Ukraine arrests Clop ransomware gang members, seizes servers

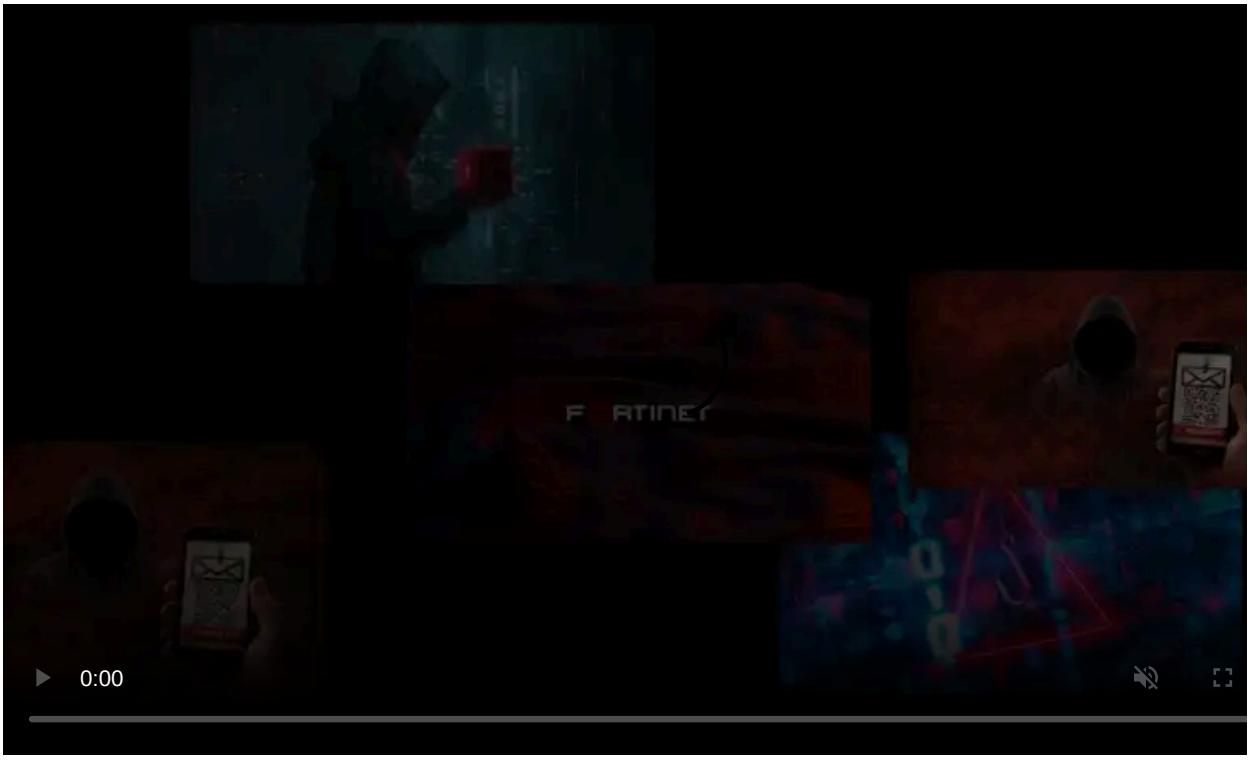
By Sergiu Gatlan

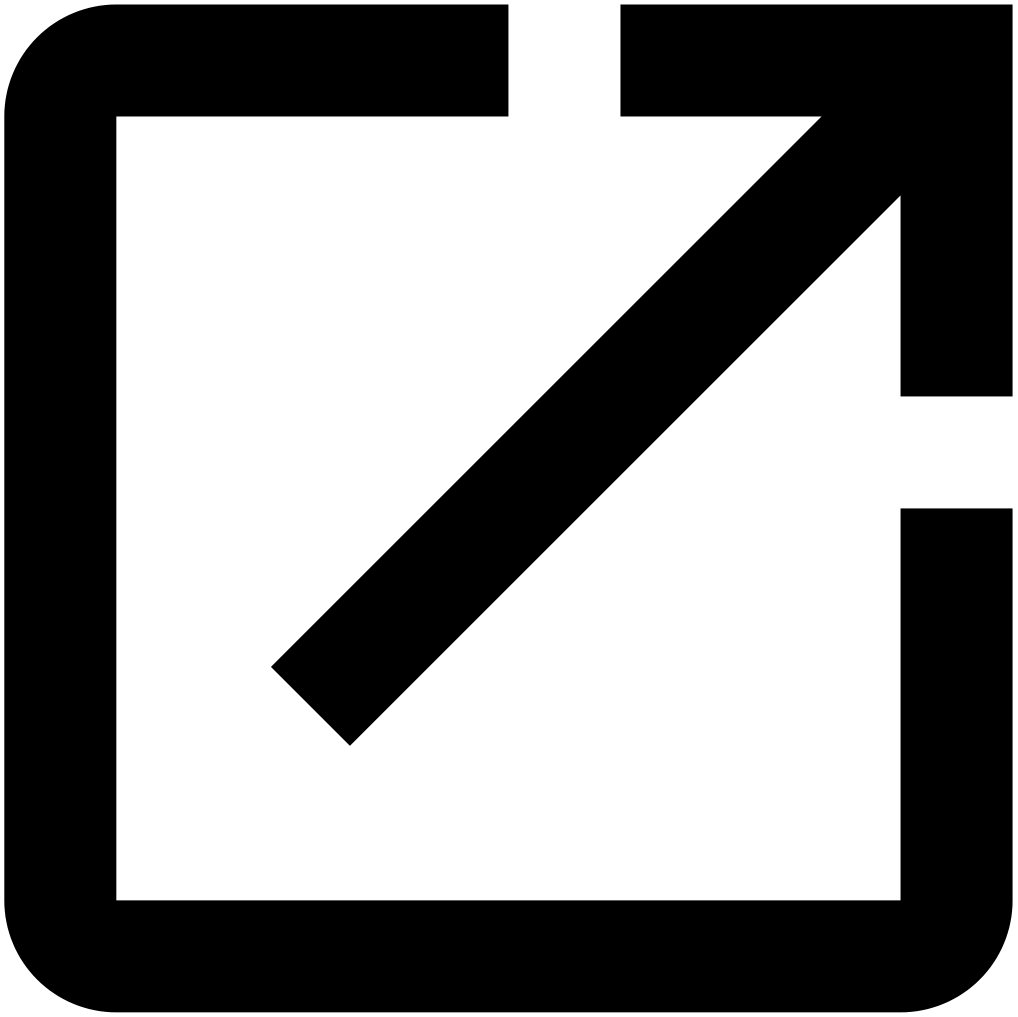
Published: 2021-06-16 · Archived: 2026-04-06 02:59:10 UTC

Ukrainian law enforcement arrested cybercriminals associated with the Clop ransomware gang and shut down infrastructure used in attacks targeting victims worldwide since at least 2019.

According to the Cyberpolice Department of the National Police of Ukraine the ransomware group is behind total financial damages of roughly $500 million.

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


0:00



"Law enforcement officers conducted 21 searches in the capital and Kyiv region, in the homes of the defendants, and in their cars."

"The defendants face up to eight years in prison. Investigative actions continue. Procedural guidance is provided by the Office of the Prosecutor General of Ukraine."

Based on Ukrainian police's press release, it is not yet clear if the arrested individuals are affiliates or core members of the ransomware operation.

The cybercriminals were arrested following an international operation in conjunction with law enforcement officers from the United States and the Republic of Korea.

Cybersecurity company Intel 471 told BleepingComputer that the Ukrainian authorities arrested only individuals involved in laundering money for the Clop gang since its core members are likely out of harm's way in Russia.

"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.

"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."

Clop ransomware operation's previous activity

In addition to encrypting attacks, the Clop ransomware gang was linked to the recent wave of Accellion data breaches which led to a drastic increase in average ransom payments calculated for the first three months of 2021.

While as part of regular ransomware attacks the victims' data is encrypted, Clop's attacks did not encrypt a single byte but instead exfiltrated large amounts of data from high-profile companies that used Accellion's legacy File Transfer Appliance (FTA).

The gang used the stolen data as leverage to extort the compromised companies with high ransom demands.

Starting with January, BleepingComputer reported Clop attacks abusing Accellion to breach:

- energy giant Shell, cybersecurity firm Qualys,
- supermarket giant Kroger,
- the Reserve Bank of New Zealand,
- Singtel,
- the Australian Securities and Investments Commission (ASIC),
- the Office of the Washington State Auditor ("SAO"),
- as well as multiple universities and other organizations.

Clop also claimed to have stolen 2 million credit cards from Korean retailer E-Land's servers using point-of-sale (POS) malware before deploying ransomware on their network one year later, in November 2020.

Previously, Clop ransomware was behind attacks on Maastricht University, Software AG IT, ExecuPharm, and Indiabulls.

Clop's Tor payment site and data leak site are still operational, so it looks like the Clop ransomware operation has not been completely shut down at this time.

BleepingComputer has reached out to the FBI for comment on their involvement in the investigation but had not heard back at the time of this publication.

Source: https://www.bleepingcomputer.com/news/security/ukraine-arrests-clop-ransomware-gang-members-seizes-servers/