**DATA STEAL FROM KEY NORTH CAROLINA HOSPITAL BY CLOP GANG**



**A number of cybercrimes at significant North Carolina hospitals have been attributed by researchers at the healthcare technology company Nuance to the Clop gang.**



The Progress MOVEit Transfer campaign saw the Clop extortion gang steal personal information from important North Carolina institutions, according to the Microsoft-owned healthcare technology company Nuance.

Enterprises use MOVEit Transfer, a managed file transfer service, to safely move data via SFTP, SCP, and HTTP-based uploads.

Microsoft credited the campaign that took use of a zero-day vulnerability in the MOVEit Transfer platform, identified as CVE-2023-34362, to the Clop ransomware gang (also known as Lace Tempest).

The MOVEit Transfer vulnerability was used by the Clop ransomware organization to allegedly breach into hundreds of companies worldwide in June.

The health-care technology division of Microsoft, Nuance, is also one of the victims of the Clop gang.

With the aid of cyber security specialists and a law company, Nuance opened an inquiry into the event.

On Friday, the business claimed that the Clop group may have stolen personal information from multiple hospitals and other healthcare facilities in North Carolina, including:

* [Atrium Health](https://atriumhealth.org/?gclid=CjwKCAjwpJWoBhA8EiwAHZFzfmRSW25Zs0bA0ngZeUTGpPeXVwE1fqizULLIK_TOr2Gc0DNQKygmBxoCB9wQAvD_BwE), the Charlotte-based health care system giant.
* [Catawba Valley Medical Center](https://www.catawbavalleyhealth.org/)in Hickory.
* [Charlotte Radiology](https://www.charlotteradiology.com/).
* [Duke University Health System](https://www.dukehealth.org/).
* DLP [Central Carolina Medical Center](https://www.centralcarolinahosp.com/)in Sanford.
* Greenville-based [ECU Health](https://www.ecuhealth.org/).
* Pinehurst-based [FirstHealth of the Carolinas](https://www.firsthealth.org/" \t "_blank).
* Asheville-based [Mission Health System](https://missionhealth.org/).
* Winston-Salem-based [Novant Health](https://www.novanthealth.org/pf/?utm_source=google&utm_term=novant%20health&utm_cmpid=1070255209&utm_adgid=59293428704&utm_tgtid=kwd-302442297305&utm_mt=e&utm_adid=423668156296&utm_dvc=c&utm_ntwk=g&utm_adpos&utm_plcmnt&utm_feeditemid&utm_devicemdl&utm_plcmnttgt&utm_locphysid=9009940&utm_locintid&gclid=CjwKCAjwpJWoBhA8EiwAHZFzfl1a1TfKkpTEi7VrQH-RXK-ND9Jhyq50nQGc9QLQ1UEKpmdxDGAgFhoCM7wQAvD_BwE).
* [Novant Health New Hanover Regional Medical Center](https://www.novanthealth.org/locations/medical-centers/new-hanover-regional-medical-center/)in Wilmington.
* Chapel Hill-based [UNC Health](https://www.unchealth.org/home).
* Raleigh-based [Wake Radiology Diagnostic Imaging](https://www.wakerad.com/).
* Raleigh-based [WakeMed Health & Hospitals](https://www.wakemed.org/" \t "_blank).

According to the Nuance news release. threat actors also had access to services people received and their demographic information.

Compromised data included the services people received and their demographic information,

Nuance announced to have immediately addressed the issue after the software vendor, Progress, disclosed the flaw and released security updates to fix it on May 31.

“Patches were installed as soon as they were available,” the Nuance release said in a press release. “Data privacy and security are among Nuance’s highest priorities,” reads a statement published by the company. “The company has extensive measures in place to protect information entrusted to us.”

People are recommended to review account statements and monitor their [free credit reports](https://www.annualcreditreport.com/index.action)for suspicious activity.

US hospitals are under pressure, and recent cyberattacks have hit multiple facilities.

Because it disclosed the intrusion of Prospect Medical Holdings and the theft of personal data from the company, the Rhysida ransomware group recently garnered news.

Several hospitals run by Prospect Medical Holdings that are spread across several states, including California, Texas, Connecticut, Rhode Island, and Pennsylvania, had their computer systems affected by a cyberattack in the early days of August.

Due to a cyberattack on their networks, some emergency departments in numerous hospitals across various states had to close, and ambulances had to be rerouted.

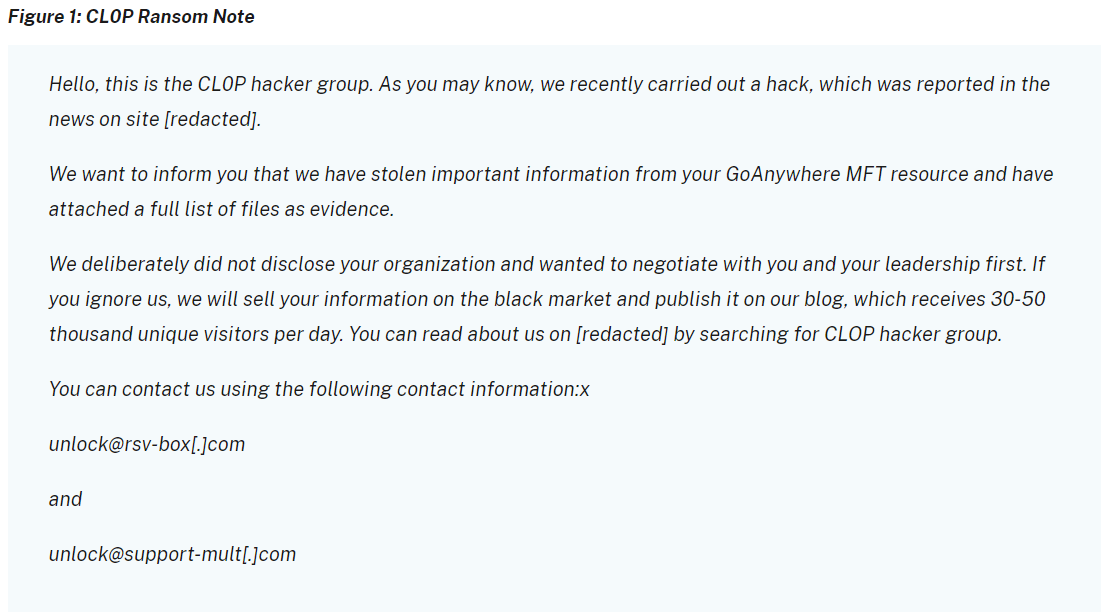
The second largest employer on the Mississippi Gulf Coast is the Singing River Health System, which operates 3 hospitals and 10 clinics.

The operations of the Idaho Falls Community Hospital were affected by a cyberattack that occurred in June. Hospital representatives stated that several clinics had to close as a result of the cyberattack, and some ambulances had to be redirected to hospitals close by.

The Mountain View Hospital, another hospital in the same area, had a cyber attack. Authorities revealed that a malware had compromised a few of the hospital's IT systems.

**ACTIONS TO TAKE TODAY TO MITIGATE CYBER THREATS FROM CL0P RANSOMWARE:**

1. **Take an inventory of assets and data, identifying authorized and unauthorized devices and software.**
2. **Grant admin privileges and access only when necessary, establishing a software allow list that only executes legitimate applications.**
3. **Monitor network ports, protocols, and services, activating security configurations on network infrastructure devices such as firewalls and routers**
4. **Regularly patch and update software and applications to their latest versions, and conduct regular vulnerability assessments.**



CL0P’s toolkit contains several malware types to collect information, including the following:

* [**FlawedAmmyy**](https://attack.mitre.org/versions/v13/software/S0381/)**/[FlawedGrace](https://attack.mitre.org/software/S0383/" \o "FlawedGrace)**remote access trojan (RAT) collects information and attempts to communicate with the Command and Control (C2) server to enable the download of additional malware components [[T1071](https://attack.mitre.org/versions/v13/techniques/T1071/)], [[T1105](https://attack.mitre.org/versions/v13/techniques/T1105/)].
* [**SDBot**](https://attack.mitre.org/versions/v13/software/S0461/) RAT propagates the infection, exploiting vulnerabilities and dropping copies of itself in removable drives and network shares [[T1105](https://attack.mitre.org/versions/v13/techniques/T1105/)]. It is also capable of propagating when shared though peer-to-peer (P2P) networks. SDBot is used as a backdoor [[T1059.001](https://attack.mitre.org/versions/v13/techniques/T1059/001/)] to enable other commands and functions to be executed in the compromised computer. This malware uses application shimming for persistence and to avoid detection [[T1546.011](https://attack.mitre.org/versions/v13/techniques/T1546/011/)].
* **Truebot** is a first-stage downloader module that can collect system information and take screenshots [[T1113](https://attack.mitre.org/versions/v13/techniques/T1113/)], developed and attributed to the [Silence](https://attack.mitre.org/groups/G0091/) hacking group. After connecting to the C2 infrastructure, Truebot can be instructed to load shell code [[T1055](https://attack.mitre.org/versions/v13/techniques/T1055/)] or DLLs [[T1574.002](https://attack.mitre.org/versions/v13/techniques/T1574/002/)], download additional modules [[T1129](https://attack.mitre.org/versions/v13/techniques/T1129/)], run them, or delete itself [[T1070](https://attack.mitre.org/versions/v13/techniques/T1070/)]. In the case of TA505, Truebot has been used to download FlawedGrace or Cobalt Strike beacons.
* [Cobalt Strike](https://attack.mitre.org/versions/v13/software/S0154/) is used to expand network access after gaining access to the Active Directory (AD) server [[T1018](https://attack.mitre.org/versions/v13/techniques/T1018/)].
* **DEWMODE** is a web shell written in PHP designed to target Accellion FTA devices and interact with the underlying MySQL database and is used to steal data from the compromised device [[1505.003](https://attack.mitre.org/versions/v13/techniques/T1505/003/)].
* **LEMURLOOT** is a web shell written in C# designed to target the MOVEit Transfer platform. The web shell authenticates incoming http requests via a hard-coded password and can run commands that will download files from the MOVEit Transfer system, extract its Azure system settings, retrieve detailed record information, create, insert, or delete a particular user. When responding to the request, the web shell returns data in a gzip compressed format.

Credits:

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a>

<https://securityaffairs.com/150949/cyber-crime/north-carolina-hospitals-data-breach.html>