G

# GandCrab Ransomware: What it was and how recovery works

What it is GandCrab was a prominent ransomware family and ransomware-as-a-service operation active mainly during 2018 and 2019. Affiliates used the malware to encrypt files and demand cryptocurrency payments, while the core developers...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

## What it is

GandCrab was a prominent ransomware family and ransomware-as-a-service operation active mainly during 2018 and 2019. Affiliates used the malware to encrypt files and demand cryptocurrency payments, while the core developers maintained the platform. Multiple versions appeared, with different extensions, ransom notes, and technical details.

## How it works

Campaigns used phishing attachments, exploit kits, compromised websites, exposed remote services, and malicious downloads. After execution, GandCrab searched local and connected storage for target files, encrypted them, and created a ransom note. Some variants also

attempted to hinder recovery or avoid systems configured for particular regions.

## Key points

- The operators announced retirement, but old infections, archived samples, and copycat claims still appear.
- Correctly identifying the exact variant matters because free decryption options were released for some versions.
- A ransom note name or extension is evidence, but a trusted identification service should confirm the family.

## What to do

- Isolate the computer and disconnect writable backup and network storage.
- Preserve the ransom note and copies of encrypted files before attempting repair.
- Check reputable decryptor projects for the confirmed variant and work only on duplicate data.
- Remove the infection or rebuild the system before restoring clean backups.