G

GandCrab Ransomware: Identification and Decryption

GandCrab was a major ransomware-as-a-service family active mainly in 2018–2019. Learn how to identify a suspected version, preserve the ransom note, check official decryptor compatibility, and recover safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How to recognize a possible GandCrab infection
02 How GandCrab spread
03 Is free GandCrab decryption available?
04 Safe recovery process
05 Avoid recovery scams
06 Should you pay?
07 Frequently asked questions

GandCrab was a prominent ransomware family and ransomware-as-a-service operation active mainly in 2018 and 2019. Its developers maintained the malware and payment infrastructure while affiliates distributed it and shared the proceeds. Multiple versions

changed encryption, ransom-note names, file extensions, and delivery methods.

The operators announced retirement in 2019, but old encrypted drives, archived samples, misidentifications, and fraudulent “recovery” offers still appear. A current detection using the name GandCrab does not by itself prove a new campaign.

01 How to recognize a possible GandCrab infection

Evidence varies by version:

Version group	Common clue	Caution
Version 1	`.GDCB` extension and a GandCrab note	Extension alone can be copied by another program
Versions 2–3	`.GDCB` or `.CRAB` in documented samples	Decryptor support differs by version
Version 4	`.KRAB` and a version-specific note	Preserve the note before cleanup
Version 5 family	Random-looking uppercase extension and an HTML or text note	The random extension is not a universal identifier

Do not rename encrypted files or assume a version from one clue. Preserve the ransom note, a small set of encrypted files and any matching originals, security logs, file timestamps, and the detected executable if your incident procedure permits it. Use a reputable ransomware identification service or qualified responder.

02 How GandCrab spread

Documented campaigns used phishing, exploit kits, malicious downloads, compromised websites, exposed remote services, and other malware. After execution, the ransomware enumerated reachable data, encrypted selected files, and created payment instructions. Some versions attempted to interfere with recovery. The initial-access method must be investigated separately; removing the encryptor does not close a stolen account or vulnerable service.

03 Is free GandCrab decryption available?

Law-enforcement and security partners released free GandCrab decryptors through the **No More Ransom** initiative. Europol reported a widely applicable recovery tool, but compatibility still depends on the exact variant and available artifacts. Official instructions for the tool identify supported version groups and may require at least one intact ransom note to recover the needed information.

Do not interpret “universal” as a promise for every damaged file or every sample calling itself GandCrab. Work on copies, read the current tool documentation, and retain the originals in case a later method becomes available.

04 Safe recovery process

1. **Isolate affected systems** and disconnect writable network shares and backup media.
2. **Preserve evidence** before antivirus cleanup: note, extensions, encrypted samples, first affected host, logs, and suspicious files.
3. **Determine scope and entry point.** Review email, web, remote-access, identity, endpoint, firewall, and server logs.
4. **Remove attacker access.** Disable compromised accounts, patch exposed services, rotate credentials and tokens, and hunt for other payloads.
5. **Check an official decryptor.** Reach No More Ransom through its known domain, verify the family and supported version, and test duplicate files first.
6. **Rebuild compromised hosts** before restoring verified data. Do not restore into an environment where the attacker or malware remains active.
7. **Monitor recovery** for recurring access, malicious email, new encryption, or unexpected data transfer.

05 Avoid recovery scams

- Do not upload sensitive files or ransom notes to an unknown “specialist.”
- Do not run a decryptor delivered through an advertisement, chat message, or newly registered site.
- Ask any provider to disclose whether it will simply pay the attacker while charging a markup.
- Verify tool signatures and download instructions from No More Ransom or the named security vendor.
- Keep untouched encrypted originals and record every recovery action.

06 Should you pay?

Payment does not guarantee a working key, safe software, complete restoration, deletion of stolen data, or protection from another demand. It can also create legal or sanctions concerns. Follow law-enforcement, insurer, legal, and regulatory guidance applicable to the incident. CISA’s general position is to focus on containment, reporting, clean restoration, and improved resilience.

07 Frequently asked questions

Can antivirus decrypt GandCrab files?

Antivirus can remove detected malware but does not automatically reverse encryption. Recovery requires a compatible decryptor, clean backup, or another validated method.

Should I delete the ransom note?

No. Official GandCrab recovery instructions may use information from the note. Preserve it with encrypted samples before cleanup.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com