Glossary of Cybersecurity Terms

This glossary contains selected terms associated with cybersecurity.

A

Advanced Persistent Threat (APT): A multiphase and long-term network attack in which unauthorized users gain access to, and harvest, valuable enterprise data.

Authentication: A security service that provides proof that a user of a computer system is genuinely who they claim to be.

B

Backup: Ensuring all important data is stored in a secure offline location to protect it from being lost if a computer is hacked.

Botnet: A grouping of computer systems, potentially anywhere in the world, that have been infected by a malicious piece of software. The software allows the infected computers to be networked together by a hacker. The hacker gains full control of all the bots in the network and is able to conduct malicious tasks.

Breach: The moment an unauthorized user or intruder (hacker) successfully exploits a vulnerability in a computer or device and gains access to its files and network.

Brute-Force Attack: A technique a hacker can use to break into a computer system, such as trying to “guess” its password.

C

Cloud: A collection of computers with large storage capabilities that remotely serve customer file requests; the technology allows access to files through the internet, from anywhere in the world.

Command-and-Control Center: An application that controls all bots in a botnet. A hacker sends a command through an application, which then relays the command to all compromised computers in a network.

Cyberattack: Malicious attempts to damage, disrupt, or gain unauthorized access to computer systems, networks, or devices, through cyber means.

Cybersecurity: The preservation of confidentiality, integrity, and availability of information in the cyberspace.

D

Digital Signature: Information that is encrypted with a private key and is appended to a message or object to assure the recipient of the authenticity and integrity of the message or object.

Distributed Denial of Service (DDoS): A form of a cyberattack that is intended to make a service, such as a website, unusable by “flooding” it with malicious traffic or data from multiple sources (often botnets).

E

Encryption: An algorithmic technique that changes the contents of a file into something unreadable to those outside the chain of communication.

Exploit: A malicious application or script that can be used to take advantage of a computer’s vulnerability.

F

Firewall: A hardware or software-based defensive technology focused on preventing unauthorized access. A “wall” or filter is created that judges each attempted interaction with a user's computer and internet connection to determine, “should this be allowed entry or not?”

H

Honeypot: A defensive cybersecurity technique. This technique involves the use of a computer (server) designed to look like a legitimate and high-value target on a network. The intent is to entice hackers to focus on the computer and not on actual high-value computers or data.

The honeypot technique allows administrators to watch hackers “in the act” and learn how to protect against their attack methods.

I

Insider Threat: A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors, or business associates, who have “inside information” concerning the organization’s security practices, data, and computer systems.

J

Jailbreak: Bypassing software constraints on a device such that a user has access to the root access of the operating system, or kernel. This method is often used in the context of mobile phone security.

M

Malware: An umbrella term that describes all forms of malicious software designed to cause havoc on a computer. Typical forms of malware include viruses, Trojan Horses, worms, and ransomware.

Man-in-the-Middle (MitM): An intrusion in which an attacker intercepts messages between a user and a website in order to observe and record transactions. MitM attacks are advanced variations of phishing and pharming attacks. In an MitM attack, a user who has logged into a website is unaware that all the information exchanged between them and the website is actually passing through an intermediate website. A criminal is able to use the intermediate website to see any private information and alter transactions.

O

One-Time Password: A password that is generated for use in one login session. It is sometimes communicated between the client and the server through a secure channel.

Open Wi-Fi: A public network with limited or no restrictions that potentially exposes connected users’ devices and activity (traffic) to all other users of that network.

P

Patch: A new piece of software released as a “fix.” Most software requires thousands of lines of programming language to create, so it’s difficult for a developer to ensure all vulnerabilities are covered. When entry points are discovered by hackers or a developer, software vendors will often release new pieces of software as a fix.

Phishing (Attack): A technique used by hackers to obtain sensitive information, including passwords, bank accounts, or credit cards. Often, an email disguised as being from a legitimate source is received unexpectedly by a user. In many cases, a hacker will attempt to trick the recipient into either replying with the information they seek, such as bank details, or tempt them to click a malicious link or run an attachment.

R

Ransomware: A form of malware that deliberately prevents access to files on a computer. If a computer is infected by malware designed for this purpose, it will typically encrypt files and request that a “ransom” be paid in order to have them decrypted.

T

Token: An item that authorizes access to a network service. In general, a hardware security token or authentication token refers to small hardware devices, such as smart cards and key fobs, that users have in their possession, to authorize access to a network service.

Trojan Horse: A piece of malware that often allows a hacker to gain remote access to a computer. A system infected by a Trojan Horse creates an entry point for a perpetrator to download files or watch a user's keystrokes.

Two-Factor Authentication: The use of two different components to verify a user’s claimed identity.

V

Virus: A type of malware for personal computers. Viruses were first encountered with the use floppy disks. Viruses typically aim to corrupt, erase, or modify information on a computer before spreading to others, with some also able to cause physical damage.

Virtual Private Network (VPN): A tool that allows a user to remain anonymous while using the internet. A VPN provides anonymity by masking location and encrypting traffic as it travels between the user's computer and the website they are visiting.

W

Watering-Hole (Attack): An attack targeting a special interest group by placing malicious code on a website frequented by a specific audience. Example: In 2013, visitors to several energy and utility company websites were exposed to malicious code that could infect their computer.

White Hat Hacker: A person who uses their hacking skills for an ethical purpose. In contrast, a “black hat” hacker typically has a malicious intent. Businesses will often hire white hat hackers to test their cybersecurity capabilities.

Worm: A piece of malware that can replicate itself in order to spread an infection to other connected computers. Malware actively hunts for weak systems in a network to exploit and spread.

Z

Zero-Day (Attack): A particular form of software exploit, usually malware. What makes a zero-day exploit unique is that it is unknown to the public or a software vendor. In other words, because few people are aware of the vulnerability, they have “zero days” to protect themselves from its use.