ZEROFOX Intelligence

Flash

Clop Ransomware Collective Targets New Victims Across Multiple Sectors

F-2023-06-15b

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Ransomware, Threat Actor Activity

June 15, 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 3:00 PM (EDT) on June 15, 2023; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Clop Ransomware Collective Targets New Victims Across Multiple Sectors

› Key Findings

- After a noticeable decline in activity over the past two months, the Clop ransomware collective announced 27 new victims on its shame site between June 14-15, 2023.
- Victims represent a wide variety of industries and geographic locations.
- ZeroFox has not independently verified claims that the latest attacks are likely the result of the collective exploiting the latest MOVEit vulnerability.
- As reported by ZeroFox researchers on June 2, 2023, a zero-day vulnerability was identified in MOVEit Transfer, a secure managed file transfer software, with reports stating it is being actively exploited in attacks.

| Analyst Commentary

Clop has not made any of the recently-announced victim data available for download.

Currently Announced Victims	
shell[.]com	1stsource[.]com
datasite[.]com	putnam[.]com
studentclearinghouse[.]org	oekk[.]ch
uhcsr[.]com	landal[.]com
greenshield[.]ca	heidelberg[.]com
bankers-bank[.]com	leggett[.]com
uga[.]edu	healthequity[.]com
synlab[.]fr	cuanswers[.]com
navaxx[.]lu	delawarelife[.]com
316fiduciaries[.]com	enzo[.]com
careservicesllc[.]com	genericon[.]at
brault[.]us	aplusfcu[.]org
barharbor[.]bank	powerfi[.]org
eastwestbank[.]com	

Judging from the list above, Clop ransomware attacks have impacted a range of industries, including Financial Services, Insurance, Healthcare, Manufacturing, Technology, Energy, Non-Profit, and Education. Multiple countries—including the United States, the United Kingdom, Switzerland, Belgium, Germany, Canada, France, Luxembourg, and Austria—have been targeted, with a significant portion of the victims based in the United States. While there are claims that the latest attacks are likely the result of the collective exploiting the latest MOVEit vulnerability, ZeroFox researchers have not independently verified these claims.

Recommendations

- Subscribe to ZeroFox Advanced Dark Web Intelligence for updates on new ransomware targets.
- Utilize the ZeroFox Platform's Intelligence Search interface to investigate Indicators of Compromise and metadata related to Ransomware.
- Reset service account credentials for affected systems and MOVEit Service Accounts.
- Patch MOVEit Transfer versions: 2021.0.x, 2021.1.x, 2022.0.x, 2022.1.x, and 2023.0.0.
- Users are advised to upgrade to versions 2021.0.6, 2021.1.4, 2022.0.4, 2022.1.5, and 2023.0.1.
- Disable all HTTP and HTTPs traffic to your MOVEit Transfer environment.
- Confirm files have been successfully deleted and no unauthorized accounts remain.

Appendix: 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.