C

Crysis (Dharma) Ransomware: Identification and Recovery

Crysis, also called Dharma, is a long-running ransomware family with many variants. Learn how to identify an incident, contain it, and evaluate recovery.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
5 min

CONTENTS

In this guide

01 Are Crysis and Dharma the same?

02 How Dharma infections commonly happen

03 Signs of a possible incident

04 Immediate containment

05 Can Crysis or Dharma files be decrypted?

06 Recovery process

07 Prevention

08 Frequently asked questions

Quick answer: Crysis, commonly called Dharma, is a long-running Windows ransomware family with many variants. It has frequently been delivered through compromised Remote Desktop Protocol (RDP) access, but phishing and disguised installers have also been reported. Do not identify it from a filename extension alone: preserve the ransom note and sample, use a reputable identification service, and confirm whether a decryptor supports the exact variant.

01 Are Crysis and Dharma the same?

Dharma is generally treated as a later branch or name within the Crysis family, and reports may also use names such as CrySiS or Wadhrama. The family has evolved over years, with changing extensions, contact addresses, notes, and keys. Those visible details help classification but are not unique enough to prove identity by themselves.

A typical encrypted filename may include a victim identifier, attacker contact address, and variant-specific extension. However, extensions can be copied by unrelated malware, and different Dharma variants can use different cryptographic material. Advice that works for one early variant may not work for a newer one.

02 How Dharma infections commonly happen

Exposed RDP has been a recurring access route. Attackers may brute-force weak passwords, use credentials stolen elsewhere, or take advantage of poorly protected remote access. After logging in, they can disable defenses, map shares, copy tools, and run ransomware with administrative privileges. Unit 42's Dharma threat assessment also documents phishing attachments and installers disguised as legitimate software.

That history does not prove RDP was used in every incident. Authentication logs, firewall/VPN records, endpoint telemetry, email evidence, and process history should determine the real entry path.

03 Signs of a possible incident

- Files suddenly receive unfamiliar extensions or cannot be opened.
- Ransom notes appear on desktops or in affected directories and contain a victim ID or contact address.
- Many files are modified rapidly by one process or account across local and network storage.
- Unrecognized RDP logons, new administrators, security exclusions, or tools appear before encryption.
- Backup services, shadow copies, or security processes are stopped unexpectedly.

Preserve the note as a file and screenshot, several encrypted files, an original copy of the same file if available, suspicious executables, and relevant logs. Do not rename encrypted files or run random “decryptors” from search advertisements; fraudulent recovery tools can add malware or damage evidence.

04 Immediate containment

1. **Disconnect affected machines and shares.** Use network isolation while keeping systems powered when forensic collection is planned.
2. **Disable confirmed compromised accounts.** Revoke sessions and rotate passwords from a known-clean device, prioritizing administrators and remote-access accounts.
3. **Restrict remote access.** Remove direct RDP exposure, review VPN and gateway access, and block the confirmed intrusion path.
4. **Protect backups.** Disconnect reachable backup repositories if they are at risk, without overwriting clean recovery points.
5. **Determine scope.** Hunt for the same logons, processes, notes, files, and persistence on other endpoints and servers.

If encryption is still active and formal isolation is unavailable, disconnect the network cable or Wi-Fi. Avoid mass shutdowns before coordinating with responders because volatile evidence may explain credentials, processes, and lateral movement.

05 Can Crysis or Dharma files be decrypted?

Some older Crysis variants have supported free decryptors after keys became available, but there is no universal tool for every Dharma variant. The No More Ransom decryption tools repository lists vetted tools and identifies their supported families. Check the exact tool documentation and work on copies of encrypted data.

A tool listing “Crysis” support does not guarantee support for a particular extension or key. First identify the ransomware with the ransom note and sample, then test a copy. Keep untouched originals in case a future key or improved method becomes available. Paying does not guarantee a valid key, safe software, or recovery and may have legal or sanctions implications.

06 Recovery process

1. Find the earliest malicious access and close it before restoring systems.
2. Rebuild compromised servers and workstations from trusted media when administrative access or system integrity is uncertain.
3. Patch operating systems and remote-access software, remove unauthorized accounts and tools, and reset affected secrets.
4. Restore prioritized data from offline, immutable, or otherwise verified clean backups.
5. Validate applications and permissions, reconnect in stages, and monitor for repeated access or encryption.

File restoration alone is incomplete. If an intruder used RDP interactively, assume they may have accessed other data and credentials until investigation shows otherwise.

07 Prevention

Do not expose RDP directly to the internet. Place it behind a maintained VPN or remote desktop gateway, require phishing-resistant MFA, restrict source networks, and alert on unusual logon times or repeated failures followed by success. Use unique passwords, separate administrator accounts, least privilege, endpoint protection with tamper controls, and network segmentation.

Keep tested backups isolated from everyday administrative credentials.

08 Frequently asked questions

Does a .dharma extension prove the ransomware family?

No. Treat the extension as a clue and confirm it with the note, sample, behavior, and reputable identification sources.

Should I delete the ransom note?

No. Preserve it because the victim ID and variant details can help identification and recovery assessment.

Is opening RDP safe after changing the password?

Not by itself. Remove direct exposure, review accounts and persistence, require MFA through a secure gateway, and determine whether the host must be rebuilt.

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