Cybersecurity Jargon Buster

A Glossary of Terms
Table of Contents

2FA (2-Factor Authentication) ................................................................................................................................................................. 11
Access control ................................................................................................................................................................................................................................. 11
Active attack ......................................................................................................................................................................................................................................... 11
Active content ..................................................................................................................................................................................................................................... 11
Adware ................................................................................................................................................................................................................................................. 11
Algorithm (encryption) ................................................................................................................................................................................................................. 11
Antivirus ........................................................................................................................................................................................................................................... 11
APT (Advanced Persistent Threat) ..................................................................................................................................................................................... 11
Attack ............................................................................................................................................................................................................................................... 12
Attack signature ................................................................................................................................................................................................................................. 12
Attack surface ................................................................................................................................................................................................................................. 12
Auditing .............................................................................................................................................................................................................................................. 12
Authentication ................................................................................................................................................................................................................................. 12
Authorization ................................................................................................................................................................................................................................. 12
Availability ................................................................................................................................................................................................................................. 12
Backdoor ............................................................................................................................................................................................................................................ 12
BEC (Business Email Compromise) ..................................................................................................................................................................................... 12
Behavior monitoring ....................................................................................................................................................................................................................... 12
Biometrics ................................................................................................................................................................................................................................. 13
Black hat ................................................................................................................................................................................................................................. 13
Blacklist ................................................................................................................................................................................................................................. 13
Blended threat ..............................................................................................................................................................................................13
Bot ..............................................................................................................................................................................................................13
Botnet ..............................................................................................................................................................................................................13
Breach ..............................................................................................................................................................................................................13
Brute force attack ..............................................................................................................................................................................................................13
Business continuity plan ..............................................................................................................................................................................................................13
BYOD (Bring Your Own Device) ..............................................................................................................................................................................................................14
Certificate ..............................................................................................................................................................................................................14
Certificate-based authentication ..............................................................................................................................................................................................................14
Cipher text ..............................................................................................................................................................................................................14
Clickjacking ..............................................................................................................................................................................................................14
Clone phishing ..............................................................................................................................................................................................................14
Cloud computing ..............................................................................................................................................................................................................14
Cookie ..............................................................................................................................................................................................................15
Critical infrastructure ..............................................................................................................................................................................................................15
Cross-site scripting ..............................................................................................................................................................................................................15
Cryptography ..............................................................................................................................................................................................................15
Cyberattack ..............................................................................................................................................................................................................15
Cyber ecosystem ..............................................................................................................................................................................................................15
Cyberespionage ..............................................................................................................................................................................................................15
Cybersecurity ..............................................................................................................................................................................................................16
Darkweb ..............................................................................................................................................................................................................16
Data breach ..............................................................................................................................................................................................................16
Data disclosure ..............................................................................................................................................................................................................16
Data integrity.......................................................................................................................................................................................................................................16
Data mining...........................................................................................................................................................................................................................................16
Day zero........................................................................................................................................................................................................................................16
Decryption...............................................................................................................................................................................................................................17
Defacement...............................................................................................................................................................................................................................17
Defense in-depth ......................................................................................................................................................................................................................17
DES (Data Encryption Standard)...................................................................................................................................................................................17
Dictionary attack ......................................................................................................................................................................................................................17
Digital certificate......................................................................................................................................................................................................................17
Digital forensics......................................................................................................................................................................................................................17
Digital signature......................................................................................................................................................................................................................17
Distributed Denial-of-Service (DDoS) attack..........................................................................................................................................................17
DLP (Data Loss Prevention)..................................................................................................................................................................................................18
DMZ (Demilitarized Zone) ...........................................................................................................................................................................................................18
DoS (Denial of Service)...........................................................................................................................................................................................................18
DoS attack ...............................................................................................................................................................................................................................18
Domain...............................................................................................................................................................................................................................18
Domain hijacking......................................................................................................................................................................................................................18
Domain name ...............................................................................................................................................................................................................................18
DRP (Disaster Recovery Plan) ...................................................................................................................................................................................18
Drive-by download...................................................................................................................................................................................................................19
Dumpster diving......................................................................................................................................................................................................................19
Elevation of privilege ......................................................................................................................................................................................................................19
Encryption...............................................................................................................................................................................................................................19
Endpoint security ......................................................................................................................................................................................................................19
Event ......................................................................................................................................................................................... 19
Eavesdropping ........................................................................................................................................................................................................... 19
Exfiltration ......................................................................................................................................................................................................................... 20
Exploit ................................................................................................................................................................................................................................. 20
Exposure ................................................................................................................................................................................................................................. 20
External network ................................................................................................................................................................................................................. 20
Firewall ................................................................................................................................................................................................................................. 20
Forensics (Digital Forensics) ......................................................................................................................................................................................... 20
FTP (File Transfer Protocol) ......................................................................................................................................................................................... 20
Gateway ................................................................................................................................................................................................................................. 20
Hacker ................................................................................................................................................................................................................................. 21
Hash ................................................................................................................................................................................................................................. 21
Hacktivism ......................................................................................................................................................................................................................... 21
Hardening ................................................................................................................................................................................................................................. 21
HTTP (Hyper Text Transfer Protocol) ................................................................................................................................................................. 21
HTTPS (Secure HTTP) ................................................................................................................................................................................................................. 21
Honeypot ................................................................................................................................................................................................................................. 21
Host ................................................................................................................................................................................................................................. 21
IDS (Intrusion Detection System) ............................................................................................................................................................................... 22
Incident ................................................................................................................................................................................................................................. 22
Incident management (Incident response) ................................................................................................................................................................. 22
Information security policy ........................................................................................................................................................................................................... 22
Insider threat................................................................. 22
Intrusion detection ....................................................... 22
IP address .................................................................... 22
IPS (Intrusion Prevention System) ............................... 22
IPSec (Internet Protocol Security) .............................. 22
IP spoofing .................................................................. 23
Java Security Exploit .................................................. 23
Keylogger .................................................................... 23
Least privilege ............................................................ 23
Link jacking ................................................................. 23
MAC (Mandatory Access Control) ............................ 24
Machine learning ....................................................... 24
Malware ...................................................................... 24
Man-in-the-middle (MitM) attack ............................... 24
MFA (Multi-Factor Authentication) ............................ 24
Mitigation ................................................................... 24
MSSP (Managed Security Service Provider) .............. 24
NGFW (Next-generation firewall) ....................... 25
NIST (National Institute for Standards and Technology) 25
Non-repudiation ......................................................... 25
Open source software....................................................................................................................................................................................................................25

Packet sniffing.....................................................................................................................................................................................................................................25
Passive attack..............................................................................................................................................................................................................................25
Passphrase............................................................................................................................................................................................................................26
Password..............................................................................................................................................................................................................................26
Password caching....................................................................................................................................................................................................................26
Password cracking.................................................................................................................................................................................................................26
Password sniffing....................................................................................................................................................................................................................26
Patch.................................................................................................................................................................................................................................26
Patching..........................................................................................................................................................................................................................26
Patch management...........................................................................................................................................................................................................26
Payload..........................................................................................................................................................................................................................26
Penetration...................................................................................................................................................................................................................26
Pen testing........................................................................................................................................................................................................................26
Personal firewall..................................................................................................................................................................................................................27
Pharming...................................................................................................................................................................................................................27
Phishing....................................................................................................................................................................................................................27
Ping.............................................................................................................................................................................................................................27
Polymorphism.............................................................................................................................................................................................................27
Port...............................................................................................................................................................................................................................27
Port scan......................................................................................................................................................................................................................27
Program policy...............................................................................................................................................................................................................28
Protocol..................................................................................................................................................................................................................28
Proxy server..................................................................................................................................................................................................................28

Q .............................................................................................................................................................................................................................28
QoS – Quality of Service (QoS).............................................................................................................................................................................................28

R.................................................................................................................................................................................................................................................................28
Ransomware..........................................................................................................................................................................................................................28

Red team..........................................................................................................................................................................................................................28

Redundancy..........................................................................................................................................................................................................................28

Remote access tool..................................................................................................................................................................................................................28

Resilience..............................................................................................................................................................................................................................29

Reverse engineering..................................................................................................................................................................................................................29

Risk............................................................................................................................................................................................................................................29

Risk assessment...............................................................................................................................................................................................................29

Risk management...............................................................................................................................................................................................................29

Role based access control....................................................................................................................................................................................................29

Rootkit...............................................................................................................................................................................................................................29

S .............................................................................................................................................................................................................................................29

Sandboxing..........................................................................................................................................................................................................................29

Segmentation..................................................................................................................................................................................................................29

Security automation........................................................................................................................................................................................................29

Security perimeter...............................................................................................................................................................................................................30

Security policy..................................................................................................................................................................................................................30

Security posture................................................................................................................................................................................................................30

Session.............................................................................................................................................................................................................................30

Session hijacking................................................................................................................................................................................................................30

SIEM (Security Information and Event Management)........................................................................................................................................30

Signature..........................................................................................................................................................................................................................30

Single sign-on..................................................................................................................................................................................................................30

Situational awareness........................................................................................................................................................................................................30
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission Control Protocol (TCP)</td>
<td>33</td>
</tr>
<tr>
<td>Trojan (Trojan Horse)</td>
<td>34</td>
</tr>
<tr>
<td>Trust</td>
<td>34</td>
</tr>
<tr>
<td>Trusted network</td>
<td>34</td>
</tr>
<tr>
<td>U</td>
<td>34</td>
</tr>
<tr>
<td>UTM (Unified Threat Management)</td>
<td>34</td>
</tr>
<tr>
<td>V</td>
<td>34</td>
</tr>
<tr>
<td>Virus</td>
<td>34</td>
</tr>
<tr>
<td>Validation</td>
<td>34</td>
</tr>
<tr>
<td>Verification</td>
<td>35</td>
</tr>
<tr>
<td>VPN (Virtual Private Network)</td>
<td>35</td>
</tr>
<tr>
<td>Vulnerability</td>
<td>35</td>
</tr>
<tr>
<td>Vulnerability assessment</td>
<td>35</td>
</tr>
<tr>
<td>Vishing</td>
<td>35</td>
</tr>
<tr>
<td>Virus</td>
<td>35</td>
</tr>
<tr>
<td>W</td>
<td>35</td>
</tr>
<tr>
<td>Watering Hole</td>
<td>35</td>
</tr>
<tr>
<td>War Driving</td>
<td>36</td>
</tr>
<tr>
<td>WEP (Wired Equivalent Privacy)</td>
<td>36</td>
</tr>
<tr>
<td>Whaling</td>
<td>36</td>
</tr>
<tr>
<td>White hat</td>
<td>36</td>
</tr>
<tr>
<td>Whitelist</td>
<td>36</td>
</tr>
<tr>
<td>Worm</td>
<td>36</td>
</tr>
<tr>
<td>WPA (Wi-Fi Protected Access)</td>
<td>37</td>
</tr>
<tr>
<td>X</td>
<td>37</td>
</tr>
<tr>
<td>Y</td>
<td>37</td>
</tr>
</tbody>
</table>
Z ......................................................................................................................................................37
Zero day................................................................................................................................................37
Zero-day attack...............................................................................................................................................37
Zombies........................................................................................................................................................37
2FA (2-Factor Authentication)

An enhanced means of verifying identity that requires you to present two pieces of evidence — your credentials — in order to gain access to an account or other secure/restricted area. Your credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card or a token device), or something you are (like your fingerprint, voice recognition or other biometric). 2FA is a form of Multi-Factor Authentication.

Access control

Access Control ensures that resources are only granted to those users who are entitled to them.

Active attack

An assault perpetrated by an intentional threat source that attempts to alter a system, its resources, its data, or its operations.

Active content

Software that is able to automatically carry out or trigger actions without the explicit intervention of a user.

Adware

Software distributed to the user free of cost with advertisements embedded into them. As such, it displays advertisements, and redirects your queries to sponsor’s websites. Adware helps advertisers collect data for marketing purposes, without a user’s permission to do so.

Algorithm (encryption)

A set of mathematical rules (logic) for the process of encryption and decryption. Through the use of an algorithm, information is made into meaningless cipher text and requires the use of a key to transform the data back into its original form.

Antivirus

A security program that can run on a computer or mobile device and protects you by identifying and stopping the spread of malware on your system. Antivirus cannot detect all malware, so even if it is active, your system might still get infected. Anti-virus can also be used at the organizational level. Anti-virus tools are sometimes called “anti-malware,” because these products are designed to defend against various types of malicious software.

APT (Advanced Persistent Threat)

A set of stealthy and continuous computer backing processes, often orchestrated by human(s) targeting a specific entity. APT usually targets nations or organizations for business or political motives.
Attack
An attempt to break into a system.

Attack signature
A characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks.

Attack surface
The set of ways in which a hacker can enter a system and potentially cause damage.

Auditing
The process of information gathering and analysis of assets to ensure things such as policy compliance and security from vulnerabilities.

Authentication
One of the five pillars of information assurance, it is the process of confirming a user’s identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authorization
The process of giving individuals access to system or its components based on their identity.

Availability
The need to ensure that the business purpose of a system can be met and that it is accessible to all those who need to use it.

B

Backdoor
A design fault, planned or accidental, that allows an attacker access to the compromised system around any security mechanisms that are in place.

BEC (Business Email Compromise)
An exploit in which the attacker gains access to a corporate email account and spoofs the owner’s identity to defraud the company or its employees, customers or partners of money.

Behavior monitoring
Recording the events and activities of a system and its users. The recorded events are compared against security policy and behavioral baselines to evaluate compliance or discover violations. Behavioral monitoring can include the tracking of trends, setting of thresholds and defining responses.
**Biometrics**
A method of identification that uses physical characteristics of the users to determine access.

**Black hat**
A person of malicious intent who researches, develops, and uses techniques to defeat security measures and invade computer networks.

**Blacklist**
A blacklist is compiled list, such as usernames, IP addresses, applications, etc. that are denied access to a certain system or protocol because they are deemed to be malicious or otherwise unwanted. When a blacklist is used for access control, all entities are allowed access, except those listed in the blacklist. The opposite of a blacklist is a whitelist.

**Blended threat**
Threats that combine the characteristics of viruses, worms, Trojan horses, and other malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By using multiple methods and techniques, blended threats can rapidly spread and cause widespread damage.

**Bot**
Also known as a zombie, is an Internet-connected computer that has been infected and compromised by malicious code in order to use the computer for something other than what was intended.

**Botnet**
A network of compromised computers that are infected with small bits of malicious code (bots). They are frequently used by hackers for disreputable purposes, such as to launch denial of service attacks, or send messages like spam and malicious code without it being traceable. These infected machines allow a remote computer to control by a “botmaster” who has the ability to manipulate them individually, or collectively as bot armies that act in concert.

**Breach**
An incident that results in the disclosure or potential exposure of data.

**Brute force attack**
The attempt to gain access to a network using repeated guesses at passwords or data encryption keys.

**Business continuity plan**
A Business Continuity Plan is the plan for emergency response, backup operations, and post-disaster recovery steps that will ensure the availability of critical resources and facilitate the continuation of operations in an emergency situation. The goal of BCP is to restore and sustain mission critical processes when they have been damaged or taken off-line by a breach or accident.
BYOD (Bring Your Own Device)
A company's security policy dictating whether or not workers can bring in their own devices into the work environment, whether or not such devices can be connected to the company network and to what extent that connection allows interaction with company resources.

Certificate
An electronic document attached to someone's public key by a trusted third party, which attests that the public key belongs to a legitimate owner and has not been compromised. Certificates are intended to help you verify that a file or message actually comes from the entity it claims to come from.

Certificate-based authentication
Certificate-Based Authentication is the use of security protocols and certificates to authenticate and encrypt web traffic.

Cipher text
The result of encrypting either characters or bits using some algorithm. Cipher text is unreadable until it is decrypted.

Clickjacking
A malicious technique by which a victim is tricked into clicking on a URL, button or other screen object other than that intended by or perceived by the user. Clickjacking can be performed by loading a web page transparently behind another visible page (a facade), so clicking on an obvious link actually causes the hidden page's link to be selected.

Clone phishing
An attack where targets are presented with a copy (or "clone") of a legitimate message they had received earlier, but with specific changes made to ensnare the target (e.g. malicious attachments, invalid URL links, etc.). Because this attack is based on a previously seen, legitimate message, it can be highly effective in fooling a target.

Cloud computing
A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Cookie
A text file passed from a web site's server to a web site user's browser. They are used to identify a user and could record personal information such as ID and password, mailing address, credit card number, and more. A cookie is what enables your favorite web site to "recognize" you each time you revisit it.

Critical infrastructure
The physical or virtual systems and assets that are vital to an organization or country. If these systems are compromised, the result would be catastrophic. If an organization's mission critical processes are interrupted, this could result in the organization ceasing to exist.

Cross-site scripting
An attack performed through Web browsers, taking advantage of poorly-written Web applications. Cross-site scripting attacks can take many forms. One common form is for an attacker to trick a user into clicking on a specially-crafted, malicious hyperlink. The link appears to lead to an innocent site, but the site is actually the attacker’s, and includes embedded scripts. What the script does is up to the attacker; commonly, it collects data the victim might enter, such as a credit card number or password.

Cryptography
The art and science of encoding and decoding messages using mathematical algorithms that utilize a secret key. The concept has broadened to include managing messages that have some combination of: privacy (by being unreadable to anyone but the sender and receiver); integrity (not modified while en route), and non-repudiation (digitally signed in such a way that the originator cannot plausibly claim he or she did not originate it).

Cyberattack
Any attempt to violate the security perimeter of a logical environment. An attack can focus on gathering information, damaging business processes, exploiting flaws, monitoring targets, interrupting business tasks, extracting value, causing damage to logical or physical assets or using system resources to support attacks against other targets.

Cyber ecosystem
The interconnected information infrastructure of interactions among persons, processes, data, systems and technologies, along with the environment and conditions that influence those interactions.

Cyberespionage
The unethical act of violating the privacy and security of an organization in order to leak data or disclose internal/private/confidential information. Cyberespionage can be performed by individuals, organization or
governments for the direct purpose of causing harm to the violated entity to benefit individuals, organizations or governments.

Cybersecurity
The efforts to design, implement, and maintain security for an organization’s network. It is a combination of logical/technical-, physical- and personnel-focused countermeasures, safeguards and security controls.

Darkweb
The dark Web is comprised of websites that are visible to the public, but their IP address details are intentionally hidden. These websites can be visited by anyone on Internet, but it is not easy to find the server details and it is difficult to track the one hosting the site. Sites on the darkweb are not indexed and don’t appear on search engines. Hidden web real estate can (and is) used for good as well as nefarious purposes.

Data breach
The occurrence of disclosure of confidential information, access to confidential information, destruction of data assets or abusive use of a private IT environment. Generally, a data breach results in internal data being made accessible to external entities without authorization.

Data disclosure
A breach situation where it has been confirmed that data was actually disclosed (not just exposed) to an unauthorized party.

Data integrity
The property that data is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner.

Data mining
The activity of analyzing and/or searching through electronic data in order to find items of relevance, significance or value. The results of data mining are known as meta-data. Data mining can be a discovery of individual important data items, a summary or overview of numerous data items or a consolidation or clarification of a collection of data items.

Day zero
Also known as "Zero Day," this is a term used to mark the day a new vulnerability is made known for which no patch may yet be available (day one = the day at which the patch is made available).
Decryption
Decryption is the process of transforming an encrypted message into its original readable text.

Defacement
Defacement is the method of modifying the content of a website in such a way that it becomes “vandalized” or embarrassing to the website owner.

Defense in-depth
Defense In-Depth is the approach of using multiple layers of security to guard against failure of a single security component.

DES (Data Encryption Standard)
A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

Dictionary attack
An attempt to guess a password by systematically trying every word in a dictionary as the password. This attack is usually automated, using a dictionary of the hacker’s choosing, which may include both ordinary words and jargon, names, and slang.

Digital certificate
An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

Digital forensics
The means of gathering digital information to be used as evidence in a legal procedure. Digital forensics focuses on gathering, preserving and analyzing the fragile and volatile data from a computer system and/or network.

Digital signature
Used to uniquely identify a sender, it is a value computed with a cryptographic process and then attached to a data object, thereby digitally distinguishing the data.

Distributed Denial-of-Service (DDoS) attack
A type of attack where multiple infected/compromised systems, are used to send traffic to target a single system causing a Denial of Service (DoS). It is analogous to a group of people crowding the entry door or
gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting normal operations.

**DLP (Data Loss Prevention)**
A strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

**DMZ (Demilitarized Zone)**
A secure intermediate network or path between an organization's internal network and the external, or non-proprietary network. A DMZ is primarily implemented to secure an internal network from interaction with and exploitation and access by external nodes and networks. A demilitarized zone may also be known as a network perimeter or perimeter network.

**DoS (Denial of Service)**
Refers to any outwardly-induced condition that prevents access to a computer resource (rendering it unusable), thus "denying service" to an authorized or legitimate.

**DoS attack**
A type of attack aimed at making the targeted system or network unusable, often by monopolizing system resources.

**Domain**
On the Internet, a domain consists of a set of network addresses. In a Windows NT environment, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network.

**Domain hijacking**
Domain hijacking is an attack by which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his own server up in its place.

**Domain name**
A domain name locates an organization or other entity on the Internet. For example, the domain name "www.sans.org" locates an Internet address for "sans.org" at Internet point 199.0.0.2 and a particular host server named "www."

**DRP (Disaster Recovery Plan)**
The process of recovery of IT systems in the event of a disruption or disaster.
**Drive-by download**
An attack that exploits vulnerabilities in your web browser or its plugins when you simply surf to an attacker-controlled website. Some computer attackers set up their own malicious websites that are designed to automatically attack and exploit anyone that visits it. Other attackers compromise trusted websites such as ecommerce sites and deploy their exploit software there. Often these attacks occur without the victims realizing that they are under attack.

**Dumpster diving**
Obtaining passwords and corporate directories by searching through discarded media.

**Elevation of privilege**
Almost every computer program has some form of "privilege" built in, meaning, permission to do some set of actions on the system. Permissions are granted to individuals based on their ability to present proper credentials (for example, a username and password). Privilege has levels -- for example, a guest account typically has fewer privileges than an administrator account. Many network attacks begin with an attacker obtaining limited privileges on a system, then attempting to leverage those privileges into greater privileges that might ultimately lead to controlling the system. Any attempt to gain greater permissions illicitly, is considered an "elevation of privilege."

**Encryption**
The process of transforming data (called "plaintext") into a form (called "cipher text") that hides its content. As used in a network security context, encryption is usually accomplished by putting the data through any of several established mathematical algorithms developed specifically for this purpose.

**Endpoint security**
In network security, this refers to a methodology of protecting the corporate network when accessed via end users including remote devices such as laptops or other wireless and mobile devices. Each device with a connection to the network creates a potential entry point for security threats.

**Event**
Any observable occurrence in a system or network that prompts some kind of log entry or other notification.

**Eavesdropping**
The act of listening in on a transaction, communication, data transfer or conversation. Eavesdropping can be used to refer to both data packet capture on a network link (also known as sniffing or packet capture) and to audio recording using a microphone.
Exfiltration
The unauthorized transfer of information from an information system.

Exploit
Code that is designed to take advantage of a vulnerability. An exploit is designed to give an attacker the ability to execute additional malicious programs on the compromised system or to provide unauthorized access to affected data or application.

Exposure
A threat action whereby sensitive data is directly released to an unauthorized entity.

External network
Any network that can employees would typically be trusted on your network, a primary vendor's network connects to yours, with which you have neither a trusted or semi-trusted relationship. For example, a company's might be semi-trusted, but the public Internet would be untrusted — hence, External.

Firewall
Software or hardware that monitors and control the incoming and outgoing traffic on a network based on predetermined security rules. It establishes a barrier between a trusted, secure internal network and untrusted networks (e.g., Internet) to prevent unauthorized access to data or resources.

Forensics (Digital Forensics)
The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes.

FTP (File Transfer Protocol)
The most common protocol for specifying the transfer of text or binary files across a network or over the Internet.

Gateway
A network point that acts as an entrance to another network. A firewall will often serve as the gateway between the Internet and your network.
**H**

**Hacker**
A person who has knowledge and skill in analyzing program code or a computer system, modifying its functions or operations and altering its abilities and capabilities. A hacker may be ethical and authorized (see Whitehat) or may be malicious and unauthorized (see Blackhat).

**Hash**
A value or values generated from a string of text using a mathematical function. Hashing is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect the security of the transmission against tampering.

**Hacktivism**
Attackers who hack for a cause or belief rather than some form of personal gain. Hacktivism is often viewed by attackers as a form of protest or fighting for their perceived “right” or “justice.”

**Hardening**
The process of identifying and fixing vulnerabilities on a system.

**HTTP (Hyper Text Transfer Protocol)**
A communications standard designed and used to transfer information and documents between servers or from a server to a client. This standard is what enables your web browser to fetch pages from the Internet.

**HTTPS (Secure HTTP)**
A variation of HTTP enabling the secure transmission of data. Generally used in conjunction with an enhanced by a security mechanism, (usually SSL) which encrypts the HTTP.

**Honeypot**
A trap set to detect, deflect or in some manner, counteract attempts at unauthorized use of information systems. Consists of computer data or a network site that appears to be part of a network but is actually isolated and monitored. A honey pot can be used to log access attempts to those ports including a would-be attacker’s keystrokes.

**Host**
Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more web sites.
IDS (Intrusion Detection System)
A security management system that gathers, analyzes and reports on traffic information from various areas within a network. It identifies possible security breaches in progress including both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Incident
An adverse security-related network event that compromises the integrity, confidentiality or availability of an information asset.

Incident management (Incident response)
A term describing the activities of an organization to identify, analyze, and correct a security incident to prevent a future re-occurrence.

Information security policy
A formalized written account of the security strategy and goals of an organization. A security policy is usually comprised of standards, policies, operating procedures and guidelines.

Insider threat
One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.

Intrusion detection
The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.

IP address
A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols.

IPS (Intrusion Prevention System)
A network security appliance that identifies malicious system activity, logs information about this activity, attempts to block/stop it, and reports it.

IPSec (Internet Protocol Security)
A methodology of exchanging data over the public Internet while protecting the data from prying eyes as it travels from the originator to the recipient. IPSec provides encryption and authentication options to maximize the confidentiality of data transmissions, employing cryptographic protocols.
**IP spoofing**

The act of inserting a false (but ordinary-seeming) sender IP address into the "From" field of an Internet transmission’s header in order to hide the actual origin of the transmission. There are few, if any, legitimate reasons to perform IP spoofing; the technique is usually one aspect of an attack.

**Java Security Exploit**

A term that refers to any number of security flaws in Oracle’s Java software, which has a long history of having security vulnerabilities. Java is a high-level programming language that is a commonly used foundation for developing and delivering interactive content on the Web.

**Keylogger**

Any means by which the keystrokes of a victim are recorded as they are typed into the physical keyboard. A keylogger can be a software solution or a hardware device used to capture anything that a user might type in including passwords, answers to secret questions or details and information from e-mails, chats and documents.

**Least privilege**

The principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

**Link jacking**

A potentially unethical practice of redirecting a link to a middle-man or aggregator site or location rather than the original site the link seemed to indicate it was directed towards.
MAC (Mandatory Access Control)
A security approach that contains the ability of an individual resource owner to grant or deny access to resources or files on the system.

Machine learning
A field concerned with designing and developing artificial intelligence processes for automated knowledge discovery and innovation by information systems.

Malware
Short for “malicious software.” It is a generic description for any type of code or program cyber attackers use to perform malicious actions (capturing information, sabotaging the system, holding it for ransom). Typical forms of malware include viruses, worms, trojans and spyware. Traditionally, different types of malware have been classified according to their capabilities and means of propagation. However modern malware typically combines the characteristics from several or all of these in a single program (seen in blended malware attacks).

Man-in-the-middle (MitM) attack
A type of cyber-attack in which the actor intercepts, alters, or eavesdrops on data as it travels between the sender and recipient. An example of this is intercepting messages through an unencrypted Wi-Fi connection.

MFA (Multi-Factor Authentication)
An enhanced means of verifying identity that requires you to present two or more pieces of evidence – your credentials – when logging in to an account. Your credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card or a token device), or something you are (like your fingerprint, voice recognition or other biometric).

Mitigation
The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.

MSSP (Managed Security Service Provider)
An outsourced provider of network security services. Businesses turn to managed security services provider to alleviate the pressures they face daily related to information security. Functions of a managed security service include round-the-clock monitoring and management of intrusion detection systems and firewalls, overseeing patch management and upgrades, performing security assessments and security audits, and responding to security incidents.
NGFW (Next-generation firewall)
An integrated network platform that combines a traditional firewall with other network security functionalities such as deep packet inspection, intrusion prevention, website filtering, bandwidth management, antivirus inspection and third-party integration (i.e. Active Directory). Gartner defines an NGFW as “a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks.”

NIST (National Institute for Standards and Technology)
A division of the U.S. Department of Commerce that publishes open interoperability standards. It is also responsible for distributing complete and accurate information about computer security issues to government and the general public.

Non-repudiation
Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message. A method to protect against an individual or entity falsely denying having performed a particular action related to data.

Open source software
A term applied when the source code of a computer program is made available free of charge to the general public. The concept relies on peer review to find and eliminate bugs in the program code. One of the most famous examples of open source software is Linux.

Packet sniffing
The act of collecting frames or packets off of a data network communication. This activity allows the evaluation of the header contents as well as the payload of network communications.

Passive attack
An assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.
Passphrase
An easy-to-remember phrase which offers better security than a single-word password, because it is longer and thus harder to guess or calculate.

Password
A secret sequence of characters or a word that a user submits to a system for purposes of authentication, validation, or verification. Passphrases are typically recommended in place of passwords.

Password caching
The temporary storage of a user’s username and password by an application.

Password cracking
Password cracking is the process of attempting to guess passwords, given the password file information.

Password sniffing
Passive wiretapping, usually on a local area network, to gain knowledge of passwords.

Patch
A patch is a small update released by a software manufacturer to fix bugs or vulnerabilities in an existing program. Your computer and mobile devices should be updated to install the latest vendor’s patches in a timely fashion. Some vendors release patches on a monthly or quarterly basis. Therefore, having a computer that is unpatched for even a few weeks could leave it vulnerable.

Patching
The process of updating software to a more current version.

Patch management
The management activity related to researching, testing, approving and installing updates and patches to computer systems, which includes firmware, operating systems and applications.

Payload
The actual application data a packet contains. It is part of the transmitted data which is the fundamental purpose of the transmission. In summary, payload refers to the actual intended message in a transmission.

Penetration
Gaining unauthorized logical access to sensitive data by circumventing a system’s protections.

Pen testing
An authorized, simulated attack exercise used to evaluate the security of IT infrastructures. It uses a controlled environment to safely attack, identify, and exploit vulnerabilities that may exist in operating systems, services, networks, applications. Penetration testing is also useful in validating the efficacy of defensive mechanisms and determining how well end-users adhere to security policies.
Personal firewall
A firewall that is installed and run on individual device.

Pharming
This is a more sophisticated form of Man-in-the-middle attack. A user’s session is redirected to a masquerading website. By changing the pointers on a web server (e.g., www.worldbank.com), the URL can be redirected to send traffic to the IP of the pseudo/fake website. At the pseudo website, transactions can be mimicked and information like login credentials can be gathered. With this the attacker can access the real www.worldbank.com site and conduct transactions using the credentials of a valid user on that website.

Phishing
A social engineering technique where the attacker tries to trick the victim into giving up sensitive information by masquerading as a trusted entity. In a common phishing attack, a spoofed email message is sent by the attacker. The attacker tries to steal authentication credentials by providing a link to a fake login form on a malicious website designed to look legitimate (e.g., your bank). Once the victim logs in to a site they think is their bank, their login and password would then be stolen by the attacker. The term has evolved and often means not just attacks designed to steal your password, but emails designed to send you to websites that hack into your browser, or emails with infected attachments.

Ping
A utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply; hence, it was named after the sound echo sonar makes when trying to locate an object.

Polymorphism
Polymorphism is the process by which malicious software changes its underlying code to avoid detection.

Port
On a computer, a port is an interface to which you can connect a device (printer, keyboard, etc.). Within an internet-based environment, a port is a communication endpoint/connection within a network. The port number identifies what type of port it is. For example, port 80 is used for web traffic.

Port scan
A series of messages sent by someone attempting to break into a computer to learn which computer network services, each associated with a “well-known” port number, the computer provides. Port scanning, a favorite approach of computer cracker, gives the assailant an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness.
Program policy
A program policy is a high-level policy that sets the overall tone of an organization’s security approach.

Protocol
A set of formal rules describing how to transmit data across a network. They exist at several levels in a telecommunications connection.

Proxy server
A server that sits between a client application (such as a web browser) and a “real” server. The proxy server intercepts client requests and forwards them to the other server. Its purpose is two-fold: for outgoing traffic, it allows private, non-routable machines to reach a machine which can reach the Internet for them. Secondly, as it receives responses to the client machine requests (for example, web pages) it can cache them locally so that further client requests can be answered locally and immediately.

Q

QoS – Quality of Service (QoS)
The overall performance of a telephone or computer network, particularly the performance (speed and quality of connection) seen by the users of the network.

R

Ransomware
A form of malware that holds a victim’s data hostage on their computer typically through robust encryption. This is followed by a demand for payment in the form of Bitcoin (an untraceable digital currency) in order to release control of the captured data back to the user.

Red team
A group authorized and organized to emulate a potential adversary’s attack or exploitation capabilities against an organization’s cybersecurity posture.

Redundancy
Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.

Remote access tool
A piece of software used to remotely access or control a computer. This tool can be used legitimately by system administrators for accessing the client computers. They can also be used by a malicious actor to control the system without the knowledge of the victim.
Resilience
The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

Reverse engineering
Acquiring sensitive data by disassembling and analyzing the design of a system component.

Risk
Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.

Risk assessment
The process by which risks are identified and the impact of those risks determined.

Risk management
The process of performing a risk assessment and evaluating the responses to risk in order to mitigate or otherwise handle the identified risks. Countermeasures, safeguards or security controls are selected that may eliminate or reduce risk.

Role based access control
Role based access control assigns users to roles based on their organizational functions and determines authorization based on those roles.

Rootkit
A collection of tools (programs) that a hacker uses to mask intrusion and obtain administrator-level access to a computer or computer network.

Sandboxing
A means of isolating applications, code or entire operating systems in order to perform testing or evaluation. The sandbox limits the actions and resources available to the constrained item. This allows for the isolated item to be used for evaluation while preventing any harm or damage to be caused to the host system or related data or storage devices. In computer security, a sandbox is a security mechanism for separating running programs. It is often used to execute untested code, or untrusted programs from unverified third parties, suppliers, untrusted users and untrusted websites.

Segmentation
A technique of protecting confidential information by restricting access to only those who actually need it to perform their job. By restricting access to information, data the risk to business objectives is limited. Segmentation can be either physical or logical.
Security automation
The use of information technology in place of manual processes for cyber incident response and management.

Security perimeter
The boundary of a network or private environment where specific security policies and rules are enforced. The systems and users within the security boundary are forced into compliance with local security rules while anything outside is not under such restrictions. The security perimeter prevents any interactions between outside entities and internal entities that might violate or threaten the security of the internal systems.

Security policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

Security posture
The security status of an enterprise’s networks, information, and systems based on IA resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes.

Session
A virtual connection between two hosts by which network traffic is passed.

Session hijacking
An intrusion technique whereby a hacker sends a command to an already existing connection between two machines, in order to wrest control of the connection away from the machine that initiated it. The hacker’s goal is to gain access to a server while bypassing normal authentication measures.

SIEM (Security Information and Event Management)
An approach to security management that seeks to provide a holistic view of an organization’s information technology (IT) security. The acronym is pronounced “sim” with a silent e.

Signature
A Signature is a distinct pattern in network traffic that can be identified to a specific tool or exploit.

Single sign-on
A computer log-in routine in which one logon provides access to all resources on the network.

Situational awareness
In cybersecurity, comprehending the current status and security posture with respect to availability, confidentiality, and integrity of networks, systems, users, and data, along with projecting their future states.
Smishing
Short for SMS Phishing. It is a form of phishing that utilizes social engineering techniques and SMS systems to send bogus text messages that can attempt to infect a device with malware.

Smurf
An attack that works by spoofing the target address and sending a ping to the broadcast address for a remote network, which results in a large amount of ping replies being sent to the target.

Sniffer
A tool that monitors network traffic as it received in a network interface.

Sniffing
A synonym for "passive wiretapping."

Snowshoeing
Also known as “hit and run” spam, it is a strategy where spam messages are propagated over several domains and IP addresses to weaken reputation metrics and avoid filters. The increasing number of IP addresses makes recognizing and capturing spam difficult.

SOC (Security Operations Center)
A centralized unit that deals with security issues on an organizational and technical level. A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology.

Social engineering
A psychological attack used by cyber attackers to deceive their victims into taking an action that will place the victim at risk. For example, cyber attackers may trick you into revealing your password or fool you into installing malicious software on your computer. They often do this by pretending to be someone you know or trust, such as a bank, company or even a friend.

Spam
An electronic version of junk mail. Unwanted or unsolicited emails, typically sent to numerous recipients with the hope of enticing people to read the embedded advertisements, click on a link or open an attachment. Spam is often used to convince recipients to purchase illegal or questionable products and services, such as pharmaceuticals from fake companies. Spam is also often used to distribute malware to potential victims.

Spear phishing
Spear phishing describes a type of phishing attack that targets specific victims. The attacker uses details gathered about the targeted individuals to increase the credibility of the attack message. Specially crafted emails are sent to very specific individuals, usually all at the same organization. Because of the targeted
nature of this attack, spear phishing attacks are often harder to detect and usually more effective at fooling their victims.

**Spoofing**

Sending an email disguised to look like it is coming from someplace besides its actual origin. The IP address may be changed, the email address may mimic a known domain, and the email formatting may imitate the design attached to a well-known company or site. It is generally used when a hacker wants to make it difficult to trace where an attack is coming from.

**Spyware**

A type of malware that is designed to spy on the victim's activities, capturing sensitive data such as the person's passwords, online shopping, and screen contents. One popular type of spyware, a keylogger, is optimized for logging the victim's keyboard activity and transmitting the captured information to the remote attacker.

**SQL injection**

SQL injection is a type of input validation attack specific to database-driven applications where SQL code is inserted into application queries to manipulate the database.

**SSL (Secure Sockets Layer)**

A computer networking protocol for transmitting private communication over the Internet between servers and clients. It manages security and encrypted communications.

**Stealthing**

A term that refers to approaches used by malicious code to conceal its presence on the infected system.

**Stateful inspection**

A firewall architecture that works at the network layer which examines not just the header information, but also the contents of the packet up through the application layer in order to determine more about the packet (malicious vs. non-malicious behavior).

**Tactical Threat Intelligence**

Information about how threat actors are conducting attacks.

**TCP/IP**

The basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).
**Threat**

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

**Threat agent (Threat actor)**

An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

**Threat analysis**

The detailed evaluation of the characteristics of individual threats.

**Threat assessment**

The process of identifying different types of threats that an organization might be exposed to. Threat assessment is an element of risk assessment and management.

**Threat model**

A threat model is used to describe a given threat and the harm it could do to a system if it has a vulnerability.

**Threat vector**

The method a threat uses to get to the target.

**Token**

Also called a security token or an authentication token. Something a person has that evidences validity, or identity. It is usually a hardware device that resembles a hand-held calculator, since it often has some sort of display and perhaps a keypad for entering numbers. Tokens achieve the goal of "two-factor authentication," considered a strong standard of security when validating who a user is, because accessing a network that uses tokens requires two factors: something the person knows (a password) and something the person has (the token)

**Tor**

Is free software for enabling anonymous communication. The name is an acronym derived from the original software project name *The Onion Router*. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user’s location and usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult for Internet activity to be traced back to the user and is a popular communication protocol utilized on the “darkweb.”

**Transmission Control Protocol (TCP)**

Is a core protocol of the Internet. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP.
Trojan (Trojan Horse)

Are “impostor” files that claim to be something desirable to evade security mechanisms but, in fact, are malicious. A very important distinction from true viruses is that they do not replicate themselves, as viruses do. Trojans contain malicious code, that, when triggered, cause loss, or even theft, of data. In order for a Trojan horse to spread, you must, in effect, invite these programs onto your computers. An example is when you download and install a free screensaver (which actually works well as a screensaver) that also contains malicious code that infects your computer once you install it.

Trust

A methodology that determines which permissions and what actions other systems or users can perform on remote machines.

Trusted network

The private network which you intend your firewall to primarily protect. The Trusted network is usually where your most sensitive corporate resources reside or where home office employees do their work.

UTM (Unified Threat Management)

A network security solution that is the evolution of the traditional firewall into an all-inclusive security product. UTMs are able to perform multiple security functions within one single system: network firewalls, network intrusion prevention and gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data loss prevention and on-appliance reporting.

V

Virus

A small program written to alter the way a computer, server or other device operates, without the permission or knowledge of the user. Some viruses are programmed to damage the infected device and others are not designed for damage. In order to be considered a virus, a program must execute itself. It will often place its own code in the path of execution of another program. It must also replicate itself. For example, it may replace other executable files with a copy of the virus infected file.

Validation

The act of examining information provided by a person (or a system) to ascertain what rights, privileges, or permissions they may (or may not) have to perform some action. For example, when you attempt to charge
a purchase at a retail store to a credit card, the cashier validates your identity by examining your identification and comparing your signature on the receipt with the signature on the credit card.

**Verification**

In cryptography, the act of testing the authenticity of a digital signature. Verification proves that the information was actually sent by the signer and that the message has not been subsequently altered by anyone else.

**VPN (Virtual Private Network)**

A means of having the security benefits of a private, dedicated, leased-line network, without the cost of actually owning one. VPN uses cryptography to scramble data so it’s unreadable while traveling over the Internet, thus providing privacy over public lines. Companies with branch offices commonly use VPNs to connect multiple locations.

**Vulnerability**

In cybersecurity, a flaw in a system or device that can leave it open to unauthorized access and attack. It may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat. A tool used to take advantage of a vulnerability is called an exploit.

**Vulnerability assessment**

A process that searches computers, network, or communications infrastructure for known vulnerabilities which hackers can exploit.

**Vishing**

A form of phishing attack which relies on social engineering that takes place over the phone. In this attack, the attacker uses phone systems and voice messages to steal identities and financial resources.

**Virus**

A hidden, self-replicating section of computer software, usually malicious code, that propagates by infecting (i.e., inserting a copy of itself into and becoming part of) another program. A virus cannot run by itself; it requires that its host program be run to make the virus active.

**Watering Hole**

A computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more
of them with malware. Eventually, some member of the targeted group gets infected. Relying on websites that the group trusts makes this strategy efficient, even with groups that are resistant to spear phishing and other forms of phishing.

**War Driving**

War driving is the process of traveling around looking for wireless access point signals that can be used to get network access.

**WEP (Wired Equivalent Privacy)**

A standard that enables wireless devices and laptops to access a network via radio frequencies instead of physical wiring. WEP has three tasks: 1) to authenticate clients to access points; 2) to encrypt the data exchanged between the clients and access points; and 3) to include an integrity check with every packet exchanged. The initial implementation of WEP provides weak security. While it is not completely useless, it is best used as another layer of security in conjunction with stronger measures.

**Whaling**

A type of spear-phishing attack specifically targeted at high-ranking executives in an organization.

**White hat**

A person who investigates flaws in network security measures in order to strengthen them and to prevent computer networks from being invaded. When such a researcher discovers new security flaws, he or she reports them to the appropriate vendor to be fixed, rather than using the knowledge illicitly.

**Whitelist**

A whitelist is compiled list, such as usernames, IP addresses, applications, etc. that are granted access to a certain system or protocol. When a whitelist is used, all entities are denied access, except those included in the whitelist. The opposite of a whitelist is a blacklist, which allows access from all items, except those included the list.

**Worm**

Programs that replicate themselves from system to system without the use of a host file. This is in contrast to viruses, which requires the spreading of an infected host file. Although worms generally exist inside of other files, often Word or Excel documents, there is a difference between how worms and viruses use the host file. Usually the worm will release a document that already has the "worm" macro inside the document. The entire document will travel from computer to computer, so the entire document should be considered the worm.
WPA (Wi-Fi Protected Access)
A data encryption specification for 802.11 wireless networks. Wireless networks rely on radio waves, which broadcast in all directions. Any device within range of a wireless access point could eavesdrop upon its transmissions. WPA encrypts wireless data so that an eavesdropper intercepts gibberish, while authorized endpoints receive clear, decrypted data. WPA replaces WEP, a weaker wireless encryption standard that attackers can readily break.

X
No entries at this time.

Y
No entries at this time.

Z
Zero day
Also known as "Day Zero," this is a term used to mark the day a new vulnerability is made known for which no patch may yet be available (day one = the day at which the patch is made available).

Zero-day attack
A computer threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software developer knows about the vulnerability.

Zombies
A zombie computer (often shortened as zombie) is a computer connected to the Internet that has been compromised by a hacker, a computer virus, or a trojan horse. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.