Ukrainian police arrest Clop ransomware members, seize server infrastructure

therecord.media/ukrainian-police-arrest-clop-ransomware-members-seize-server-infrastructure/

June 16, 2021

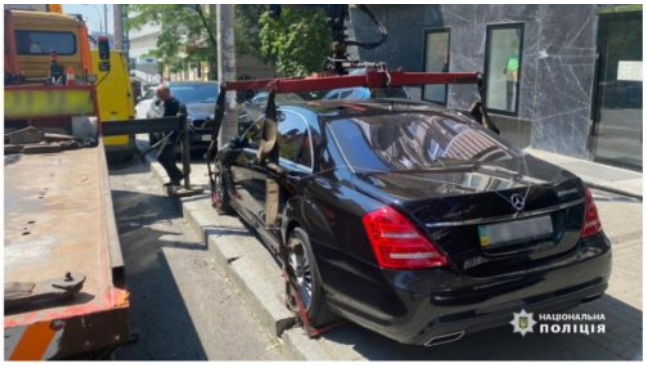
Multiple suspects believed to be linked to the Clop ransomware cartel have been detained in Ukraine this week after a joint operation from law enforcement agencies from Ukraine, South Korea, and the US.

The arrests, reported today by the Ukraine National Police and the country's Cyber Police division, come after authorities conducted searches at 21 residences in Kyiv, the country's capital, and nearby regions.

Following the operation, authorities reported that they successfully shut down server infrastructure used by the gang members to launch past attacks.

Computers, smartphones, and server equipment were seized, together with 5 million Ukrainian hryvnias ($185,000), which authorities believe were obtained from ransoming companies across the world.

Several expensive cars, such as Tesla, Mercedes, and Lexus models, were also seized from the gang members' homes.



Authorities said they arrested six members of the Clop group, but did not expand on their role in the overall Clop gang structure. If found guilty, the suspects face up to eight years in prison.

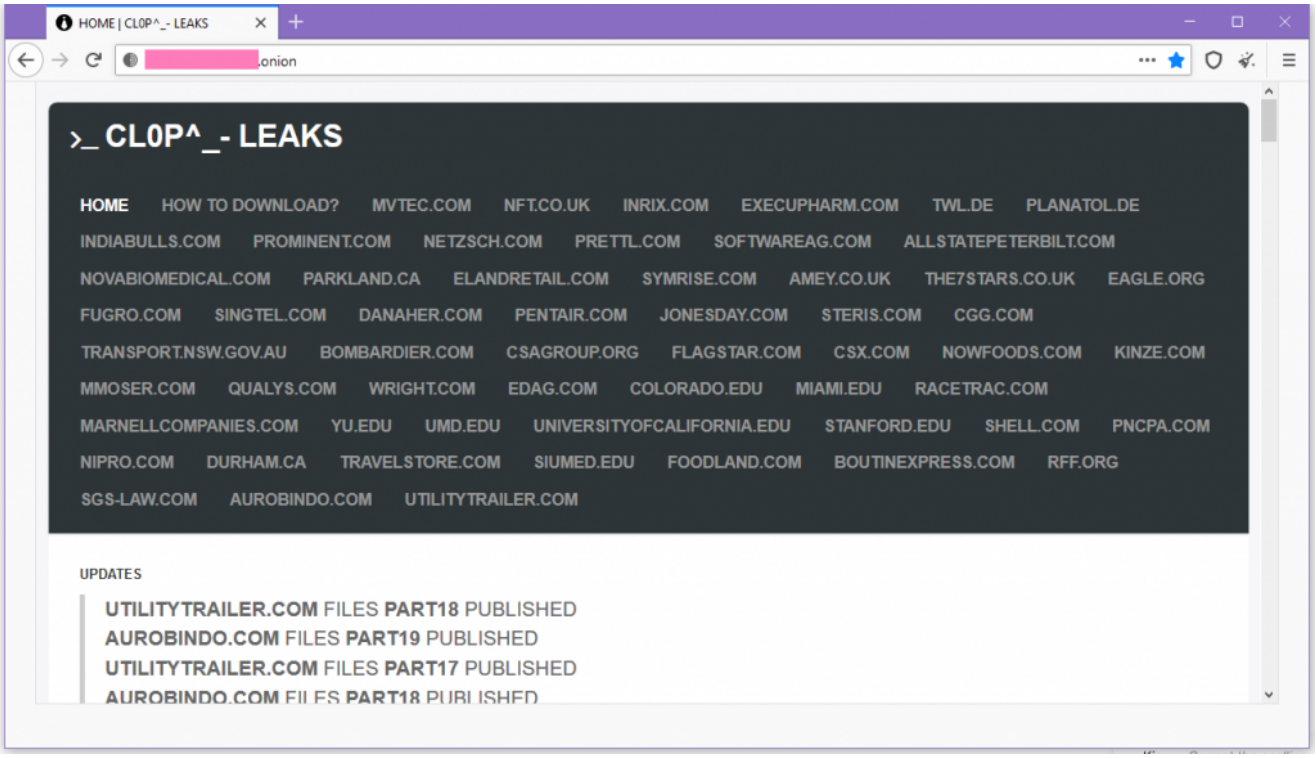
A short history of Clop

Prior to today's arrests, incidents with the Clop ransomware have been documented as early as February 2019.

The gang is what security researchers would call a "big-game hunter," a term that describes ransomware groups that go only after large IT networks rather than home consumers.

Across its more than two years of activity, the Clop gang has breached many large corporations and demanded payments of up to tens of millions of US dollars per victim.

If companies refused to pay, the Clop gang would resort to a double-extortion tactic and threaten to leak victims' data on a dark web "leak portal." The leak site is still up and running at the time of writing.



A November 2020 Fox-IT report claimed the Clop gang had close ties to a malware distribution group known as TA505, which would often allow the gang's members to deploy Clop ransomware strains on computers previously infected with the SDBbot malware.

A February 2021 FireEye report also claimed the Clop gang appears to have struck a deal with the FIN11 cybercrime group, allowing FIN11 operators to list data the group previously stole from hacked Accellion FTA file-sharing devices.

Clop's South Korean victims get their revenge

The arrests come in investigations that started back in 2019 when the Clop ransomware gang breached four South Korean companies and encrypted their files, asking for huge payouts.

Sources close to the investigation have told *The Record* that South Korean police ramped up its investigation into the gang last year after the Clop gang infected the network of South Korean e-commerce giant E-Land in November 2020, forcing the Korean company to close almost have of its stores.

In a rare practice, South Korean police officers were physically present during the raids on Clop suspects this week, something that is customarily left to local law enforcement agencies.

Watch Video At:

https://youtu.be/PqGaZgepNTE

Tags

- arrests
- Cl0p
- Clop
- cybercrime
- FIN11
- Ransomware
- South Korea
- TA505
- Ukraine

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.