Clop ransomware is now extorting 66 Cleo data-theft victims

By Bill Toulas

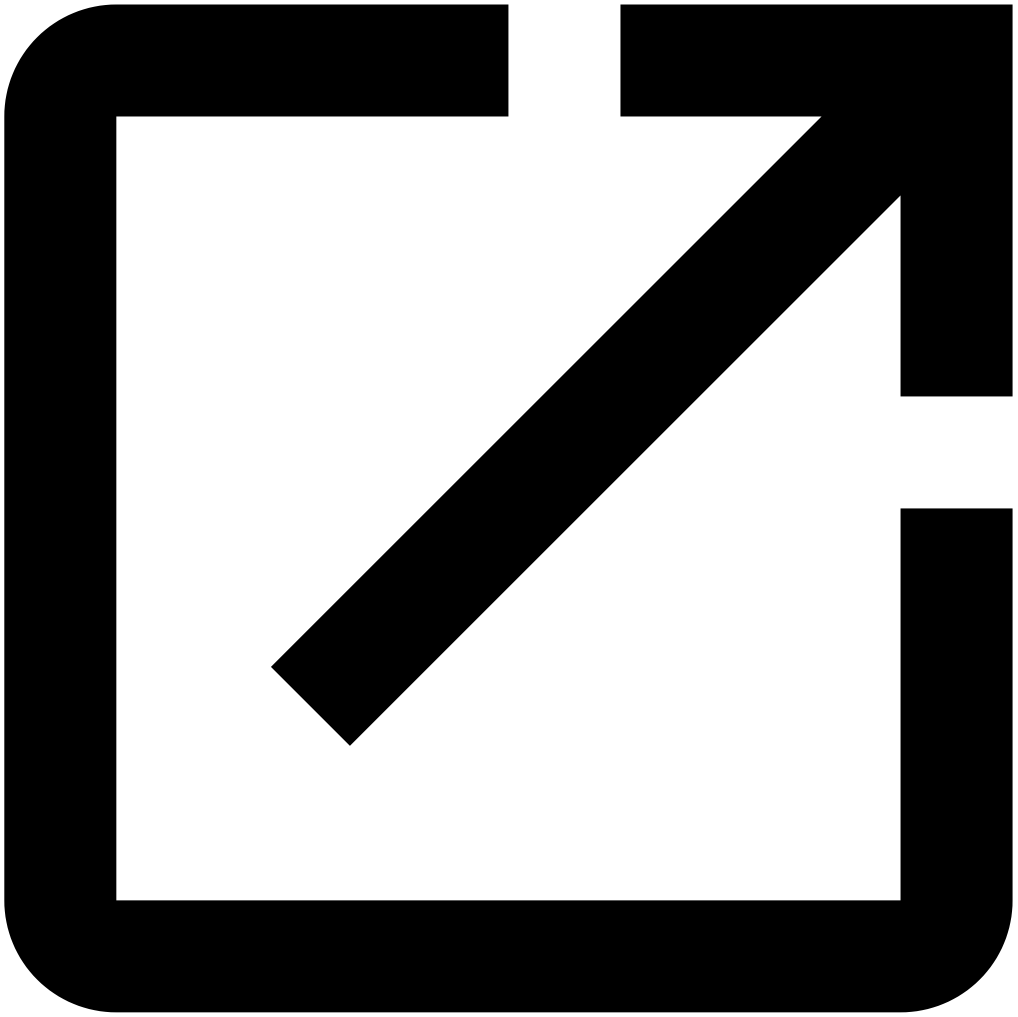
Published: 2024-12-24 · Archived: 2026-04-05 13:05:19 UTC

The Clop ransomware gang started to extort victims of its Cleo data theft attacks and announced on its dark web portal that 66 companies have 48 hours to respond to the demands.

The cybercriminals announced that they are contacting those companies directly to provide links to a secure chat channel for conducting ransom payment negotiations. They also provided email addresses where victims can reach out themselves.

In the notification on their leak site, Clop lists 66 partial names of companies that did not engage the hackers for negotiations. If these companies continue to ignore, Clop threatens to disclose their full name in 48 hours.


DIE LINKE.
0:00



Source: BleepingComputer

The hackers note that the list represents only victims that have been contacted but did not respond to the message, suggesting that the list of affected companies may be larger.

Clop achieves another major breach

The Cleo data theft attack represents another major success for Clop, who leveraged leveraging a zero-day vulnerability in Cleo LexiCom, VLTransfer, and Harmony products to steal data from the networks of breached companies.

In the past, Clop ransomware accessed company networks by exploiting zero-day vulnerabilities in Accellion FTA secure file transfer platform, GoAnywhere MFT platform, and MOVEit Transfer platform.

The gang is also responsible for another hacking spree targeting companies running the SolarWinds Serv-U FTP software.

The zero-day flaw exploited this time is now tracked as CVE-2024-50623 and it allows a remote attacker to perform unrestricted file uploads and downloads, leading to remote code execution.

A fix is available for Cleo Harmony, VLTrader, and LexiCom version 5.8.0.21 and the vendor warned in a private advisory that hackers were exploiting it to open reverse shells on compromised networks.

Earlier this month, Huntress publicly disclosed that the vulnerability was actively exploited and sounded the alarm that the vendor's fix could be bypassed. The researchers also provided a proof-of-concept (PoC) exploit to demonstrate their findings.

A few days later, Clop ransomware confirmed to BleepingComputer that it was responsible for exploiting CVE-2024-50623.

The infamous ransomware group declared that data from previous attacks will now be deleted from its platform as it focuses on the new extortion round.

In an email to BleepingComputer, Macnica researcher Yutaka Sejiyama said that even with the incomplete company names that Clop published on its data leak site, it is possible to identify some of the victims by simply cross checking the hacker's hints with owners of Cleo servers exposed on the public web.

At this time, it is unknown how many companies have been compromised by Clop's latest attack wave, but Cleo claims that its software is used by more than 4,000 organizations worldwide.

Source: https://www.bleepingcomputer.com/news/security/clop-ransomware-is-now-extorting-66-cleo-data-theft-victims/