U.S. ARMY
CYBER COMMAND

www.arcyber.army.mil | Follow @arcyber

Cybersecurity Terminology

Botnets, backdoors, Trojan Horses, malware, Denial of Service attacks – the language of cybersecurity is filled with distinct jargon to describe its multitude of tools and tactics.

WHAT'S IT ALL MEAN?

The Army Criminal Investigation Command (CID) has put together a glossary of basic cybersecurity terminology to help users distinguish spam from cookies and worms from viruses.

- **Adware:** Free software supported by advertisements that includes features such as enhanced search tools or programs such as games or utilities. The programs are free to use, but require the user to watch advertisements as long as the programs are open.
- **Antivirus Software:** uses virus definitions to determine whether a file contains a virus and must be updated regularly to protect systems and networks against new attack signatures.
- **Attack:** an intrusion against an information system (computer) resulting in the degradation, denial, or destruction of the information or information system (computer).
- **Authentication Factor:** Data that is used to identify an individual for access to an information system. Authentication factors can be something you know (usernames, passwords, secret questions), something you have (USB token, smart card, PKI certificate), something you are (fingerprint, DNA, retina pattern), something you do (annotating text from an image, clicking only images of storefronts), or somewhere you are (GPS location).
- **Backdoor:** Refers to any method which allows an authorized or unauthorized user to bypass some or all security measures to gain access to a computer system, network, or software application. Not all backdoors are nefarious—they can be used to assist users who become locked out of their system.
- **Baiting:** Leaving a piece of portable electronic storage media such as a CD, laptop or USB drive near a target's workplace to tempt the curious victim into seeing what's on it. When the victim attempts to use the media a malware program releases a virus or exposes personal and financial information to hackers.
- **Beacon:** A type of malware that systematically calls out to a specified IP address or URL from a victimized system. A waiting threat agent can answer this beacon, establishing a connection that provides partial or even full remote access to the victimized system.
- **Black Hat:** A hacker that breaks into a network or device without consent to conduct malicious activities that can be used to harm the owner/users.
- **Bot/Botnet:** a software application or tool that performs tasks on command, allowing an attacker to take control remotely of an affected computer—a collection of infected computers is a botnet.
- **Brute Force Attack:** A programming style that does not include any shortcuts to improve performance, but relies on sheer computing power to try all possibilities until the solution to a problem is found
- **Cache:** contains copies of web pages saved by the browser that was used to view them. These files are used to increase the speed of web browsing and are sometimes called temporary internet files.

- **Ciphertext:** The unreadable, unintelligible group of alpha-numeric characters produced from a cipher (an algorithm for performing encryption or decryption) or the input to an inverse cipher.
- **Clickjacking:** An attack that tricks victims into clicking on a disguised link, potentially causing the victim to reveal confidential information or allowing others access to the victim's system.
- **Client:** A host that is seeking to use the resources of a server. Client/Server Network: In this network, individual work-stations send requests to a central server, and the server provides all resources.
- **Client/Server Network:** A network in which individual workstations send requests to a central server, and the server provides all resources.
- **Cloud:** a collection of computers with large storage capabilities that remotely serve requests, allowing you to access files and services through the internet from anywhere in the world.
- **Computer Network Exploitation (CNE):** Consists of techniques and processes that use computers or computer networks to gather data on targeted systems and networks.
- **Cookie:** an information packet sent from a website to a web browser that records a user's activity on that website. The information packet is stored on the user's computer and used to provide more personalized services for each subsequent visit to the website.
- **Cracking:** When an attacker generates a set of values that represent possible legitimate authentication factors and then tests those values against the authentication system to see which is correct.
- **Cross-site Scripting (XSS):** Occurs when an attacker sends a script that is executed by a victim system's web browser or in another browser window accessing a different site.
- **Cryptocurrency:** Or simply crypto, is any digital currency that uses an online ledger and cryptography to secure transactions.
- **Cryptography:** The discipline that embodies the principles, means and methods for the transformation of data to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
- **Dark Web:** Is a subset of the deep web. Its content is not indexed and consists of overlaying networks that use the public internet but require unique software, configuration, or authorization to access; designed to hide the identity of the user. Commonly contains anonymous journalism and marketplaces for illegal goods and services, and is regularly used by threat actors.
- **Decryption:** The process of transforming ciphertext into plain text.
- **Deepfake:** An audio or video clip that has been edited and manipulated to seem real or (make two lines believable.
- **Deep Web:** Online content that is not indexed by traditional search engines. The content is available to the general public but is harder to find unless you have the exact URL. Legitimate uses of the deep web include online banking, web mail, cloud storage, and legal documents.
- **Denial of Service (DoS):** Is an attack that inhibits a computer resource from communicating on a network, preventing it from being available to fulfill its purpose either temporarily or permanently.
- **Directory:** Is a centralized listing of resources such as users, groups, files and applications. Directories are also known as folders.
- **Distributed Denial of Service (DDoS):** Is a DoS attack that is sourced/distributed from many different host systems. In other words, it is an attack that involves using many computers to flood a single target simultaneously, causing a denial-of-service condition. The acronym D/DoS is a common method for referring to both DoS and DDoS attacks.
- **DNS:** Domain Name System is a hierarchical naming system built on a distributed database. This system transforms domain names to IP addresses and makes it possible to assign domain names to groups of Internet resources and users, regardless of the entities' physical location.

- **DNS Hijacking:** A malicious exploit in which a hacker or other party redirects users through the use of a rogue DNS server or other strategy that changes the IP address to which an Internet user is directed.
- **Domain Name:** a text-based translation of the numerical IP address assigned to an internet resource. Most networks and websites have text-based domain names that people can remember, such as www.army.mil. Domain names are also referred to as internet addresses.
- **Doxxing:** The process of gathering information about a person or business using online public sources such as social media profiles, reverse phone lookup and search engines. Doxxing typically leads to an anonymous person's identity being revealed.
- **Encryption:** The conversion of plain text to ciphertext through the use of a cryptographic algorithm. Encryption is commonly used to ensure the confidentiality and integrity of electronic communications and is a direct application of cryptography.
- **Exploit:** a malicious application/tool used to take advantage of a system's vulnerabilities.
- **Firewall:** an access control device (can be software or hardware) that performs specific security activities such as detecting failed attempts at access.
- **Hacker:** an unauthorized user who attempts to or gains access to an information system, the act of which is known as hacking.
- **Hacktivist:** Formed by combining "hack" with "activism," hacktivism is the act of hacking into a website or computer system to communicate a politically or socially motivated message. For the hacktivist, it is an Internet-enabled way to practice civil disobedience and protest.
- **Hardware:** the physical components of a computer. Host: Any device, such as a computer, that connects to a network.
- **Host:** Any device, such as a computer, that connects to a network.
- **Information System:** a complementary network of hardware and software that are used to collect, process, create, store, and disseminate data.
- **Internet Protocol (IP) address:** a unique identifier for each machine or device on a network for the purpose of routing data. An example of an IP address is 131.107.10.7.
- **Internet Service Provider (ISP):** a company that offers access to the internet.
- **Intrusion:** the unauthorized act of bypassing the security mechanisms of an information system. Unauthorized access to a computer.
- **IPv4:** Or IP version 4, is a 32-bit numeric address written as four sets of numbers, called octets, separated by periods (e.g., 131.107.10.7).
- **IPv6:** Or IP version 6, is a new method for IP addressing being implemented on newer computers and networking equipment that provides a larger address space than the IPv4. It is written as eight groups of hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:08d3:1319:8a2e:0370:7334).
- **Malware:** malicious software that attacks a computer. Malware has three categories: viruses; Trojans; and worms. Malware is commonly used to commit fraud and intrusions.
- **Metadata:** Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Or more simply, metadata is data about data.
- **Network:** two or more devices that are connected (via wires or wirelessly) and communicate with each other.
- **Network Intrusion:** the compromise of one or more devices on a network or networks, and at least partial access to the resources within.
- **Packet:** A small amount of computer data sent over a network. Each packet contains the address of its origin and destination, and information that connects it to the related packets being sent.
- **Packet Sniffers:** Tools commonly used by network technicians to diagnose network-related problems.

Packet sniffers can also be used by hackers for spying on network user traffic and collecting passwords.

- **Personally Identifiable Information (PII):** A type of data that identifies the unique identity of an individual. It includes basic personal information such as name, gender, address, telephone number email address or basic biometric data information that is electronically stored in a device or application.
- **Phishing:** sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords or credit card numbers.
- **Ransomware:** A form of malware that either deliberately prevents the victim from accessing computer files—holding data hostage until a ransom is paid—or threatens to release the victim's data unless a ransom is paid.
- **Rootkit:** A set of programs placed by an intruder in the system root (the directory where operating systems files are stored) to manipulate the system and make it easier to hide his or her presence.
- **Script:** A list of commands that are executed by a program.
- **Script Kiddie:** A person, normally someone who is not technologically sophisticated, who randomly seeks out a specific weakness over the Internet to gain root access to a system.
- **Secure Socket Layer (SSL):** A networking protocol that manages server authentication, client authentication and encrypted communication between servers and clients.
- **Server:** A piece of hardware or software that provides services to other devices or programs in a network. In other words, a host that receives requests to use its resources.
- **Shoulder Surfing:** The act of obtaining personal or sensitive information through direct observation. Shoulder surfing involves looking over a person's shoulder while the victim is preoccupied using a device. This is especially effective in crowded places where a person uses a computer, smartphone or ATM. Binoculars, video cameras and vision-enhancing devices also are used.
- **Smishing:** a form of phishing in which an attacker uses text messaging to trick targeted recipients into clicking a link and sending the attacker private information or downloading malicious programs to a smartphone.
- **Social Engineering:** a technique used to manipulate and deceive a person in order to gain sensitive and private information or access. Social engineering makes use of previously attained information usually garnered from social media.
- **Software:** a set of programs that can be installed and used to tell a computer to perform a task. Spam: unsolicited advertising or other information sent out via email or other messaging services.
- **Spam:** Unsolicited advertising or other information sent out via email or other messaging services
- **Spear phishing:** an email or electronic communications targeted at a specific individual, organization or business, intended to steal data for malicious purposes or install malware on the targeted user's computer.
- **Spoofing:** Deceptive behavior on computer systems or on other computer users. This is typically done by hiding one's identity or faking the identity of another user. Spoofing can take the form of false emails, IP addresses and online identities.
- **Structured Query Language (SQL) Injection:** An attack in which unauthorized SQL commands (or simply database commands) are used to trick a server into processing data input as a regular database query. SQL injections allow hackers to exploit the security vulnerabilities of the software that runs a website.
- **Surface Web:** Contains content for the general public that is indexed by traditional search engines and readily available by use of any internet browser. Examples include websites for news, social networking, and even the U.S. Army's website.
- **Threat:** The potential source of an adverse event.

- **Threat Agent (or Threat Actor):** a specific person or event that executes unauthorized actions against a system.
- **Trojan Horse:** a computer program that appears to have a useful function but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system.
- **Two Factor Authentication (also known as strong authentication):** A security mechanism that requires two types of credentials for authentication, that is designed to minimize security breaches by providing an additional layer of validation.
- **Unauthorized Access:** gaining access to any computer resource without permission.
- **URL:** short for Uniform Resource Locator, is a standardized address used to make website connections. Also known as a web address, an example URL is https://www.cid.army.mil.
- **Virtual Private Network (VPN):** a tool that creates a private network connection across a public network connection, providing privacy, anonymity, and security while on 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 device.
- **Vishing:** a combination of "voice" and "phishing", it is the phone version of email phishing, using automated voice messages to trick individuals into sharing their confidential information via a phone call.
- **Vulnerability:** a weakness in an information system, system security procedures, or internal controls that could be exploited to gain unauthorized access.
- **Web Browser:** also simply browser, is an application which allows users to browse/access the internet. Commonly used browsers include Internet Explorer, Google Chrome, Safari, Opera, and Mozilla Firefox.
- **Web Crawler:** Also known as a robot; spider; or simply crawler, is a program that can be used to automatically browse a site and follow and save all available links. Search engines use crawlers to browse the internet and build an index of available sites to provide its users efficient search results.
- **Whaling:** masquerading as a senior member of an organization to directly target senior or other important individuals at an organization to steal money or sensitive information or gain access to computer systems for criminal purposes.
- **White Hat:** A hacker that breaches a network to gain sensitive information with the owner's consent; usually employed to test infrastructure vulnerabilities.
- **Wireless Hotspot:** used to refer to a location or device which allows individuals to connect to the internet wirelessly. Cellphones can be used as mobile hotspots, sharing its cellular data connection with another device wirelessly.
- **Worm:** a self-replicating, self-spreading, self-contained program that uses networking tools to spread itself. Or more simply, a worm is a computer program that replicates itself across network connections to other systems.
- **Worms vs. Viruses:** viruses cannot be executed (carried out) unless the infected file is opened while worms are immediately executable. Viruses will not spread to other computers on a network unless a user sends the virus to another computer and a user on that second computer opens the infected file. However, worms send themselves to other computers and sometimes run exploits against other computers, infecting them automatically.
- **Zero Day:** A previously unknown vulnerability that leaves users with no time to mitigate it before potential or actual exploitation.

SOURCE: https://www.cid.army.mil/assets/docs/lookout/CyberTermsPT2.pdf