



| Flash |

CI0p Claims Responsibility for Zero-Day Exploitation

F-2024-12-17a

Classification: TLP:CLEAR

Criticality: Medium

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

December 17, 2024

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 9:00 AM (EST) on December 17, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Cl0p Claims Responsibility for Zero-Day Exploitation

| Key Findings

- On December 15, 2024, the ransomware group Cl0p reportedly claimed responsibility for a recent spate of data theft attacks that targeted organizations using Cleo managed file transfer (MFT) software solutions.
- In October 2024, Cleo divulged a vulnerability tracked as CVE-2024-50623 that permitted unrestricted file uploads and downloads. A second vulnerability was discovered in December 2024 (tracked as CVE-2024-55956).
- While ZeroFox cannot verify Cl0p's claims, they are likely true given that the collective has not historically sought unwarranted attention. At the time of writing, the extent of the attacks and any ongoing extortion activity is unclear.
- If Cl0p's claims are legitimate, there is a roughly even chance that additional organizations will be compromised in the coming weeks before they are named on the victim leak site to apply additional extortion pressure.

| Details

On December 15, 2024, the ransomware group ClOp reportedly claimed responsibility for a recent spate of data theft attacks that targeted organizations using Cleo MFT software solutions.¹ While ZeroFox cannot confirm if ClOp's claims are legitimate, they are likely true given that the collective has not historically sought unwarranted attention. At the time of writing, the extent of the attacks and any ongoing extortion activity is unclear.

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 5.8.0.21.²
- On December 13, 2024, the Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2024-50623 to its Known Exploited Vulnerabilities (KEV) catalog and confirmed it had been exploited in ransomware campaigns.³

Cleo software received additional attention in early December 2024 when 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-2024-55956.⁴

- Though CVE-2024-55956 was initially thought to be a bypass of the patched CVE-2024-50623, recent research has identified it as a separate vulnerability.⁵

¹

[hXXps://www.bleepingcomputer.com/news/security/clOp-ransomware-claims-responsibility-for-cleo-data-theft-attacks/](https://www.bleepingcomputer.com/news/security/clOp-ransomware-claims-responsibility-for-cleo-data-theft-attacks/)

²

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

³

[hXXps://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-50623&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=](https://www.cisa.gov/known-exploited-vulnerabilities-catalog?search_api_fulltext=CVE-2024-50623&field_date_added_wrapper=all&field_cve=&sort_by=field_date_added&items_per_page=20&url=)

⁴ [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)

⁵ [hXXps://attackerkb.com/topics/geR0H8dgrE/cve-2024-55956/rapid7-analysis](https://attackerkb.com/topics/geR0H8dgrE/cve-2024-55956/rapid7-analysis)

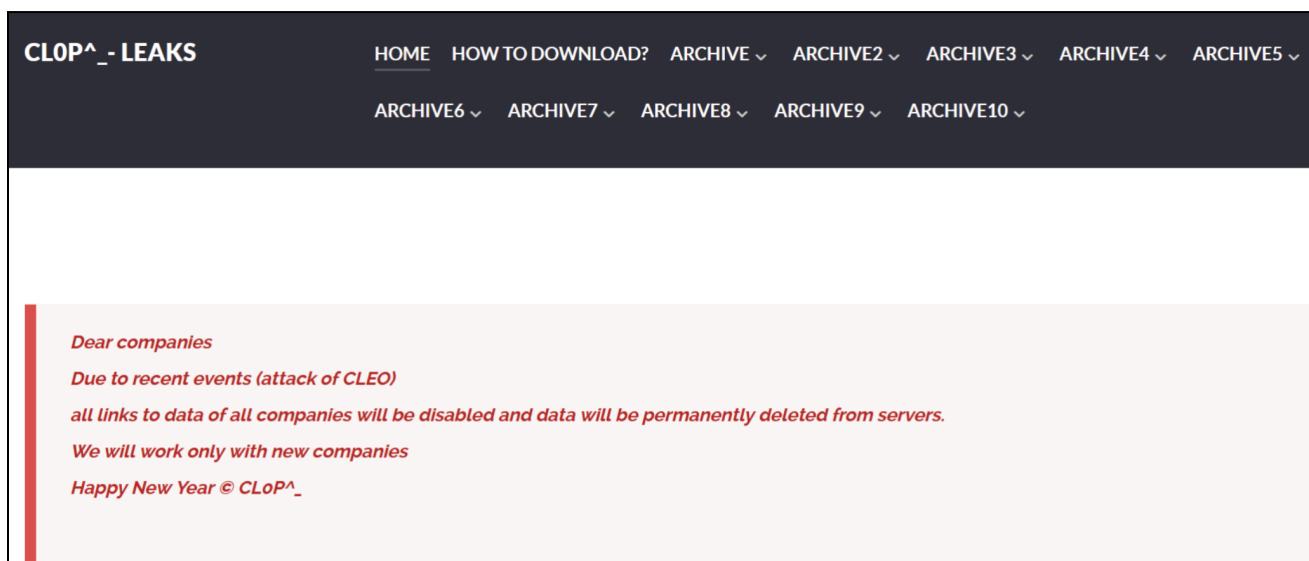
Flash | ClOp Claims Responsibility for Zero-Day Exploitation

F-2024-12-17a

TLP:CLEAR

- At the time of writing, neither CVE-2024-50623 nor CVE-2024-55956 has been assigned a CVSS 4.0 Risk Severity Score.⁶⁷

Shortly after claiming responsibility for the exploitation activity, a notice was posted to ClOp's [.]onion victim leak site that seemingly indicated all data relating to pre-existing victims of the collective's malicious activity will be deleted. The exact meaning of this is unclear, though there is a likely chance that ClOp intends this notice to serve as further proof of its responsibility claim. "New companies" very likely refers to those compromised by the recent Cleo exploitation.



ClOp victim leak site post claiming that the collective will only work with "new" companies

Source: ZeroFox Intelligence

In recent years, ClOp's attack tempo has been largely dictated by success in a small number of digital extortion campaigns targeting MFTs—notably Accellion in 2021 and both GoAnywhere and MOVEit in 2023. In each of these campaigns, ClOp leveraged a zero-day vulnerability to target the software provider before extorting large numbers of customer and supply chain organizations using ransomware.⁸

⁶ [hXXps://nvd.nist.gov/vuln/detail/CVE-2024-55956](https://nvd.nist.gov/vuln/detail/CVE-2024-55956)

⁷ [hXXps://nvd.nist.gov/vuln/detail/CVE-2024-50623](https://nvd.nist.gov/vuln/detail/CVE-2024-50623)

⁸ [hXXps://www.zerofox.com/blog/flash-report-analysis-of-clop-activity/](https://www.zerofox.com/blog/flash-report-analysis-of-clop-activity/)

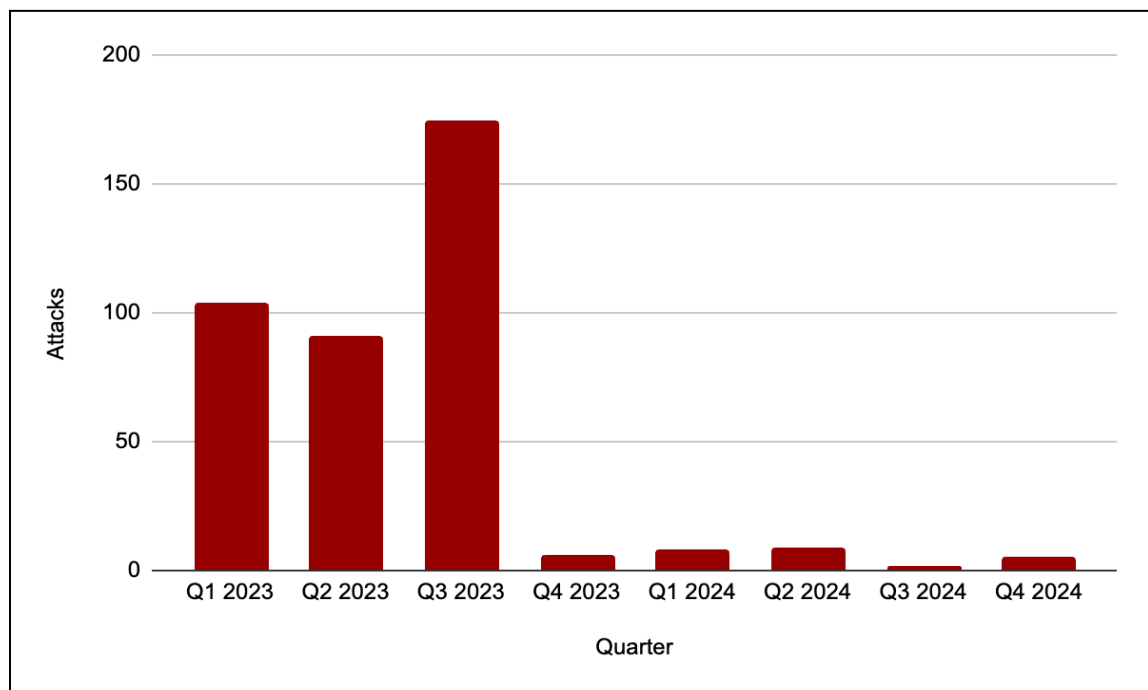
Flash | CI0p Claims Responsibility for Zero-Day Exploitation

F-2024-12-17a

TLP:CLEAR

The prominence and widespread exploitation of these campaigns resulted in CI0p being the third most-active ransomware collective in 2023. They were responsible for approximately 9 percent of all attacks observed by ZeroFox, behind only LockBit and ALPHV.

- These tactics, techniques, and procedures (TTPs) led to large spikes in activity over a period of several weeks following the initial exploitation, followed by a dramatic fall in attack tempo.
- CI0p's disposition toward exploiting zero-day vulnerabilities leads to unpredictability in both when activity will take place and the "success" the collective will achieve in compromising large numbers of associated organizations.
- To achieve the results previously obtained in prominent MFT compromises, CI0p will very likely seek to compromise a large number of organizations before they are able to protect their networks with manufacturer security patches.



CI0p attacks by quarter

Source: ZeroFox Intelligence

|Flash| CI0p Claims Responsibility for Zero-Day Exploitation

F-2024-12-17a

TLP:CLEAR

ZeroFox has not observed any extortion campaigns of notable scale from CI0p during 2024; the group averaged approximately three attacks per month throughout the year. Since the initial exploitation of CVE-2024-50623, five alleged victim organizations have been added to CI0p's leaksite (all in October 2024).

There is a likely chance that CI0p is responsible, as claimed, for the recent exploitation of vulnerabilities CVE-2024-50623 and CVE-2024-55956—particularly given the collective's propensity for targeting organizations that offer MFT services. If CI0p's claims are legitimate, there is a roughly even chance that additional organizations will be compromised in the coming weeks before they are named on the victim leak site to apply additional extortion pressure.

The extent of the compromise and the number of victim organizations will be heavily dependent on CI0p's ability to conduct widespread exploitation activities before effective security patches are implemented.

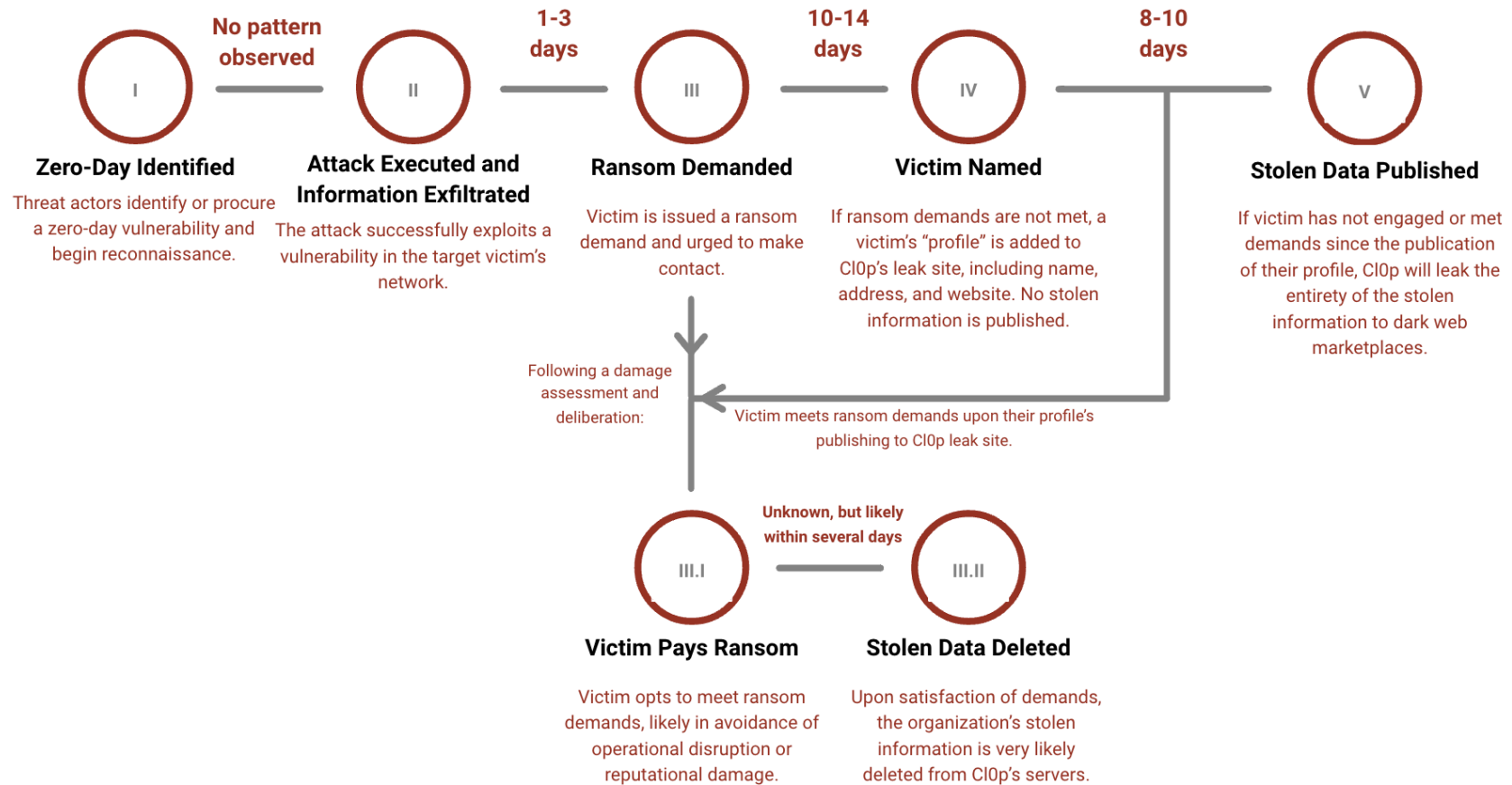
Flash | ClOp Claims Responsibility for Zero-Day Exploitation

F-2024-12-17a
TLP:CLEAR



Typical Timescales for ClOp's Extortion*

*Medium-confidence assessment based on observed procedures and timeframes



Source: ZeroFox Intelligence

| Recommendations

- Ensure that Cleo Harmony, VLTrader, and LexiCom have implemented the most recent security patches. Seek manufacturer guidance in the Cleo Solutions Center:
 - [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)
- 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%