

# Internet Worm - What it is, how it spreads, and how to stop it fast

Gridinsoft Help Center

## What it is

An internet worm is self-spreading malware that copies itself across networks without you clicking or installing anything. Unlike a classic virus that needs an infected file to run, a worm exploits bugs and weak settings to move automatically from one device to the next.

## How it spreads - quick tour

- Scans the internet or local network for known vulnerabilities
- Uses default passwords or misconfigurations to slip in
- Drops a loader, then propagates to new targets from the infected host
- Can add payloads like ransomware or cryptominers once inside

## What you may notice

- Sudden network slowdowns or bandwidth spikes
- Services crashing or machines rebooting unexpectedly
- New firewall rules or admin accounts you did not create
- Security alerts about blocked exploit attempts across many hosts

## If it hits - first moves

- Isolate affected systems from the network.
- Patch the exploited vulnerability on all hosts before reconnecting.
- Run a full anti-malware scan and remove persistence tasks or services.
- Rotate admin passwords and keys from a clean machine.
- Review logs to confirm containment and find patient zero.

## Prevent it

- Patch fast on internet-facing apps, VPNs, and OS services
- Disable or restrict unused ports and services
- Enforce strong, unique passwords and MFA for admin access
- Segment networks and apply egress filtering to limit spread
- Use EDR and IDS/IPS to spot scanning and exploitation early
- Keep backups offline and test restores