UNITED STATES ARMY
CRIMINAL INVESTIGATION COMMAND

Media contact: 571-305-4041 FOR IMMEDIATE RELEASE

CID LOOKOUT
ON POINT FOR THE ARMY

Understanding Cyber Terminology is Key to Prevention

QUANTICO, VA (July 7, 2021) – Cyber is now mainstream and part of everyday lives. Since April, more than 200,000 incidents have been reported to the Internet Crime Complaint Center, a major pipeline was shut down in the U.S., and the world's largest meat processing company was a victim of ransomware.

According to the Army Criminal Investigation Command's Major Cybercrime Unit, the best way to protect against cybercrime is with knowledge and understanding of what cybercrime entails.

The below commonly used cyber terms is a follow-up to Cyber Terminology 101 and should be used as a quick reference guide to intermediate well-known cyber terms.

Commonly Used Terms

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.

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.

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.

Computer Network Exploitation (CNE): Consists of techniques and processes that use computers or computer networks to gather data on targeted systems and networks.

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.

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.

Host: Any device, such as a computer, that connects to a network.

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).

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.

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.

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.

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, is a specific person or event that executes unauthorized actions against a system.

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.

White Hat: A hacker that breaches a network to gain sensitive information with the owner's consent; usually employed to test infrastructure vulnerabilities.

Cybercrime Prevention Flyers (CPFs) are produced as part of the CID Cyber Lookout program to promote internet safety for the collective Army family and to provide recommendations to strengthen your cyber security posture and prevent cybercrime before it occurs. This CPF and all past CPFs are available at https://www.cid.army.mil/mcu-advisories.html.

Additional cyber terminology can be found at CyberTerminology101.pdf (army.mil).