GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

D

STOP/Djvu Ransomware: Identification, Decryption, and Recovery

A realistic STOP/Djvu recovery guide covering identification, online and offline encryption keys, the Emsisoft decryptor, backups, and credential theft risk.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	4 min

STOP/Djvu is a long-running Windows ransomware family associated with many four-letter file extensions and ransom notes commonly named `_readme.txt`. It has often spread through cracks, key generators, fake activators, and unofficial software downloads. The same installer may also deliver password stealers, so recovery is not only a file-decryption problem.

Do not assume that every file with a particular extension is STOP/Djvu. Identify the ransomware from the ransom note, encrypted-file samples, detection results, and the personal ID shown in the note or system files.

First steps after a STOP/Djvu infection

1. **Disconnect the affected computer.** Unplug external drives and network shares to prevent further encryption or synchronization of damaged files.

2. **Preserve evidence.** Save a copy of the ransom note, several encrypted files, their original filenames and extensions, and the personal ID. Keep the suspected installer if it can be handled safely.

3. **Do not rename or edit encrypted originals.** Make copies before testing any decryptor or repair technique. An unsupported tool can damage the only recoverable copy.

4. **Remove the infection before restoring data.** Scan the system from a trusted environment and check for stealers and other payloads. Reinstall Windows when system integrity cannot be established.

5. **Secure exposed accounts from a clean device.** Revoke sessions and change passwords used on the infected PC, beginning with email, browsers, password managers, financial services, and work accounts.

Online key vs. offline key: why it matters

Newer STOP/Djvu variants normally try to obtain a unique **online key** from attacker infrastructure. That key is different for each victim and is not available to a public decryptor unless it is later recovered or released.

If the malware cannot reach its server, some variants use an **offline key** shared among victims of that variant. Emsisoft's decryptor can recover files only when it supports the variant and the required offline key is known. An ID ending in `t1` has historically indicated an offline ID, but let the current decryptor evaluate the files rather than relying on the suffix alone.

A message such as “No key for New Variant online ID” means that the current tool cannot decrypt those files with the information available. It does not mean the decryptor is broken, and it does not justify trying random keys.

How to use the official Emsisoft decryptor safely

1. Download the current Emsisoft Decryptor for STOP/Djvu from Emsisoft's official site.

2. Work on copies of encrypted files, not your only originals.

3. Read the result for each file. “Decrypted,” “offline key not yet available,” and “online ID” have different meanings.
4. Verify that recovered files open correctly before deleting any encrypted copy.

Older pre-August-2019 Djvu variants used a different scheme. Emsisoft documents a limited known-plaintext approach for some old variants, which requires an original/encrypted file pair. That method does not unlock modern STOP/Djvu infections.

Recovery options when decryption is unavailable

- **Offline or versioned backups:** restore only after the ransomware has been removed. Confirm that backup versions predate the infection.
- **Cloud version history:** some services retain older versions or deleted files. Pause synchronization first and contact the provider if necessary.
- **Previous versions and snapshots:** check them, but ransomware often deletes local shadow copies.
- **File carving:** recovery from unused disk space may help in limited cases, especially if originals were deleted, but SSD TRIM and continued use reduce the chances.
- **Partial media repair:** a few large audio or video files may retain unencrypted data, but repair is format-specific and does not recover documents generally.

Keep an offline copy of encrypted data if it is valuable. A key or improved tool may become available later, but there is no guarantee.

Should you pay the ransom?

Payment does not guarantee a working key, complete recovery, or deletion of stolen data, and it funds further crime. For an organization, any decision must involve leadership, legal counsel, insurers, and law enforcement and account for applicable sanctions rules. Consumers should first use trusted identification resources such as No More Ransom.

STOP/Djvu FAQ

Can I remove the extension to decrypt a file?

No. Renaming changes only the filename; the contents remain encrypted.

Can a different antivirus decrypt the files?

Antivirus can remove active malware, but decryption requires the correct cryptographic key or a flaw in the ransomware.

Why must I change passwords?

STOP/Djvu installers have frequently been paired with information stealers. Assume browser passwords and active sessions may be exposed until investigation shows otherwise.

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