**Cybersecurity Threat Landscape (Part II - Report Analysis)**

Answer the below questions using the reports provided. You may have to do some independent scouring to find the answers to each question.

**Group Member Names:**

*Source: Symantec Internet Security Threat Report Volume 24 - February 2019*

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 1 | The 2018 Year In Review portion of the report highlights eight key themes. Describe each of them. |  |
| 2 | What if Formjacking and how was it introduced and used in the breach of TicketMaster |  |
| 3 | The Executive Summary starts out: "Like flies to honey, miscreants swarm to the latest exploits that promise quick bucks with minimal effort. Ransomware and cryptojacking had their day; now it's formjacking's turn."  You work in a large enterprise and your boss reads this and says we no longer have to worry about Ransomware. Using the full report, explain why that statement is in error and clarify the current trends. |  |
| 4 | What is Emotet? Provide details of how much it is used and what makes it so dangerous. |  |

|  |  |  |
| --- | --- | --- |
| 5 | When it comes to targeted attacks, what is the number one infection vector? What is the number two infection vector? How do each of these work? |  |
| 6 | What is the main purpose of these targeted attacks? |  |
| 7 | What percentage of Android users are on the newest major version?  What percentage of iOS devices are on the newest major version?  Why is there a discrepancy?  What are the security implications of this and what choices might it make for an enterprise environment? |  |
| 8 | What IoT device has increased in being compromised in 2018 detail that changes. |  |
| 9 | What are the top three usernames and passwords used on IoT devices? |  |
| 10 | What is the top attack vector for IoT devices? |  |
| 11 | Seeing the trend, postulate what the trend will be for 2019 and what type of IoT devices may become more prominent? |  |

|  |  |  |
| --- | --- | --- |
| 12 | What type of email attachment represents nearly half on the malicious attachments and how has that changed since 2017? |  |
| 13 | What are the top three industries effected by malicious emails? |  |
| 14 | Are users in small or larger organizations more likely to be targeted, explain the numbers? |  |

Source: *Akamai – State of the Internet / Security Volume 5, Special Media Edition*

*Credential Stuffing: Attacks and Economics*

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 15 | What is credential stuffing? What are other names this is known by? |  |
| 16 | According to the report, what industries are being targeted and why? |  |
| 17 | How many of these attacks have been detected and what were the peaks during 2018? |  |
| 18 | Where were the 620 million passwords/usernames referenced in the report obtained from? |  |
| 19 | What is an AIO? What is one of the AIO referenced in the report and how much does it cost? |  |
| 20 | What is the cost to purchase a compromised account? What if those credentials no longer work? What does that imply about the seller? |  |
| 21 | What are some of the challenges in mitigating the ATO risk? |  |

Source: *Akamai – State of the Internet / Security Volume 5, Issue 1*

*DDoS and Application Attacks*

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 22 | The report has a guest author article on Mental Health, why is this relevent? |  |
| 23 | What situations at work as a Cyber Security Professional might effect your mental health? |  |
| 24 | Name six common signs of potential mental health issues. |  |
| 25 | Akamai's research discoved a vulnerability in jQuery. Does this effect all jQuery, explain? |  |
| 26 | Why when Akamai found 875,000 requests per second assumed to be a DDOS attack? |  |
| 27 | Was it an attack?  What was the root cause?  Was this still a DDOS situation? |  |
| 28 | What is a BOT and are they good or bad? |  |
| 29 | What are common catagories for known bots? |  |
| 30 | Looking at the Job Description in the report, what are the key takeaways? |  |
| 31 | What are some of the methods used by bad bots to avoaid detection? |  |

Source: *Verizon* *2018 Data Breach Investigations Report (11th Edition)*

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 32 | According to the report, what is the difference between a breach and an incident? |  |
| 33 | On average what is the average time interval that takes place to compromise a breached system? What is the average time interval that it takes to discover and contain a breach? |  |
| 34 | What are the two main varieties of social attacks? Define them. |  |
| 35 | What percentage of malware is spread via email? What percentage is spread via the web at large? |  |
| 36 | What percentage of people in a given phishing campaign click it? What do the authors mean when they say: “The vampire only needs one person to let them in?” |  |
| 37 | What are the primary motivators in phishing attacks? |  |
| 38 | Provide some characteristics of ransomware |  |
| 39 | Define botnet. According to this report, what are two ways that botnet attacks can occur. |  |
| 40 | Define a DDOS attack.  What is the median length of a DDOS attack? |  |
| 41 | Who are the most common threat actors targeting the public sector? What varieties of attacks are most commonly used? |  |
| 42 | What is the top action category with regards to incidents? What is the top action category with regards to breaches? |  |
| 43 | Who are the top external actors with regards to breaches? Who are the top internal actor varieties? |  |
| 44 | What top two forms (file types) does malware typically take according to this report? |  |