Clop ransomware now uses torrents to leak data and evade takedowns

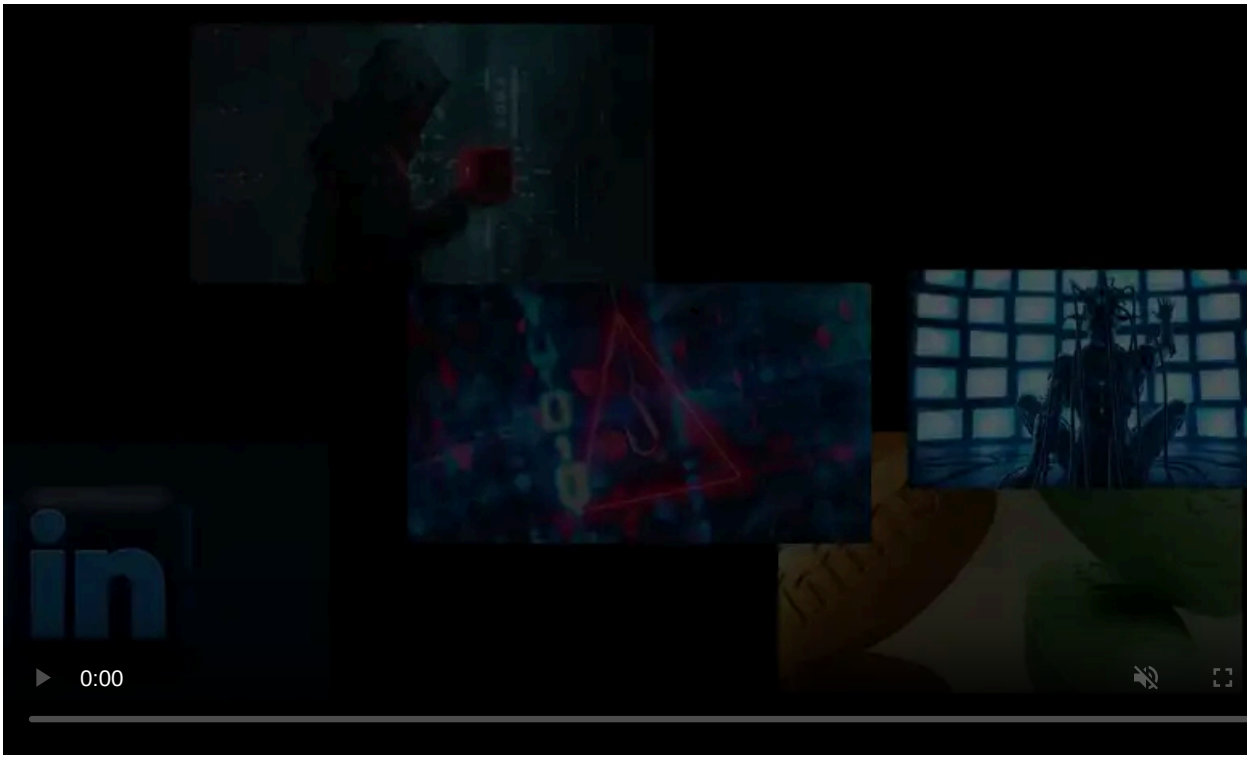
By Lawrence Abrams

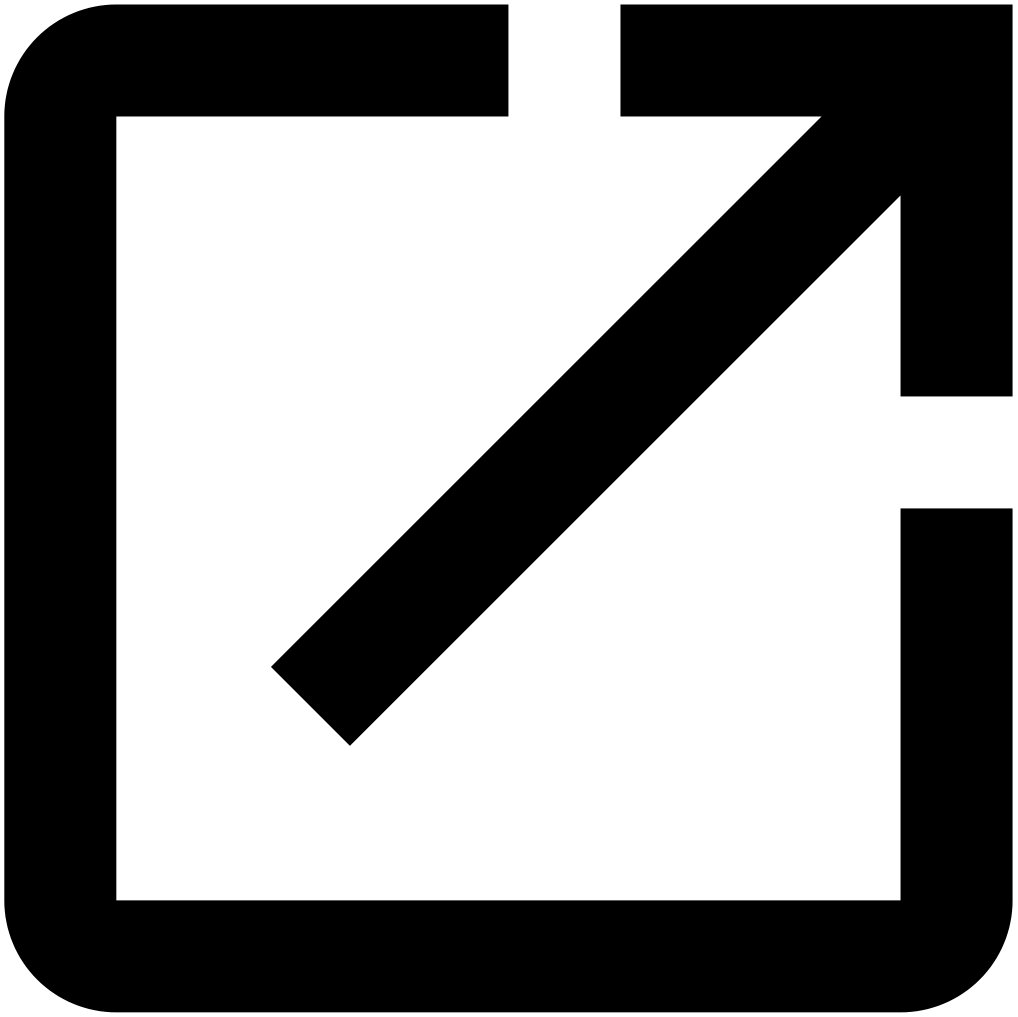
Published: 2023-08-05 · Archived: 2026-04-05 17:06:11 UTC

The Clop ransomware gang has once again altered extortion tactics and is now using torrents to leak data stolen in MOVEit attacks.

Starting on May 27th, the Clop ransomware gang launched a wave of data-theft attacks exploiting a zero-day vulnerability in the MOVEit Transfer secure file transfer platform.

Exploiting this zero-day allowed the threat actors to steal data from almost 600 organizations worldwide before they realized they were hacked.


0:00



On June 14th, the ransomware gang began extorting its victims, slowly adding names to their Tor data leak site and eventually publicly releasing the files.

However, leaking data via a Tor site comes with some drawbacks, as the download speed is slow, making the leak, in some cases, not as damaging as it could be if it was easier to access the data.

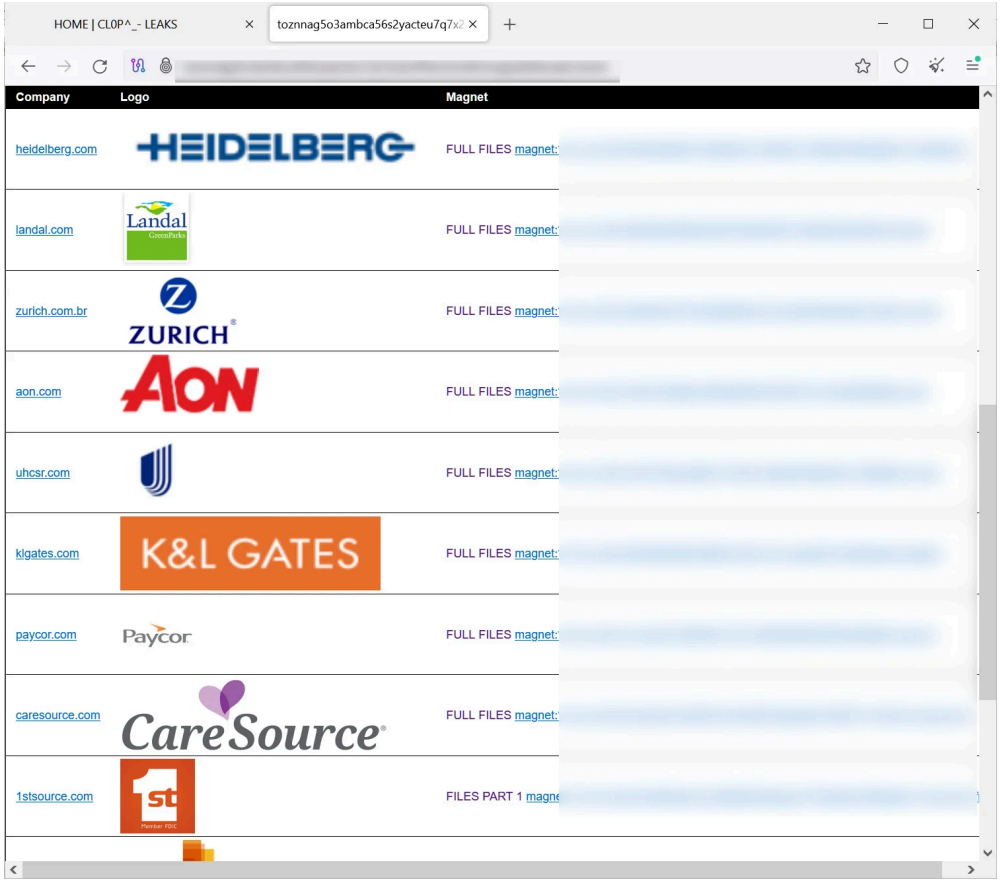
To overcome this, Clop created clearweb sites to leak stolen for some of the MOVEit data theft victims, but these types of domains are easier for law enforcement and companies to take down.

Moving to torrents

As a new solution to these issues, Clop has begun to use torrents to distribute data stolen from MOVEit attack.

According to security researcher Dominic Alvieri, who first spotted this new tactic, torrents have been created for twenty victims, including Aon, K & L Gates, Putnam, Delaware Life, Zurich Brazil, and Heidelberg.

As part of this new extortion method, Clop has set up a new Tor site providing instructions on how to use torrent clients to download the leaked data and lists of magnet links for the twenty victims.



List of available Clop torrents

Source: BleepingComputer

As torrents use peer-to-peer transfer among different users, the transfer speeds are faster than the traditional Tor data leak sites.

In a brief test by BleepingComputer, this method resolved the poor data transfer issues, as we were receiving 5.4 Mbps data transfer speeds, even though it was only seeded from one IP address in Russia.

Furthermore, as this distribution method is decentralized, there is no easy way for law enforcement to shut it down. Even if the original seeder is taken offline, a new device can be used to seed the stolen data as necessary.

If this proves successful for Clop, we will likely see them continue to utilize this method to leak data as it's easier to set up, does not require a complex website, and may further pressure victims due the increased potential for broader distribution of stolen data.

Coveware says Clop is expected to earn $75-$100 million dollars in extortion payments. Not because many victims are paying but because the threat actors have successfully convinced a small number of companies to pay very large ransom demands.

Whether or not the use of torrents will lead to more payments is yet to be determined; however, with these earnings, it may not matter.

Source: https://www.bleepingcomputer.com/news/security/clop-ransomware-now-uses-torrents-to-leak-data-and-evade-takedowns/