C

CryptoLocker Ransomware: History, Identification, and Recovery

Learn what the original CryptoLocker was, how to distinguish a historical family name from modern copycats, and how to respond to encrypted files safely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What is CryptoLocker?
02 How the original CryptoLocker worked
03 CryptoLocker vs. modern copycats
04 What to do immediately
05 Can CryptoLocker files be decrypted?
06 Should you pay the ransom?
07 Safe recovery process
08 How to prevent similar ransomware attacks

CryptoLocker was a ransomware family that became widely known in 2013–2014 for encrypting victims' files and demanding payment. Law-enforcement action disrupted the original operation, but criminals continue to reuse the CryptoLocker name in ransom

notes, file extensions, websites, and misleading “recovery” offers.

A note that says CryptoLocker does not prove the original malware is involved. Correct identification matters because each ransomware family can use different encryption, keys, persistence, and recovery options.

01 What is CryptoLocker?

The name **CryptoLocker** properly refers to the historical ransomware operation disrupted in 2014, not to every program that encrypts files for ransom. It is now also used informally—and sometimes incorrectly—as a generic label for crypto-ransomware. When responding to a current incident, identify the actual family or variant before selecting removal or recovery instructions.

02 How the original CryptoLocker worked

The original campaign commonly arrived through malicious attachments and botnet activity. After execution, it contacted attacker-controlled infrastructure, encrypted selected files using public-key cryptography, and displayed a deadline for payment. The private key needed for decryption was not normally stored on the victim’s computer.

Modern ransomware operations often add credential theft, network-wide deployment, backup destruction, and data extortion. Those behaviors should not automatically be attributed to the historical CryptoLocker family.

03 CryptoLocker vs. modern copycats

Attackers can choose any name for a ransom note. File extensions and wallpaper are also easy to imitate. Analysts identify ransomware using multiple artifacts: the note filename and text, encrypted-file format, extension, malware hash, process behavior, contact address, payment instructions, and reliable threat intelligence.

Do not rename encrypted files or run random decryptors merely because a search result mentions the same extension.

04 What to do immediately

1. Disconnect affected systems from wired, wireless, and shared storage where safe to do so.
2. Preserve the ransom note, several encrypted files, suspicious emails, logs, and timestamps.
3. Protect unaffected backups, identity systems, and management tools.
4. Notify the organization’s incident-response team or obtain qualified assistance.
5. Report the incident through appropriate national law-enforcement or cybersecurity channels.

Avoid wiping or reinstalling before evidence and the scope of the intrusion are understood.

05 Can CryptoLocker files be decrypted?

Some historical ransomware keys or family-specific decryptors have been recovered, but there is no universal ransomware decryptor. A legitimate tool must match the exact variant. Use established public-private initiatives, law-enforcement resources, or a trusted incident-response provider. Work on copies and preserve original encrypted files in case a safe recovery method becomes available later.

Removing the ransomware stops its program from running but does not decrypt files it already changed. Recovery requires a matching decryptor, clean backup, or another family-specific method; anyone promising guaranteed recovery without first identifying the variant should be treated cautiously.

06 Should you pay the ransom?

The FBI and other authorities discourage ransom payments because payment does not guarantee recovery or deletion of stolen data and may encourage further crime. It can also create sanctions, legal, insurance, or reporting issues. An organization should involve executive, legal, law-enforcement, insurance, and incident-response stakeholders rather than letting one administrator decide under pressure.

07 Safe recovery process

Determine the initial access method, remove attacker persistence, rebuild compromised systems from known-good media, and rotate exposed passwords, tokens, and keys. Restore clean data only after the environment is contained. Monitor restored systems for renewed access and keep encrypted evidence separate from production.

08 How to prevent similar ransomware attacks

- Patch Internet-facing and known-exploited vulnerabilities quickly.
- Require phishing-resistant MFA for email, remote access, and administrators.
- Block unneeded executable attachments and restrict scripts and macros.
- Use least privilege and segment critical systems.
- Maintain offline or immutable, separately administered backups.
- Practice the response and restoration plan.

For current attacks, follow the broader ransomware response and recovery guide rather than assuming the incident is the original CryptoLocker.

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