REvil Ransomware - what it is, how attacks unfold, and how to prevent and respond

Gridinsoft Help Center

What it is

REvil is a high-impact ransomware family run as ransomware-as-a-service (RaaS). The core crew builds the malware and portal, while affiliates break in, steal data, and deploy the encryptor; profits are split between them. REvil uses "double extortion" - it locks files and threatens to leak stolen data to force payment - and it spreads quickly across shared drives and backups. Background and case studies: https://gridinsoft.com/blogs/tag/revil-ransomware/

Why it matters

One foothold can halt operations, expose sensitive data, and trigger breach notifications. Paying is risky, can encourage repeat targeting, and still may not recover everything.

How it works - quick tour

- Entry: phishing, vulnerable VPN/RDP, or exploited apps.
- Prep: disables defenses, enumerates the network, and steals data first.
- Impact: kills backups/shadow copies, encrypts files/shares, drops notes.
- Extort: posts proofs on a leak site and sets a crypto payment deadline.

Red flags

- Sudden shadow-copy deletions and backup failures.
- New admin accounts or PsExec/mini-RDP usage across hosts.
- Many files renamed with a uniform extension plus ransom notes everywhere.
- Outbound traffic to unfamiliar TOR/proxy endpoints during the event.

Prevent it

- Patch exposed services fast; disable or lock down RDP and enforce phishing-resistant MFA.
- Segment networks and use least privilege to slow lateral movement.
- Keep 3-2-1 backups with an offline copy; test restores regularly.
- Block macros from the internet; restrict script interpreters; deploy EDR with ransomware behavior blocks.
- Practice an incident playbook (isolate, preserve logs, notify, restore from clean backups).