Cl0p in Your Network? Here's How to Find Out

By Robert Lemos

Published: 2023-06-26 · Archived: 2026-04-05 23:33:11 UTC

5 Min Read

Source: Andrey Popov via Shutterstock

Widespread attacks against companies and government agencies through a trio of zero-day vulnerabilities in the MOVEit Managed File Transfer platform has granted notoriety to the Cl0p ransomware group.

The list of affected data continues to grow, including personal data on millions of workers investing in the CalPERS pension fund, employee information from more than 100,000 workers at the BBC and British Airways, sensitive data from the US Department of Energy, and personal information on citizens of Nova Scotia.

The widespread impact of the attack speaks volumes of the group's technical capabilities, says Steve Povolny, director of security research at Exabeam, a cybersecurity and compliance services firm.

"The shift that I see with these large threat actors, especially the ransomware gangs, [is that] they're well-funded, they're well-resourced, they have large organizations, and they're not just finding zero days on GitHub anymore,"

he says. "These are careful, dedicated, planned attacks that are designed to be very quiet and then be very loud all at once."

Determining the technical indicators that indicate the adversary behind any attack is always tricky since tactics change. The following indicators give organizations a starting point to investigate whether the Cl0p group has exploited the vulnerabilities in MOVEit file transfer utilities and may be in the network.

The MOVEit Attack: 'Human2' Fingerprint

The group behind Cl0p has used a number of vulnerabilities in file transfer services, such as GoAnywhere MFT in January (CVE-2023-0669) and the MOVEit managed file transfer platforms in late May and early June (CVE-2023-34362).

Initially, the attackers installed a Web shell, named LEMURLOOT, using the name "human2.aspx" and used commands sent through HTTP requests with the header field set to "X-siLock-Comment". The advisory from the Cybersecurity and Infrastructure Security Agency also includes four YARA rules for detecting a MOVEit breach.

The attack also leaves behind administrative accounts in associated databases for persistence — even if the Web server has been completely reinstalled, the attackers can revive their compromise. Sessions in the "activesessions" database with Timeout = '9999' or users in the User database with Permission = '30' and Deleted = '0' may indicate attacker activity, according to CrowdStrike.

One hallmark of the MOVEit attack, however, is that it typically leaves few technical indicators behind. The extended success of the Cl0p attack against MOVEit managed file transfer software and the difficulty in finding indicators of compromise show that product vendors need to spend additional effort on ensuring that forensically useful logging is available, says Caitlin Condon, a security manager with vulnerability-management firm Rapid7.

"There's a lot of tracks here — there's a lot to follow," she says. "Often, in looking to remediate the vulnerability and eradicate threat-actor access, a lot of companies were completely wiping the application, and that also will wipe the evidence."

Signs of Cl0p Ransomware

At some point during an attack, the Cl0p group will likely deploy ransomware of the same name. Originally, the malware was installed via phishing attacks, but increasingly attacks have targeted large organizations, often with exploits for new or recent vulnerabilities in file transfer or management software.

Typically, the group uses legitimate code-signing certificates to evade detection by security software. In the past, for example, the Cl0p ransomware installer has used either a certificate from Corsair Software Solution Inc. dated Friday, Feb. 12, 2021, or one from Insite Software Inc. dated Friday, Dec. 25, 2020, according to a technical advisory published by Palo Alto Networks.

The attackers will also stop several system processes, including those belonging to backup programs and security solutions.

Following execution, the Cl0p ransomware appends a variety of extensions to the victim's files, including .clop, .CIIp, .Cllp, and .C_L_O_P. Ideally, companies would want to detect the ransomware before the point files are decrypted.

As with any technical indicators, static signatures are of limited use because attackers will often customize their methods as a way to bypass detection based on fixed rules, according to cyberthreat experts.

Other Signs: Truebot and Raspberry Robin

Other common technical indicators of the Cl0p group are the ancillary tools they use to extend their compromise or alternative ways that they gain initial access.

The Truebot downloader, for example, is a popular intermediary payload that often leads to a Cl0p infection and is linked to the Silence group. Truebot often leads to the installation of Cobalt Strike and/or the Grace downloader malware, according to an analysis by Cisco's Talos group. For exfiltration, a custom tool known as Teleport is commonly used as well.

Silence has used a worm delivered through USB drives, known as Raspberry Robin, and sometimes through a third-party pay-per-install service, according to Microsoft, which now tracks the group under its new taxonomy as Lace Tempest. As of April, Microsoft noted that Raspberry Robin had been seen in nearly 1,000 organizations by almost 3,000 devices, with Truebot and/or Cobalt Strike following soon after, as Lace Tempest attempted to compromise more systems.

Raspberry Robin infections can be stopped by using Group Policy or registry settings to prevent autorun or the execution of code upon inserting a USB drive, according to Microsoft.

Finally, companies should always look for signs that a large volume of data is being exfiltrated, especially to infrastructure known to be used by the Cl0p group, says Mike Stokkel, a senior threat intelligence analyst in NCC

Group's FOX-IT security-services group.

"Standard security measurements can already help by, for example, deploying [endpoint detection and response] solutions on file transfer applications on a MOVEit system or a GoAnywhere system," he says. "Using a network sensor and tracking outgoing outbound network traffic can also help. When you see 600 gigabytes going outside of your network, that's quite an anomaly."

About the Author

Contributing Writer

Veteran technology journalist of more than 20 years. Former research engineer. Written for more than two dozen publications, including CNET News.com, Dark Reading, MIT's Technology Review, Popular Science, and Wired News. Five awards for journalism, including Best Deadline Journalism (Online) in 2003 for coverage of the Blaster worm. Crunches numbers on various trends using Python and R. Recent reports include analyses of the shortage in cybersecurity workers and annual vulnerability trends.
