C

Cerber Ransomware: Identification, Containment, and Recovery

Cerber is a historic ransomware family with many variants. Learn why filenames alone are insufficient, how to contain an incident, and how to assess recovery options.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What is Cerber ransomware?
02 How an infection may appear
03 Immediate response
04 Can Cerber files be decrypted?
05 Removal and recovery
06 Prevention
07 Frequently asked questions

Quick answer: Cerber is a ransomware family that became widespread in 2016 through ransomware-as-a-service campaigns. It encrypted files, changed their names or extensions, and left payment instructions, sometimes with an audio message. Because variants changed over time, identify the exact sample before attempting decryption. Isolate affected devices, preserve evidence, close the entry path, and restore from verified clean backups.

01 What is Cerber ransomware?

Cerber was offered to affiliates who distributed the malware while sharing payments with its operators. Campaigns used malicious email attachments, downloader scripts, and exploit kits that targeted vulnerable browsers or plug-ins. Different affiliates and versions produced different delivery chains and visible indicators.

Historic reports describe extensions such as `.cerber`, `.cerber2`, and `.cerber3`, as well as later randomized extensions. Ransom notes and filenames also changed. These artifacts are useful clues but are not enough to identify a current incident because unrelated malware can copy names and extensions.

02 How an infection may appear

- Documents, photos, databases, or other files become unreadable and receive changed names or extensions.
- HTML, text, or image ransom notes appear in multiple directories.
- A synthetic voice or audio file announces that files were encrypted in some variants.
- One endpoint rapidly modifies local files and writable network shares.
- Email, browser, script, or process telemetry shows an earlier downloader or exploit.

Preserve the ransom note, several encrypted files, an original copy of the same file if available, suspicious executables, process trees, email, browser history, and security logs. Record timestamps and extensions before renaming anything.

03 Immediate response

1. **Isolate affected devices.** Disconnect network access or use endpoint isolation to stop access to shared storage.
2. **Protect clean backups.** Prevent compromised accounts and hosts from reaching backup repositories without deleting recovery points.
3. **Disable confirmed compromised accounts.** Revoke sessions and rotate credentials from a trusted device.
4. **Find the delivery path.** Review email attachments, downloads, exposed services, browser exploitation, and administrator activity.
5. **Hunt for related activity.** Search other systems for the same file, process, account, note, destination, and preceding downloader.

Do not begin by deleting every artifact. Representative evidence helps distinguish Cerber from another family and determines whether data theft or additional malware occurred. Historic Cerber is best known for encryption, but a compromised host may contain unrelated stealers or backdoors from the same access chain.

04 Can Cerber files be decrypted?

There is no universal decryptor for every Cerber version. Some tools support specific early variants or particular circumstances. Search the No More Ransom decryption tools repository and read the supported-version details carefully. Work on copies, preserve untouched encrypted originals, and verify output before applying any tool broadly.

A website claiming to decrypt “all Cerber versions” should be treated skeptically. Fake recovery utilities can install more malware or charge for freely available software. Use recognized security vendors, national cyber authorities, or an experienced incident-response provider. Paying does not guarantee a valid key, safe software, complete restoration, or lawful processing.

05 Removal and recovery

1. Determine the earliest malicious activity and all affected identities, endpoints, servers, and shares.
2. Remove persistence and close the entry path. Patch exploited software and secure remote or email access.
3. Reimage systems when administrative compromise, additional payloads, or uncertain integrity makes cleaning unreliable.
4. Restore prioritized data from offline or immutable backups created before the intrusion.
5. Validate restored files and applications in an isolated environment, then reconnect systems in stages.
6. Monitor for renewed access, new encryption, or use of stolen credentials.

File decryption and malware removal solve different problems. A decryptor may restore data but leave the original loader or stolen account active. An antivirus may remove a payload but cannot reverse encryption automatically.

06 Prevention

Filter executable and script attachments, block or constrain internet-origin macros, and analyze suspicious archives and links. Patch browsers, operating systems, and exposed applications; remove unsupported plug-ins. Use application control and least privilege so ordinary users cannot run unapproved scripts or disable protection.

Segment workstations from critical file servers, limit share permissions, and alert when one account changes many files quickly. Maintain offline or immutable backups under separate credentials and test restoration. Phishing-resistant MFA and secure remote access reduce the value of stolen passwords, although they do not replace endpoint controls.

07 Frequently asked questions

Does a .cerber extension prove Cerber infection?

No. Use the extension as one clue and confirm with the note, sample, process behavior, and reputable identification tools.

Should encrypted files be deleted?

No. Keep protected copies because a supported key or improved recovery method may become available later.

Can I restore immediately after the ransom note appears?

Restore only after isolating the incident, closing attacker access, and verifying that the recovery environment and backups are clean.

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