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?** 
   * The use of malicious JavaScript code to steal credit card information
2. **How many websites are compromised each month with formjacking code?** 
   * 4818 each month in 2018
3. **What is Powershell?**
   * PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and the associated scripting language.

* **What was the annual percentage increase in malicious Powershell scripts?**  
   - 1,000 percent increase in malicious PowerShell scripts blocked in 2018 on the endpoint.

1. **What is a coinminer?**

* A coinminer is software/hardware used to “mine” or generate cryptocurrencies like Bitcoin or Doge for example

1. **How much can data from a single credit card can be sold for?**

* With data from a single credit card being sold for up to $45 on underground markets, just 10 credit cards stolen from compromised websites could result in a yield of up to $2.2 million for cyber criminals each month.

1. **How did Magecart successfully attack Ticketmaster?**

* Magecart in many cases targeting third-party services in order to get its code onto targeted websites. In the high-profile breach of Ticketmaster, for example, 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.

1. **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

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

* It dropped by 52%

1. **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.

1. **How does an exploit kit work?**

**Step 1: Contact**

The attacker often use spammed email and social engineering lures to make people click the link of an exploit kit server. In another form, a user clicks on a malicious advertisement (malvertisement) found in a legitimate website.

**Step 2: Redirect**

The exploit kit generator screens for its target and then filters out victims who don’t meet certain requirements. For example, an exploit kit operator can target a specific country by filtering client IP address by geolocation.

**Step 3: Exploit**

The victims are then directed into the exploit kit’s landing page. The landing page determines which vulnerabilities should be used in the ensuing attack.

**Step 4: Infect**

After successfully exploiting a vulnerability, the attacker can now download and execute malware in the victim’s environment.

1. **What does the criminal group SamSam specialize in?**

* "The SamSam group's modus operandi is to gain access to an organization's network, spend time performing reconnaissance by mapping out the network, before encrypting as many computers as possible and presenting the organization with a single ransom demand,"

1. **How many SamSam attacks did Symantec find evidence of in 2018?**

* 67 different organizations in 2018

1. **Even though ransomware attacks declined in 2017-2018, what was one dramatic change that occurred?**

* 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
* **In 2018, what was the primary ransomware distribution method?**  
  During 2018, the chief ransomware distribution method was email campaigns.

1. **What operating systems do most types of ransomware attacks still target?**

* Windows-based computers

1. **What are “living off the land” attacks? What is the advantage to hackers?**Living off the land attacks is a method where hackers use your own computer tools against you. The advantage is that no new downloads are required, it is stealthy, and most anti-virus software do not recognize the attack.

1. **What is an example of a tool that’s used in “living off the land” attacks?**

examples of “tools” are things already on your computer like Windows Registry, Windows Management Instrument, and can hide in folders already on your computer.

**19. What are zero-day exploits?**

* Zero-Day Exploits Defined "Zero-day" is a loose term for a recently discovered vulnerability or exploit for a vulnerability that hackers can use to attack systems. These threats are incredibly dangerous because only the attacker is aware of their existence.

**20. By what percentage did zero-day exploits decline in 2018?**

* dropped by 4% in 2018 from 27% to 23%.

1. **What are two techniques that worms such as Emotet and Qakbot use?**  
     
   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.

1. **What are supply chain attacks? By how much did they increase in 2018?**

* Supply chain attacks, which exploit third-party services and software to compromise a final target, take many forms, including hijacking software updates and injecting malicious code into legitimate software. These attacks increased by 78% in 2018.

1. **What challenge do supply chain attacks and living off the land attacks highlight for organizations?**

* 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.

1. **The 20 most active groups tracked by Symantec targeted an average of how many organizations between 2016 and 2018?**

* The 20 most active groups tracked by Symantec targeted an average of 55 organizations

1. **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 were indicted during 2018. Some of the countries with these indictments were from Russia, China, Iran, and North Korea.

1. **When it comes to the increased number of cloud cybersecurity attacks, what is the common theme?**

* Poorly secured cloud databases/poor configuration continued to be a common theme for organizations.

1. **What is the implication for successful cloud exploitation that provides access to memory locations that are normally forbidden?**

* A more insidious threat to the cloud emerged in 2018 with the revelation of several vulnerabilities in hardware chips. Meltdown and Spectre exploit vulnerabilities in a process known as speculative execution. Successful exploitation 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.

1. **What are two examples of the above cloud attack?**

* Meltdown and Spectre exploit vulnerabilities in a process known as speculative execution.

1. **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.

1. **What is the Mirai worm and what does it do?**

* Mirai is a piece of software that is used to form a malicious botnet; a large number of connected devices (bots) that can be controlled to attack others on the Internet. This is done without the owner’s consent. Generally, these attacks take the form of Distributed Denial of Service (DDoS) attacks.

1. **Why was Mirai the third most common IoT threat in 2018?**

* The Mirai threat is the third most popular threat because it can be introduced via internet routers. They’re also attractive as they provide an effective jumping-off point for attackers.

1. **What was unique about VPNFilter with regards to IoT threats?**

* The VPNFilter was unique because of its ability to survive a reboot making it very difficult to remove.  
  It also includes a destructive capability which can “brick,” or wipe a device at the attackers’ command, should they wish to destroy evidence.

1. **What type of attack targeted the Democratic National Committee in 2019?**

* A spear phishing attack

1. **What were 48% of malicious email attachments in 2018?**

* 48% of malicious email attachments were Office Files

1. **What were the top two malicious email themes in 2018?**

* The top two malicious email themes in 2018 were “Bill” and “Email Delivery Failure”

1. **What was the top malicious email attachment type in 2018?**

* The top malicious email attachment type was: “.doc, .dot”

1. **Which country had the highest email phishing rate? Which country had the lowest email phishing rate?**

* The highest was: Saudi Arabia
* The lowest was: Belgium

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

* Emotet is a Trojan that is primarily spread through spam emails accounting for 16 percent of financial Trojans, up from 4 percent in 2017.

1. **What was the top malware threat of the year? How many of those attacks were blocked?**

* The top malware threat of the year was Heur.AdvML.C and it was blocked 43,999,373 times.

1. **Malware primarily attacks which type of operating system?**

* Windows

1. **What was the top coinminer of 2018 and how many of those attacks were blocked?**

* The top coinminer of 2018 was JS.Webcoinminer and was blocked 2,768,721 times

1. **What were the top three financial Trojans of 2018?**

* The top three financial trojans were: Ramnit, Zbot, Emotet

1. **What was the most common avenue of attack in 2018?**

* Spear-phishing emails remained the most popular avenue for attack and were used by 65 percent of all known groups

1. **What is destructive malware? By what percent did these attacks increase in 2018?**

* Most destructive malware variants cause destruction through the deletion, or wiping, of ﬁles that are critical to the operating system’s ability to run. It increased by 6%.

1. **What was the top user name used in IoT attacks?**

* The top user name used in IoT attacks was: Root

1. **What was the top password used in IoT attacks?**

* the top password used in IoT attacks was: 123456

1. **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 in IoT attacks were: telnet, , http, and https  
  the top two ports used in IoT attacks were: Telnet and World Wide Web HTTP

1. **In the underground economy, how much can someone get for the following?**

1. Stolen or fake identity: **$.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**