Microsoft: Clop and LockBit ransomware behind PaperCut server hacks

By Lawrence Abrams

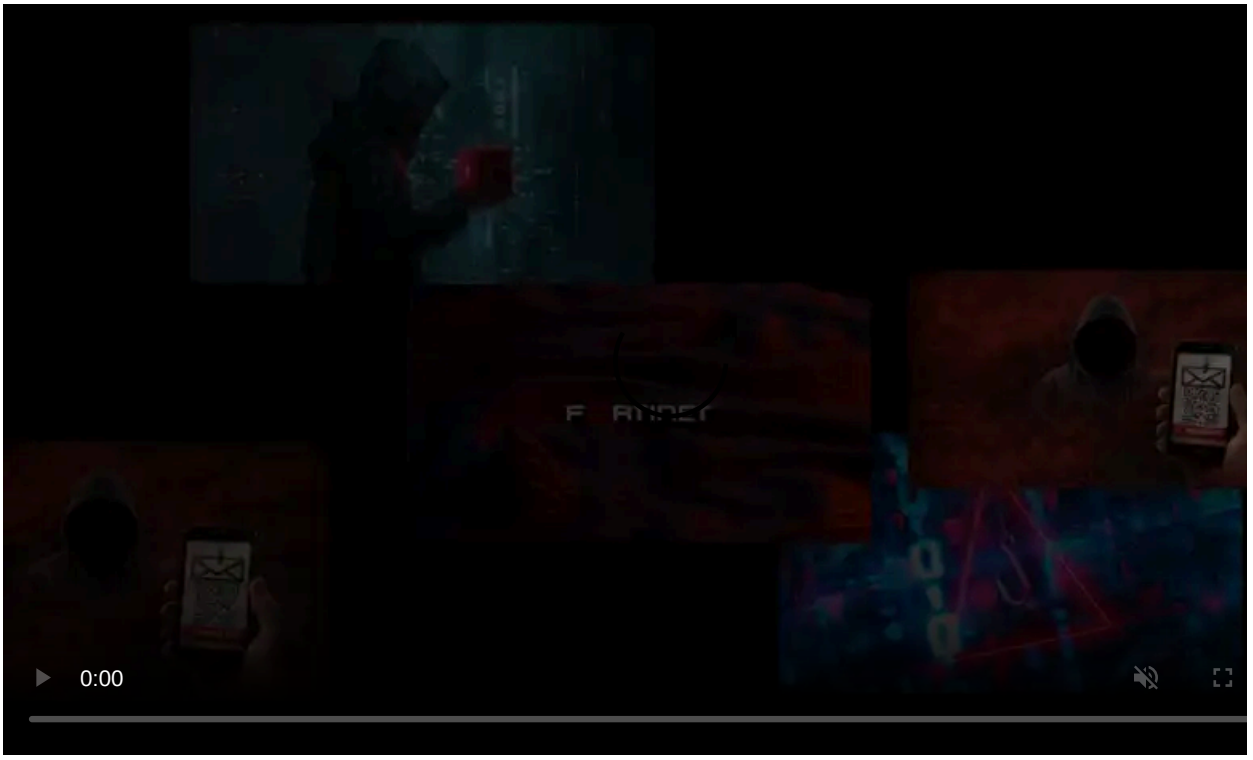
Published: 2023-04-26 · Archived: 2026-04-06 03:17:39 UTC

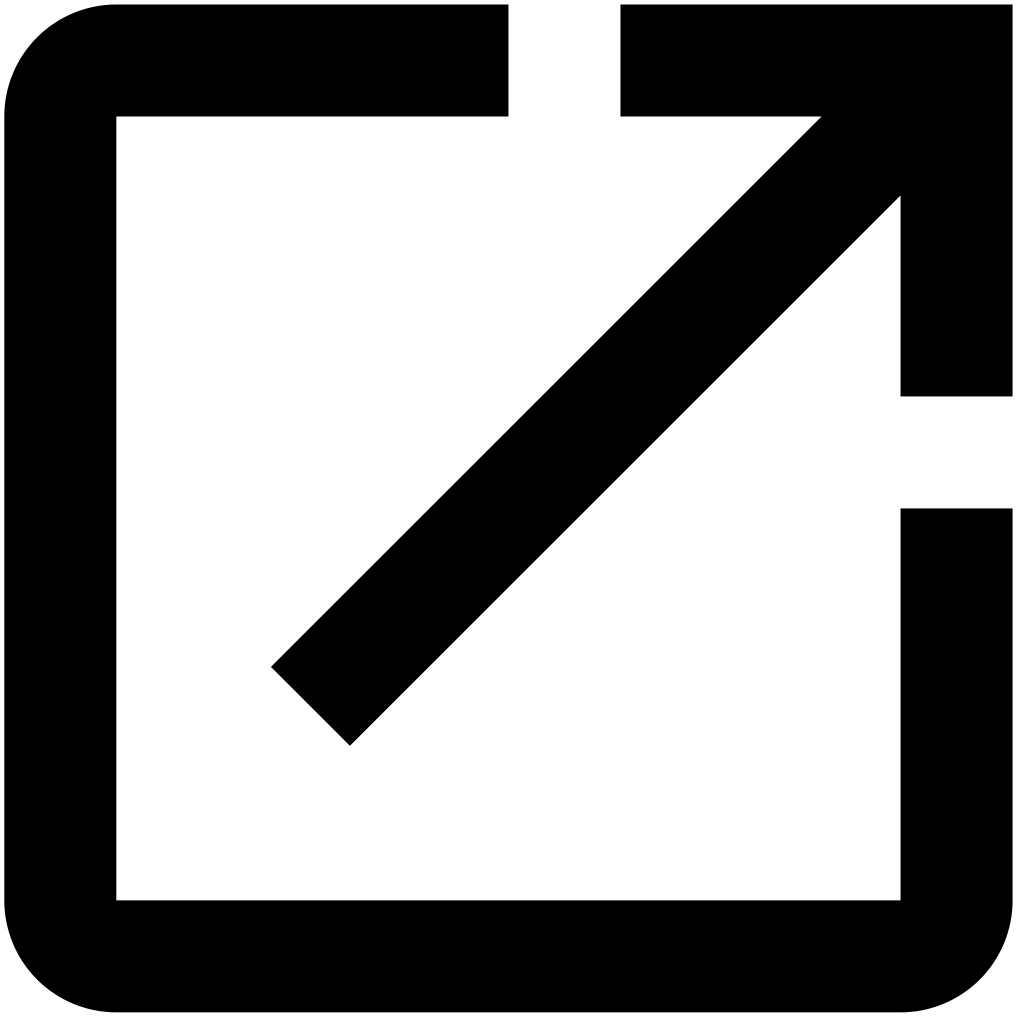
Microsoft has attributed recent attacks on PaperCut servers to the Clop and LockBit ransomware operations, which used the vulnerabilities to steal corporate data.

Last month, two vulnerabilities were fixed in the PaperCut Application Server that allows remote attackers to perform unauthenticated remote code execution and information disclosure:

- **CVE-2023–27350 / ZDI-CAN-18987 / PO-1216**: Unauthenticated remote code execution flaw impacting all PaperCut MF or NG versions 8.0 or later on all OS platforms, for both application and site servers. (CVSS v3.1 score: 9.8 – critical)
- **CVE-2023–27351 / ZDI-CAN-19226 / PO-1219**: Unauthenticated information disclosure flaw impacting all PaperCut MF or NG versions 15.0 or later on all OS platforms for application servers. (CVSS v3.1 score: 8.2 – high)

On April 19th, PaperCut disclosed that these flaws were actively exploited in the wild, urging admins to upgrade their servers to the latest version.


0:00



A PoC exploit for the RCE flaw was released a few days later, allowing further threat actors to breach the servers using these exploits.

Ransomware gangs behind attacks

Today, Microsoft disclosed that the Clop and LockBit ransomware gangs are behind these PaperCut attacks and using them to steal corporate data from vulnerable servers.

PaperCut is a printing management software compatible with all major printer brands and platforms. It is used by large companies, state organizations, and education institutes, with the company's website claiming it is used by hundreds of millions of people from over 100 countries.

In a series of tweets posted Wednesday afternoon, Microsoft states that it has attributed the recent PaperCut attacks to the Clop ransomware gang.

"Microsoft is attributing the recently reported attacks exploiting the CVE-2023-27350 and CVE-2023-27351 vulnerabilities in print management software PaperCut to deliver Clop ransomware to the threat actor tracked as Lace Tempest (overlaps with FIN11 and TA505)," tweeted Microsoft's Threat Intelligence researchers.

Microsoft tracks this particular threat actor as 'Lace Tempest,' whose activity overlaps with FIN11 and TA505, both linked to the Clop ransomware operation.

Microsoft says that the threat actor has been exploiting the PaperCut vulnerabilities since April 13th for initial access to the corporate network.

Once they gained access to the server, they deployed the TrueBot malware, which has also been previously linked to the Clop ransomware operation.

Ultimately, Microsoft says a Cobalt Strike beacon was deployed and used to spread laterally through the network while stealing data using the MegaSync file-sharing application.

In addition to Clop, Microsoft says some intrusions have led to LockBit ransomware attacks. However, it's unclear if these attacks began after the exploits were publicly released.

Microsoft recommends admins apply the available patches as soon as possible as other threat actors will likely begin exploiting the vulnerabilities.

A prime target for Clop

The exploitation of PaperCut servers fits a general pattern we have seen with the Clop ransomware gang over the past three years.

While the Clop operation still encrypts files in attacks, they have told BleepingComputer that they prefer to steal data to extort companies into paying a ransom.

This shift in tactics was first seen in 2020 when Clop exploited an Accellion FTA zero-day vulnerability to steal data from approximately 100 companies.

The Clop gang recently utilized zero-day vulnerabilities in the GoAnywhere MFT secure file-sharing platform to steal data from 130 companies.

PaperCut includes a 'Print Archiving' feature that saves all print jobs and documents sent through the server, making it a good candidate for data exfiltration attacks from the operation.

All organizations utilizing PaperCut MF or NG are strongly advised to upgrade to versions 20.1.7, 21.2.11, and 22.0.9 immediately and later to fix these vulnerabilities.

Update 4/27/28: The Clop ransomware operation confirmed to BleepingComputer that they were behind the attacks on PaperCut servers, which they started exploiting on April 13th.

However, they said that they used the vulnerabilities for initial access to networks, rather than to steal documents from the server itself.

In reply to our questions about the LockBit attacks, Microsoft said they had nothing further to share.

Source: https://www.bleepingcomputer.com/news/security/microsoft-clop-and-lockbit-ransomware-behind-papercut-server-hacks/