Clop ransomware is back in business after recent arrests

By Lawrence Abrams

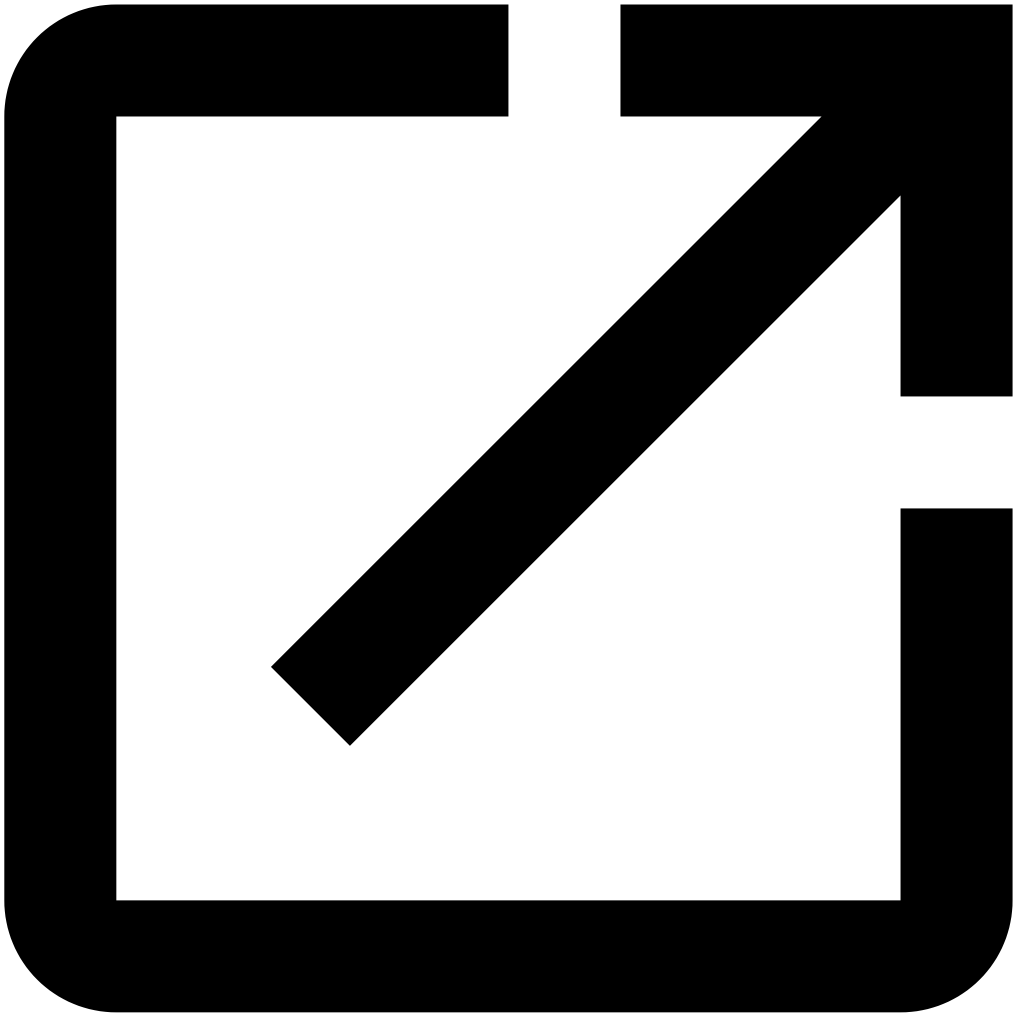
Published: 2021-06-23 · Archived: 2026-04-05 13:22:40 UTC

The Clop ransomware operation is back in business after recent arrests and has begun listing new victims on their data leak site again.

Last week, a law enforcement operation conducted by the National Police of Ukraine, the Korean National Police Agency, and the USA led to the arrest of Clop Ransomware gang members.

A video shared by the Ukrainian police shows law enforcement searching homes and seizing property, including 500 million Ukrainian hryvnias (approximately $180,000), computer equipment, documents, and high-end cars, such as Tesla and Mercedes.


DIE LINKE.
0:00



In a press release, the Ukrainian police described the arrests as a significant blow against the operations and its money laundering of ransom payments.

"Together, law enforcement has managed to shut down the infrastructure from which the virus spreads and block channels for legalizing criminally acquired cryptocurrencies," said the press statement.

Clop reawakens

While the Clop operation laid low for about a week, the ransomware gang has sprung back into action yesterday after releasing the data for two new victims on their ransomware data leak site.

As explained by cybersecurity firm Intel 471, the continued ransomware operation is likely because last week's arrests targeted the money laundering portion of the operation and that the core members were not apprehended.

"The law enforcement raids in Ukraine associated with CLOP ransomware were limited to the cash-out/money laundering side of CLOP's business only," Intel 471 said at the time of the arrests.

"We do not believe that any core actors behind CLOP were apprehended and we believe they are probably living in Russia.

"The overall impact to CLOP is expected to be minor although this law enforcement attention may result in the CLOP brand getting abandoned as we've recently seen with other ransomware groups like DarkSide and Babuk."

While Clop is back in action, law enforcement operations have dealt numerous blows to ransomware groups this year by targeting affiliates and the infrastructure that fuels the criminal activities.

Earlier this year, Bulgarian police seized servers belonging to the Netwalker ransomware, and Ukrainian police arrested Egregor ransomware members. Both ransomware operations shut down after the law enforcement action.

More recently, the FBI arrested a developer for the notorious TrickBot trojan responsible for developing a new ransomware operation.

Who is Clop?

The Clop ransomware gang has been operating since March 2019, when it first began targeting the enterprise using a variant of the CryptoMix ransomware.

Clop will gain an initial foothold on a corporate computer to perform their attacks and then slowly spread throughout the network while stealing data and documents. When they have harvested everything of value, they will deploy the ransomware on the network to encrypt its devices.

Since then, Clop has been responsible for numerous large-scale ransomware attacks, including those against Maastricht University, Software AG IT, ExecuPharm, and Indiabulls.

More recently, Clop had been stealing data from Accellion FTA file transfer devices using a zero-day vulnerability and then threatening to release the data if not paid $10 million or more.

Some of the victims of Accellion attacks include energy giant Shell, cybersecurity firm Qualys, Flagstar Bank, the University of Miami, and the University of California, to name a few.

The Ukrainian police estimate that Clop's total damages reach as high as $500 million.

Source: https://www.bleepingcomputer.com/news/security/clop-ransomware-is-back-in-business-after-recent-arrests/