Security 101 Homework-Shea Padilla

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?**

   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.

   Once a website user enters their payment card data on an e-commerce payment page and clicks “submit,” the malicious JavaScript code is what collects the entered information. The malicious JavaScript code that has been installed by the cyberthieves can collect information such as payment card details, home and business addresses, phone numbers and more. Once the information has been collected, it is then transferred to the attacker’s servers. The cyberthieves can then use this information for financial gain themselves, or they can sell the information on the dark web. With this information, cybercriminals can then use the data for identity theft or payment card fraud.

2. **How many websites are compromised each month with formjacking code?**

   There are an average of 4,800 websites compromised by Formjacking each month.

3. **What is Powershell?**

   Powershell is a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting language. Unlike most shells, which accept and return text, PoweShell is built on top of .NET Common Language Runtime (CLR), and accepts and returns .NET objects. This fundamental change brings entirely new tools and methods for automation.

   PowerShell Script is Really nothing more than a simple text file. The file contains a series of PowerShell commands, with each command appearing on a separate line. For the text file to be treated as a PowerShell script, its filename needs to use the . PS1 extension.

4. **What was the annual percentage increase in malicious Powershell scripts?**

There was a 100% increase in malicious PowerShell scripts.

5. What is a coinminer?

Coinminers (also called cryptocurrency miners) are programs that generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity. When intentionally run for one's own benefit, they may prove a valuable source of income.

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

Data from a single credit card can be sold for up to $45 in the underground market and just 10 credit cards stolen from compromised websites could result in a yield of up to $2.2 million for cyber criminals each month. Therefore, the appeal of formjacking for cyber criminals is clear.

7. How did Magecart successfully attack Ticketmaster?

Magecart compromised a third-party chatbot, which loaded malicious code into the web browser of visitors to Ticketmaster’s website, with the aim of harvesting customers' payment data.

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

The growth of 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 card details on the cyber underground are probably more assured than the value of cryptocurrencies in the current climate.

Just like any worker, hackers and cybercriminals look for the most efficient way to do their jobs. That's one of the reasons for the recent increase in formjacking, in which credit card data and other personal information is stolen via illicit JavaScript from the forms on e-commerce sites.

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

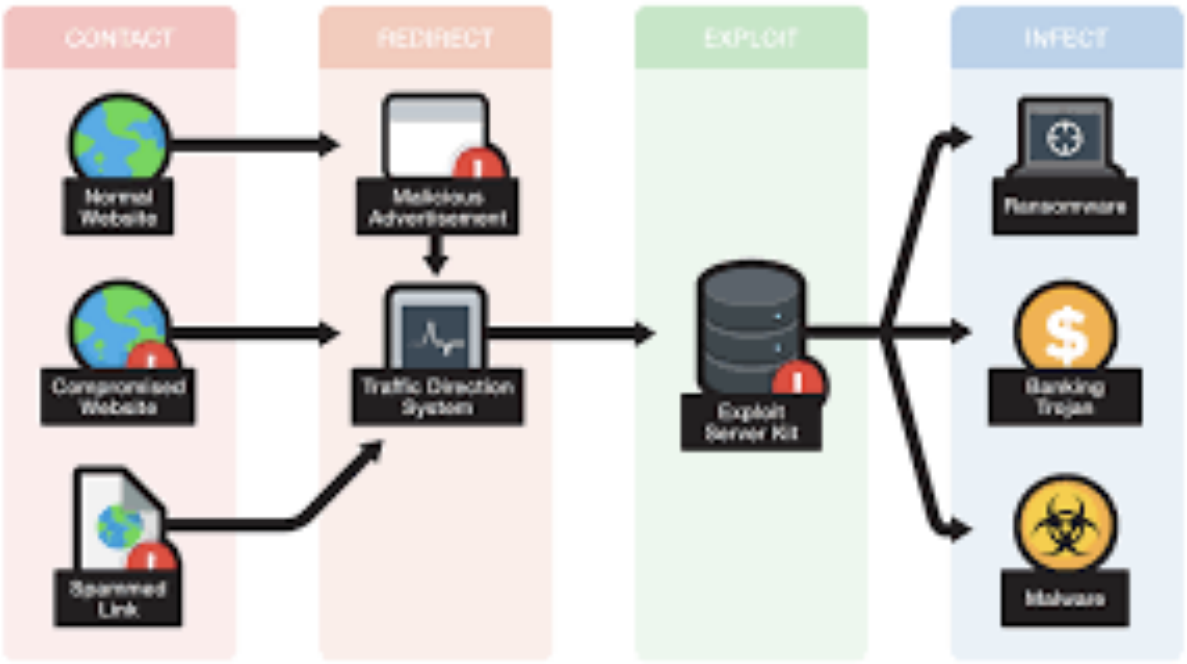
Cryptojacking activity declined by 52% between January and December of 2018.

10. If a web page contains a coinmining script, what happens?

Cybercriminals have taken advantage of cryptocurrency mining in order to make a profit and they generally use malware or potentially unwanted applications they install on the victim's machine in order to turn a dishonest penny. With coinmining it is performed directly within the browser when the user browses to certain websites. Thus, there is no need to infect the victim's machine or to exploit vulnerabilities. All that is needed is a browser with JavaScript activated, which is the default state of most browsers.

11. How does an exploit kit work?

An exploit is a program or piece of code that finds and takes advantage of a security flaw in an application or system so that cybercriminals can use it for their benefit. An exploit kit doesn't infect your computer; but it opens the door to let the malware in. The exploit kit then gathers information on a victim's machine, finds vulnerabilities and determines the appropriate exploit, and delivers the exploit, which typically silently drive-by downloads and executes malware, and further running post-exploitation modules to maintain further remote access to the compromised system.



12. What does the criminal group SamSam specialize in?

SamSam specializes in targeted ransomware attacks, breaking into networks and encrypting multiple computers across an organization before issuing a high-value ransom demand. The group is believed to be behind the attack on the city of Atlanta in March, which saw numerous municipal computers encrypted.

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

In 2018 there was evidence of 67 SamSam attacks, mostly against organizations in the U.S.

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

Overall there was a decrease in ransomware infractions, however, enterprise infections went up by 12% in 2018. The shift in victim decline was most likely due to exploit kit activity which was previously an important channel for ranswome delivery. Also contributing to the decline is the fact that some cybercrime gangs were losing interest in ransomware and moved to delivering other malware such as banking Trojans and information stealers.

15. In 2018, what was the primary ransomware distribution method?

Email campaigns that used spear phishing and other **methods** to ensnare victims became the **primary method** of **distributing ransomware in 2018**, according to Symantec's ISTR. Instead, Symantec is turning to technologies such as behavioral analysis and machine learning to block **ransomware** earlier in the infection **process**.

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

Eighty-five percent of managed service providers (MSPs) say the Windows OS is targeted most frequently by ransomware attacks. The reason? Windows-based computers are typically more affordable, therefore more people use them.

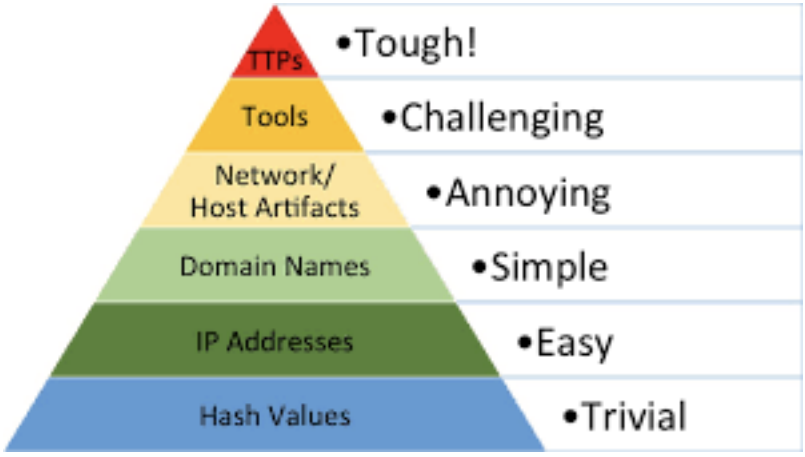
17. What are “living off the land” attacks? What is the advantage to hackers?

In the technology world, LotL refers to attacker behavior that uses tools or features that already exist in the target environment. There are several advantages to hackers including:

- Fly Under the Radar/Avoid Detection

Attackers may choose to fly under the radar of either prevention or detection technologies. Typically, prevention technologies will use a signature-based approach to detect and quarantine malicious processes. They may also use hash values or other indicators of comprise (IOCs) to detect a process.

- While attackers can change (indicators of compromise) IOCs relatively easily (see The Pyramid of Pain), using pre-existing software avoids the process being flagged as suspicious. It also saves the attacker cycles in developing the binary to deliver an attack.
- The Pyramid of Pain
    - The pyramid of pain represents the difficulty level for attackers to change indicators that a defender might use to detect their activity.



- Use Power Tools Already Embedded in Operating Systems
    - Operating systems typically carry tooling for automation and scripting administrative activities. Windows PowerShell is a good example. Every Windows OS since November 2006 includes PowerShell. This makes it a pervasive tool in a typical enterprise environment. These tools will typically provide easy access to both local and domain-based configuration. For example, with PowerShell, you can configure anything from Active Directory objects to local raw disks.

18. **What is an example of a tool that's used in "living off the land" attacks?**

Typically, an attacker will scope out a target, but he or she may not know the entire environment the tools operate in. This creates some hurdles for building, compiling, and testing program. These tools should allow for a variety of operating systems and environments, and it may be difficult, if not impossible, to test for every possible scenario.

Attackers that use already existing tooling avoid the need to build, test, and QA tools. They don't have to worry about compatibility, dependencies, and so forth. It's also challenging to build programs that are stealthy enough to avoid detection, particularly if something runs at kernel level. Ultimately, it's probably cheaper and quicker to use existing tooling.

From an attacker's perspective, using already existing tools and features makes the defender's job inherently more difficult. Picking out the malicious use of built-in tools versus the authorized use of tools by the system administrator can be somewhat like looking for a needle in a haystack.

One of the interesting things with combating LotL attacks is that you can begin to see the tactics, techniques, and procedures (TTPs) that a particular attacker uses. Once you can detect TTPs, it becomes a bigger challenge for the attacker to change, rather than just changing a hash value to avoid detection.

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

A zero-day vulnerability, at its core, is a flaw. It is an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong. In fact, a zero-day exploit leaves NO opportunity for detection ... at first.

A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability—hence "zero-day." Let's break down the steps of the window of vulnerability:

- A company's developers create software, but unbeknownst to them it contains a vulnerability.
- The threat actor spots that vulnerability either before the developer does or acts on it before the developer has a chance to fix it.
- The attacker writes and implements exploit code while the vulnerability is still open and available
- After releasing the exploit, either the public recognizes it in the form of identity or information theft or the developer catches it and creates a patch to staunch the cyber-bleeding.

Once a patch is written and used, the exploit is no longer called a zero-day exploit. These attacks are rarely discovered right away. In fact, it often takes not just days but months and sometimes years before a developer learns of the vulnerability that led to an attack.

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

In 2018 there was a 23% decline in zero-day exploits/vulnerabilities.

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

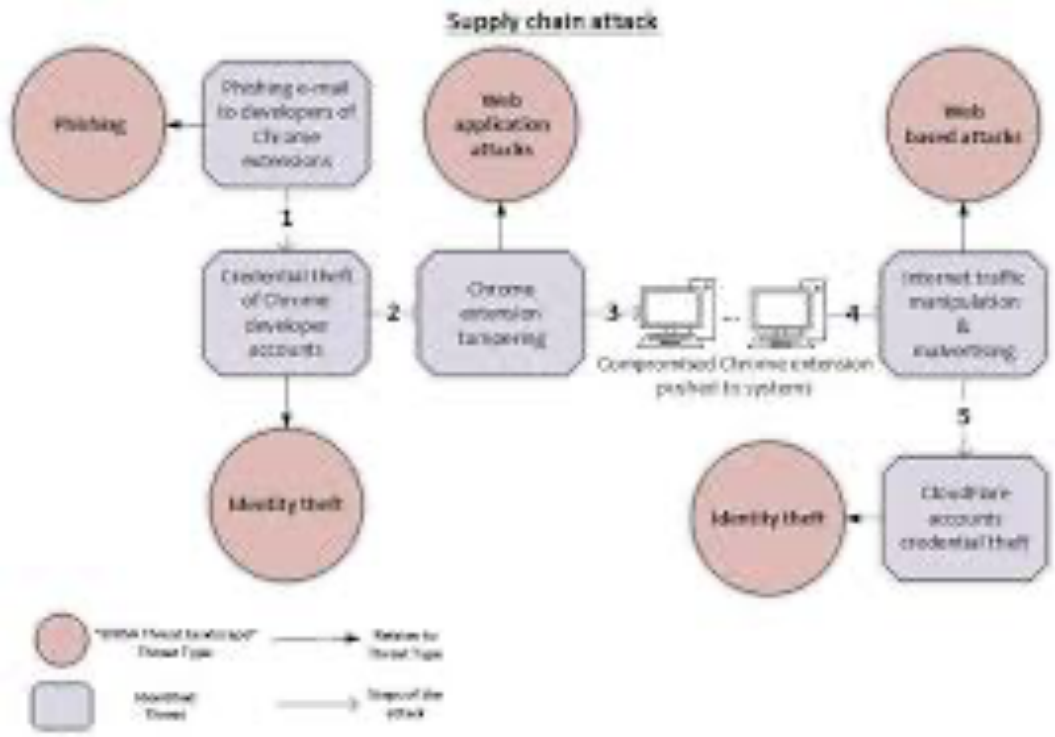
Emotet and Qakbot are use simple techniques including dumping passwords from memory or brute-forcing access to network shares to laterally move across a network.

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

Supply chain attacks increased by 78% in 2018.

A supply chain attack is a cyber-attack that seeks to damage an organization by targeting less-secure elements in the supply network. A supply chain attack can occur in any industry, from the financial sector, oil industry or government sector. (Exploit third party services/libraries)

Supply chain attacks may involve different types of cyber-threats. The figure below uses the security incident of the compromised Chrome extensions as a use-case and presents the steps involved in the attack. This supply chain attack involves threat types that have been described in ENISA's Threat Landscape (Phishing, Identity Theft, Web application attacks, Web based attacks).



Identifying the cyber-threats involved in this supply chain attack. The Landscape for more security recommendations. Indicative recommendations for the compromised Chrome extensions chain supply attack, are the following:

- **Phishing.** End-users should use two-factor authentication whenever possible. Companies should raise awareness regarding elaborate phishing campaigns through proper training.
- **Identity Theft.** Users should use long, complex, unique and secure passwords as well as two-factor authentication whenever possible.
- **Web application attacks.** Disable software, e.g. browser extensions, that is not actively used or needed.
- **Web based attacks.** Keep the operating system and installed software updated as soon as new updates are available.

23. **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. While they block on average 115,000 malicious PowerShell scripts each month, this only accounts for less than 1 percent of overall PowerShell usage. Effectively identifying and blocking these attacks requires the use of advanced detection methods such as analytics and machine learning.

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

Between 2016 and 2018 there was an average of 55 organizations targeted per each of the 20 groups for a total of around 1,100 organizations.

25. How many individuals or organizations were indicted for cyber criminal activities in 2018? What are some of the countries that these entities were from?

There were 49 individuals or organizations that were indicted during 2018 for cyber criminals. There were Russian Nationals, 19 Chinese Nationals/Organizations, along with 11 Iranians and 1 North Korean.

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

It seems that poorly secured cloud databases continue to be a weak point for organizations when dealing with Cybersecurity attacks in the cloud.

27. **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 elevation of several vulnerabilities in hardware chips. 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.

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

Meltdown and Spectre aren't two examples of the above cloud attack and they weren't isolated cases. Several variants of these attacks were subsequently released into the public domain throughout 2018 They were also followed up by similar chip-level vulnerabilities such as Speculative Store Bypass and Foreshadow, or L1 Terminal Fault. This is likely just the start, as researchers and attackers home in on vulnerabilities at the chip level and indicates that there are challenging times ahead for the cloud.

29. **Regarding Internet of Things (IoT) attacks, what were the two most common infected devices and what percentage of IoT attacks were attributed to them?**

While worms and bots continued to account for the vast majority of IoT attacks in 2018, a new breed of threat emerged as targeted attack actors displayed an interest in IoT as an infection vector.

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

The notorious Mirai took advantage of insecure IoT devices in a simple but cleaver way. It scanned big blocks of the internet for open Telnet ports, then attempted to log in default passwords. In this way it was able to amass a botnet army.

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

Mirai distributed denial of service (DDoS) worm remained an active threat and with 16% of the attacks. It is constantly evolving and variants use up to increase the success rate for infection, as devices often remain unpatched.

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

It was an evolution of IoT threats and were the first widespread persistent IoT threat with the ability to survive a reboot making it very difficult to remove. The VPNFilter was a departure from traditional IoT threat activity such as DDoS and coin mining. It also includes destructive capability which can “brick” or wipe a device at the attackers command, should they wish to destroy evidence. VPNFilters are the work for a skilled and well-resourced threat actor and demonstrates how IoT devices are now facing attacks from many fronts.

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

Malicious emails, also known as Phishing, was the attack used on the DNC in 2019.

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

The 48% of malicious email attachments in 2018 were office files.

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

The top two malicious email themes in 2018 were bills at 15.7% and then email delivery failure at 13.3%

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

The top malicious email attachment type of 2018 was a .doc, .dot which was at 37%.

37. Which country had the highest email phishing rate? Which country had the lowest email phishing rate?

The lowest email phishing rate was Saudi Arabia at 675 and then the country with the highest rate was Poland at 9,653.

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

In 2018 Emotet continued to aggressively expand its market share and accounted for 16% of financial Trojans, up from 4% in 2017.

Emotet is a Trojan that is primarily spread through spam emails. The infection may arrive either via malicious script, macro-enabled document files, or malicious link. Emotet emails may contain familiar branding designed to look like a legitimate email. Emotet may try to persuade users to click the malicious files by using tempting language about “Your Invoice,” “Payment Details,” or possibly an upcoming shipment from well-known parcel companies.

Emotet has gone through a few iterations. Early versions arrived as a malicious JavaScript file. Later versions evolved to use macro-enabled documents to retrieve the virus payload from command and control (C&C) servers run by the attackers.

Emotet uses a number of tricks to try and prevent detection and analysis. Notably, Emotet knows if it’s running inside a virtual machine (VM) and will lay dormant if it detects a sandbox environment, which is a tool cybersecurity researchers use to observe malware within a safe, controlled space.

Emotet also uses C&C servers to receive updates. This works in the same way as the operating system updates on your PC and can happen seamlessly and without any outward signs. This allows the attackers to install updated versions of the software, install additional malware such as other banking Trojans, or to act as a dumping ground for stolen information such as financial credentials, usernames and passwords, and email addresses.

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

The top malware threats in 2018 were banking trojans and Emotet was the most pervasive threat. There were 69 million cryptojacking events that were blocked in 2018, which was 4x as many events that were blocked in 2017.

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

Windows continue to be the Operating System of choice for Malware user attacks.

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

JS.Web was the top Coinminer of 2018 with 2,768,721 being blocked.

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

Emotet, LokiBot and TrickBot were the top three financial Trojans for 2018.

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

Spear-phishing emails reamined the most popular avenue for attack and were used by 65%of all known groups in 2018.

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

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.

These attacks increased by 25% in 2018.

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

The top user name used in IoT attacks was “root” at 38.1%.

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

The top password used in IoT attacks was 123456 at 24.6%.

47. **What were the top three protocols used in IoT attacks? What were the top two ports used in IoT attacks?**

The top three protocols utilized in IoT attacks were:

1. Telnet @ 90.9%
2. Http @ 6.6%
3. Https @ 1.0

The top two ports utilized in IoT attacks were:

1. 23 Telenet @ 85%
2. 80 World Wide Web HTTP @ 6.5%

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

1. **Stolen or fake identity:**
    1. $.10-1.50

b. Stolen medical records:

1. $.10-35

c. Hacker for hire:

1. $100 +

d. Single credit card with full details:

1. $.50-20

e. 500 social media followers:

1. $2-6

Cybersecurity Threat Landscape (Part 2 - Akamai)

In this part, you should primarily use the *Akamai_Security_Year_in_Review_2019* and *Akamai State of the Internet/ Security* plus independent research to answer the below questions.

---

1. **DDOS attack events from January 2019 to September 2019 largely targeted which industry?**

   The Gaming Industry was largely targeted from January-September 2019 with DDoS attacks.

2. **Almost 50% of unique targets for DDoS attacks from January 2019-September 2019 largely targeted which industry?**

   The Financial Services Industry was largely targeted from January-September 2019 with Unique Targets.

3. **Which companies are the top phishing targets, according to Akamai?**

   The top companies for phishing are:

   - DHL
   - DocuSign
   - Dropbox
   - LinkedIn
   - Microsoft
   - PayPal

4. **What is credential stuffing?**

   Credential stuffing is a type of cyberattack where stolen account credentials typically consisting of lists of usernames and/or email addresses and the corresponding passwords are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application.

5. **Which country is the number one source of credential abuse attacks? Which country is number 2?**

The United States with 25,393,327,336 malicious logins is the Number one source and then the second is Russia at 6,114,186,048 malicious logins.

6. **Which country is the number one source of web application attacks? Which country is number 2?**

The United States with 1,434,231,212 application attacks is the Number one source and then the second is Russia 1,093,219,355 application attacks.

7. In Akamai's State of the Internet report, it refers to a possible DDoS team that the company thought was affecting a customer in Asia (starts on page 11).

- Describe what was happening.
  - There was abnormal traffic that was being monitored that at its peak almost overflowed the database Akamai utilized to log that type of activity, The traffic was initially flagged by another department that they felt need to be investigated by the SOCC. Because it was detected by another department and not by normal channels they felt something was seriously wrong.

    When SOCC started researching the issue they did notice a large amount of HTTP requests going to customer's URL's; which lead to the assumption there was an attack happening. There were initially 4 billion request that almost crashed the logging system.

- What did the team believe the source of the attack was?

  Initially the SIRT team had examined the traffic to the URL a few days prior the the incident and had noticed something interesting. Initial analysis had shown than half of the IPs wer flagged by Akamai as NAT gateways. Additional packet and header analysis confirmed the traffic in question was generated by a windows COM Object (WinhttpRequest).

  Over 28 hours, the SOCC migrated more than 4 billion requests from 15,582 IP addresses. It was determined that the base platform used by the customer mitigated 98% of the problematic traffic without intervention, all thanks to rate controls alone.

- What did the team actually discover?

The earlier analysis, which was supported by the SIRT team, concluded that the high volume of traffic hammering the customer's URL was the result of a warranty tool gone haywire. Once the SOCC started filtering traffic, the warranty took kept visiting the URL. However the subsequent visits didn't alter anything in the headers that could've assisted in bypassing mitigations, proving that this incident wasn't a malicious attack. This conclusion was later confirmed by the customer as well as the vendor responsible for the tool. A fix was pushed within hours to all of the affected systems.

8. **What is an example of a performance issue with bot traffic?**

Two examples of performance issues with bot traffic would be slow websites and frustrated customers.

9. **Known-good bots are bots that perform useful or helpful tasks, and not do anything malicious to sites or servers. What are the main categories of known-good bots.**

Categories of known-good bots:

- SEARCH ENGINE CRAWLERS – web search engines operate for a wide variety of purposes, going from global search engines (e.g., Google, Bing) to more targeted ones such as job search engines, media and entertainment, commerce-focused search engines, or academic and research (publications, citation search, semantic analysis).

- WEB ARCHIVES – scanning the web periodically and recording its content to searchable indexed databases.

- SEARCH ENGINE OPTIMIZATION, AUDIENCE ANALYTICS, AND MARKETING SERVICE – scraping websites and social media for content that might provide customers with market insights such as positioning, mentions, and other references.

- SITE MONITORING SERVICES – automated tools that monitor a site's health, availability, and performance under load.

- CONTENT AGGREGATORS – bots operated in this category would scan multiple sources on the web such as news, trends, product updates, price changes, stock quotes, etc.

10. What are two evasion techniques that malicious bots use?

To avoid detection, the bots visiting your website will employ various tricks and tactics. The most basic evasion technique is altering the User Agent, or other HTTP header values, allowing the bot to impersonate widely used browsers, mobile applications, or even known-good bots.

Bots will also change the IP addresses used in order to mask their origin, or use multiple IP addresses. The IP address change-out is also used to bypass rate limitations, as the bot will use a “low and slow” method where multiple IP addresses send a low number of requests each hour.

Other rate limitation evasion methods include using mobile and API endpoints, as well as morphing IP addresses via proxies, VPNs, and Tor.

Some bots will tamper with browser properties, spoofing known fingerprint characteristics that are often whitelisted. Bots may also do cookie tampering in the hopes of evading detection, such as dropping cookies, or harvesting good cookies and playing them back.

Cybersecurity Threat Landscape (Part 3 - Verizon)

In this part, you should primarily use the *Verizon Data Breaches Investigation Report* plus independent research to answer the below questions.

---

1. **What is the difference between an incident and a breach?**

   Incident

   > A security event that compromises the integrity, confidentiality or availability of an information asset.

   Breach

   > An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.

2. **What percentage of breaches were perpetrated by outside actors? What percentage were perpetrated by internal actors?**

   > Breaches perpetrated at Verizon by outside actors accounted for 69% and then 34% were done by internal actors.

3. **What percentage of breaches were perpetrated by organized criminal groups?**

   > Criminal groups accounted for 39% of the breaches at Verizon in this report.

4. **What percentage of breaches were financially motivated?**

Verizon stated that 71% of the breaches were financially motivated.

5. **Define the following**:

Denial of Service:
A distributed denial-of-service (**DDoS**) attack is a malicious attempt to disrupt normal traffic to a web property.

Any attack intended to compromise the availability of networks and systems. This includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service.

Command and Control:

A **command-and-control** [C&C or C2] server is a computer controlled by an attacker or cybercriminal which is used to send **commands** to systems compromised by **malware** and receive stolen data from a target network. It can be used to disseminate **commands** that can steal data, spread **malware**, disrupt web services, and more.They are typically found in both security incidents and breaches.

Backdoor:

A malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.They are typically found in both security incidents and breaches.

Keylogger:

Type of monitoring software designed to record keystrokes made by a user. One of the oldest forms of cyber threat, these keystroke loggers record the information you type into a website or application and send back to a third party. Criminals use keyloggers to steal personal or financial information such as banking details, which they can then sell or use for profit. However, they also have legitimate uses within businesses to troubleshoot, improve user experience, or monitor employees. Law enforcement and intelligence agencies also use keylogging for surveillance purposes.

6. **The time from an attacker's first action to the initial compromise of an asset is typically measured in which one? Seconds, minutes, hours, days?**

The initial compromise of an assessed is typically measured in minutes.

7. **When it comes to phishing, which industry has the highest click rates?**

The Education Industry typically has the highest click rates at 4.93%.