T

TeslaCrypt Ransomware: File encryption, variants, and recovery

What it is TeslaCrypt was a ransomware family first observed in 2015. Early versions emphasized files associated with computer games, including saves and custom content, while later variants encrypted a broader range of documents and...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

TeslaCrypt was a ransomware family first observed in 2015. Early versions emphasized files associated with computer games, including saves and custom content, while later variants encrypted a broader range of documents and personal data. The malware displayed a ransom demand after making files inaccessible.

How it works

Campaigns used exploit kits, compromised websites, malicious advertising, and deceptive downloads. Variant details changed over time, including extensions and cryptographic implementation. In 2016, the operators shut down their service and released a master decryption

key, enabling reputable security researchers to provide a free recovery tool for supported TeslaCrypt infections.

Key points

- A free decryptor helps only when the family is correctly identified and files have not been damaged by another process.
- Random tools advertised through comments or videos can corrupt data or install more malware.
- An old ransomware family can still appear in archived disks, old backups, or misclassified modern incidents.

What to do

- Isolate the device and preserve the ransom note and sample encrypted files.
- Confirm the family with a reputable identification service before using a decryptor.
- Work on copies of encrypted data and keep the originals unchanged.
- Remove or rebuild the infected system before restoring clean files and backups.