BeyondTrust

11 Most Common Types of Malware, & Essential Defenses

Explore the most common types of malware and discover how BeyondTrust provides a powerful, blended defense against them.

1 Worm

Self-propagating malware that exploits vulnerabilities to replicate, potentially causing network disruptions or server failures. They often hide in attachments, scan networks for vulnerable systems, and can be bandwidth-intensive or stealthy.

First known instance:

Creeper System, 1971.

DEC PDP-10 computers running TENEX at BBN Technologies.

Prominent examples:

Raspberry Robin **Morris Worm** **Mydoom**

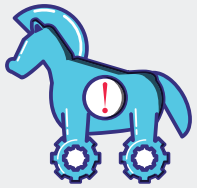
2 Trojan

Disguises itself as a legitimate file or app to deceive users into downloading it. Once executed, the payload can deliver various types of malware. It then executes using the privileges of the deceived user.

First known instance:

ANIMAL, 1975.

A non-malicious program on the UNIVAC 1108, an early 36-bit computer system.



Prominent examples:

GameOver ZeuS **Emotet** **ANIMAL**

3 Ransomware

Locks files—typically through encryption—and demands a ransom, usually in the form of digital cryptocurrencies like Bitcoin to unlock them. Paying the ransom doesn't always guarantee data or asset recovery.

First known instance:

AIDS Trojan / PC Cyborg, 1989.

Distributed 20,000 infected floppy disks to researchers globally. Infection stayed dormant for 90 days, activated, then demanded a ransom of $189 to decrypt files.

Prominent examples:

WannaCry **Petya** **DarkSide**

4 Bot/Botnet

A software application or script that performs automated tasks on command. A bot infected by malicious code can become part of a network of infected machines (botnet)—all controlled by a single attacker (bot herder) or attack group. These botnets are often used to launch DDoS attacks against websites, or to host cybercrime infrastructure.

First known instance:

PrettyPark, 1999.

An email attachment that stole information from host computers.

Prominent examples:

Mirai **Earthlink Spammer** **Mariposa**

5 Credential Stealer

A specific form of spyware that resides in an infected computer and gathers credential data to send back to the attacker. Typical targets are credentials used in online banking services, social media sites, email platforms, or SaaS applications.

First known instance:

Melissa, 1999.

A self-replicating worm that spread by sending infected emails to the first 50 contacts in the victim's Microsoft Outlook address book.

Prominent examples:

Azorult **Koobface** **Zeus**

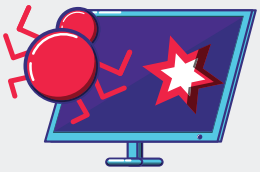
6 Rootkit

Sneaky malware that exploits a privileged process or user to gain root-level (i.e., admin) access, embedding itself in the operating systems or bootloader to stay hidden. Once activated, rootkits open backdoors to spread more malware, like ransomware, bots, keyloggers, or trojans, which infiltrate and move laterally to other systems.

First known instance:

NT Rootkit, 1999.

Infected Windows NT operating systems.



Prominent examples:

Stuxnet **NTRootkit** **Knark**

7 Spyware

Surveils user activity by monitoring screens, capturing keystrokes, and accessing files; even hijacking webcams and microphones. The collected data is sent online or stored locally for threat actors, and may include credentials used to hijack privileged accounts.

First known instance:

Reader Rabbit, 2000.

Educational software sending user data back to Mattel.

Prominent examples:

Pegasus **DarkHotel** **Hawkeye**

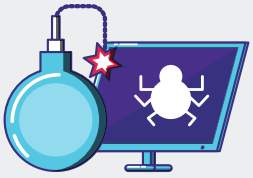
8 Fileless Malware

Operates solely in a computer's memory, leaving no traces on the hard drive, making it difficult to detect. It exploits native tools built into operating systems (living-off-the-land), using legitimate scripting tools like PowerShell to avoid detection. Advanced persistent threats often use fileless malware to stay hidden while progressing an attack over time.

First known instance:

CodeRed, 2001.

Exploited a buffer overrun vulnerability in Microsoft IIS web servers.



Prominent examples:

Frodo **The Dark Avenger** **CodeRed**

9 Adware

Delivers unwanted, and potentially illegal, ads to users. At best, these ads simply generate revenue for the attackers. At worst, they can expose users to further risk by phishing with fake ads or persuading them into downloading additional malicious software.

First known instance:

Gator, 2002.

Pop-up ads are used to trick users into downloading its adware bundle.

Prominent examples:

Gator **Fireball** **Ask Toolbar**

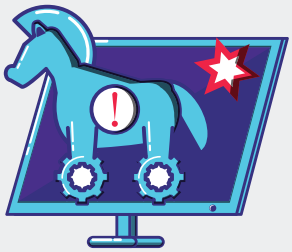
10 Banking Trojan

A spyware variant designed to both collect online banking credentials and hijack sessions to transfer money while the user is logged in to their banking platform. Once exfiltrated to an attacker, this information can be used to steal money and commit other forms of fraud, such as identity theft.

First known instance:

Zeus (ZBOT), 2006.

A trojan malware package that runs on versions of Microsoft Windows. Often used to steal banking information by man-in-the-browser keystroke logging and form-grabbing.



Prominent examples:

Gozi **Zeus (ZBOT)** **Dridex**

11 Wiper

Intends to erase (or "wipe") the hard drive or other static memory of the computer it infects, deleting data and programs. Wipers are generally used by nation states or political threat actors trying to disrupt rival organizations.

First known instance:

Shamoon, 2012.

Targeted Saudi Arabian and Qatari oil companies, destroying over 30,000 computer systems and causing a global spike in the price of hard drives.

Prominent examples:

NotPetya **Sony Pictures Hack** **Shamoon**

Protect Identities, Endpoints, and Data with a Blended Malware Defense from BeyondTrust

BeyondTrust Identity Security and Privileged Access Management (PAM) solutions defend against the most common malware attack vectors, including unsecure remote access pathways and privileged access. Our products also protect against sophisticated edge cases that leverage social engineering, macros, and other vulnerabilities.

Key ways the BeyondTrust platform protects identities, endpoints, and data from modern and legacy malware threats include:

- Removes admin rights and implements least privilege and just-in-time access, preventing malware from executing with privileges that can be used to compromise or move laterally across systems.
- Applies pragmatic application control, including allow lists, block lists, and grey lists, to broadly ensure only access to legitimate, authorized application functionality—and in the right context.
- Implements Trusted Application Protection to defend against tricky fileless threats by applying context to control child processes and DLLs.
- Provides granular, least privilege remote access for vendors and employees, granting full visibility and control over sessions to detect and block the execution of illegitimate applications and malware.
- Manages privileged credentials and accounts, DevOps secrets, and workforce passwords to protect human and machine identities against account hijacking, password reuse attacks, and stolen passwords that could be used by malware.
- Monitors and manages all privileged sessions with the ability to pinpoint anomalous activity and pause, or terminate, an in-progress session compromised by malware.
- Provides visibility over all identities, accounts, and privileges with Identity Security Insights to proactively harden identities against attacks—and detect when they have been targeted by malware.

Contact BeyondTrust to improve your organization's detection of, and resistance to, malware and other threats.

BeyondTrust is the worldwide leader in intelligent identity and access security, enabling organizations to protect identities, stop threats, and deliver dynamic access. We are leading the charge in innovating identity-first security and are trusted by 20,000 customers, including 75 of the Fortune 100, plus a global ecosystem of partners. Learn more at www.beyondtrust.com