HC3: Sector Alert

April 28, 2023 TLP:CLEAR Report: 202304281500

New Data Breaches from Cl0p and Lockbit Ransomware Groups

Executive Summary

Ransomware-as-a-service (RaaS) groups Cl0p and Lockbit recently conducted several distinct attacks, exploiting three known vulnerabilities (CVE-2023-27351, CVE-2023-27350, and CVE-2023-0669). The Cybersecurity and Infrastructure Security Agency (CISA) added the latter two vulnerabilities to its Known Exploited Vulnerabilities Catalog but has not yet added the first. This Sector Alert follows previous HC3 products on Cl0p (Cl0p Allegedly Targeting Healthcare Industry and Cl0p Ransomware) and Lockbit (Lockbit Ransomware, LockBit 3.0, and LockBit 2.0 IOCs), and provides an update on the recent attacks, and recommendations to detect and protect against future ransomware attacks.

Report

As early as April 13, 2023, Microsoft attributed exploitations on a software company's servers to the RaaS group known as Cl0p. On April 19, the printing management software company revealed the vulnerabilities in the widely used PaperCut MF/NG print management software and urged administrators to upgrade their servers to the latest versions (20.1.7, 21.2.11, and 22.0.9 and later). The software developer claims that its software is used by more than 100 million users from over 70,000 companies worldwide. On April 21, CISA added the CVE-2023-27350 flaw to its Known Exploited Vulnerabilities catalog, ordering federal agencies to secure their systems against ongoing exploitation within three weeks by May 12, 2023.

On April 26, Microsoft revealed that both RaaS groups, Cl0p and LockBit, were behind the attacks and used them to steal corporate data from vulnerable servers. They disclosed that the Cl0p ransomware used was traced to the threat actor known as Lace Tempest, and overlapped with FIN11 and TA505, both linked to the ransomware operation. In its exploits, the threat actor deployed TrueBot malware, which has also been previously linked to Cl0p.

Additionally, Microsoft said that some of the intrusions have led to LockBit ransomware attacks. However, industry experts report that it is unclear whether or not the attacks began after the exploits were publicly released.

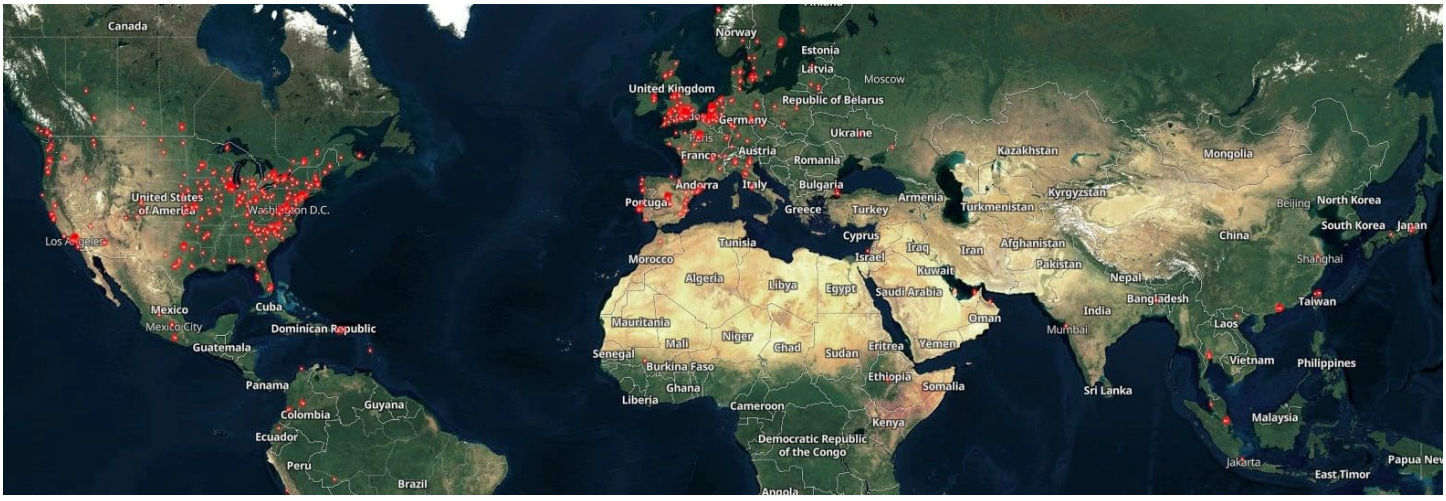

Figure 1: Map of Internet-exposed PaperCut software. *(Source: Bleeping Computer)*

These recent attacks follow a pattern of Cl0p in stealing data to extort companies into paying a ransom.

HC3: Sector Alert

April 28, 2023 TLP:CLEAR Report: 202304281500

This trend was first identified in 2020 when the RaaS group stole data from approximately 100 companies by exploiting an Accellion FTA zero-day vulnerability. As noted in a recent HC3 Secor Alert, in early February, Cl0p also claimed attribution for a mass attack on more than 130 organizations, including those in the healthcare sector, using a zero-day vulnerability in secure file transfer software, GoAnywhere MFT.

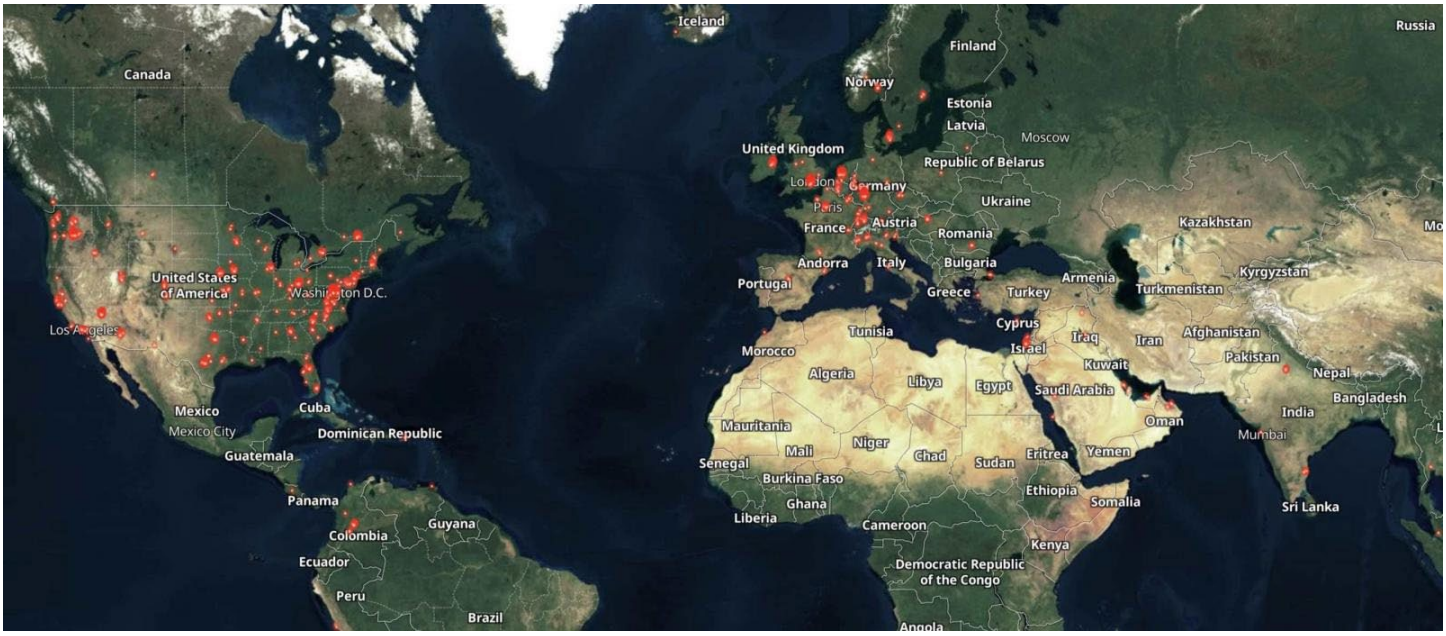

Figure 2: Map of Internet-exposed GoAnywhere MFT appliances. *(Source: Bleeping Computer)*

Since CISA added the CVE-2023-0669 flaw to its Known Exploited Vulnerabilities catalog, a separate company recently completed its own investigation into the previous 10-day exploitation of the vulnerability in the GoAnwhere MFT software. Cl0p utilized the vulnerability to create unauthorized user accounts in some MFTaaS customer environments, using some of the accounts to download files. The threat actor then deployed two additional tools ("Netcat" and "Errors.jsp), with only some of the installation attempts recorded as being successful. Netcat, a legitimate program for managing reading and writing data over a network, can be used to establish back doors, conduct port scanning, or transfer files between a compromised system and its server. The JavaServer Pages (JSP) file is used for creating dymanic web pages. However, it is still unknown how the file was used in the attacks.

Industry experts also noted that the recent increase in ransomware attacks this past March was attributed to the exploitation of the GoAnywhere MTF vulnerability. There was a 91% increase in attacks since February 2023, with 459 attacks recorded in March alone. Of those attacks, Cl0p targeted 129 victims. Unlike other RaaS groups, Cl0p unabashedly and almost exclusively targets the healthcare sector. In the calendar year 2021 alone, 77% (959) of its attack attempts were on this critical infrastructure industry. The attacks in March of this year mark the second time that the threat group known as LockBit has been knocked off the top spot since September 2021.

Vulnerabilities

CVE-2023-27350 (Last Modified April 26, 2023)		
Description	Vulnerability	This vulnerability allows remote attackers to bypass authentication on affected installations of PaperCut NG 22.0.5 (Build 63914). Authentication is not required to

		exploit this vulnerability. The specific flaw exists within the SetupCompleted class. The issue results from improper access control. An attacker can leverage this vulnerability to bypass authentication and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-18987.
	CVSS Score	9.8 Critical
Weakness Enumeration	CWE-ID	CWE-284
	CWE Name	Improper Access Control
	Source	Zero Day Initiative

CVE-2023-27351 (Last Modified April 20, 2023)		
Description	Vulnerability	This vulnerability allows remote attackers to bypass authentication on affected installations of PaperCut NG 22.0.5 (Build 63914). Authentication is not required to exploit this vulnerability. The specific flaw exists within the SecurityRequestFilter class. The issue results from improper implementation of the authentication algorithm. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-19226.
	CVSS Score	8.2 High
Weakness Enumeration	CWE-ID	CWE-287
	CWE Name	Improper Authentication
	Source	Zero Day Initiative

CVE-2023-0669 (Last Modified April 10, 2023)		
Description	Vulnerability	GoAnywhere MFT suffers from a pre-authentication command injection vulnerability in the License Reponse Servlet due to deserializing an arbitrary attacker-controlled object. This issue was patched in version 7.1.2.
	CVSS Score	7.2 High
Weakness Enumeration	CWE-ID	CWE-502
	CWE Name	Deserialization of Untrusted Data
	Source	NIST/Rapid7, Inc.

Patches, Mitigations, and Workarounds

For both CVE-2023-27351 and CVE-2023-27350 vulnerabilities, security researchers advise administrators unable to promptly patch their servers to take measures to prevent remote exploitation. This includes blocking all traffic to the web management port (default port 9191) from external IP addresses on an edge device, as well as blocking all traffic to the same port on the server's firewall to restrict management access solely to the server and prevent potential network breaches.

For the CVE-2023-0669 vulnerability, the company recommends that users rotate the Master Encryption Key, reset all credentials, review audit logs, and delete any suspicious administrator or user accounts.

Way Forward

In addition to previous HC3 Analyst Note product recommendations on how to safeguard against ClOp and other ransomware/extortion attacks, some cyber security professionals advise that the healthcare industry acknowledge the ubiquitous threat of cyberwar against them and recommend that their cybersecurity teams implement the following steps:

- Educate and train staff to reduce the risk of social engineering attacks via email and network access.

- Assess enterprise risk against all potential vulnerabilities and prioritize implementing the security plan with the necessary budget, staff, and tools.
- Develop a cybersecurity roadmap that everyone in the healthcare organization understands.

Furthermore, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) provides links to online government resources (general information, frequently asked questions, tips, and a ransomware readiness self-assessment) to proactively and reactively aid healthcare organizations.

The probability of cyber threat actors, including ClOp, targeting the healthcare industry remains high. Prioritizing security by maintaining awareness of the threat landscape, assessing their situation, and providing staff with tools and resources necessary to prevent an cyberattack remains the best way forward for healthcare organizations.

Relevant HHS Reports

HC3: Alert - LockBit 2.0 IOCs (February 7, 2022)

HC3: Alert - LockBit Ransomware (September 23, 2021)

HC3: Alert - Russian State-Sponsored and Criminal Cryber Threats to Critical Infrastructure (May 9, 2022)

HC3: Analyst Note - Clop Ransomware (January 4, 2023)

HC3: Analyst Note - LockBit 3.0 (December 12, 2022)

HC3: Sector Alert - Clop Allegedly Targeting Healthcare Industry (February 22, 2023)

References

Abrams, Lawrence. “Clop, Lockbit ransomware gangs behind PaperCut server attacks,” *Bleeping Computer*. April 26, 2023. https://www.bleepingcomputer.com/news/security/clop-lockbit-ransomware-gangs-behind-papercut-server-attacks/

Gatlan, Sergiu. “Clop ransomware claims it breached 130 orgs using GoAnywhere zero-day,” *Bleeping Computer*. February 10, 2023. https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-it-breached-130-orgs-using-goanywhere-zero-day/

Gatlan, Sergiu. “Exploit released for PaperCut flaw abused to hijack servers, patch now,” *Bleeping Computer*. April 24, 2023. https://www.bleepingcomputer.com/news/security/exploit-released-for-papercut-flaw-abused-to-hijack-servers-patch-now/

Lakshmanan, Ravie. “Fortra Sheds Light on GoAnywhere MFT Zero-Day Exploit Used in Ransomware Attacks,” *The Hacker News*. April 20, 2023. https://thehackernews.com/2023/04/fortra-sheds-light-on-goanywhere-mft.html

“National Vulnerability Database: CVE-2023-0669 Detail,” National Institute of Standards and Technology. Last modified April 10, 2023. https://nvd.nist.gov/vuln/detail/CVE-2023-0669#

"National Vulnerability Database: CVE-2023-27350 Detail," National Institute of Standards and Technology. Last modified April 26, 2023. https://nvd.nist.gov/vuln/detail/CVE-2023-27350

"National Vulnerability Database: CVE-2023-27351 Detail," National Institute of Standards and Technology. Last modified April 20, 2023. https://nvd.nist.gov/vuln/detail/CVE-2023-27351

Toulas, Bill. "Fortra shares findings on GoAnywhere MFT zero-day attacks," *Bleeping Computer*. April 19, 2023. https://www.bleepingcomputer.com/news/security/fortra-shares-findings-on-goanywhere-mft-zero-day-attacks/

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback