# Cryptovirology: What it is, why it powers ransomware, and how to defend against it

Gridinsoft Help Center

## What it is

Cryptovirology is the study (and misuse) of cryptography for attacks. Instead of protecting data, it uses strong encryption and crypto tricks to power malware-most famously ransomware that locks files with keys victims can’t guess or brute-force.

## Why it matters

Modern ransomware isn’t "just a virus." It’s math-backed extortion: files are encrypted with solid algorithms, keys are kept off-device, and victims face a pay-or-lose dilemma. The same ideas also enable stealthy data theft and untraceable command channels.

## How it works

- Public-key traps: malware encrypts your files with an attacker’s public key; only their private key can unlock them.

- Key hygiene: keys never live on the victim’s machine, blocking easy recovery.

- Hybrid crypto: fast symmetric ciphers encrypt data; a public key protects those session keys.

- Double extortion: crypto locks files while stolen data is used as leverage.

## Real-world impact

- Strong crypto makes decryption impractical without the attacker’s key.

- Cleanups focus on containment, restore, and hardening, not cracking the cipher.

- Even backups can be threatened if they aren’t offline or immutable.

## Defend smart

- Backups that can’t be altered (offline/immutable) + practiced restore drills.

- MFA everywhere, least privilege, and segmented networks to limit blast radius.

- Patch fast on internet-facing apps; tighten email and web filtering.

- EDR with behavior rules (mass encryption, shadow copy deletion, unusual key use).

- Train teams to spot phishing and fake updates; rehearse incident response.