|  |  |  |
| --- | --- | --- |
| Categories | Name | Description |
| Data Breach | Compromise of organizational information systems to facilitate exfiltration of data/information | Adversary implant malware into internal information systems, where the malware gradually identifies and then exfiltrate valuable information. |
| Host Exploit | Poorly configured or unauthorized information systems exposed to the internet  Wireless jamming attacks | Adversary gains access through the internet-accessible resource unavailable to intended users or prevent the resource from functioning efficiently or at all.  Adversary takes measures to interfere with wireless communications from reaching intended recipients |
| Denial of Service | Distributed denial of service (DDoS)  Simple DoS attack  Targeted DoS attack | Adversary uses multiple compromised information systems to attack single target, hence causing denial of service for users of the targeted information system  Adversary attempts to make an Internet-accessible resource unavailable to intended users or prevent the resource from functioning efficiently or at all.  Adversary targets DoS attacks to critical information systems, components or supporting devices, based on adversary knowledge of dependencies. |
| Confidential Breach | Compromise of encryption materials  Release of Personal Identifiable information. | Adversary is able to gain access to encryption keys.  Intentional or unintentional release of Personal Information. |
| Delayed Technology refresh | Resource depletion  Unreadable display | Degraded processing performance due to resource depletion  Display is unreadable due to aging of equipment |
| Internal Threat | Robbery | The act of unlawfully taking the property of another by intimidation or violence |
| Lack of Internal Control | Incomplete data deletion in multi-tenant environment | Adversary obtains unauthorized access to information due to insecure/ uncompleted data deletion. (eg. cloud computing) |
| Physical Exploit | Cyber-physical attacks on organizational facilities | Adversary conducts a cyber-physical attack on organizational facilities |
| Category | Name | Description |
| Third Party | Pervasive disk error | Multiple disk errors due to aging of a set of devices all acquired at the same time and from the same supplier. |
| Unauthorized Backdoor | Obfuscate adversary actions | Adversary takes action to inhibit the effectiveness of intrusion detection systems or auditing capabilities within an organization. |
| Unintended Data Leak | Incorrect privilege settings | Internal users or authorized users make an error of granting privileges to a lower level user thus information can be easily leaked. |
| Vishing | Compromise or gaining access to critical or very sensitive information systems | Using voice systems as social engineering technique to break into, compromise or gain access to critical information systems . |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |