T

TeslaCrypt Ransomware: Identification, Free Decryption, and Recovery

TeslaCrypt is a historical ransomware family whose operators released the master key. Learn how to identify a supported variant and use a reputable decryptor without risking the originals.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How to identify TeslaCrypt
02 How TeslaCrypt reached computers
03 Is there a free TeslaCrypt decryptor?
04 What not to do
05 Frequently asked questions

TeslaCrypt is a ransomware family first observed in 2015. Early campaigns focused heavily on game saves and related files, while later variants encrypted documents, photos, databases, and other common data. The operation shut down in 2016 and released a master decryption key, which means many correctly identified TeslaCrypt

infections can be recovered with a reputable free decryptor.

Recovery outlook: TeslaCrypt is one of the ransomware families for which free decryption is often possible. Confirm the family and variant first, preserve the originals, and obtain the tool from a recognized security organization rather than a download video or forum comment.

01 How to identify TeslaCrypt

No single clue is conclusive. Use a combination of the ransom note, encrypted-file structure, extension, malware sample, and a trusted ransomware identification service. TeslaCrypt changed repeatedly during its lifetime.

Clue	What it may indicate	Limit
Extensions such as .ecc, .ezz, .exx, .xyz, .zzz, .aaa, .abc, .ccc, or .vvv	Seen in different TeslaCrypt generations	Extensions can be copied by unrelated malware
No added extension	Some later TeslaCrypt versions retained original names	A normal filename does not mean the contents are intact
HTML or text ransom instructions	Can provide campaign and payment-site details	Names and templates can be reused
Encrypted file plus clean original	Helps specialists validate a family and recovery result	Do not send confidential files to an untrusted service

TeslaCrypt originally drew attention for targeting data associated with games, but it should not be described only as “game ransomware.” Later versions covered a much wider set of file types.

02 How TeslaCrypt reached computers

Historical campaigns used exploit kits on compromised sites, malicious advertising, deceptive downloads, and email-based delivery. After execution, the malware searched local and connected storage for targeted files, encrypted their contents, and displayed payment instructions. Some versions attempted to interfere with local recovery options such as Windows shadow copies.

Because the malware is historical, a TeslaCrypt-like discovery today may come from an old disk, archived backup, previously disconnected system, or a misidentified newer family. Do not assume the infection time from the family name alone.

03 Is there a free TeslaCrypt decryptor?

Yes, reputable security organizations published TeslaCrypt recovery tools, and the operators' released master key expanded recovery coverage. Support still depends on correct identification and the condition of the files. A decryptor removes encryption from supported data; it does not remove malware, repair damaged storage, or prove that another threat is absent.

Safe decryption workflow

1. **Isolate the affected device.** Disconnect network shares and removable storage to prevent further writes.
2. **Preserve evidence.** Keep the ransom note, several encrypted files of different types, suspicious executables, and relevant logs.
3. **Create a separate copy.** Never test a decryptor on the only copy of encrypted data. Preserve the original disk or files unchanged.
4. **Confirm TeslaCrypt.** Use a trusted identification service or qualified responder. The extension alone is insufficient.
5. **Remove the infection or rebuild.** Decryption should occur in a controlled environment, not while the ransomware may still be active.
6. **Download a recognized tool.** Use a security vendor or established anti-ransomware initiative and verify the publisher or signature.
7. **Test a small sample.** Check that recovered documents open correctly before processing the entire copy.
8. **Restore clean data.** Prefer a verified offline backup when it is newer and complete.

04 What not to do

- Do not rename extensions in the hope that files will become readable; encryption changes the contents, not only the name.
- Do not delete the ransom note or every suspicious file before collecting evidence needed for identification.
- Do not install an unknown “TeslaCrypt decoder” from an advertisement, comment, or file-sharing site.
- Do not restore a backup onto a system that has not been cleaned or rebuilt.

05 Frequently asked questions

Does the released master key recover every file?

It enables broad recovery, but not every damaged, partially overwritten, or incorrectly identified file is guaranteed to decrypt. Always test copies and keep the originals.

Can TeslaCrypt still spread today?

The original operation is inactive, but old samples and compromised archives can still execute. Modern patched systems and current security controls reduce the historical delivery routes, but unknown executables should still be handled cautiously.

Should I pay a TeslaCrypt ransom?

No active legitimate TeslaCrypt payment service is needed for supported variants, and criminals or impersonators may exploit victims searching for help. Start with verified backups and reputable free recovery resources.

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