**Cybersecurity Threat Landscape (Part I - Vocabulary)**

Fill in the below tables using the reports provided and independent research.

In the first table, we’ll ask you to use all the reports plus independent research to define terms. Each definition should be at least a few sentences, and you should be able to confidentially explain them to a fellow student or the class. Try to be as detailed as possible and stick to language that could be easily understood by a lay person.

In the second table, you should primarily use the *Symantec Internet Security Threat Report (Volume 23)* plus independent research to provide a definition of the terms plus their context/significance. This will be more challenging than the first one but it will help you to better read reports to identify information. Also include and define four new terms in the report that you’ve never encountered before but believe are important.

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Incident |  |
| Breach |  |
| Vulnerability |  |
| Exploit |  |
| Insider and Privilege Misuse |  |
| Payment Card Skimmers |  |
| Point of Sale Intrusions |  |
| Physical Theft and Loss |  |
| Web Application Attacks |  |
| DDOS |  |

Source: *Symantec Internet Security Threat Report (Volume 23)*

|  |  |  |
| --- | --- | --- |
| **Term** | **Definition** | **Context / Significance** |
| Coinminer Attack |  |  |
| Ransomware |  |  |
| Zero Day |  |  |
| Malware |  |  |
| “Living Off the Land” |  |  |
| Spear Phishing |  |  |
| Infection Vector |  |  |
| Trojan |  |  |
| Targeted Attack |  |  |
| Off-The-Shelf Attack Tools |  |  |
| Watering Hole Attacks |  |  |
| Lateral Movement Techniques |  |  |
| DDoS Attacks |  | . |
| DNS |  |  |
| BGP Hijacking |  |  |
| Man in the Middle Attack |  |  |
| <NEW TERM> |  |  |
| <NEW TERM> |  |  |
| <NEW TERM> |  |  |
| <NEW TERM> |  |  |