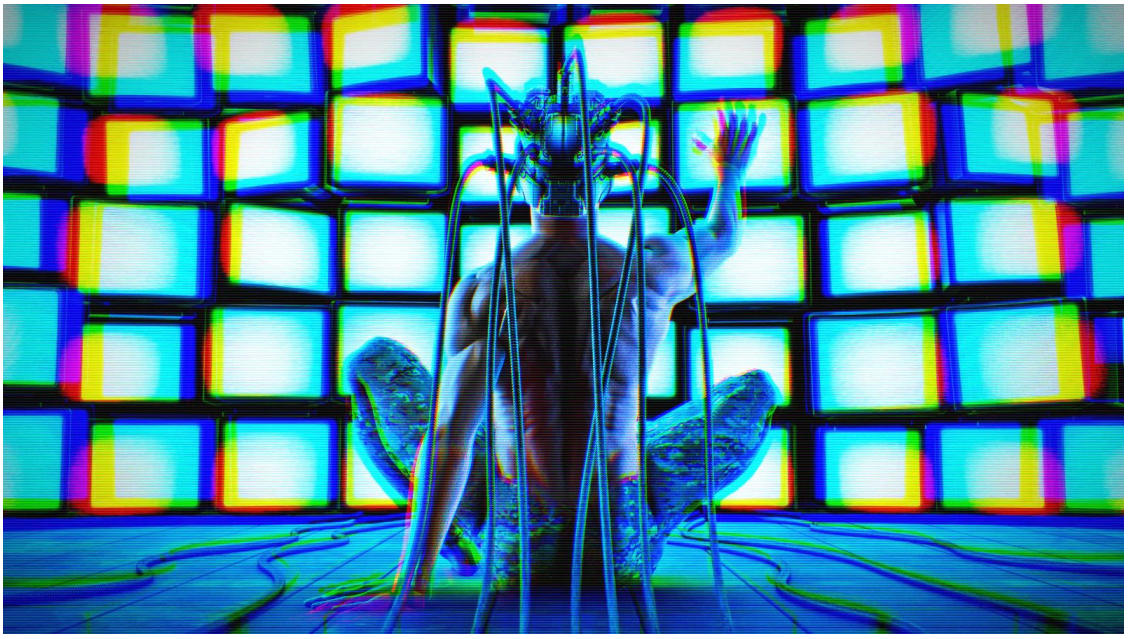
Clop now leaks data stolen in MOVEit attacks on clearweb sites

By Lawrence Abrams

Published: 2023-07-23 · Archived: 2026-04-05 13:33:46 UTC

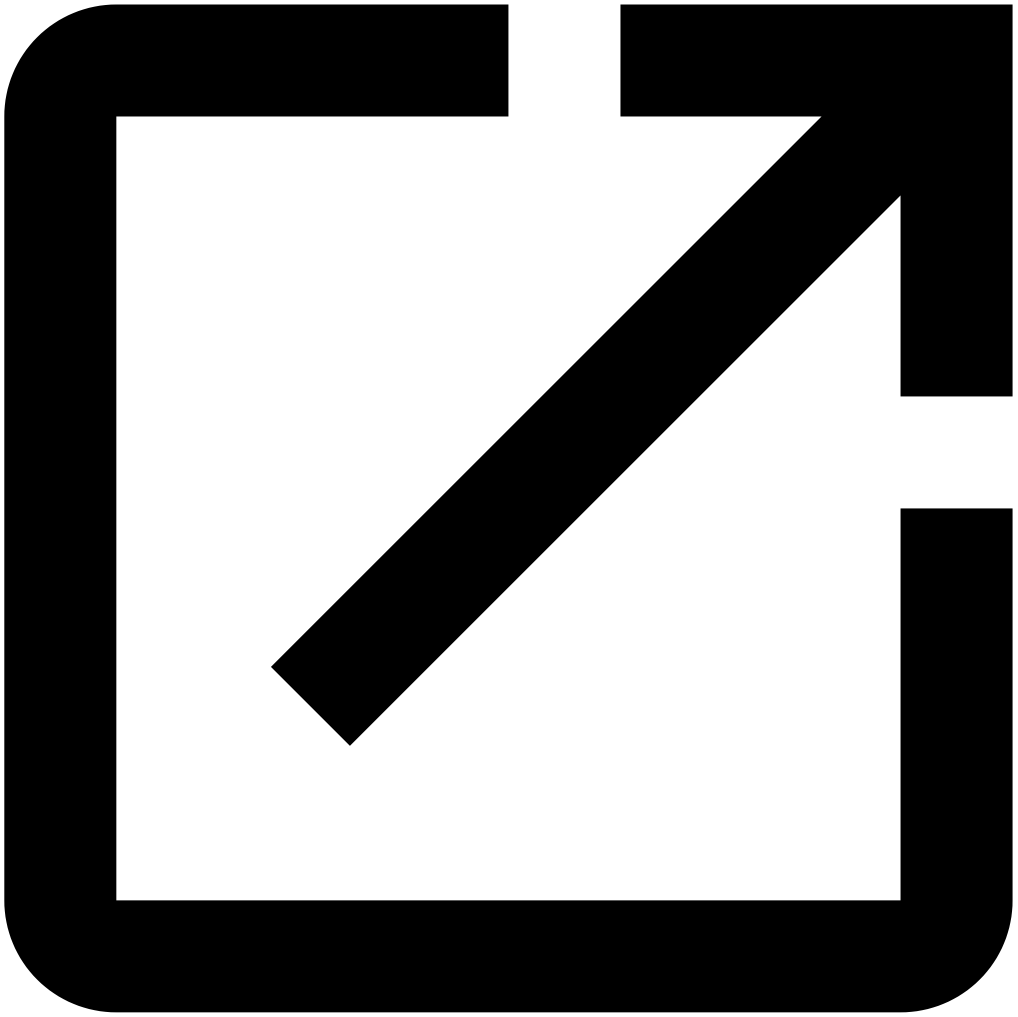


The Clop ransomware gang is copying an ALPHV ransomware gang extortion tactic by creating Internet-accessible websites dedicated to specific victims, making it easier to leak stolen data and further pressuring victims into paying a ransom.

When a ransomware gang attacks a corporate target, they first steal data from the network and then encrypt files. This stolen data is used as leverage in double-extortion attacks, warning victims that the data will be leaked if a ransom is not paid.

Ransomware data leak sites are usually located on the Tor network as it makes it harder for the website to be taken down or for law enforcement to seize their infrastructure.


DIE LINKE.
0:00



However, this hosting method comes with its own issues for the ransomware operators, as a specialized Tor browser is required to access the sites, search engines do not index the leaked data, and the download speeds are typically very slow.

To overcome these obstacles, last year, the ALPHV ransomware operation, also known as BlackCat, introduced a new extortion tactic of creating clearweb websites to leak stolen data that were promoted as a way for employees to check if their data was leaked.

A clearweb website is hosted directly on the Internet rather than on anonymous networks like Tor, which require special software to access.

This new method makes it easier to access the data and will likely cause it to be indexed by search engines, further expanding the spread of the leaked information.

Clop ransomware gang adopts tactic

Last Tuesday, security researcher Dominic Alvieri told BleepingComputer that the Clop ransomware gang had started to create clearweb websites to leak data stolen during the recent and widespread MOVEit Transfer data theft attacks.

The first site created by the threat actors was for business consulting firm PWC, creating a website that leaked the company's stolen data in four spanned ZIP archives.

Soon after Alvieri told BleepingComputer, the threat actors also created websites for Aon, EY (Ernst & Young), Kirkland, and TD Ameritrade.

None of Clop's sites are as sophisticated as the ones created by ALPHV last year, as they simply list links to download the data rather than having a searchable database like BlackCat's sites.

Clearweb site created to leak PWC data

Source: BleepingComputer

A waste of time?

These sites aim to scare employees, executives, and business partners who may have been impacted by the stolen data, hoping it causes them to exert further pressure on a company to pay the ransom.

However, while there may be some benefits to leaking data in this way, they also come with their own problems, as putting them on the Internet, rather than Tor, makes them far more easily taken down.

At this time, all of the known Clop clearweb extortion sites have been taken offline.

It is unclear if these sites are down due to law enforcement seizures, DDoS attacks by cybersecurity firms, or hosting providers and registrars shutting down the sites.

Due to the ease with which they can be shut down, it is doubtful that this extortion tactic is worth the effort.

Source: https://www.bleepingcomputer.com/news/security/clop-now-leaks-data-stolen-in-moveit-attacks-on-clearweb-sites/