# **Cybersecurity Terminology**

**Advanced Persistent Threat (APT)** – Targeted attacks differ from APTs in the same way a handgun differs from a state-of-the-art military issued rifle: sophistication, engineering, and user. APTs are attacks that use code and tools that have been designed from the group up by groups of well-talented salaried engineers. APTs are also state-sponsored attacks—which means that actual governments are behind them, rather than just a small group of hackers as is in the case of targeted attacks. APTs are much more serious in scope and firepower than targeted attacks, and typically only go after big targets like government agencies.

**Alert** –A brief, usually human-readable, technical notification regarding current vulnerabilities, exploits, and other security issues. Also known as an advisory, bulletin, or vulnerability note.

**Attack** – an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

**Attack signature** – A characteristic byte pattern used in malicious code or an indicator, or set of indicators, that allows the identification of malicious network activities.

**Attribution** – the process of tracking, identifying, and laying blame on the perpetrator of a cyberattack or other hacking exploit.

**Authentication** – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

**Authorization** -– Access privileges granted to a user, program, or process or the act of granting those privileges.

**Backdoor** – An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.

**Brute Force Attack** – A method of accessing an obstructed device through attempting multiple combinations of numeric and/or alphanumeric passwords.

**Call back** – Procedure for identifying and authenticating a remote information system terminal, whereby the host system disconnects the terminal and reestablishes contact.

**Compromise** – Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

**Continuous Monitoring** – Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

**Controlled Unclassified Information** – Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

**CONUS** – CONUS refers to the continental United States. To state that delivery is CONUS is to say that a procurement delivery could be anywhere in the continental U.S, excluding Hawaii and Alaska.

**Cybercrime operation** – the biggest difference between a targeted attack and a cybercrime operation is the scope. A cybercrime operation aims to victimize as many users as possible in the shortest amount of time to outrace security efforts, while a targeted attack has a narrow scope. Targeted attacks are deliberate, purposeful, and persistent while cybercrime operations are usually automated, opportunistic, or indiscriminate in nature. Cybercrime operations are also mostly driven by financial intentions, while targeted attacks have the primary goal of stealing information.

**Cybersecurity Event** – Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

**Cybersecurity Incident** – An assessed occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system; or the information the system processes, stores, or transmits; or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

**Cybersecurity Threat** – See *threat.*

**Data breach** – a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so.

**Data leak/Inadvertent disclosure** – Type of incident involving accidental exposure of information to an individual not authorized access.

**Data Loss Prevention (DLP) –** DLP software detects potential data breaches/data ex-filtration transmissions and prevents them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). In data leakage incidents, sensitive data is disclosed to unauthorized parties by either malicious intent or an inadvertent mistake. Sensitive data includes private or company information, [intellectual property](https://en.wikipedia.org/wiki/Intellectual_property) (IP), financial or patient information, credit-card data and other information ([Wikipedia](https://en.wikipedia.org/wiki/Data_loss_prevention_software))

**Demilitarized Zone (DMZ)** - In network security, a network that is isolated from, and serves as a neutral zone between, a trusted network (for example, a private intranet) and an untrusted network (for example, the Internet). One or more secure gateways usually control access to the DMZ from the trusted or the untrusted network

**Digital Forensics** – The application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.

**DoS/DDoS** – The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.). DDoS is a denial-of-service technique that uses numerous hosts to perform the attack.

**Encryption** – Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

**Exploit** – Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks.

**Exposure** – A system configuration issue or a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

**Firewall** – A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy.

**Hacktivism** – or activism-related hacking attacks are different from targeted attacks due to the former’s one-off, vandalistic nature. They are often more like nuisances—not that harmful, and something that can be dealt with easily, like the defacement of a public wall. Hacktivism attacks often yield no network penetration and little to no information theft of any soft. They are also done with the maximum amount of visibility—they are designed to be seen, rather than staying out of sight like targeted attacks are designed to do.

**Hardening** - the process of securing a system by reducing its surface of vulnerability.

**Host Intrusion Detection System (HIDS)** - A host-based intrusion detection system is an intrusion detection system that is capable of monitoring and analyzing the internals of a computing system as well as the network packets on its network interfaces, similar to the way a network-based intrusion detection system operates.

**Host Intrusion Prevention System (HIPS)** - HIPS is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. In other words, a Host Intrusion Prevention System aims to stop malware by monitoring the behavior of code. This makes it possible to help keep your system secure without depending on a specific threat to be added to a detection update.

**Indicator** – A technical artifact or observable that suggests an attack is imminent or is currently underway, or that a compromise may have already occurred.

**Information Sharing and Analysis Organization (ISAO)** – Any entity or collaboration created or employed by public- or private sector organizations, for purposes of gathering and analyzing critical cyber and related information in order to better understand security problems and interdependencies related to cyber systems, so as to ensure their availability, integrity, and reliability.

**Intrusion Detection System (IDS)** - Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS, which become part of your network to detect and stop potential incidents.

**Intrusion Prevention System (IPS)** - Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS, which become part of your network to detect and stop potential incidents.

**IP Reputation Block** – the process of correlating source IP addresses against databases of known malicious IP addresses, and stopping them before they have a chance to make it into a network.

**Malware** – A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim’s data, applications, or operating system or of otherwise annoying or disrupting the victim.

**Multi-factor Authentication (MFA)** – Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric).

**Network Access Control (NAC)** - a [computer](https://en.wikipedia.org/wiki/Computer) [networking](https://en.wikipedia.org/wiki/Computer_network) solution that uses a set of [protocols](https://en.wikipedia.org/wiki/Protocol_(computing)) to define and implement a policy that describes how to secure access to network [nodes](https://en.wikipedia.org/wiki/Node_(networking)) by devices when they initially attempt to access the network

**Network Forensics Tool (NFT)** -Network Forensics tools provide the ability to store, analyze and display all network data to reconstitute an even so an investigator can determine what happened on the network.

**Observation** – An event (benign or malicious) on a network or system.

**Passive attack** – An attack against an authentication protocol where the Attacker intercepts data traveling along the network between the Claimant and Verifier, but does not alter the data (i.e., eavesdropping). An attack that does not alter systems or data.

**Patch** – An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

**Penetration testing** – Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

**Personal identifying information** – means information that alone or in conjunction with other information identifies an individual, including an individual's: (A) name, social security number, date of birth, or government-issued identification number; (B) mother's maiden name; (C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (D) unique electronic identification number, address, or routing code; and (E) telecommunication access device as defined by Section 32.51, Penal Code.

**Phishing** – A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.

**Plaintext/Cleartext** – Intelligible data that has meaning and can be understood without the application of decryption. Unencrypted information.

**Port** – A physical entry or exit point of a cryptographic module that provides access to the module for physical signals, represented by logical information flows (physically separated ports do not share the same physical pin or wire).

**Port scanning** – Using a program to remotely determine which ports on a system are open (e.g., whether systems allow connections through those ports).

**Protocol** – Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.

**Reconnaissance/information gathering** – the process of collecting information about an intended target of a malicious hack by probing the target system.

**Risk** – A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the State/Nation.

**Role-based access control** – Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

**Rootkit** – A set of tools used by an attacker after gaining root-level access to a host to conceal the attacker’s activities on the host and permit the attacker to maintain root-level access to the host through covert means.

**Scanning** – Sending packets or requests to another system to gain information to be used in a potential subsequent attack.

**Security Controls** – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

**Segmentation** - Network segmentation in computer networking is the act or practice of splitting a computer network into subnetworks, each being a network segment. Advantages of such splitting are primarily for boosting performance and improving security.

**Sensor** – An intrusion detection and prevention system component that monitors and analyzes network activity and may also perform prevention actions.

**Sensitive personal information** – means (A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (i) social security number; (ii) driver's license number or government-issued identification number; or (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (B) information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual.

**Sniffing** – A passive technique that monitors network communication, decodes protocols, and examines headers and payloads for information of interest. It is both a review technique and a target identification and analysis technique.

**Social engineering** – A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.

**Spoofing** – 1. Faking the sending address of a transmission to gain illegal entry into a secure system. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. 2. The deliberate inducement of a user or resource to take incorrect action.

**Tactics, Techniques, and Procedures (TTPs)** – The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

**Targeted attack** – An attack that fulfills three main criteria: 1.) the attackers have a specific target in mind and has been shown to have spent considerable time, resources, and effort in setting up or carrying out the targeted attack. 2.) the main aim of the targeted attack is to infiltrate the target’s network and steal information from their servers or significantly impact the availability, integrity, confidentiality, or non-repudiation of the affected information systems. 3.) the attack is persistent, with attackers expending considerable effort to ensure the attack continues beyond the initial network penetration and exfiltration of data. Targeted attacks are often discovered years after the fact.

**Threat** – Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

**Threat Actor** – An individual or a group posing a threat.

**Threat Information** – Any information related to a threat that might help an organization protect itself against a threat or detect the activities of an actor. Major types of threat information include indicators, TTPs, security alerts, threat intelligence reports, and tool configurations.

**Threat Intelligence** –Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

**Threat Intelligence Report** – A prose document that describes TTPs, actors, types of systems and information being targeted, and other threat-related information.

**Threat Shifting** – The response of actors to perceived safeguards and/or countermeasures (i.e., security controls), in which actors change some characteristic of their intent/targeting in order to avoid and/or overcome those safeguards/countermeasures.

**Tool Configuration** – A recommendation for setting up and using tools that support the automated collection, exchange, processing, analysis, and use of threat information

**TOR** – is free software for enabling anonymous communication. The name is derived from an acronym for the original software project name "The Onion Router". Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays[[](https://en.wikipedia.org/wiki/Tor_(anonymity_network)#cite_note-torstatus-10) to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms".  Tor's intended use is to protect the personal privacy of its users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

**Virtual Local Area Network (VLAN) -** a logical subnetwork that can group together a collection of devices from different physical [LANs](https://www.lifewire.com/local-area-network-816382). Larger [business computer networks](https://www.lifewire.com/business-computer-networks-817883) often set up VLANs to re-partition their network for improved traffic management.

**Virtual Private Network (VPN)** - a method employing encryption to provide secure access to a remote computer over the Internet.

**Virus** – A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk.

**Vulnerability** – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**Watering Hole Attack** – A security exploit where the attacker infects websites that are frequently visited by members of the group being attacked, with a goal of infecting a computer used by one of the targeted group when they visit the infected website.

**Zero-day** – A zero-day vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating the vulnerability. Until the vulnerability is mitigated, hackers can exploit it to adversely affect computer programs, data, additional computers or a network.

**Sources**

**National Institute for Standards and Technology Special Publication definitions:** <https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf>

**Texas Administrative Code RULE §202.1:** <http://texreg.sos.state.tx.us/public/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=1&pt=10&ch=202&rl=1>

**Chapter 521, Texas Business and Commerce Code:** <https://statutes.capitol.texas.gov/Docs/BC/htm/BC.521.htm>

**Understanding a Targeted Attack:** <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/understanding-targeted-attacks-what-is-a-targeted-attack>