* How does an exploit kit work?   
  Exploit kits are automated programs used by attackers to exploit known vulnerabilities in systems or applications. They can be used to secretly launch attacks while victims are browsing the web, with the goal being to download and execute some type of malware. Because exploit kits work in the background, it can be difficult to know when you’re under attack.
* What does the criminal group SamSam specialize in?   
  Ransomware Attacks
* How many SamSam attacks did Symantec find evidence of in 2018?   
  67
* Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?   
  Most attacks targeted businesses.
* In 2018, what was the primary ransomware distribution method?   
  The chief ransomware distribution method was email campaigns. Enterprises tend to be more affected by email-based attacks since email remains the primary communication tool for organizations.
* What operating systems do most types of ransomware attacks still target?

Windows based computers. A few Macs

* What are “living off the land” attacks? What is the advantage to hackers? Living off the land attacks make use of what is already in the environment. They don’t need to develop malware to attack. Rather they use exploit points of entry that already exist in IT systems.
* What is an example of a tool that’s used in “living off the land” attacks?  
  -Microsoft Office Dynamic Data Exchange (DDE) protocol.

-A "reverse\_tcp" payload from Metasploit: The attackers use obfuscated shellcode that is executed via PowerShell to download this reverse shell.

-A legitimate version of the WinZip console: This creates a task to execute commands and communicate with the command-and-control (C&C) server. It’s likely this WinZip console is used to archive data, probably for exfiltration.

-The Rex PowerShell library, which is publicly available on GitHub, is also seen on victim machines. This library helps create and manipulate PowerShell scripts for use with Metasploit exploits.

* What are zero-day exploits?  
  A zero-day exploit is the method hackers use to attack systems with a previously unidentified vulnerability.
* By what percentage did zero-day exploits decline in 2018?   
  4%
* What are two techniques that worms such as Emotet and Qakbot use?  
  They use simple techniques including dumping passwords from memory or brute-forcing access to network shares to laterally move across a network.
* What are supply chain attacks? By how much did they increase in 2018?  
  Attackers hunt for unsecure network protocols, unprotected server infrastructures, and unsafe coding practices. They break in, change source codes, and hide malware in build and update processes. Because software is built and released by trusted vendors, these apps and updates are signed and certified. In software supply chain attacks, vendors are likely unaware that their apps or updates are infected with malicious code when they’re released to the public. The malicious code then runs with the same trust and permissions as the app.

78% increase in 2018

* What challenge do supply chain attacks and living off the land attacks highlight for organizations?   
  The attacks increasingly arrived through trusted channels, using fileless attack methods or legitimate tools for malicious purposes.
* 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.
* How many individuals or organizations were indicted for cyber criminal activities in 2018? What are some of the countries that these entities were from?   
  Forty-nine individuals or organizations.
* When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?   
  Poor configuration
* What is the implication for successful cloud exploitation that 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.
* What are two examples of the above cloud attack?   
  Speculative Store Bypass and Foreshadow, or L1 Terminal Fault
* 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.
* What is the Mirai worm and what does it do?   
  Denial of service (DDoS) worm
* 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.
* 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.
* What type of attack targeted the Democratic National Committee in 2019?   
  It was targeted by an unsuccessful spear-phishing attack.
* What were 48% of malicious email attachments in 2018?

Office Files

* What were the top two malicious email themes in 2018?   
  Bill and Email Delivery Failure
* What was the top malicious email attachment type in 2018?   
  .doc, .dot
* Which country had the highest email phishing rate? Which country had the lowest email phishing rate?  
  Poland and Saudi Arabia respectively.
* What is Emotet and how much did it jump in 2018?   
  The Emotet banking [Trojan](https://www.malwarebytes.com/trojan/) was first identified by security researchers in 2014. Emotet was originally designed as a banking [malware](https://www.malwarebytes.com/malware/) that attempted to sneak onto your computer and steal sensitive and private information. Later versions of the software saw the addition of spamming and malware delivery services—including other banking Trojans. Emotet uses functionality that helps the software evade detection by some anti-malware products. Emotet uses [worm-like capabilities](https://blog.malwarebytes.com/detections/worm/) to help spread to other connected computers.
* What was the top malware threat of the year? How many of those attacks were blocked?Heur.AdvML.C – 43,999,373 attacks blocked
* Malware primarily attacks which type of operating system?   
  Windows
* What was the top coinminer of 2018 and how many of those attacks were blocked?   
  JS.Webcoinminer – 2,768,721
* What were the top three financial Trojans of 2018?   
  Ramnit, Zbot, Emotet
* What was the most common avenue of attack in 2018?   
  Spear-phishing emails
* What is destructive malware? By what percent did these attacks increase in 2018?   
  Malware which can “brick,” or wipe a device at the attackers’ command. Up 25%
* What was the top user name used in IoT attacks?   
  Root
* What was the top password used in IoT attacks?   
  123456
* What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?   
  Telnet, http, https. 23,80
* In the underground economy, how much can someone get for the following?
* Stolen or fake identity: $0.10–1.50
* Stolen medical records: $15–20
* Hacker for hire: $100+
* Single credit card with full details: $1–45
* 500 social media followers: $2–6