P

Pseudoransomware: Fake Encryption, Wipers, and Response

Pseudoransomware imitates ransomware while files may be untouched, irreversibly damaged, or wiped. Identification is essential before recovery decisions.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 Three situations that look like ransomware
02 Why correct identification matters
03 Evidence to preserve
04 Immediate response
05 Should a victim pay?
06 Prevention
07 Sources

Quick answer: Pseudoransomware is a descriptive term for malware or a scam that looks like ransomware but does not provide the normal technical possibility of restoring data with an attacker-held decryption key. Files may be untouched behind a fake lock screen, encrypted with a key that was never saved, corrupted, or deliberately wiped.

01 Three situations that look like ransomware

- **Fake lock or scare message:** a full-screen warning claims files are encrypted, but the data remains accessible after removing the blocker.
- **Destructive encryption:** files are transformed with random or discarded keys, so the attacker cannot provide working decryption even if paid.
- **Wiper disguised as ransomware:** disk structures, files, or systems are overwritten while a ransom note creates cover or confusion.

These differ from conventional ransomware, where operators intend to exchange a decryption capability for payment, and from pure data-extortion attacks that steal information without encrypting it. Real incidents can combine theft, encryption, wiping, and false claims.

02 Why correct identification matters

Paying cannot recover data when no usable key exists, but assuming every incident is a wiper can cause responders to abandon valid recovery options. A lock screen alone does not prove encryption, and changed extensions do not prove files were cryptographically transformed. Analysis should determine what operations occurred on representative copies.

CISA documented destructive malware such as WhisperGate that was disguised as ransomware. Microsoft’s 2026 GigaWiper research describes destructive modules including fake ransomware and encryption with randomly generated keys that were never saved. The underlying behavior, not the ransom-note wording, determines recoverability.

03 Evidence to preserve

- The ransom note, contact details, wallet addresses, filenames, extensions, and timestamps.
- Memory, running processes, command lines, scheduled tasks, logs, network connections, and security alerts.
- Copies of affected and unaffected files, disk metadata, backups, cloud versions, and snapshots.
- The initial message, download, vulnerable service, compromised account, and evidence of data exfiltration.

Do not run an unknown “decryptor” on original evidence. Work from forensic copies and obtain tools from recognized law-enforcement, security-vendor, or trusted incident-response sources.

04 Immediate response

1. Isolate affected systems and network segments. Stop automated synchronization that could propagate damaged files, while preserving evidence.
2. Activate the incident-response team and determine scope, initial access, privileged identities, lateral movement, and whether data left the environment.
3. Protect backups and management systems with separate credentials. Verify that clean restore points predate the intrusion.
4. Identify the malware through trusted analysis and consult law enforcement or established response partners about known recovery options.
5. Rebuild systems from trusted media and restore validated data only after closing the entry path and removing persistence.

05 Should a victim pay?

Payment provides no technical guarantee, and pseudoransomware operators may be unable to restore anything. It can also create legal, sanctions, insurance, and further-extortion risks. Organizations should involve leadership, legal counsel, insurers, law enforcement, and incident-response specialists rather than negotiating from the affected machine.

06 Prevention

Maintain offline or otherwise protected backups and test full restoration. Segment networks, restrict administrative tools, patch internet-facing services, use phishing-resistant MFA, monitor destructive disk and file behavior, and protect backup credentials. Practice scenarios where recovery keys do not exist and where data theft occurred before destruction.

07 Sources

Response guidance follows the CISA StopRansomware Guide. Destructive malware disguised as ransomware is documented in the CISA/FBI Ukraine advisory.

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