Cyber Attack Types

Threat actors use many types of cyberattacks.

Malware (short for malicious software) is a common type of cyberattack that is designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Click the links below to learn more

Common Malware Types

Malware Purposes

Common Attack Types

Common Types of Malware

Common types of malware include:

Virus
A computer virus is code that can replicate itself and spread from one computer to another. It requires user intervention or execution to replicate and/or cause damage.

Network worm
A variant of the computer virus, a network worm is a piece of self-replicating code designed to spread itself across computer networks. It does not require intervention or execution to replicate.

Botnet
Derived from robot network, a botnet is a large, automated and distributed network of previously compromised computers or devices that can be simultaneously controlled to launch large-scale attacks such as DDoS.

Trojan horse
A Trojan horse is a piece of malware that gains access to a targeted system by hiding within a genuine application. Trojan horses are often broken down into categories reflecting their purposes. A common Trojan horse program is used to install remote access trojan (RAT) capabilities on the compromised target.

Malware Purpose

Some specific types of malware are characterized by their purpose:

Spyware
A class of malware that gathers information about a person or enterprise without the knowledge of the person or enterprise

Adware
A type of malware designed to present advertisements (generally unwanted) to users

Ransomware
A kind of extortive malware (also called hostage code) that leverages cryptovirology to lock or encrypt data or functions and demand payment to unlock them

Keylogger
A class of malware that secretly records user keystrokes and, in some cases, screen content

Rootkit
A class of malware that hides the existence of other malware by modifying the underlying operating system

Common Attack Types

Advanced persistent threats (APTs)
Complex and coordinated attacks directed at a specific entity or enterprise. They require a substantial amount of research and time, often taking months or even years to fully execute. APT is a term indicating the class of complexity; however, whether a particular attack is APT cannot be tested. After an attack is discovered, and the level of complexity is determined and the amount of time and resources spent on the attack are investigated, then the attack can be classified as an attack by an APT.

Backdoor
A means of regaining access to a compromised system by installing software or configuring existing software to enable remote access under attacker-defined conditions.

Brute force attack
An attack made by trying all possible combinations of passwords or encryption keys until the correct one is found.

Buffer overflow
An attack in which a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Buffer overflow is an increasingly common type of security attack on data integrity.

Cross-site scripting (XSS)
A type of injection in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser-side script, to a different end user. Flaws that allow XSS attacks to succeed are widespread and occur anywhere a web application uses input from a user within the output it generates (i.e., without validating or encoding it).

Denial-of-service (DoS) attack
An assault on a service from a single source that floods it with so many requests that it becomes overwhelmed and is either stopped completely or operates at a significantly reduced rate.

Man-in-the-middle attack
An attack in which the actor intercepts communication between two parts of the victim system and then replaces the traffic with the intruder's own, eventually assuming control of the communication.

Phishing
A type of email attack that attempts to convince a user that the originator is genuine, but with the intention of obtaining information for use in social engineering.

Social engineering
An attempt to exploit social vulnerabilities to gain access to information and/or systems. It aims to trick the victim into divulging information or opening malicious software or programs.

Spear phishing
An attack in which social engineering techniques are used to masquerade as a trusted party to obtain important information such as passwords from the victim.

Spoofing
Faking the sending address of a transmission to gain illegal entry into a secure system.

Structured query language (SQL) injection
According to OWASP, a SQL-injection attack consists of insertion or injection of a SQL query via the input data from the client to the application. This can result in the malicious actor being able to read sensitive data from the database, modify (insert/update/delete) database data, or execute administrative operations, such as shutting down the DBMS.168

Zero-day exploit
A vulnerability that is exploited before the software creator/vendor is even aware of its existence.