



| Brief |

Analysis of Clop Activity

B-2023-07-17a

Classification: TLP:GREEN

July 17, 2023

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 (EDT) on July 17, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

Brief | Analysis of Clop Activity

Executive Summary

- Clop (a.k.a. Cl0p) activity is typically characterized by very low levels of activity for a period of several months, followed by several weeks of a high tempo of attacks.
- Clop ransomware attacks likely coincide with the discovering or procuring of critical vulnerabilities that enable the simultaneous targeting of multiple high-payoff victims.
- Clop's exploitation of zero-day vulnerabilities makes the timing of their campaigns unpredictable. However, victim's typically experience similar timelines guiding the sequence of attacks and post-attack exploitation.
- Victims of Clop attacks are typically targeted by data exfiltration followed by ransom demands, rather than the implementation of encrypting ransomware. This is likely a method deemed at lower risk of failure.

| Findings

> When is Clop deployment most prolific?

ZeroFox Intelligence has identified no evidence of trends in the timings of spikes in Clop activity, when analyzing the day of the week, month and year attacks occur. Typically, the strain is deployed at very low levels or is inactive throughout the year, before sharp spikes in activity. It is atypical of Clop to have two high profile campaigns in quick succession, as has been the case in 2023 with the exploitation of GoAnywhere MFT secure file transfer tool (CVE-2023-0669) and MOVEit Transfer software (CVE-2023-34362). Evidence suggests that operatives adjust the timings of their attacks—within constraints—to maximize impact on end users.

Clop's exploitation of zero-day vulnerabilities makes the timing of campaigns unpredictable. Operatives are required to research and identify, or procure zero-day vulnerabilities to leverage in attacks, the cadence of which is almost certainly limited given Clop's focus on file transfer software. Given the undisclosed nature of these exploits, operatives very likely have a small window within which attacks can be timed to maximize impact, but must execute attacks before vulnerabilities are identified by security vendors or researchers, and patches are deployed.

Clop operatives' ability to time—and even delay—their attacks to maximize impact was demonstrated during the May 2023 exploitation of a zero-day vulnerability disclosed in MOVEit Transfer (CVE-2023-34362). Unconfirmed reports suggest operatives may have identified the vulnerability as early as March 2023, but chose to delay their attack so that it took place over the U.S. Memorial Day weekend, very likely a result of the fact the majority of MOVEit servers were located in the U.S., and operatives could take advantage of companies operating with skeleton security teams.

> Is there a pattern to Clop operatives' activity?

Although the timing is unpredictable, Clop attacks and extortion of victims typically follow a common sequence of activity. Attacks likely follow extensive reconnaissance activity. Attacks themselves are swift and surgically executed, focusing on mass data exfiltration before intrusions are identified and mitigated. High-payoff opportunities are

typically selected, such as file-transfer platforms that hold proprietary information belonging to numerous organizations. While focusing on swift attacks, should subsequently-released patches be unsuccessful, there is a roughly even chance that operatives will conduct additional attacks, as seen during the 2021 Accellion File Transfer Appliance (FTA) breaches (CVE-2021-27101 through CVE-27104). Clop typically avoids encrypting data, rather focusing on exfiltration, a process likely deemed quicker and of lower risk of failure.

Ransom demands are typically issued within several days, whereby victims are informed of the information stolen along with procedures to prevent publishing. Victims are typically given between 10-14 days to pay the ransom demand—or possibly engage with operatives—before they are named on Clop’s Tor-based leak site, “CLOP^_ - LEAKS”, often including their name, HQ address and website URL. This time period very likely varies in length, depending upon the nature of correspondence received from the victim. From the point of being named, victims are typically given a further period of 8-10 days to meet demands—or progress negotiations—before victim’s data is made available for download on Clop’s leak site. This timeframe is likely staggered to draw maximum media attention and increase pressure on victims. If the victim pays the ransom demands during this time, Clop likely deletes exfiltrated data from their servers prior to publishing. This process can likely be significantly prolonged due to protracted negotiations processes, resulting in the publishing of stolen information many weeks after deadlines are past. This is more likely to be observed during larger campaigns involving a multitude of victims.

› **Timing of posts on leak site site**

ZeroFox Intelligence has observed no typical pattern in activity with regards to when victims are named on Clop’s leak site or their data made available for download. Operatives likely post at their own discretion, prioritizing victims based on the negotiation process, the profile of the victim, whether or not the operatives feel they have been “respected”, and what would be the most embarrassing for the victim with regards to timing.

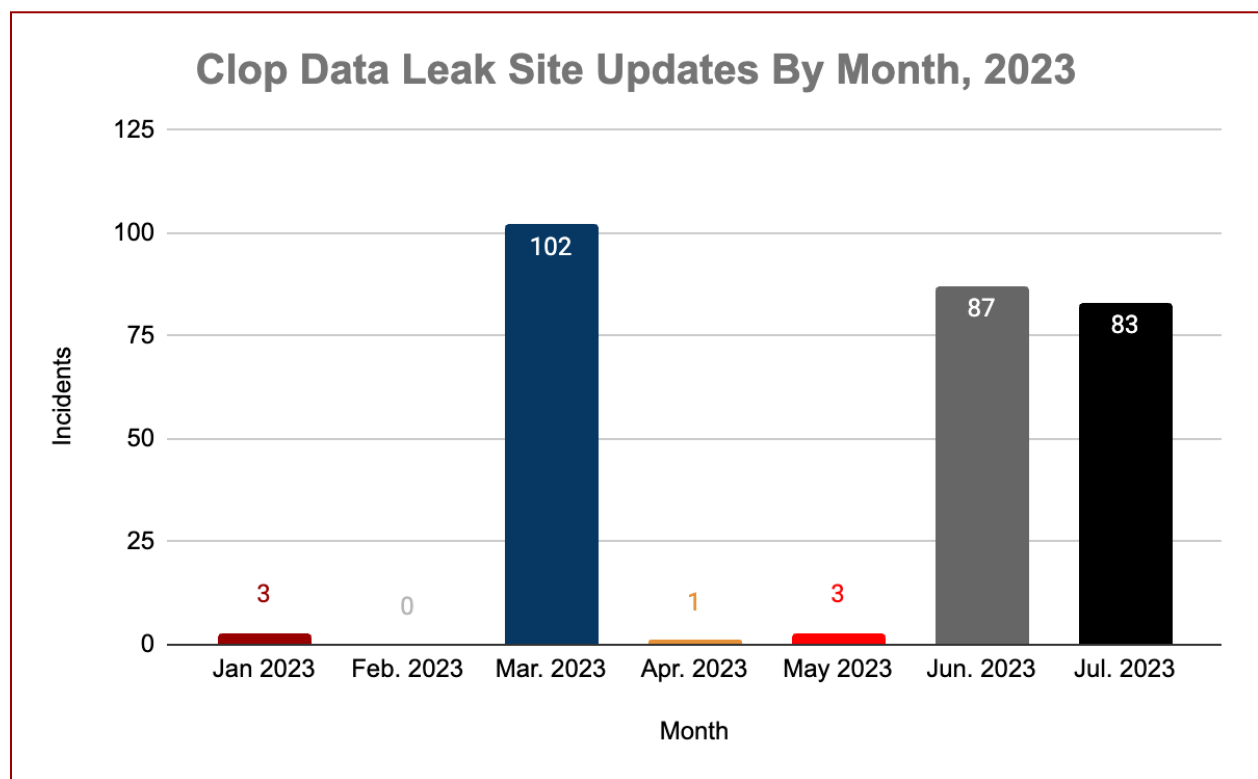
Brief | Analysis of Clop Activity

B-2023-07-17a

TLP:GREEN



Leak Site Additions By Day Top 3	Leak Site Additions By Week Top 3	Leak Site Additions By Month Top 3
Mar. 28, 2023 - 33	Mar. 27 - Apr. 2, 2023 - 64	March 2023 - 102
Mar. 27, 2023 - 30	Jul. 10 - Jul. 16, 2023 - 51	June, 2023 - 87
Mar. 21, 2023 - 26	Mar. 20 - Mar. 26, 2023 - 35	July 2023 - 83 (to date)

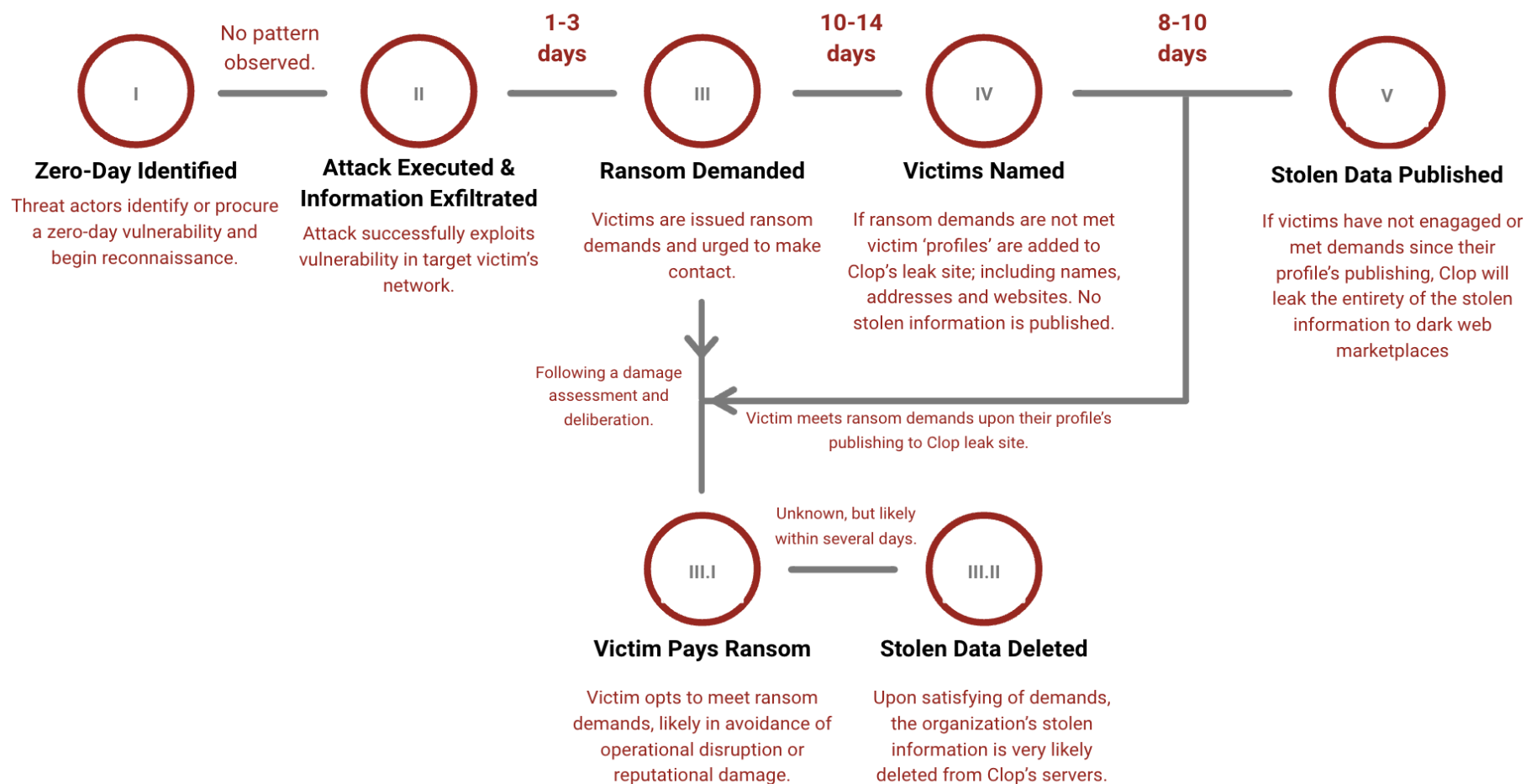


Clop Data Leak Site Updates by Month, 2023

Source: ZeroFox Intelligence

> Typical Timescales for Clop's Extortion*

*Medium confidence assessment based on observed procedures and timeframes.



Source: ZeroFox Intelligence

| Recommendations

- Implement a culture of security awareness into workplaces with the delivery of both proactive and reactive education covering cyber hygiene measures and contemporary threats.
- Provide educational training to ensure employees are aware of commonly-used social engineering methods and how to identify phishing attempts.
- Develop a comprehensive cybersecurity policy outlining acceptable use of technology, user security procedures (SyOps), credential guidance, audit processes, and data handling procedures.
- Maintain a clear and comprehensive incident response strategy consisting of business resilience and continuity plans, incident reporting procedures, and key authorities.
- Ensure all business IT assets are updated with the latest manufacturer software updates and security patches, supported by the implementation of an effective patch management system.
- Liaise with external cybersecurity companies to maintain an up-to-date understanding of the contemporary threats against organizations within Five Eyes nations and how mitigating measures can best be applied to safeguard against business vulnerabilities.
- Protect end-point devices with the use of business-grade, anti-malware solutions, two-factor authentication (2FA) methods, and by granting users the minimum privileges necessary according to their role.
- Ensure critical or proprietary data is always backed up to secure, off-site or cloud servers. Sensitive information should be properly compartmentalized, avoiding aggregation or unnecessary accumulation.

Appendix A: Traffic Light Protocol for 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 judgements 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 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%