Clop ransomware gang is back, hits 21 victims in a single month

bleepingcomputer.com/news/security/clop-ransomware-gang-is-back-hits-21-victims-in-a-single-month/

Sergiu Gatlan

By
Sergiu Gatlan

- May 28, 2022
- 11:10 AM
- 0

After effectively shutting down their entire operation for several months, between November and February, the Clop ransomware is now back, according to NCC Group researchers.

"CL0P had an explosive and unexpected return to the forefront of the ransomware threat landscape, jumping from the least active threat actor in March to the fourth most active in April," NCC Group said.

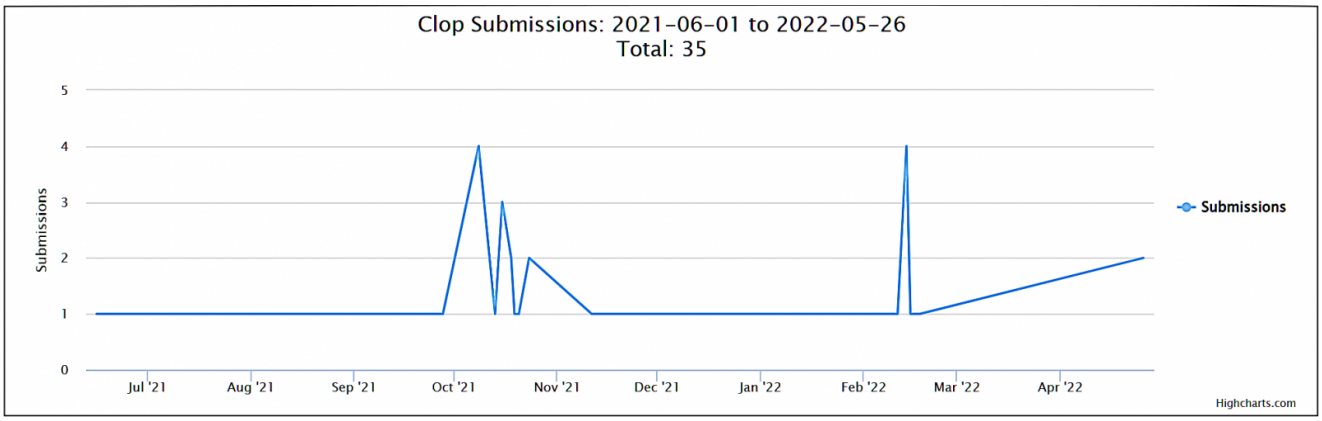
This surge in activity was noticed after the ransomware group added 21 new victims to their data leak site within a single month, in April.

"There were notable fluctuations in threat actor targeting in April. While Lockbit 2.0 (103 victims) and Conti (45 victims) remain the most prolific threat actors, victims of CL0P increased massively, from 1 to 21," NCC Group added.

Clop's most targeted sector was the industrial sector, with 45% of Clop ransomware attacks hitting industrial organizations and 27% targeting tech companies.

Because of this, NCC Group's strategic threat intelligence global lead Matt Hull warned orgs within the ransomware group's most targeted sectors to consider the possibility of being this gang's next target and prepare accordingly.

However, despite already leaking data from almost two dozen victims, the ransomware group doesn't seem very active based on the number of submissions on the ID Ransomware service.



Clop ransomware activity (ID Ransomware)

Part of a shutdown process?

While some of the recent victims are confirmed to be new attacks, one theory is that the Clop gang might finally be shutting down their operation after being inactive for so long.

As part of this process, the ransomware gang would likely publish the data of all previously unpublished victims.

This is similar to what the Conti group appears to be doing right now as part of their own ongoing shutdown.

Whether these are old or new victims will likely be confirmed if they release breach notifications or publish confirmations (some of them have already done it).

Who is Clop?

The Clop ransomware gang's activity lull is easily explained by some of its infrastructure getting shut down in June 2021 following an international law enforcement operation codenamed Operation Cyclone coordinated by the INTERPOL.

Six individuals suspected of laundering money and providing cash-out services for the Clop ransomware gang were arrested by Ukrainian authorities after 21 home searches in the Kyiv region.

"The overall impact to CLOP is expected to be minor," cybersecurity company Intel 471 told BleepingComputer.

While targeting victims worldwide in ransomware attacks since at least 2019 (some of its victims include Maastricht University, Software AG IT, ExecuPharm, and Indiabulls), the Clop gang was also linked to a massive wave of Accellion data breaches leading to a substantial increase in average ransom payments for the first three months of 2021.

In the Accellion attacks, Clop's operators only exfiltrated large amounts of data from high-profile companies using Accellion's legacy File Transfer Appliance (FTA).

The gang later used this stolen data as leverage to extort the compromised companies, forcing them to pay high ransom demands not to have their data leaked online.

The list of companies that had their Accellion FTA servers hacked by Clop includes, among others, energy giant Shell, cybersecurity firm Qualys, supermarket giant Kroger, and multiple universities worldwide (the University of Colorado, University of Miami, Stanford Medicine, University of Maryland Baltimore (UMB), and the University of California.)

Related Articles:

Microsoft links Holy Ghost ransomware operation to North Korean hackers

New Lilith ransomware emerges with extortion site, lists first victim

Bandai Namco confirms hack after ALPHV ransomware data leak threat

Hackers impersonate cybersecurity firms in callback phishing attacks

Ransomware gang now lets you search their stolen data