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	When something abnormal happens.
Breach	When a wall is broken into.
Vulnerability	When there's a potential attack that may allow easy access.
Exploit	A tool that can take advantage of ones belongings or full control of the organization from within the company's device.
Insider and Privilege Misuse	Insider is a person who is accepted in an organization who have permission to gain access to confidential information/ Privilege Misuse is the same as abuse of privilege which pertains to creating a scene that seems lawful.
Payment Card Skimmers	A Skimmer is a theft that is able to steal any customer's credit card or debit card data when the customer is at the ATM, allowing them to make purchases and or to resell it.
Point of Sale Intrusions	is a remote attack against the environments where retail transactions are conducted, specifically where card-present purchases are made.
Physical Theft and Loss	When ones belonging is physically taken and never to be returned.
Web Application Attacks	SQL injections,using components with known vulnerabilities and cross-site scripting
DDOS	Form of electronic attack involving multiple computers, which send repeated HTTP requests or pings to a server to load it down

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

Term	**Definition**	**Context / Significance**
Coinminer Attack	If you haven't opened the detected website on your own, you are possibly redirected to the detected website via redirection mechanisms like malicious advertisement or a compromised website hosting an iframe or JavaScript which redirects to the detected website. The JavaScript runs as long as the user stays on the web page. As long as the website being visited is injected with the coin mining javascript, the website will be blocked by this signature.	Coin mining executables can be caught by traditional security tools, including the following components in Symantec Endpoint Protection (SEP): Antivirus, Download Insight, Advanced Machine Learning, and SONAR. Undetected malicious executables can be discovered by SymDiag's Threat Analysis Scan. The more SEP components that are installed and enabled, the greater the chance of detecting these threats.
Ransomware	a type of malicious software designed to block access to a computer system until a sum of money is paid.	**Use antimalware software.** Everyone needs to run at least one antimalware program. Windows comes with Windows Defender, but there are dozens of commercial competitors and some good freebies. Ransomware is malware. Antimalware software can stop the majority of variants before they hit.
Zero Day	deriving from or relating to a previously unknown vulnerability to attack in some software.	A main component of these solutions is a browser security solution, developed by Invincea, which detects malicious activity long before the antivirus companies know it even exists.
Malware	software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.	So to keep your machine clean, invest in security software and layer it up with the following: Use firewall, anti-malware, anti-ransomware, and anti-exploit technology. Your firewall can detect and block some of the known bad guys

“Living Off the Land”	attackers utilizing living off the land tactics, where they use whatever tools are already installed on the targeted system	Hiding malware on the hard disk has always been a goal of attackers as the less artifacts present, the less that can be detected. In the past we have seen obfuscated file infectors, the use of alternative data stream (ADS) on NTFS or inside RAR files, and even the new Wolf Compressed streams in Windows 10 being used to hide files from forensic analysis.
Spear Phishing	is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer	Spear phishing is the number one infection vector employed by 71 percent of organized groups in 2017
Infection Vector	the method by which a computer virus spreads	The attacker attempts to infect any computer of the targeted organization and once inside they will usually move across to go through the network of that target.
Trojan	t**rojan** is a type of malware that is often disguised as legitimate software.	are common but dangerous programs that hide within other seemingly harmless programs. They **work** the same way the ancient **Trojan horse**did: Once they're installed, the program will infect other files throughout your system and potentially wreak havoc on your computer.

Targeted Attack	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)	they’re usually driven by a small number of motivations: intelligence gathering, disruption, sabotage, or financial. Broadly speaking “targeted attacks” corresponds to espionage, although the lines are starting to blur and, in recent times, we’ve seen a number of groups branch out beyond espionage.
Off-The-Shelf Attack Tools	means attackers leave less distinctive fingerprints behind	Attackers have the ability to cause serious disruption to energy network. The danger is that they could, at a time of their choosing
Watering Hole Attacks	websites which 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.	example: if their target is in the aviation sector, they may compromise an aviation forum From causing collateral damages attackers will employ exploit kit which will only infect users coming from a pre-selected internet protocol range.
Lateral Movement Techniques	When attackers oftener use hacking software tools to obtain credentials from compromised computer and then use them to attempt to log into other computers on the network.	- “Pass the hash” — where attackers steal and reuse the underlying hashed version of a password and, without cracking it, can use it to authentic themselves on other computers or servers.
DDoS Attacks	Distribution Denial of Service uses ransomeware as a decoy, sowing confusion among the victims and delaying an effective response.	DDoS attacks can knock an org. offline, meaning that its systems admins will be busy trying to stem the attack and may be too distracted to notice suspicious activity on their network indicating that a targeted attack is underway.

DNS	Domain Name Server	The Domain Name System, or DNS, serves as a crucial protocol running under the hood of the internet: It translates domain names in alphanumeric characters (like google.com) to IP addresses (like 74.125.236.195) that represent the actual locations of the computers hosting websites or other services on those machines
BGP Hijacking	This allows attackers to intercept requests for updates from these IP addresses, and instead send down a Trojanized update	In September 2017, some variants of the FinFisher malware appear to have used this attack vector to compromise target computers.
Man in the Middle Attack	used to intercept and decrypt SSL traffic, or to manipulate content in transit to or from the device	- Sometimes this can be down to a misconfigured router that can expose certain data
<NEW TERM>		
<NEW TERM>		
<NEW TERM>		
<NEW TERM>		