C

CTB-Locker Ransomware: Identification, Response, and Recovery

Learn what the historical CTB-Locker ransomware was, how to avoid confusing it with copycats, and how to preserve evidence and assess recovery options.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What is CTB-Locker ransomware?
02 How CTB-Locker attacks worked
03 How to identify the exact ransomware family
04 Immediate response steps
05 Can CTB-Locker files be decrypted?
06 Why removing malware does not decrypt files
07 Safe recovery process
08 Preventing similar attacks

CTB-Locker is a historical crypto-ransomware family associated with campaigns that encrypted files and directed victims to payment instructions through the Tor network. Its name has been expanded as “Curve-Tor-Bitcoin,” referring to its use of elliptic-curve cryptography, Tor-based infrastructure, and Bitcoin demands.

A ransom note that uses the CTB-Locker name does not prove the original family is responsible. Copycats can imitate names, extensions, and payment pages, so recovery must start with evidence-based identification.

01 What is CTB-Locker ransomware?

CTB-Locker, also called Critroni in historical reporting, is file-encrypting ransomware that appeared in the 2010s. It is crypto-ransomware rather than screen-locking ransomware: its main effect is transforming selected files so they cannot be opened without the correct key. The family name is now historical, but current ransom notes may reuse it inaccurately.

02 How CTB-Locker attacks worked

Historical campaigns commonly used malicious email attachments or downloaders. Once executed, the ransomware searched for selected files, encrypted them, changed filenames or extensions, and presented a deadline. Later campaigns and unrelated imitators may use different delivery, persistence, and encryption methods.

Modern ransomware response should also consider credential theft, lateral movement, backup access, and data exfiltration even if the visible symptom is file encryption.

03 How to identify the exact ransomware family

Preserve the ransom note, several small encrypted files, the original malicious message, suspicious executables, and relevant logs. Analysts compare note text, filenames, encrypted-file headers, extensions, contact details, payment instructions, process behavior, and malware hashes. An extension alone is not a reliable identifier.

Do not rename files or test random “CTB decryptors” on the only copy. Some tools target a copycat rather than the original CTB-Locker.

04 Immediate response steps

1. Disconnect affected systems from networks and shared storage where safe.
2. Protect unaffected backups, identity systems, and administration tools.
3. Record the time, symptoms, ransom note, logged-in user, and recent activity.
4. Preserve volatile and disk evidence before rebuilding.
5. Notify the incident-response team and appropriate authorities.

05 Can CTB-Locker files be decrypted?

There is no universal ransomware decryptor. A legitimate tool must match the specific variant and encryption implementation. Consult established public-private ransomware resources, law enforcement, or a qualified incident-response provider. Work on copies and keep the original encrypted data; future key recovery or a cryptographic flaw may change the options.

06 Why removing malware does not decrypt files

Security software may stop the ransomware process or remove its persistence, but encrypted content remains mathematically transformed. Conversely, restoring files without removing the attacker’s access can lead to immediate reinfection. Containment, eradication, and data recovery are separate phases.

07 Safe recovery process

Determine the entry point and scope, rebuild compromised systems from known-good sources, rotate exposed credentials and tokens, and restore only verified clean data. Keep recovered systems isolated until monitoring and security controls are active. Test critical applications and

permissions rather than checking only whether files open.

08 Preventing similar attacks

- Patch Internet-facing and known-exploited vulnerabilities promptly.
- Require phishing-resistant MFA for email, remote access, and administrators.
- Restrict scripts, macros, executable attachments, and remote-management tools.
- Segment important systems and use least privilege.
- Maintain offline or immutable backups with separate credentials.
- Practice the broader ransomware response plan.

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