L

Locky Ransomware: Identification, Containment, and Recovery

Locky caused major email-driven ransomware outbreaks beginning in 2016. Learn how it was delivered, how to preserve evidence, and how to assess recovery safely.

PUBLISHER
Gridinsoft Support

UPDATED
Sep 1, 2026

READ TIME
4 min

CONTENTS

In this guide

Quick answer: Locky is a ransomware family that caused large malicious-email campaigns beginning in 2016. Typical chains used an attachment or link to start a downloader, then encrypted local and writable network files and left payment instructions. Many variants and copycats used different extensions and notes, so identify the exact sample before considering a decryptor. Isolate the device and preserve encrypted files and evidence.

01 What is Locky ransomware?

Locky was distributed at high volume through spam, often using Word documents with malicious macros, JavaScript attachments, archives, or links. The initial content normally required the user to open it and, in some campaigns, enable macros. A downloader retrieved the ransomware, which contacted campaign infrastructure and began encryption.

The ecosystem and infrastructure changed over time. Historical reporting linked major waves with the Necurs botnet, but one old sender, hash, domain, or delivery technique does not define every Locky infection.

02 Variants and visible clues

Locky-related campaigns used names and extensions such as Locky, Zepto, Odin, Thor, Aesir, Diablo6, and Lukitus. Ransom notes and desktop backgrounds also changed. Extensions are useful for initial triage but can be copied by unrelated ransomware.

Preserve the note, several encrypted files, an original version of one file when available, the attachment or downloaded payload, email headers, and endpoint logs. Use a reputable ransomware identification service and security-vendor analysis to confirm the family and variant.

03 What happens during infection

1. A malicious document, script, link, or archive reaches the user.
2. User action or a vulnerable component launches a script or downloader.

3. The payload starts, gathers system information, and may contact command infrastructure.
4. Files on fixed, removable, and accessible network locations are encrypted according to the variant.
5. Names or extensions change and ransom instructions appear.

The ransomware may delete local recovery artifacts where permissions allow. Other malware in the delivery chain can steal credentials or provide access, so the incident should not be scoped only to encrypted files.

04 Immediate containment

1. **Disconnect the affected host.** Use managed isolation or remove network access to stop encryption of shares.
2. **Protect backups.** Prevent compromised accounts and systems from reaching recovery repositories.
3. **Preserve evidence.** Keep the original email, attachment, ransom note, payload, encrypted samples, process data, and security logs.
4. **Find other recipients.** Search mailboxes, gateways, endpoints, and downloads for the same campaign.
5. **Protect credentials.** Reset exposed accounts and revoke sessions from a clean device if the delivery chain or attacker had credential access.

05 Can Locky files be decrypted?

There is no universal recovery tool for every Locky variant. Do not assume that a tool for PyLocky, a similarly named family, or one old extension supports original Locky. Check the No More Ransom repository and the tool vendor’s supported variants. Work on copies and preserve untouched originals.

Fake decryptors and recovery services may install malware, resell free tools, or make unsupported promises. Payment does not guarantee a working key, complete recovery, or lawful processing.

06 Recovery workflow

1. Identify the earliest malicious activity, delivery path, and all affected systems and accounts.
2. Remove the downloader, ransomware, persistence, and other payloads; close the access path.
3. Reimage compromised systems from trusted media when integrity is uncertain.
4. Restore prioritized data from offline, immutable, or verified clean backups.
5. Validate applications and files in a segmented environment before reconnecting.
6. Monitor for repeated delivery, account use, or encryption.

Antivirus removal does not decrypt data, and file restoration does not prove the attacker is gone. Complete both security eradication and business recovery.

07 Prevention

Block executable and script attachments that the business does not need, scan archives, and detonate suspicious content in a controlled sandbox. Disable internet-origin macros by policy and train users not to enable content in unexpected documents. Patch operating systems, browsers, and document software.

Use application allow-listing, least privilege, network segmentation, and narrow share permissions. Alert on one process or account changing many files quickly. Maintain offline or immutable backups under separate credentials and test restoration.

08 Frequently asked questions

Does a .locky extension prove Locky?

No. Confirm with the note, payload, behavior, and reputable identification sources.

Is Locky the same as LockBit?

No. They are separate ransomware families and operations from different periods.

Should I delete encrypted files after restoring?

Keep protected samples until identification, legal, insurance, and recovery needs are complete; future recovery options may improve.

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