Clop

Archived: 2026-04-05 14:30:45 UTC

The Clop Ransomware Group

Clop (also known as Cl0p) is an extortionist ransomware-type malware. It originated in 2019. It operates on the Ransomware-as-a-Service (RaaS) model. It is a variant of the CryptoMix ransomware family. There have been several improved versions of the malware.

How It Works

The ransomware itself, cl0p, is a Win32 PE file. It is distributed using executables that have been digitally signed by a verified signer. This makes it appear more legitimate. It helps it bypass security software detection. Once the ransomware strain infiltrates the system, it then attempts to disable Windows Defender. It also removes the Microsoft Security Essentials.

The ransomware gang stayed outside the spotlight for the last two years. This was since their high-profile attack on Accellion. That attack led to the arrest of six of their operators by the Ukrainian government. However, the group has made significant impacts on the cyber threat landscape.

Cl0p Ransomware TTPs

Since its start in 2019, Flashpoint has observed the ransomware group use several tools in its digital arsenal. The ransomware gang has used DDoS attacks and various phishing tactics. This is done to infect target organizations with their ransomware strain. However, cl0p has recently used potent vulnerability exploits to gain notoriety.

Notable Ransomware Attacks

In 2023, Clop made headlines. It used two vulnerability exploits against its victims: GoAnywhere MFT and MOVEit. We've previously examined the full details of both of these attacks. Both data compromise events resulted in hundreds of victims being listed on the clop ransomware leak site.

Frequently Asked Questions (FAQ)

Q: What is Clop, and what is its primary operating model?

A: Clop (or Cl0p) is an extortionist ransomware-type malware that started in 2019. It primarily operates on the Ransomware-as-a-Service (RaaS) model, where the code is leased to affiliates for profit sharing.

Q: What types of attacks does Clop commonly use?

A: Clop uses a variety of tactics, including DDoS attacks and phishing. Most notably, the group has recently focused on leveraging potent vulnerability exploits against file transfer products like GoAnywhere MFT and MOVEit to execute widespread data compromise events.

Q: How does Clop malware try to avoid detection?

A: Clop malware is distributed as a file digitally signed by a verified signer to appear legitimate. Once in the system, it attempts to disable common security software like Windows Defender and Microsoft Security Essentials to avoid detection and removal.
