Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/cybercrime-terminology/

EXECUTIVE GUIDE ON A REFERENCE FOR EXECUTIVES, CLAIMS PROFESSIONALS AND LEGAL TEAMS

Cybercrime Terminology, or What the Incident Report Actually Means

When a breach report or a pleading describes a botnet, a rootkit or a zero day exploit, the people who have to make decisions deserve a definition they can trust. These are the terms as a forensic examiner uses them, written for readers outside the security team.

This reference covers the attack techniques, tooling and slang that appear most often in incident reports, insurance correspondence and litigation. It was adapted from the original evestigate.com library and revised October 30, 2026 in the voice our examiners use across a conference table. For the current scoping vocabulary, including digital evidence, identity and operational technology terms, see the larger cybersecurity and forensics glossary.

The firewall and rootkit definitions below follow the primary sources: NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and the NIST rootkit definition. A glossary explains terminology.

When one of these terms appears in a report on your desk, call (800) 868-8189 or send the term to a senior examiner, who will explain what it means for your systems.

The Terms, From Adware to Zombie Drone

Use these definitions when you read an incident report or sit down with an examiner. A term describes a technique or a tool, and the examiner reads what happened inside a particular system from that system's own records. If you suspect an incident, identify the affected accounts and devices, preserve the available records through your agreed response process and call before anyone wipes, reissues or reconfigures a machine. The common digital evidence mistakes guide explains why those first few days matter so much.

Adware: Software built to force chosen advertisements onto a system. Aggressive variants pop up ads with such speed and frequency that they slow the machine and tie up its resources, and adware bundled with spyware may also collect information about the user's activity.

Back Door: A mechanism that permits access while bypassing an intended authentication or security control. It may be deliberately introduced, left behind by insecure development or installed by an attacker, and its origin and purpose must be established from evidence rather than assumed.

Black Hat: An informal term for an attacker who accesses systems without authorization for malicious purposes. Attackers often share the details of an intrusion so that others can exploit the same weakness before it is addressed.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Bot: A software robot that performs an extensive set of automated tasks on its own. Search engines use benign bots, also called spiders, to crawl and index websites. In an attacker's hands a bot can carry out destructive tasks, introduce malware to a system or network and coordinate attacks by controlling a botnet.

Botnet: A network of zombie drones under the control of a single attacker. When attackers launch a distributed denial of service attack or a spam campaign they use a botnet to do it, and the owners of the infected systems are usually unaware that their resources are involved. The arrangement hides the attacker's tracks and multiplies the force of the attack across many machines at once.

Cookies: A small packet of information from a visited web server that the browser stores on the user's system. Cookies personalize a return visit, for example by remembering the entries in a form so the visitor finds it already completed.

Cracker: The word hacker in everyday use usually means a cracker, and the two have become synonymous. Derived from safe cracker to separate the meaning from the many other uses of hacker, a cracker is someone who breaks into a computer system or network without authorization and intends to do harm. A cracker may destroy files, steal personal information such as card numbers or client data, infect a system with a virus or cause other damage. These are the black hats this glossary describes.

Denial of Service Attack (DOS): An attack designed to overwhelm a targeted website or service to the point of crashing it or making it inaccessible. Beyond sheer volume and frequency, the packets sent are sometimes malformed to add further stress to the system processing them. A successful denial of service attack can cripple any organization that depends on its online presence.

Distributed Denial of Service Attack (DDOS): A denial of service attack carried out with zombie drones, a botnet, which the attacker directs through a master program to send data to the targeted server from many systems at once. The speed and volume are magnified far beyond what a single system could produce, and as with any botnet the owners of the controlled systems are usually unaware that they took part.

Dumpster Diving: Rummaging through the trash of an individual or a business to gather information that could help an attacker gain access to a system or commit identity theft. Discarded records can expose account details and other information that supports intrusion or fraud.

Easter Egg: A harmless surprise that a developer places in a program or on a circuit board. It may be as simple as a text greeting, a signature or an embedded image, or as elaborate as a hidden video or small program. To qualify, it must be undocumented, not malicious, reproducible by anyone with the same device or software, not obvious and intended only as a harmless surprise.

Firewall: A device or program that filters traffic according to configured rules. It restricts access according to those rules, and the protection it gives depends on its placement, its rules, the inspection it supports and how well it is maintained, which is why an examiner reads its configuration alongside its logs.

Gray Hat: An informal label for activity that exposes a security weakness without the owner's authorization.

Hacker: A term whose meaning depends on context. It is used for people who explore or manipulate technical systems and, in other settings, for attackers.

Keylogger: Software or hardware that records configured keyboard activity. Authorized monitoring also raises policy and legal questions.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Logic Bomb: A malicious program designed to execute when a particular condition is met. A time bomb is one kind, triggered by a date or time, but logic bombs can be far more elaborate, firing when a certain file is opened, a key combination is pressed or any other trackable event occurs. Before the trigger condition is met, the program simply lies dormant.

Malware: Software or code used for malicious purposes, including unauthorized access, surveillance, data theft, disruption or damage. It need not visibly damage a system to be malicious.

Master Program: The program an attacker uses to transmit commands remotely to infected zombie drones, normally to carry out denial of service or spam attacks.

Payload: The part of a malware program that actually carries out its designed task.

Phishing: Social engineering carried out electronically, usually by email, to gather sensitive information. The messages often look legitimate and may imitate a social network, a familiar payment service or the recipient's own bank, with a link to a convincing site that asks the reader to verify account information. Logging in on the bogus site hands the attacker exactly what they need. Phishing takes many forms, and some are far harder to spot than others.

Phreaker: Often considered the original computer hackers, phreakers, or phone phreakers, emerged in the 1960s by circumventing telecommunications security to place calls, including long distance calls, for free. Using electronic recording devices or even the tones from a whistle, they tricked the systems into treating the call as valid. One of the first to find prominence was Captain Crunch, who realized that the toy whistle packed in a cereal box reproduced the tone frequencies telephone companies used to validate and route calls.

Polymorphic Virus: Malicious code that changes aspects of its representation as it propagates to make signature matching harder. Security products and analysts counter that by pairing signatures with behavioral and other detection methods.

Rootkit: Tools or modifications that conceal activity or maintain privileged access. Some operate at low levels of the system, they arrive by more than one method, and examiners look for them in the platform's own artifacts. Finding one on a host opens the work of measuring how far the attacker's control reached across the network, and the examination is planned around the platform and the artifacts available.

Script Kiddie: An informal term for an attacker who relies on programs or scripts written by others rather than developing the underlying technique. Borrowed tools in unskilled hands cause real harm all the same.

Social Engineering: Deceiving someone in order to obtain sensitive or personal information such as card details, user names and passwords. When a fictitious Mr. Smith calls from IT to announce new password guidelines and asks you to read yours back so he can check it, you have been targeted. Social engineers are clever, resourceful and very convincing. The defense is simple: share personal or sensitive information only with people you have verified, treat any request for a password as a warning sign, and make sure you are the one placing the call.

Spam: Unsolicited email, also known as junk email. Spammers gather lists of addresses and bombard them with messages that are often simple advertising but can also carry phishing lures or links to sites that install malware. Delete spam immediately, removal instructions included, because a reply only confirms that the

© 2026 Global Digital Forensics, Inc. All rights reserved.

address is live and invites more spam, and the confirmed address may then be sold on to other spammers. Use the spam filters your mail service provides.

Spoofing: The art of misdirection. Attackers cover their tracks by faking an IP address or altering the sender information on an email so the recipient is deceived about its origin, for example by making a message with a malicious link appear to come from a trusted friend or a familiar organization. Legitimate mail servers have controls against tampering with sender information, but spammers who run their own SMTP mail servers can alter it freely. When in doubt, check with the apparent source yourself.

Spyware: Software designed to gather information about a user's computer activity without their knowledge. Sometimes it merely tracks browsing habits to match advertisements to interests. It can also scan files and keystrokes, create pop up ads, change the home page or steer the browser to chosen websites, and a common trick is a pop up warning that the system is infected followed by a forced visit to a page selling the supposed fix. Spyware most often arrives bundled with free software such as screen savers, emoticons and social networking programs.

Time Bomb: A malicious program designed to execute at a predetermined time or date. Time bombs are often set for holidays or for dates chosen to make a political statement. On execution the program may do something benign, such as displaying a picture, or something far more damaging, such as stealing, deleting or corrupting system information. Before the trigger time arrives, it remains dormant.

Trojan: A Trojan, or Trojan horse, is a malicious program disguised as a legitimate one, which makes it hard to distinguish from the programs that belong on the system. Once introduced it can destroy files, alter information, steal passwords or other data, or carry out any other purpose it was built for, or it may lie dormant and wait for an attacker to connect remotely and take control. A Trojan behaves much like a virus, except that it spreads by deception rather than by copying itself.

Virus: A malicious program or code that attaches itself to another program file and replicates, infecting other systems whenever the infected program is used. Like its biological namesake it spreads most easily where hosts are connected: across a network, on removable media such as a disc or a memory stick, or as an email attachment. The word virus is often used loosely for malicious programs that lack self replication, such as spyware and adware.

Wardriving: Driving around with the purpose of finding open, unsecured wireless networks. A network's range often extends past the walls of a building and creates zones in public places that can be used to gain entry, and attackers may map those zones with GPS for later use or to pass on to others. Warbiking and warwalking are the same activity on two wheels or on foot. The lesson is that a wireless network must be secured, because someone is looking for the opening.

White Hat: While black hats use their skills for malicious purposes, white hats are ethical hackers who use the same knowledge to thwart attackers and protect the integrity of computer systems and networks. If a black hat targets you, a white hat is a very good person to have in the room, and our security testing and incident response practice is where you will find ours.

Worm: A destructive self contained program that, like a virus, replicates itself, but unlike a virus runs on its own, with no host program or document. A worm copies and transfers itself to other systems on a network with no user action, and left in place it can be devastating, consuming memory and bandwidth until systems

© 2026 Global Digital Forensics, Inc. All rights reserved.

become unstable and unusable even when it causes no direct damage.

Zero Day Threat/Exploit: Every threat has to start somewhere. Most protection relies on detection programs that compare the digital footprint of a suspected threat against a database of threats already detected, reported and documented, which is why antivirus software needs constant updates. That lag between deployment and documentation is what makes a zero day threat so dangerous. A zero day threat is pristine and undocumented: from the first day it is deployed until it is noticed, reported and added to the index it is unknown, and to standard protection unknown means invisible.

Zombie / Zombie Drone: A malware program that lets an attacker take remote control of a system and use it as a zombie drone for further attacks, such as spam campaigns or denial of service attacks, without the owner's knowledge. The arrangement hides the attacker's tracks and multiplies their reach by spending your resources. The infected user rarely notices, because zombies are usually benign to their host. They can arrive through an infected email attachment, but most often through file sharing sites, chat groups, adult websites and online casinos that insist on a custom media player, with the installed player as the delivery mechanism.

When the Question Calls for an Examiner

A glossary tells you what a word means. Whether the rootkit named in the report was really there, how long the back door stayed open and which records remain to answer the question are examination questions, and they are what our ransomware and data breach analysis and business email compromise analysis practices do every week for insurers, executives and law firms. Global Digital Forensics has served law firms and businesses since 1992, our examiners are court tested and certified, and the initial consultation is free. Call (800) 868-8189 as soon as the question comes up, so preservation starts while the devices and logs are in their current state.

Web Addresses for the Sources Cited

1. NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy: https://csrc.nist.gov/pubs/sp/800/41/r1/final
2. NIST rootkit definition: https://csrc.nist.gov/glossary/term/rootkit

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.