**Unit 1.2 - 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 23)*

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 1 | This report highlights five key themes in 2017. Describe each of them. |  |
| 2 | What exactly is the Eternalblue exploit? Why was it so significant in 2017? |  |
| 3 | WannaCry and Petya/NotPetya: What are they? What is their significance? How did they spread? What were their implications? |  |
| 4 | On average, how much is the average ransom amount requested in a Ransomware attack? |  |
| 5 | What exactly do the authors mean when they talk about hackers: “Living off the Land?” |  |
| 6 | 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? |  |
| 7 | According to the report, Zero Day reports continue to fall out of favor. Why is this the case and what are the security implications? |  |
| 8 | 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? |  |
| 9 | In the underground economy, how much might it cost you to have someone conduct a DDoS attack for 1 hour? How much would it cost to have someone “repair” your credit score? How much would it cost to generate a fake ID? How much would it cost to mess up a person’s online presence? How much would it cost to hack a Gmail account? What are the security implications? |  |
| 10 | What is the difference between a *vulnerability* and an *attack*? Provide an example of each mentioned in this report. |  |
| 11 | What exactly was the CCleaner Incident? What was the significance? How many people were affected? How did it occur? |  |
| 12 | What does the report mean when it says: “*Attackers typically use software update supply chain attacks to infiltrate well-protected organizations?*” Provide an example. |  |
| 13 | How are DDoS attacks used in conjunction with Ransomware? |  |
| 14 | Talk about Butterfly, Dragonfly, and Turla from the Analyst stories. What made these groups interesting to the analysts? |  |
| 15 | Describe each of the three most common techniques used in lateral movement. |  |
| 16 | What was the most common username and password attempted by hackers trying to penetrate IoT devices? |  |
| 17 | At one point in the report, the authors are quoted as saying: “No need to compromise the software vendor if you own the software.” What is meant by this message? Describe the specific case referenced in this passage. |  |
| 18 | Describe how coiminer attacks typically work. What is the difference between file-based coin mining and browser-based coin mining. What are the security implications for each? |  |
| 19 | How much of an increase was there in IoT attacks between 2016 and 2017? |  |
| 20 | According to researchers, what are the three motivations for using ransomware? Describe each of them and an example named ransomware that utilized each. |  |

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

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 21 | According to the report, what is the difference between a breach and an incident? |  |
| 22 | 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? |  |
| 23 | What percentage of malware is spread via email? What percentage is spread via the web at large? What is the security and training implication of this? |  |
| 24 | 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?” |  |
| 25 | What are the primary motivators in phishing attacks? |  |
| 26 | Who are the most common threat actors targeting the public sector? What varieties of attacks are most commonly used? |  |
| 27 | The report discusses the CIA triad at one point. Which of the elements of CIA is typically affected by the final event of a breach? |  |
| 28 | What is the top action category with regards to incidents? What is the top action category with regards to breaches? |  |
| 29 | Who are the top external actors with regards to breaches? Who are the top internal actor varieties? |  |
| 30 | What form (file type) does malware typically take according this report? |  |

Source: *Akamai State of the Internet / Security Q4 2017 Report*

|  |  |  |
| --- | --- | --- |
| **#** | **Question** | **Answer** |
| 21 | In the opening passage of the report, Chris Kubeka highlights his desire to “put away the fire extinguisher,” what does he mean by this? |  |
| 22 | Which industry has consistently shouldered the brunt of DDoS attacks over the last few years? What percentage of DDoS attacks affect them? |  |
| 23 | What exactly are “reflection” based attacks? How are they different from volumetric-based DDoS attacks? |  |
| 24 | What is the Mirai botnet? How does it work? What event triggered the Mirai botnet’s extended longevity? |  |
| 25 | Why do the nations of Egypt and Brazil appear so prominently in the botnet attack report? |  |
| 26 | According to the report, what were the two most common web attacks in 2017? Why do the authors suspect that the first vector is so dominant? |  |
| 27 | According to the report, what were the two most common web attacks in 2017? Why do the authors suspect that the first vector is so dominant? |  |
| 28 | Which two industries are most subject to credential abuse attacks? What percentage of login attempts are malicious in the case of these two industries? |  |
| 29 | What are APIs and why do the authors of Akamai believe that they are subject to increased threats in 2018? |  |