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

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

In the first 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. Also include and define four new terms in the report that you’ve never encountered before but believe are important.

In the second table, you will 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.

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

|  |  |  |
| --- | --- | --- |
| **Term** | **Definition** | **Context / Significance** |
| Coinminer Attack | Coinminer attacks are ones in which hackers use the processing power of a victim’s machine to shoulder the cost of cryptocurrency mining. These attacks are a revenue generator for hackers and rarely detected. | “The coin mining gold rush resulted in a 8,500 percent increase in detections of coinminers on endpoint computers in 2017.” |
| Ransomware | It is a type of malware, or malicious software which encrypts files on your computer or completely locks you out. It’s spread by hackers who then demand a ransom, claiming that, if you pay, you’ll receive the decryption key to recover your files. | There has been a shift in the ransomware market from 2016 to 2017. In 2017, the ransomware “market” made a correction with fewer ransomware families and lower ransom demands—signaling that ransomware has become a commodity.  Last year, the average ransom demand dropped to $522, less than half the average of the year prior. And while the number of ransomware variants increased by 46 percent, indicating the established criminal groups are still quite productive, the number of ransomware families dropped, suggesting they are innovating less and may have shifted their focus to new, higher value targets. |
| Zero Day | This is an attack that exploits zero days vulnerabilities; i.e. software vulnerabilities which were previously unknown and unpatched | Use of zero days is falling. There was a time when zero days were a valuable and powerful tool for targeted attack groups. But attackers have begun to eschew them in favor of less conspicuous tactics, namely “living off the land” |
| Malware | This is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission. | There has been a huge rise in mobile malware as well as malware injection into supply chain attacks. It also continues to be one of the most important tools used by targeted attack groups. Although many groups rely on it less than before malware is still generally used at the “pointy end” of any attack, to achieve the ultimate goal of the attack, whether it’s information stealing, spying, sabotage, or any other kind of compromise. |
| “Living Off the Land” | This is a tactic by which attackers use whatever tools are on hand, such as legitimate network administration software and operating system features. | This tactic is growing in popularity since its less conspicuous, allowing attacks to fly under the radar making them more appealing to attackers. |
| Spear Phishing | Spear phishing relies on duping the recipient into opening an attachment or following a malicious link. | Spear fishing is one of the most common infection vectors; in other words, this is how the attacker manages to get to the victim’s network in the first place. Its popularity shows how often the person sitting behind a computer can be the weakest link in an organization’s security. |
| Infection Vector | Infection vectors are the points of entry by which attackers managed to get on the victim’s network in the first place. Attackers usually attempt to compromise organizations by infecting any available computer in a targeted organiza- tion and, once inside, then move on to specific computers of interest by mapping and traversing the organization’s network. | Blocking attacks at the point of entry is the most effective way of combatting targeted attacks.  Discovering the infection vector can often be quite difficult. Groups with good operational security will often clean up as they go along, removing their tools from any computers they no longer need. That means that traces of the initial infection have often been removed by attackers by the time an attack is uncovered. |
| Trojan | This is a type of malware that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.  A Trojan acts like a bona fide application or file to trick you. It seeks to deceive you into loading and executing the malware on your device. Once installed, a Trojan can perform the action it was designed for. | There were a number of financial Trojans used specifically in the banking industry just as the Emotet banking trojan that re-emerged in 2017. |
| Targeted Attack | An attack directed at a specific target or targets as opposed to widescale indiscriminate campaigns. The work of individuals usually isn’t classed as a targeted attack.  Instead, targeted attacks are the work of organized groups. The majority of these groups are state sponsored (although there is a small number of private operators) and they’re usually driven by a small number of motivations | The motivation for a targeted attack is primarily intelligence gathering. Other motivations include disruption, sabotage, and financial gain. |
| Off-The-Shelf Attack Tools | These are existing tools that allow hackers to break into networks, steal data and overcome defenses designed to expose malware attacks. | There is an increasing use of off-the-shelf tools means attackers leave less distinctive fingerprints behind |
| Watering Hole Attacks | Watering holes are an infection vector, and are websites have been compromised by the attacker, usually without the knowledge of the website’s owner. Attackers will often compromise a website that is likely to be visited by intended targets. | This is a very common infection vector and the initial entry point for an attacker |
| Lateral Movement Techniques | This is a key phase of a targeted attack in which the attacker will find a way on to a target’s network by infecting any available computer and use those computers as a beachhead. From there, they’ll explore the network, identify targets of interest and move across the network to infect those computers. | There are many techniques used to perform lateral movement  Stolen credentials is the most common technique. Attackers often use hacking software tools to obtain credentials from a compro- mised computer and then use them to attempt to log into other computers on the network.  Another commonly used technique is exploiting open network shares |
| DDoS Attacks | This is a denial of service attack. | DDoS attacks can be a decoy for other more targeted attacks. Because admins will be busy trying to stem the DDoS attack, they may be too distracted to notice suspicious activity on their network indicating that a targeted attack is underway. |
| DNS | DNS is like the internet’s phonebook.  Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/) so browsers can load Internet resources. | In DNS hjacking, a DNS server is compromised in order to change the domain resolution to a different IP address under the attacker’s control |
| BGP Hijacking | Border Gateway Protocol (BGP) manages how packets are routed on the internet and is therefore responsible for defining the path through which a resource, such as an IP address, can be reached. Through BGP routing modification, it is possible to redirect IP addresses belonging to other entities to a new destination. | A case of BGP hijacking in December 2017 saw some of the IP addresses belonging to Microsoft and Apple, among others, rerouted through Russia. This allows attackers to intercept requests for updates from these IP addresses, and instead send down a Trojanized update. |
| Man in the Middle Attack | An attack when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, and intercepts the communication without the knowledge of the victim.  The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. | If an attacker has control over a targeted network, for example by creating a rogue Wi-Fi access point, then they can attempt to swap any requested file update using a man-in-the- middle (MitM) attack |
| <NEW TERM> |  |  |
| <NEW TERM> |  |  |
| <NEW TERM> |  |  |
| <NEW TERM> |  |  |

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Incident | An incident is a security event that compromises the integrity, confidentiality or availability of an information asset. |
| Breach | A breach is an incident that results in the confirmed disclosure— not just potential exposure—of data to an unauthorized party. |
| Vulnerability | A vulnerability is a flaw in your security. They expose your organization's assets to harm. They exist in operating systems, applications or hardware you use. How you configure software, hardware and even email or social media accounts can also create vulnerabilities. |
| Exploit | It is commonly used to describe a software program that has been developed to attack a system by taking advantage of a vulnerability. The objective of many exploits is to gain control over the system. For example, a successful exploit of a database vulnerability can provide an attacker with the means to collect or *exfiltrate* all the records from that database.  But not all exploits involve software. Scams that socially engineer an individual or employee into disclosing personal or sensitive information is one such example. |
| Insider and Privilege Misuse | All incidents tagged with the action category of Misuse—any unapproved or malicious use of organizational resources—fall within this pattern. This is mainly insider-only misuse, but outsiders (due to collusion) and partners (because they are granted privileges) show up as well. |
| Payment Card Skimmers | All incidents in which a skimming device was physically implanted (tampering) on an asset that reads magnetic stripe data from a payment card. While commonly associated with ATMs, gas pump terminals were just as likely to be targeted in this year’s dataset. |
| Point of Sale Intrusions | Remote attacks against the environments where card-present retail transactions are conducted. POS terminals and POS controllers are the targeted assets. Physical tampering of PIN entry device (PED) pads or swapping out devices is covered by Payment Card Skimmers. |
| Physical Theft and Loss | Any incident where an information asset went missing, whether through misplacement or malice. The top two assets found in Physical Theft and Loss breaches are paper documents and laptops. When recorded, the most common location of theft was at the victim’s work area, or from employee-owned vehicles. |
| Web Application Attacks | Any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms. The number of breaches in this pattern are reduced due to the filtering of botnet-related attacks on web applications using credentials stolen from customer-owned devices. Use of stolen credentials is still the top variety of hacking in breaches involving web applications, followed by SQLi. |
| DDOS | Any attack intended to compromise the availability of networks and systems. Includes both network and application attacks designed to overwhelm systems, resulting in performance degradation or interruption of service. |