Clop ransomware claims responsibility for Cleo data theft attacks

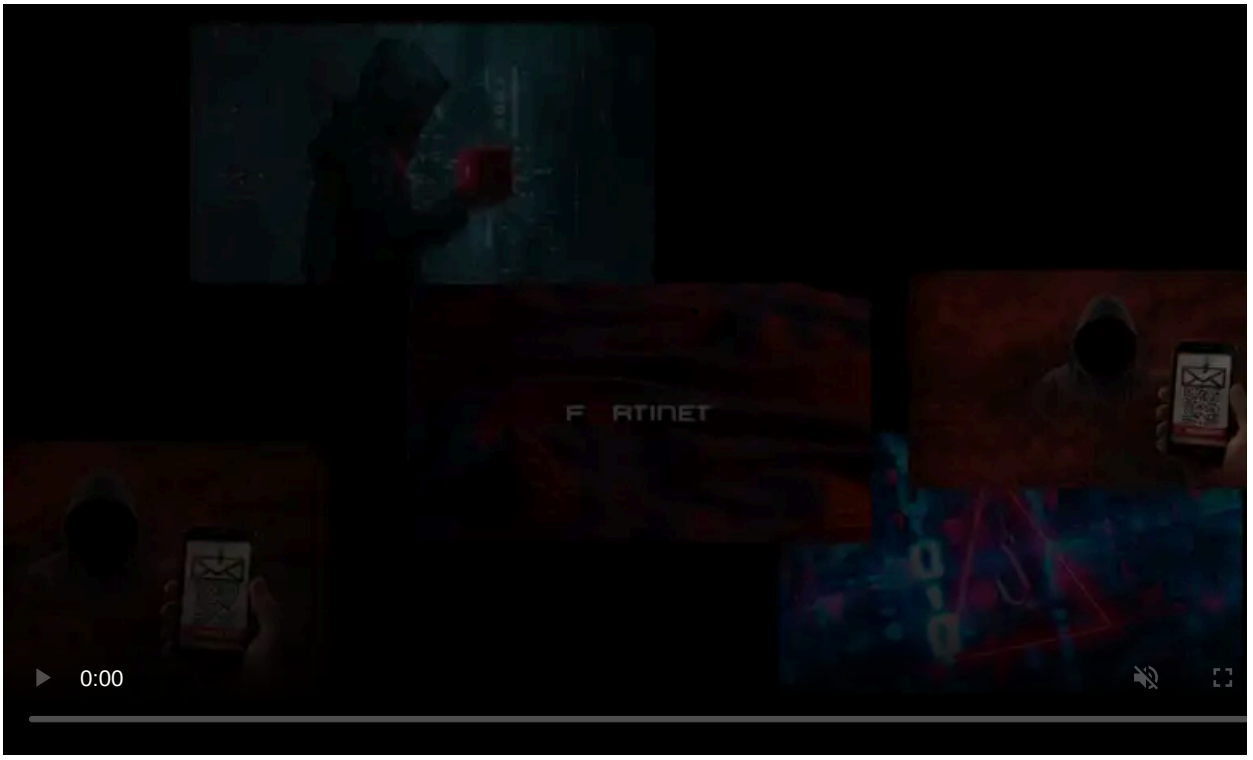
By Lawrence Abrams

Published: 2024-12-15 · Archived: 2026-04-05 21:58:02 UTC

12/16/24 update: Article updated to include new information about Cleo CVE-2024-50623 and CVE-2024-55956 flaws.

The Clop ransomware gang has confirmed to BleepingComputer that they are behind the recent Cleo data-theft attacks, utilizing zero-day exploits tracked as CVE-2024-50623 and CVE-2024-55956 to breach corporate networks and steal data.

Cleo is the developer of the managed file transfer platforms Cleo Harmony, VLTrader, and LexiCom, which companies use to securely exchange files between their business partners and customers.


F RTINET
0:00

The Cleo zero-days

In October, Cleo disclosed a vulnerability tracked as CVE-2024-50623 that allowed unrestricted file uploads and downloads, leading to remote code execution. This flaw was fixed in Cleo Harmony, VLTrader, and LexiCom version 5.8.0.21.

At the time, Cleo released a private advisory behind a support site login that warned that the vulnerability was exploited to open a reverse shell back to the threat actors, giving them remote access to the compromised device.

"This vulnerability has been leveraged to install malicious backdoor code on certain Cleo Harmony, VLTrader, and LexiCom instances in the form of a malicious Freemarker template containing server-side JavaScript," explained the advisory.

However, the attacks didn't get widespread attention until cybersecurity firm Huntress warned last week that the Cleo platforms were again being exploited in data theft attacks using a zero-day vulnerability.

"Although Cleo published an update and advisory for CVE-2024-50623—which allows unauthenticated remote code execution—Huntress security researchers have recreated the proof of concept and learned the patch does not mitigate the software flaw," reads Huntress' advisory.

The new vulnerability used in the December attacks is now tracked as CVE-2024-55956 and is fixed in Cleo Harmony, VLTrader, and LexiCom 5.8.0.24.

While exploiting this vulnerability, the threat actors uploaded a JAVA backdoor dubbed "Malichus" that allows attackers to steal data, execute commands, and gain further access to the compromised network.

On Friday, CISA confirmed that the critical CVE-2024-50623 security vulnerability in Cleo Harmony, VLTrader, and LexiCom file transfer software has been exploited in ransomware attacks but did not share any additional details.

Rapid7 has now confirmed that CVE-2024-55956 is not a patch bypass of CVE-2024-50623, as they exploit separate issues in a Cleo endpoint.

"Both CVE-2024-50623 and CVE-2024-55956 are unauthenticated file write vulnerabilities, due to separate issues in the /Synchronization endpoint," reads Rapid7's report.

"Therefore CVE-2024-55956 **is not a patch bypass** of CVE-2024-50623, but rather a new vulnerability. It is also worth highlighting that while CVE-2024-50623 allows for both reading and writing arbitrary files, CVE-2024-55956 only allows for writing arbitrary files."

Clop claims responsibility for Cleo data theft attacks

It was previously thought that the Cleo attacks were conducted by a new ransomware gang named Termite. However, the Cleo data theft attacks tracked more closely to previous attacks conducted by the Clop ransomware gang.

After contacting Clop on Tuesday, the ransomware gang confirmed to BleepingComputer that they are behind the recent exploitation of the Cleo CVE-2024-55956 vulnerability detected by Huntress as well as the exploitation of the original CVE-2024-50623 flaw fixed in October.

"As for CLEO, it was our project (including the previous cleo) - which was successfully completed.

All the information that we store, when working with it, we observe all security measures. If the data is government services, institutions, medicine, then we will immediately delete this data without hesitation (let me remind you about the last time when it was with moveit - all government data, medicine, clinics, data of scientific research at the state level were deleted), we comply with our regulations.

with love © CL0P^_"

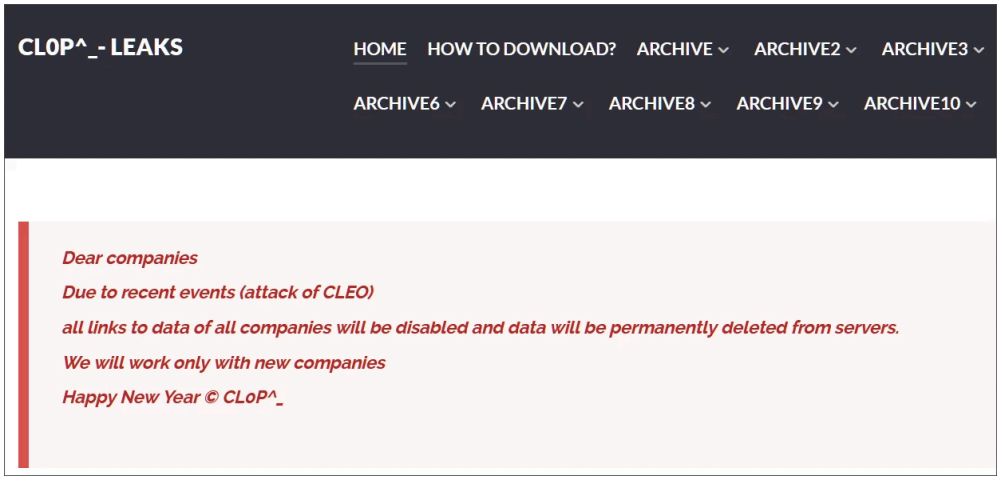
❖ Clop told BleepingComputer

When asked how many companies were impacted, Clop told BleepingComputer after publication of this story that they cannot say for sure, but "quite a lot".

The extortion gang has now announced that they are deleting data associated with past attacks from their data leak server and will only work with new companies breached in the Cleo attacks.

"Dear companies, Due to recent events (attack of CLEO) all links to data of all companies will be disabled and data will be permanently deleted from servers. We will work only with new companies," reads a new message on the gang's CL0P^_-LEAKS extortion site.

"Happy New Year © CL0P^_ all of the victims from their data leak site."



Message on the CL0P^_- LEAKS extortion site
Source: BleepingComputer

Most of the data currently archived on the Clop data leak site is for companies breached in the massive MOVEit Transfer data theft attacks that occured over the 2023 Memorial Day holiday in the US.

BleepingComputer asked Clop when the attacks began and if Clop was affiliated with the Termite ransomware gang, but did not receive a response to these questions.

BleepingComputer also contacted Cleo on Friday to confirm if Clop was behind the exploitation of the vulnerabilities but did not receive a response.

Specializing in exploit file transfer platforms

The Clop ransomware gang, aka TA505 and Cl0p, launched in March 2019, when it first began targeting the enterprise using a variant of the CryptoMix ransomware.

Like other ransomware gangs, Clop breached corporate networks and slowly spread laterally through its systems while stealing data and documents. When they have harvested everything of value, they deployed ransomware on the network to encrypt its devices.

However, since 2020, the ransomware gang has specialized in targeting previously unknown vulnerabilities in secure file transfer platforms for data theft attacks.

In December 2020, Clop exploited a zero-day in the Accellion FTA secure file transfer platform, which impacted nearly one hundred organizations.

Then in 2021, the ransomware gang exploited a zero-day in SolarWinds Serv-U FTP software to steal data and breach networks.

In 2023, Clop exploited a zero-day in the GoAnywhere MFT platform, allowing the ransomware gang to steal data from over 100 companies again.

However, their most significant attack of this kind was using a zero-day in the MOVEit Transfer platform that allowed them to steal data from 2,773 organizations, according to a report by Emsisoft.

At this time, it is not clear how many companies have been impacted by the Cleo data theft attacks, and BleepingComputer does not know of any companies who have confirmed being breached through the platform.

The U.S. State Department's Rewards for Justice program currently has a $10 million bounty for information linking the Clop ransomware attacks to a foreign government.

Source: https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-cleo-data-theft-attacks/