L

Locky Ransomware: How it spread and how to recover safely

What it is Locky is a ransomware family that became widespread in 2016 through large malicious-email campaigns. It encrypted documents and other valuable files on local and connected storage, changed filenames or extensions in different...

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
1 min

What it is

Locky is a ransomware family that became widespread in 2016 through large malicious-email campaigns. It encrypted documents and other valuable files on local and connected storage, changed filenames or extensions in different variants, and displayed a ransom note directing victims toward cryptocurrency payment sites.

How it works

Many infections began with an invoice or other business lure carrying a Word document with malicious macros, a JavaScript file, or an archive. Opening or enabling active content started a downloader, which retrieved Locky. The ransomware then searched mapped drives and shares,

encrypted matching files, and attempted to interfere with local recovery options.

Key points

- Locky is an older family, but archived samples and mislabeled incidents can still be encountered.
- The extension changed across variants, so identification should use the ransom note and technical evidence together.
- Connected backups and writable network shares can be encrypted from the compromised account.

What to do

- Disconnect affected hosts and shared storage to stop further file access.
- Preserve the ransom note, sample files, and email that delivered the payload.
- Remove or rebuild the infected system before restoring from an offline, tested backup.
- Disable unnecessary macros and filter script attachments to prevent similar delivery chains.