ZEROFOX INTELLIGENCE

Flash

Cl0p Lists Latest Wave of Victims on Leak Site

F-2026-01-28a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Ransomware, Threat Actor, Dark Web

January 28, 2026

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 7:00 AM (EST) on January 27, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Cl0p Lists Latest Wave of Victims on Leak Site

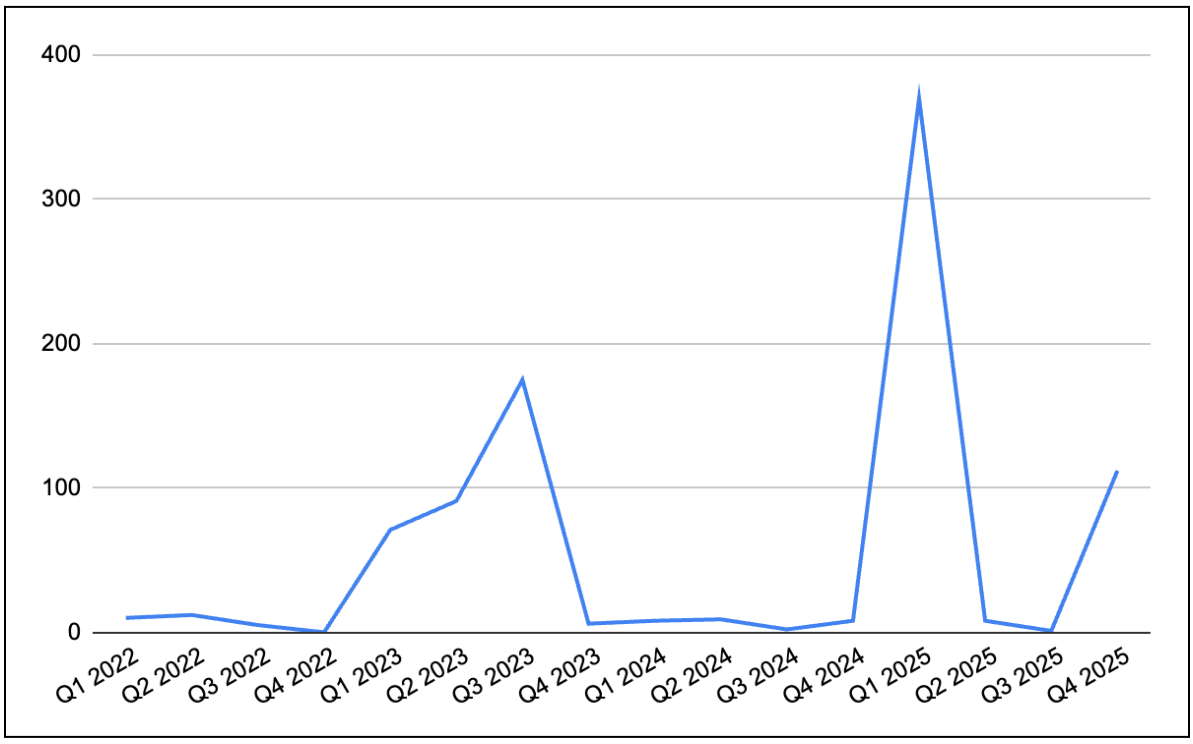
| Key Findings

- Ransomware and digital extortion (R&DE) collective Cl0p has claimed at least 46 victims on its victim shame site over the past week (an unusually high number in the short time period), portending an increase in operational tempo in the near term that is likely to increase their notoriety and pressure victims to pay the demanded ransoms.
- Since first observed in Q1 2022, Cl0p has had notable quarters of high-tempo activity very likely related to targeted extortion campaigns followed by several periods of relatively low activity.
- Although Cl0p has posted an extensive list of alleged victims on their leak site in the past week, they have not yet provided any details about an ongoing campaign or the type of data allegedly compromised.

Details

R&DE collective Cl0p has claimed at least 46 victims on its victim shame site over the past week; this is an unusually high number in a short time period and portends an increase in operational tempo in the near term that is likely to increase their notoriety and pressure alleged victims to pay the demanded ransoms. It is likely Cl0p has targeted the listed victims in a recent extortion campaign, the nature of which cannot be determined at this time.

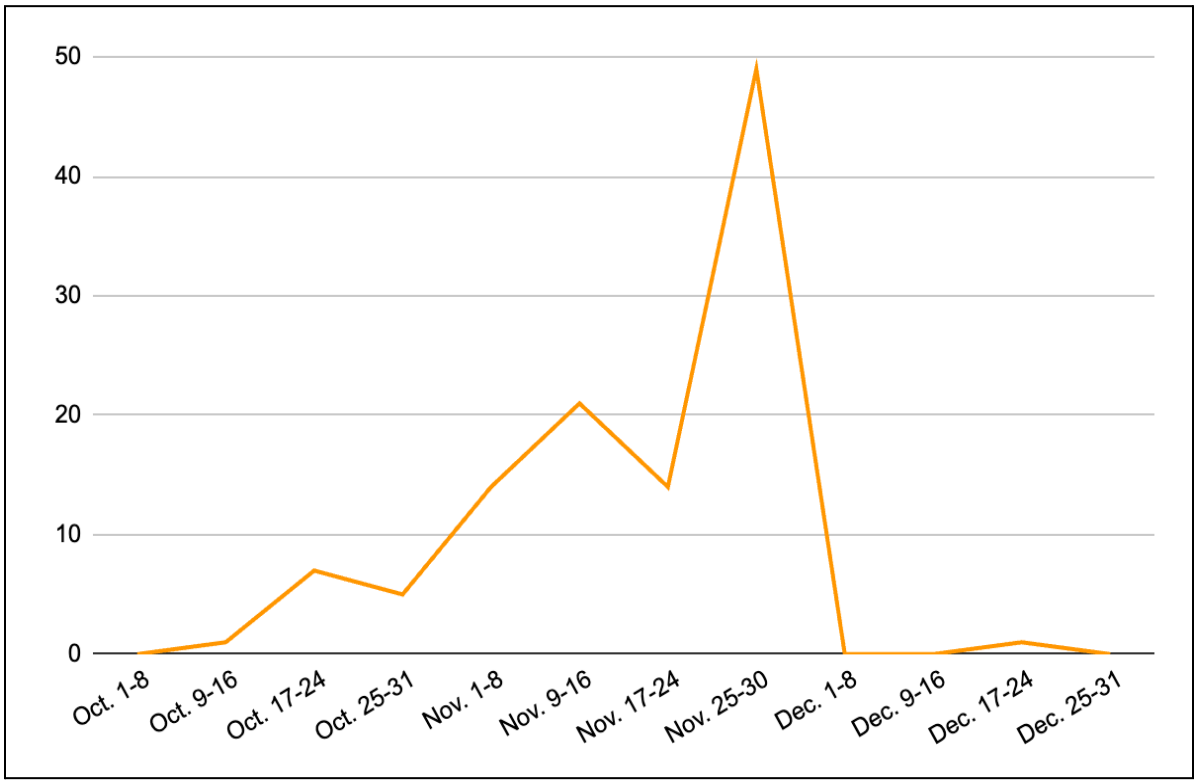
- Cl0p has been active since at least Q1 2022, making them one of the oldest ransomware collectives still active today.
- Since first observed, Cl0p has had notable quarters of high-tempo activity very likely related to targeted extortion campaigns followed by periods of relatively low activity.



Cl0p's number of incidents by quarter (Q1 2022–Q4 2025)

Source: ZeroFox Intelligence

During Q4 2025, Cl0P was responsible for at least 112 separate attacks, accounting for 5.3 percent of global R&DE incidents and making it the fourth most active collective for the period. Notably, Cl0p's Q4 2025 attacks represent the first significant activity by the collective since its then record-setting 370 attacks in Q1 2025. (Cl0p was responsible for a total of just nine attacks across both Q2 and Q3 2025.)



Cl0p's incidents by week in Q4 2025

Source: ZeroFox Intelligence

Although Cl0p has posted an extensive list of alleged victims on their leak site, they have not yet provided any details about an ongoing campaign or the type of data allegedly compromised. Notably, Cl0p maintains a relatively small online footprint compared to other threat actor collectives, with no known social media presence or Telegram channel. There is a roughly even chance that Cl0p will release further details in the coming weeks related to this recent wave of alleged attacks.

CENTAURPRODUCTS.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
INTEGRITEK.NET - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
BUREAUX.FR - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
ONYXEQUITIES.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
KCDWORLDWIDE.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
WORKFORCESOFTWARE.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
MCMATHLAW.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
BRINKS.CO.NZ - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
TRUSTPAYMENTS.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
KOROLFINANCIAL.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON

M-B.LAW - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
ARKTLA.ORG - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
COBU-ARCH.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
ESCALI.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
MCKEEGROUP.NET - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
CENTINELA.COM.BR - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
GALEINTL.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
ISLANDOUTPOST.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
KRIEGMANANDSMITH.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
NYASPHALT.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
KLMEQUITIES.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON

EXCELAS1.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
CLEARWAYGROUP.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
INSPYRSOLUTIONS.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
MODTECH.CA - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
WILDRIDGELANDSCAPE.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
RSTRT.IT - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
VISTA-TRAINING.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
4DITSOLUTIONS.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
BR-ALSETH.NO - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
VERTIGORELEASING.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
WFRFIRE.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON

ELKAIR.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
SMITHDALIA.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
BAQUS.CO.UK - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
AERIFY.IO - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
EASTPLATS.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
MONTALBAARCHITECTS.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
ITROBOTICS.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
INTEGROY.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
TOMLLAWYERS.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
WARRANTYFIRST.CO.UK - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON
ECA-USA.COM - PAGE CREATED, WARNING, WILL BE PUBLISHED SOON

Cl0p's list of recent alleged victims

Source: ZeroFox Intelligence

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- 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 (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (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%