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

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

In the second 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 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. 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.

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

|  |  |  |
| --- | --- | --- |
| **Term** | **Definition** | **Context / Significance** |
| Coinminer Attack | (also called cryptocurrency miners) are programs that generate Bitcoin, Monero, Ethereum, or other cryptocurrencies that are surging in popularity. When intentionally run for one's own benefit, they may prove a valuable source of income. | The past year, the fast rise in cryptocurrency values inspired many cyber criminals to shift to coin mining as an alternative revenue source. This coin mining gold rush resulted in an 8,500 percent increase in detections of coinminers on endpoint computers in 2017. Cyber criminals are using coinminers to steal computer processing power and cloud CPU usage from consumers and enterprises to mine cryptocurrency. |
| Ransomware | is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. | Ransomware profitability in 2016 led to a crowded market with overpriced ransom demands. 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 | refers to two things—a zero-day vulnerability or a zero-day exploit. Zero-day vulnerability refers to a security hole in software—such as browser software or operating system software—that is yet unknown to the software maker or to antivirus vendors. | 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” by using whatever tools are on hand, such as legitimate network administration software and operating system features. The use of zero days continues to fall out of favor. In fact, only 27 percent of the 140 targeted attack groups that Symantec tracks have been known to use zero-day vulnerabilities at any point in the past. |
| Malware | software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. Malware programs are usually poorly-programmed and can cause your computer to become unbearably slow and unstable in addition to all the other havoc they wreak. | Malware continues to be one of the most important tools used by targeted attack groups. Although many groups rely on it less than before (using hacking tools and legitimate software for network traversal for example), 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” | has traditionally meant a reliance on surviving through hunting, gathering, or subsistence farming.  Attacks that make use of tools already installed on targeted computers or attacks that run simple scripts and shellcode directly in memory. | “Living off the Land” techniques allow attacks to fly under the radar making them more appealing to attackers. It’s likely we’ll see an increase in threats self-propagating using these techniques.  The “Living off the Land” trend continues with attack groups opting for tried-and-trusted means to infiltrate target organizations. |
| Spear Phishing | the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information. | Spear phishing is the number one infection vector employed by 71 percent of organized groups in 2017. |
| Infection Vector | Vector(epidemiology), the method by which a disease spread. Vector (malware), the method by which a computer virus spread. | One of the key pieces of information to look for when investigating targeted attacks is the infection vector, namely how the attackers managed to get on the victim’s network in the first place. Discovering the infection vector can often be quite difficult. |
| Trojan | A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. | Emotet is a financial Trojan that first emerged in 2014 and, after a quiet period, reappeared to make waves in the second half of 2017. Its activity has steadily increased, particularly in the last few months of the year, with its activity increasing by 2,000 percent in the final quarter of 2017 |
| Targeted Attack | A targeted attack refers to a type of threat in which threat actors actively pursue and compromise a target entity's infrastructure while maintaining anonymity. These attackers have a certain level of expertise and have enough resources to conduct their schemes over a long-term period. | Overall targeted attack activity is up by 10 percent in 2017, motivated primarily (90 percent) by intelligence gathering. However, a not-so-insignificant 10 percent of attack groups engage in some form of disruptive activity. |
| Off-The-Shelf Attack Tools | off-the-shelf tools means attackers leave less distinctive fingerprints behind | Tying multiple incidents to the same group is getting increasingly hard because they’re getting better at covering their tracks. The increasing use of off-the-shelf tools means attackers leave less distinctive fingerprints behind.” |
| Watering Hole Attacks | Watering hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group becomes infected. | Watering holes is the second most popular infection vector, websites which have been compromised by the attacker, usually without the knowledge of the website’s owner. Watering hole attacks tend to be a blunter form of infection method. Attackers can’t be guaranteed that the intended target will visit the compromised website. |
| Lateral Movement Techniques | Network Lateral Movement, or what is more commonly referred to simply as, "Lateral Movement", refers to the technique’s cyber attackers, or "threat actors", use to progressively move through a network as they search for the key data and assets that are ultimately the target of their attack campaigns. | One of the key phases in most targeted attacks is what’s known as lateral movement. Attackers rarely luck out and manage to immediately compromise the computers they are interested in. Instead they’ll usually find a way on to a target’s network by infecting any available computer and use these computers as a beachhead. |
| DDoS Attacks | DDoS is short for Distributed Denial of Service. DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack. | DDoS attacks can knock an organization offline, meaning that its systems admins will be busy trying to stem the DDoS attack and may be too distracted to notice suspicious activity on their network indicating that a targeted attack is underway |
| DNS | Domain Name Servers (DNS) are the Internet's equivalent of a phone book. They maintain a directory of domain names and translate them to Internet Protocol (IP) addresses. This is necessary because, although domain names are easy for people to remember, computers or machines, access websites based on IP addresses. | In October 2016 attackers hijack Brazilian Bank’s entire DNS. |
| BGP Hijacking | BGP hijacking (sometimes referred to as prefix hijacking, route hijacking or IP hijacking) is the illegitimate takeover of groups of IP addresses by corrupting Internet routing tables maintained using the Border Gateway Protocol (BGP). | 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 | a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. | In September 2017, some variants of the FinFisher malware appear to have used this attack vector to compromise target computers. |
| <NEW TERM> |  |  |
| <NEW TERM> |  |  |
| <NEW TERM> |  |  |
| <NEW TERM> |  |  |

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Incident | as a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorized access or attempted access to a system or systems; in line with the Computer Misuse Act (1990). |
| Breach | an act of breaking or failing to observe a law, agreement, or code of conduct. A data breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion. |
| Vulnerability | is a cyber-security term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat. |
| Exploit | A computer exploit, or exploit, is an attack on a computer system, especially one that takes advantage of a particular vulnerability the system offers to intruders. Used as a verb, exploit refers to the act of successfully making such an attack. |
| Insider and Privilege Misuse | Breaches involving internal actors. All incidents tagged with the action category of Misuse—any unapproved or malicious use of organizational resources—fall within this pattern. |
| 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. |
| 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. |
| 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. |
| DDOS | A distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. |