C

Clop (CL0P) Ransomware: Campaigns, Detection, and Response

Clop is both a ransomware family and the name commonly used for the criminal operation behind it. Learn how its campaigns differ and how to respond.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What is Clop ransomware?

02 How a Clop incident can unfold

03 Evidence that deserves investigation

04 What to do if Clop activity is suspected

05 How to reduce risk

06 Frequently asked questions

Quick answer: Clop, also written CL0P, refers to a ransomware family and the criminal operation associated with it. Some Clop incidents encrypt systems after a network intrusion, while other campaigns exploit internet-facing file-transfer software, steal data, and extort victims without deploying ransomware. Therefore, the absence of encrypted files does not rule out a Clop-related breach.

01 What is Clop ransomware?

Clop emerged as a high-impact ransomware operation targeting organizations rather than individual home users. Reporting has linked it with TA505 and with affiliates or access brokers, but names used by security vendors describe observed activity, not a guaranteed legal identity. Defenders should treat “Clop” as an operational label and validate each incident from its own evidence.

Traditional Clop intrusions can include initial access, credential theft, lateral movement, data collection, exfiltration, and encryption. More recent mass-exploitation campaigns have emphasized theft from vulnerable managed file-transfer products. In the 2023 MOVEit campaign, for example, exploitation of CVE-2023-34362 enabled data theft and extortion at scale; file encryption was not required. The joint CISA and FBI CL0P advisory documents that campaign and its defensive recommendations.

02 How a Clop incident can unfold

1. **Initial access:** attackers may exploit a vulnerable public service, use stolen credentials, or obtain access through another compromised system.
2. **Discovery and persistence:** they identify valuable servers, accounts, backups, and data repositories while attempting to retain access.
3. **Collection and exfiltration:** sensitive data may be staged and transferred outside the organization before disruption occurs.
4. **Extortion:** the actor may encrypt files, threaten publication of stolen data, contact customers, or combine these methods.

This sequence varies. A list of old filenames, IP addresses, or ransom-note names is useful for historical hunting, but it is not a durable detection strategy. Infrastructure and tooling change, and exploitation of a shared supplier can expose an organization even when no Clop executable ran in its own environment.

03 Evidence that deserves investigation

- Unexpected web-shell files, new administrative accounts, or unusual processes on an internet-facing file-transfer server.
- Large or unusual outbound transfers from repositories containing customer, employee, legal, or financial information.
- Authentication from unfamiliar locations, mass access to files, or privilege changes outside an approved maintenance window.
- Security controls, logs, or backups being disabled, cleared, or modified.
- A ransom note, changed file extensions, an extortion message, or a credible notification that a supplier holding your data was compromised.

None of these signs alone proves attribution. Preserve timestamps, logs, affected files, memory where feasible, and copies of suspicious messages. Attribution should never delay containment.

04 What to do if Clop activity is suspected

1. **Isolate affected systems.** Remove compromised servers from the network without erasing them. If a vulnerable managed file-transfer product is involved, follow the vendor’s current containment instructions.
2. **Stop the exposure.** Disable the affected service or restrict access, patch the specific vulnerability, remove persistence, and block confirmed malicious access paths.
3. **Protect identities.** Revoke active sessions and rotate credentials, API keys, service-account secrets, and certificates that the affected systems could access.
4. **Determine data impact.** Identify which files were accessible or transferred and whether subsidiaries, customers, or downstream organizations are affected.

5. **Engage the right teams.** Involve incident response, legal/privacy, leadership, cyber-insurance, law enforcement, and regulators according to the organization’s plan and obligations.
6. **Recover from a trusted state.** Rebuild compromised systems where integrity cannot be established, restore tested clean data, and monitor closely for renewed access.

Do not delete evidence, communicate with an extortion actor from a compromised account, or assume that payment will delete stolen data. A ransom decision has legal, safety, and business implications and requires specialist advice; it is not a technical recovery plan.

05 How to reduce risk

Maintain an inventory of internet-facing applications and their versions, subscribe to vendor security notices, and patch actively exploited flaws quickly. Put file-transfer services behind strong access controls, restrict their service accounts, centralize logs outside the appliance, and alert on bulk downloads and administrative changes. Use phishing-resistant multifactor authentication for privileged and remote access, segment critical systems, protect backups from domain-wide credentials, and test restoration.

Also map where suppliers store your sensitive data. A third-party breach can create a Clop exposure even when your endpoints are clean. Contracts, retention limits, breach-notification routes, and an up-to-date contact list make that scenario much easier to manage.

06 Frequently asked questions

Does a Clop incident always encrypt files?

No. Some campaigns have focused on stealing data from vulnerable services and demanding payment without encrypting victim systems.

Can an antivirus scan prove that no data was stolen?

No. Endpoint scanning may find malware, but data-access logs, application logs, identity records, and network telemetry are needed to assess exfiltration.

Is Clop the same as MOVEit?

No. MOVEit Transfer is legitimate software. Clop actors exploited vulnerabilities in certain deployments; the product name and the threat actor are not interchangeable.

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