Cl0p hacker operating from Russia-Ukraine war front line – exclusive

Published: 2023-07-12 · Archived: 2026-04-15 02:13:44 UTC

As the Cl0p ransomware gang continues to sow anxiety worldwide, affecting prominent companies like the BBC and Deutsche Bank, at least one of the gang's masterminds, Cybernews discovered, is still residing in Ukraine.

Deutsche Bank, one of the world's largest banks, is the latest victim of the Cl0p gang. The bank's customer data was leaked after hackers penetrated a third-party vendor, Majorel, by exploiting the MOVEit vulnerability.

Other major banks in Europe, including Deutsche Bank-owned Postbank, ING Bank, and Comdirect, have also been affected.

Cl0p, which has a tendency to publicly name its victims in batches, has reportedly been sitting on the zero-day vulnerability for two years. As is quite common with malicious activity en masse, malicious hackers chose the Memorial Day weekend in the US (May 27th and 28th) for a "broad swath of activity."

Before the MOVEit saga, which seems far from over, Cl0p enjoyed the spotlight by exploiting Fortra's GoAnywhere vulnerability. Shell, Hitachi, Hatch Bank, Rubrik, Virgin, and many others are among its claimed victims.

Curiously, Shell has been affected by both the GoAnywhere and MOVEit flaws.

Cl0p, first observed in 2019, is quite old for a ransomware gang, given that they tend to regularly restructure and rebrand to throw law enforcement off track. The hacker group, also known by cyber pundits as Lace Tempest, Dungeon Spider, is affiliated with Russia.

In June 2021, Ukrainian law enforcement, in collaboration with US and South Korean officials, arrested six Cl0p members and dismantled the gang's infrastructure. At the time, the group was accused of causing damage amounting to $500 million.

The arrests forced the gang to shut down its operations for a short period of three to four months in 2021-2022. Unfortunately, the gang has been steadily recovering. As a matter of fact, according to dark web intelligence platform, DarkFeed, Cl0p, with 361 victims and counting, is now among the three most active ransomware groups, leaving such infamous gangs like Revil and Vice Society far behind.

New evidence points to the fact that the Russia-affiliated gang still operates from Ukraine.

Cybernews has received a new batch of evidence that one of the Cl0p ransomware strain developers is at large in the city of Kramatorsk in Eastern Ukraine, on the front line of the Russia-Ukraine war.

A security researcher, who was vetted by Cybernews and asked not to be named in the article, looked up one of the Cl0p's developers on the dark web, and contacted them via a well-known communication channel.

Because of a flaw in the platform – we're choosing not to name it to avoid giving you any naughty ideas – our anonymous hacker was able to extract the Cl0p developer's internet protocol (IP) address pointing us directly to their location in Kramatorsk.

Kramatorsk is a city in Eastern Europe that Russia has been trying to tear off Ukraine since the annexation of Crimea, a Ukrainian peninsula, in 2014. Just days before the NATO Summit in Lithuania, where Ukraine's president Volodymyr Zelensky heard more promises of accelerating Ukraine's admission to NATO, the Kremlin took a deadly strike on Kramatorsk, killing three children, among other people.