ZEROFOX INTELLIGENCE

Flash

Cl0p Shifts from Personal Data to Intellectual Property Theft

F-2026-08-21a

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Threat Actor, Malware, Data Theft

August 21, 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 10:00 AM (EDT) on August 21, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Cl0p Shifts from Personal Data to Intellectual Property Theft

| Key Findings

- Between August 14 and August 19, 2026, Cl0p posted 43 organizations to its dark web leak site and began issuing extortion demands tied to data allegedly stolen from internet-exposed server instances of product lifecycle management platforms Windchill and FlexPLM, both of which are made by software-as-a-service (SaaS) company PTC, Inc.
- The type of data targeted and the small population of Windchill and FlexPLM users mark a significant change for Cl0p and likely suggests the threat actor is entering a new phase of operations.
- Cl0p was first observed in 2019 and has shifted its operations twice before: first from strict encryption to double extortion in 2020 and then to mass data exfiltration in 2021. Both prior significant operational changes marked a new phase of threat activity and sustained campaigns.
- Cl0p is likely in the early stages of a new campaign targeting engineering-focused intellectual property on vulnerable product lifecycle management servers.

Details

Between August 14 and August 19, 2026, Cl0p posted 43 organizations to its dark web leak site and began issuing extortion demands tied to data allegedly stolen from internet-exposed server instances of product lifecycle management platforms Windchill and FlexPLM, both of which are made by SaaS company PTC, Inc.[1] The type of data targeted and the small population of Windchill and FlexPLM users mark a significant operational change for Cl0p; this likely suggests the threat actor is entering a new phase of operations.

Most prominent companies allegedly targeted by Cl0p:

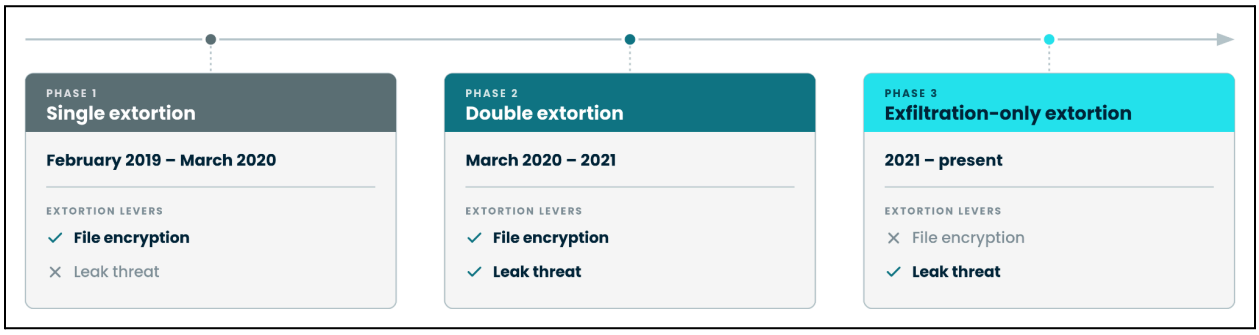
- **Shell**: Cl0p claims to have 89 gigabytes of the U.S. oil and and gas company's data, which the group has described as engineering drawings, scans of facility testing reports, photographs of facilities, and project plans. Shell has confirmed only that it is looking into the matter, stating: "We are aware of a potential incident. We are working with our security teams and relevant experts to investigate."[2][3]
- **Philips**: Cl0p claims to have 13.5 gigabytes of the U.S. healthcare technology company's data, which is described as mostly diagrams and blueprints. Philips is the only named organization to confirm a compromise, stating that it "has identified and contained an attempted cybersecurity compromise of a specific enterprise server related to internal data" that has "no impact on customer environments."[4][5]
- **General Electric**: A GE spokesperson stated the U.S. tech giant is "aware of the claim and … working to assess the potential issue."[6] Cl0p initially claimed to have stolen 391 gigabytes of data from GE[7], but notably, as of August 17, 2026, GE no

[1] hXXps://www.govinfosecurity[.]com/clop-claims-data-theft-from-more-than-40-companies-a-32581
[2] hXXps://www.bleepingcomputer[.]com/news/security/shell-investigates-potential-incident-after-clop-data-theft-claims/
[3] hXXps://thenextweb[.]com/news/clop-hacking-group-philips-shell
[4] *Ibid.*
[5] hXXps://www.bleepingcomputer[.]com/news/security/philips-and-ge-investigating-clop-ransomware-data-theft-claims/
[6] *Ibid.*
[7] *Ibid.*

longer appears on the leak site of companies that have failed to reach out to Cl0p for negotiations.[8]

- **Fiserv**: Cl0p claims to have stolen 874 gigabytes of data from the global fintech and payments company; however, Fiserv has reportedly found no evidence that customer, banking, transaction, or personal data was compromised.[9]

These claimed breaches suggest a likely shift in the data Cl0p targets away from the personal and financial records of its earlier campaigns toward engineering-focused intellectual property held in product lifecycle management platforms. Additionally, the targeting of product lifecycle management servers almost certainly suggests the chosen platforms (Windchill and FlexPLM) determined the data targeted, whereas past Cl0p incidents were very likely platform agnostic and sought to steal as much data as possible at once.



Timeline of Cl0p operational methodologies
Source: ZeroFox Intelligence

Cl0p was first observed in February 2019 as a ransomware-as-a-service operation focused on encryption and a declared methodology of attacking networks rather than computers.[10] In March 2020, the threat actor shifted to a double-extortion method, encrypting files and threatening to leak it if negotiations failed.[11] Beginning in 2021, Cl0p

[8] hXXps://www.govinfosecurity[.]com/clop-claims-data-theft-from-more-than-40-companies-a-32581
[9] *Ibid.*
[10] hXXps://www.bleepingcomputer[.]com/news/security/cryptomix-clop-ransomware-says-its-targeting-networks-not-computers/
[11] hXXps://www.bleepingcomputer[.]com/news/security/clop-ransomware-leaks-execupharms-files-after-failed-ransom/

apparently ceased the use of encryptors altogether and focused on mass data exfiltration—very likely still primarily of personal data.[12]

- The number of Windchill and FlexPLM servers is relatively small; the companies had between 80 and 100 internet-facing servers by the end of July 2026.[13]
- By contrast, previous Cl0p target MOVEit disclosed a victim tally of 2,618 organizations and more than 77 million affected individuals as of November 2023.[14]
- Targeting a relatively small population is likely an effort to test new operational methods on a victim set perceived to be less protected.

The changes in targeted data, the small number of servers in the targeted population, and the platform-specific approach of targeting product lifecycle management servers all suggest Cl0p is likely entering a new phase of operation. The group's two previous significant operational changes signaled a new campaign, the most recent of which lasted for five years. Cl0p's recent and notable change in both strategy and tactics point to a likely campaign targeting engineering-focused intellectual property on vulnerable servers.

[12] hXXps://www.cisa[.]gov/news-events/cybersecurity-advisories/aa23-158a
[13] hXXps://thehackernews[.]com/2026/07/clop-affiliates-target-internet-exposed.html
[14] hXXps://www.helpnetsecurity[.]com/2023/09/26/moveit-victim-number/

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%