



| Flash |

CI0p Publishes Data of Cleo Compromise Victims

F-2025-01-20a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Ransomware, Deep and Dark Web, Threat
Actor

January 20, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 09:00 AM (EST) on January 20, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | CI0p Publishes Data of Cleo Compromise Victims

| Key Findings

- Between January 17 and 18, 2025, the ransomware group CI0p published data allegedly belonging to three organizations that were targeted during the Q4 2024 compromise of Cleo secure managed file transfer (MFT) solutions.
- Previously, in December 2024, CI0p added the obfuscated names of 66 alleged victim organizations to their leak site. The names of these organizations were unveiled on January 14 and 15, 2025, along with a blog post threatening to publish their data on January 18, 2025.
- There is a very likely chance that CI0p will begin publishing data stolen from other named organizations in the coming weeks, beginning with those that CI0p perceives to be impeding negotiations or unlikely intending to meet demands.
- Also between January 17 and 18, 2025, CI0p posted a seemingly-unrelated statement to their victim leaksite, alluding to the collective's "downloading" of data belonging to organizations that use the MOVEit MFT solution, via a vulnerability. The meaning and intent behind CI0p's message to MOVEit customers is unclear.

| Details

Between January 17 and 18, 2025, the ransomware group CIOp added four new leak pages named after different organizations to their dark web victim leak site, three of which contain significant quantities of data available for download. These organizations are alleged victims of the collective's Q4 2024 Cleo secure MFT solutions compromise. Two other organization pages were also added, although whether these are victims of the same compromise is unclear as of the writing of this report.

- In October 2024 Cleo divulged a vulnerability tracked as CVE-2024-50623, that permitted unrestricted file uploads and downloads—leading to remote code execution (RCE) targeting the company's LexiCom, VLTrader, and Harmony secure file transfer products. Cleo did not acknowledge its exploitation “in the wild” but released an advisory to its online Solutions Center urging users to upgrade to version 5.8.0.21.¹
- In early December 2024 it was discovered that endpoints updated with the latest security patches were still being exploited—this time via a vulnerability tracked as CVE-2024-55956. A new security patch was released with an advisory from Cleo urging users to update the software to version 5.8.0.24, which reportedly mitigates the threat posed by CVE-2024-55956.²
- At the time of writing, neither CVE-2024-50623 nor CVE-2024-55956 has been assigned a CVSS 4.0 Risk Severity Score.³⁴

¹

[hXXps://support.cleo\[.\]com/hc/en-us/signin?return_to=https%3A%2F%2Fsupport.cleo.com%2Fhc%2Fen-us%2Farticles%2F27141200982423-Unrestricted-File-Upload-and-Download-Vulnerability-Mitigation-CVE-2024-50623](https://support.cleo.com/hc/en-us/signin?return_to=https%3A%2F%2Fsupport.cleo.com%2Fhc%2Fen-us%2Farticles%2F27141200982423-Unrestricted-File-Upload-and-Download-Vulnerability-Mitigation-CVE-2024-50623)

² [hXXps://support.cleo\[.\]com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956](https://support.cleo.com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956)

³ [hXXps://nvd.nist\[.\]gov/vuln/detail/CVE-2024-55956](https://nvd.nist.gov/vuln/detail/CVE-2024-55956)

⁴ [hXXps://nvd.nist\[.\]gov/vuln/detail/CVE-2024-50623](https://nvd.nist.gov/vuln/detail/CVE-2024-50623)



CI0p victim leak site, highlighting published data. Organization names obfuscated by ZeroFox

Source: ZeroFox Intelligence

In December 2024, CI0p added the obfuscated names of 66 alleged victim organizations to their leak site, alongside the threat of revealing their identities on December 26 and 27, 2024, should they not comply with demands. The names of these organizations were instead unveiled on January 14 and 15, 2025, along with a blog post threatening to publish their data on January 18, 2025. As of the writing of this report, 59 named organizations that are alleged victims of the Cleo compromise have not had any of their associated data published.

- CI0p's alleged victims of the 2024 Cleo compromise are disproportionately associated with the supply chain and logistics sectors, accounting for approximately 20 percent of the listed organizations. This is in comparison to approximately 2.8 percent observed across the ransomware threat landscape.
- North America was also disproportionately targeted in comparison to other regions-accounting for approximately 80 percent of CI0p's recent victims, in comparison to approximately 58 percent across the ransomware threat

landscape. This is likely influenced both by the distribution of Cleo MFT users, as well as CI0p's long-term preference to target North America-based organizations.

Dear companies

A new part of the companies list will be partially opened and presented on 21.01. Hurry up to contact us so that your name is not on this list!!!

Post on CI0p's victim leak site, alluding to imminent reveal of additional alleged victims

Source: ZeroFox Intelligence

There is a very likely chance that CI0p will begin publishing data stolen from the remaining 59 organizations in the coming weeks, beginning with those that CI0p perceives to be impeding negotiations or unlikely intending to meet extortion demands. Another post by CI0p indicated that the names of more victim organizations would be added to the blog on January 21, 2025. There is a roughly even chance that these names will be obfuscated to begin with, indicative of CI0p opting to stagger their extortion campaign in a manner consistent with a limited resource availability.

For those that meet extortion demands, CI0p will very likely remove their name from the victim leak site, and will likely delete any stolen data. Of the initial 66 organizations posted in December 2024, four have since been removed with no data published.

DEAR COMPANIES.

CLOP IS ONE OF TOP ORGANIZATION OFFER PENETRATION TESTING SERVICE AFTER THE FACT.

THIS IS ANNOUNCEMENT TO EDUCATE COMPANIES WHO USE PROGRESS MOVEIT PRODUCT THAT CHANCE IS THAT WE DOWNLOAD ALOT OF YOUR DATA AS PART OF EXCEPTIONAL EXPLOIT.

WE ARE THE ONLY ONE WHO PERFORM SUCH ATTACK AND RELAX BECAUSE YOUR DATA IS SAFE.

Post on CI0p's victim leak site, alluding to targeting of Progress MOVEIT software

Source: ZeroFox Intelligence

Also between January 17 and 18, 2025, CI0p posted a seemingly-unrelated statement to the victim leaksite, alluding to the collective's "downloading" of data belonging to organizations that use the MOVEit MFT solution, via a vulnerability. The statement further specifies that this data is "safe".

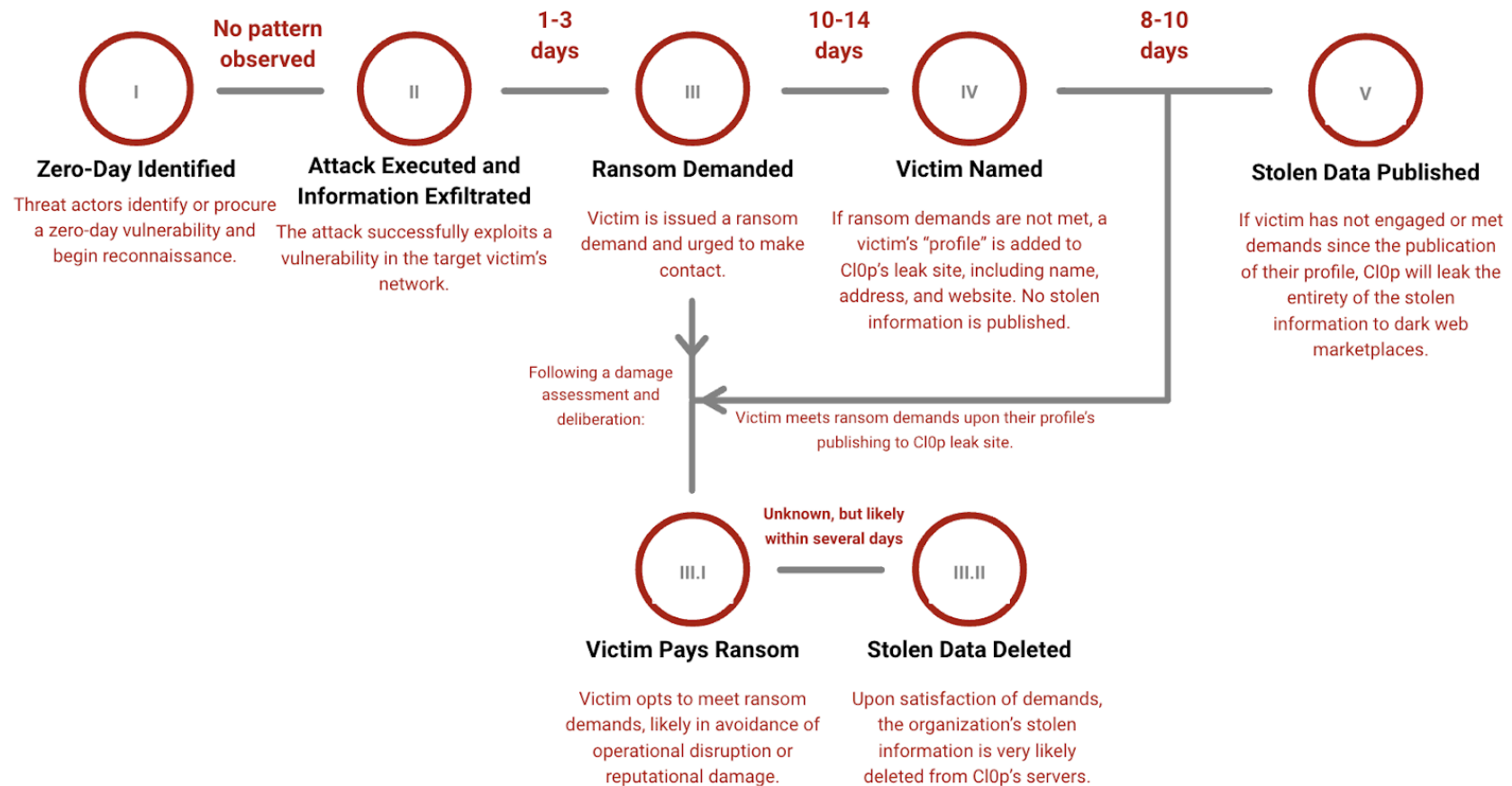
- In Q2 2023 CI0p leveraged a critical zero-day vulnerability tracked as CVE-2023-34362, exploiting a MOVEit web application. Hundreds of organizations around the globe were subsequently targeted, resulting in one of the most high-profile digital extortion campaigns ever observed.

The meaning and intent behind CI0p's message to MOVEit customers is unclear. The most likely scenario is that the referenced exploit is CVE-2023-34362, with the post being addressed to users of MOVEit that are still being exploited—most likely due to not having implemented the most recent security patches. CI0p could also be referencing a newly-found vulnerability affecting MOVEit software, enabling renewed targeting of customers. This is very unlikely however, due to the decision to publish this information rather than covertly conduct data exfiltration—which would enable a monetized extortion campaign and is more in line with CI0p's tactics, techniques, and procedures (TTPs)

- On December 23, 2024, actor "Nam3l3ss" disclosed a large number of data sets in the hacking forum BreachForums, which were allegedly stolen from MOVEit users compromised during the 2023 extortion campaign. While some of these organizations had previously been listed on CI0p's victim leak site, others had not—leading to a likely chance that they were subject to subsequent targeting.

Typical Timescales for ClOp's Extortion*

*Medium-confidence assessment based on observed procedures and timeframes



Source: ZeroFox Intelligence

| Recommendations

- Ensure that the most recent security patches are implemented. Seek manufacturer guidance from official websites and support pages:
 - [hXXps://support.cleo\[.\]com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623](https://support.cleo[.]com/hc/en-us/articles/27140294267799-Cleo-Product-Security-Advisory-CVE-2024-50623)
 - [hXXps://support.cleo\[.\]com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956](https://support.cleo[.]com/hc/en-us/articles/28408134019735-Cleo-Product-Security-Update-CVE-2024-55956)
 - [hXXps://community.progress\[.\]com/s/products-list](https://community.progress[.]com/s/products-list)
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi factor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%