Ramnit - what it is, how it spreads, and how to remove it

Gridinsoft Help Center

What it is

Ramnit is a Windows file-infecting worm with trojan capabilities. It can inject itself into EXE and DLL files, add malicious code to HTML pages, and spread via removable drives and network shares. Once established, it deploys backdoors, steals passwords and cookies, and lets attackers control the system for further payloads or data theft. Background and cleanup notes: https://gridinsoft.com/threats/ramnit

Why it matters

A file infector corrupts software across the machine, making recovery harder than removing a single payload. With credential theft and remote control, Ramnit can lead to account takeovers, lateral movement, and reinfection if cleanup is incomplete.

How it works - quick tour

- Entry: drive-by downloads, trojanized installers, or removable media.
- Infect: patches local EXE/DLLs and injects code into HTML to spread further.
- Persist: creates autoruns and contacts command servers for updates.
- Steal and control: harvests credentials and opens a backdoor for operators.

Red flags

- Legitimate executables begin triggering AV as infected or unknown.
- Sudden spikes in detections across many files after a single alert.
- New autoruns pointing to random-named files in AppData or Temp.
- Unusual outbound connections from hosts that previously had none.

Prevent it

- Block untrusted scripts and macros, and disable AutoRun for USB devices.
- Keep OS and browsers patched, and use reputable anti-malware with web filtering.
- If detected, isolate the host, reset credentials from a clean device, and restore software from known-good media.
- Prefer reimage for widespread file infection, then restore documents from clean backups.