PaladinIT

Cyber Security Glossary

Anti-Malware—Software that prevents, detects and eliminates malicious programs on computing devices.

Antivirus—Software that detects and eliminates computer viruses.

Backdoor Trojan—A virus that enables remote control of an infected device, allowing virtually any command to be enacted by the attacker. Backdoor Trojans are often used to create botnets for criminal purposes.

Botnets—A group of Internet-connected devices configured to forward transmissions (such as spam or viruses) to other devices, despite their owners being unaware of it.

Cybercrime—Also known at computer crime or netcrime, cybercrime is loosely defined as any criminal activity that involves a computer and a network, whether in the commissioning of the crime or the target.

DDoS—Distributed denial of service attack. An attempt to interrupt or suspend host services of an Internet-connected machine causing network resources, servers, or websites to be unavailable or unable to function.

Malware—An overarching term describing hostile and/or intrusive software including (but not limited to) viruses, worms, Trojans, ransomware, spyware, adware, scareware, and other more, taking the form of executables, scripts, and active content.

Phishing—An attempt to acquire sensitive information like usernames, passwords, and credit card details for malicious purposes by masquerading as a trustworthy entity in a digital environment.

Rootkit—Trojans that conceal objects or activities in a device's system, primarily to prevent other malicious programs from being detected and removed

Social Engineering—Non-technical malicious activity that exploits human interaction to subvert technical security policy, procedures, and programs, in order to gain access to secure devices and networks.

Trojan—Malicious, non-replicating programs that hide on a device as benign files and perform unauthorized actions on a device, such as deleting, blocking, modifying, or copying data, hindering performance, and more.

Zero-Day Vulnerability—a security gap in software that is unknown to its creators, which is hurriedly exploited before the software creator or vendor patches it.