Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

HC3: Sector Alert

February 22, 2023 TLP:CLEAR Report: 202302221500

Clop Allegedly Targets Healthcare Industry in Data Breach

Executive Summary

Russia-linked ransomware group Clop reportedly took responsibility for a mass attack on more than 130 organizations, including those in the healthcare industry, using a zero-day vulnerability in secure file transfer software GoAnywhere MFT. Cybersecurity & Infrastructure Security Agency (CISA) added the GoAnywhere flaw (CVE-2023-0669) to its public catalog of Known Exploited Vulnerabilities. This Sector Alert follows previous HC3 Analyst Notes on Clop (CLOP Poses Ongoing Risk to HPH Organizations and CLOP Ransomware) and provides an update on its recent attack, potential new tactics, techniques and procedures (TTPs), and recommendations to detect and protect against ransomware attacks.

Report

Clop claimed attribution to the early February attack when it informed the technology and computer tutorial website *Bleeping Computer* that it allegedly stole personal information and protected health information data over the course of 10 days. It also stated that it has the ability to encrypt affected healthcare systems by deploying ransomware payloads. The threat actor refused to provide any validation of its claims, and Bleeping Computer additionally could not independently confirm them. For now, while these claims are uncorroborated, Clop continues to exhibit a history of employing trend-setting TTPs across multiple operations.

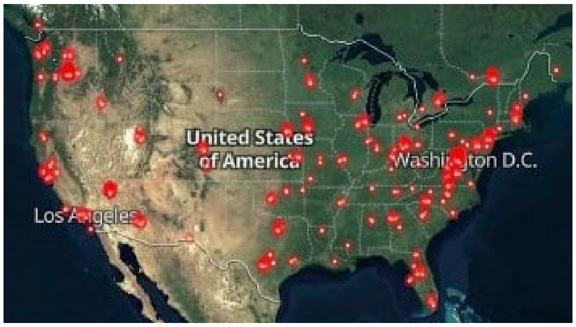

Figure 1 - Map of Vulnerable GoAnywhere MFT Servers in the United States (Bleeping Computer graphic)

HC3's previous Clop Analyst Note observed that Clop was written to target Windows systems. Subsequently, on 26 December 2022, threat research website *SentinelLabs* observed the first Linux variant of Clop ransomware. While similar to the Windows variant, the threat actor constructed the bespoke Linux version using the same encryption method and similar process logic. The nascent Linux variant, however, has several flaws, which make it possible to decrypt locked files without paying a ransom. Regardless, the prevalent use of Linux in servers and cloud workloads makes it easy to suggest that Clop could employ this new ransomware campaign to target additional industries, including healthcare.

Clop (sometimes stylied as "Cl0p") has been active since February 2019, with its first observed attack campaign run by the threat group, TA505. Its characteristic ransomware as a service (RaaS) TTP makes it one of the most successful ransomware groups in the past few years. Unlike other RaaS groups, Clop unabashedly and almost exclusively targets the healthcare sector. In 2021 alone, 77% (959) of its attack attempts were on this critical infrastructure industry. Clop appeared to suffer a major setback in June 2021 when law enforcement arrested six individuals in Ukraine linked to the group. Continued and successful attacks, however, demonstrate that this prolific group is still a viable threat to the healthcare sector.

This incident is by no means an isolated one to this industry. Healthcare is particuarly vulnerable to cyberattacks, owing to their high propensity to pay a ransom, the value of patient records, and often inadequate security. In 2022, 24 hospitals and multihospital healthcare systems were attacked, and more than 289 hospitals were potentially impacted by ransomware attacks. Clop's alleged attack this year only further exacerbates an ever-growing trend to target the healthcare industry, and highlights its vulnerabilities to future cyberattacks.

Vulnerabilities

The zero-day vulnerability in GoAnywhere MFT contains a pre-authentication remote code execution vulnerability in the License Response Servlet due to deserializing an attacker-controlled object.

Patches, Mitigations, and Workarounds

Developers of the software initially warned clients of the remote code execution vulnerability in early February. However, prior to the delivery of an emergency patch, in order to view the initial security advisory, users had to create a (free) account in order to access the vulnerability report. The use of a customer portal to view the advistory was heavily criticized by cybersecurity experts. Ben Krebs, who first detected details of the zero-day vulnerability on 02 February, publicized its details and the full text of the security advisory on the social media sharing platform Mastodon. An emergency patch (Version 7.1.2) to the affected software was finally released on 07 February.

The vulnerability (tracked as CVE-2023-0669) was added to CISA's *Known Exploited Vulnerabilities Catalog* on 10 February. As of 15 February, CISA ordered all Federal civilian executive branch agencies to patch their systems before 03 March.

Way Forward

In addition to previous HC3 Analyst Note product recommendations on how to safeguard against Clop and other ransomware/extortion attacks, some cybersecurity 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 like 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.

References

"CLOP Poses Ongoing Risk to HPH Organizations." Health Sector Cybersecurity Coordination Center (HC3) Analyst Note, Report: 202103231400. 23 March 2021. https://www.hhs.gov/sites/default/files/clop-poses-ongoing-risk-to-hph-organizations.pdf

"CLOP Ransomware." Health Sector Cybersecurity Coordination Center (HC3) Analyst Note, Report:

202301041300. 04 January 2023. https://www.hhs.gov/sites/default/files/clop-ransomware-analyst-note-tlpclear.pdf

Diaz, Naomi. “289 healthcare organizations were impacted by ransomware attacks in 2022.” Becker’s Healthcare. 03 January 2023. https://www.beckershospitalreview.com/cybersecurity/289-healthcare-organizations-were-impacted-by-ransomware-attacks-in-2022.html#:~:text=Ransomware%20attacks%20impacted%20more%20than,hospitals%2C%20according%20to%20the%20report.

Dickerson, Shawn. “Why is healthcare a top target for cybersecurity threats?” Security Magazine. 13 September 2022. https://www.securitymagazine.com/articles/98324-why-is-healthcare-a-top-target-for-cybersecurity-threats#:~:text=Healthcare%20organizations%20have%20experienced%20a,records%2C%20and%20often%20inadequate%20security.

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

Page, Carly. “A new Linux variant of Clop ransomware has major flaws, researchers say.” TechCrunch. 07 February 2023. https://techcrunch.com/2023/02/07/clop-ransomware-linux-flaw/

Page, Carly. “Ukrainian police arrest multiple Clop ransomware gang systems.” TechCrunch. 16 June 2021. https://techcrunch.com/2021/06/16/ukrainian-police-arrest-multiple-clop-ransomware-gang-suspects/

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