Romanian Netwalker ransomware affiliate sentenced to 20 years in prison

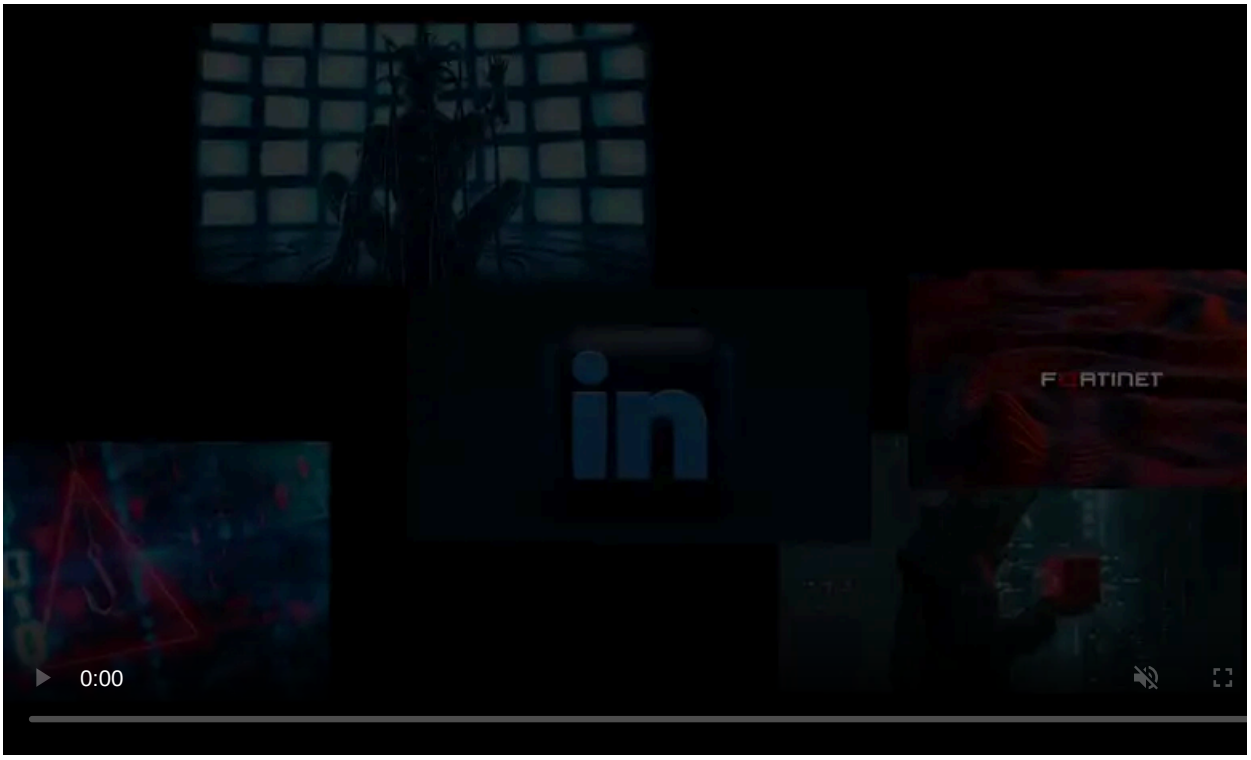
By Sergiu Gatlan

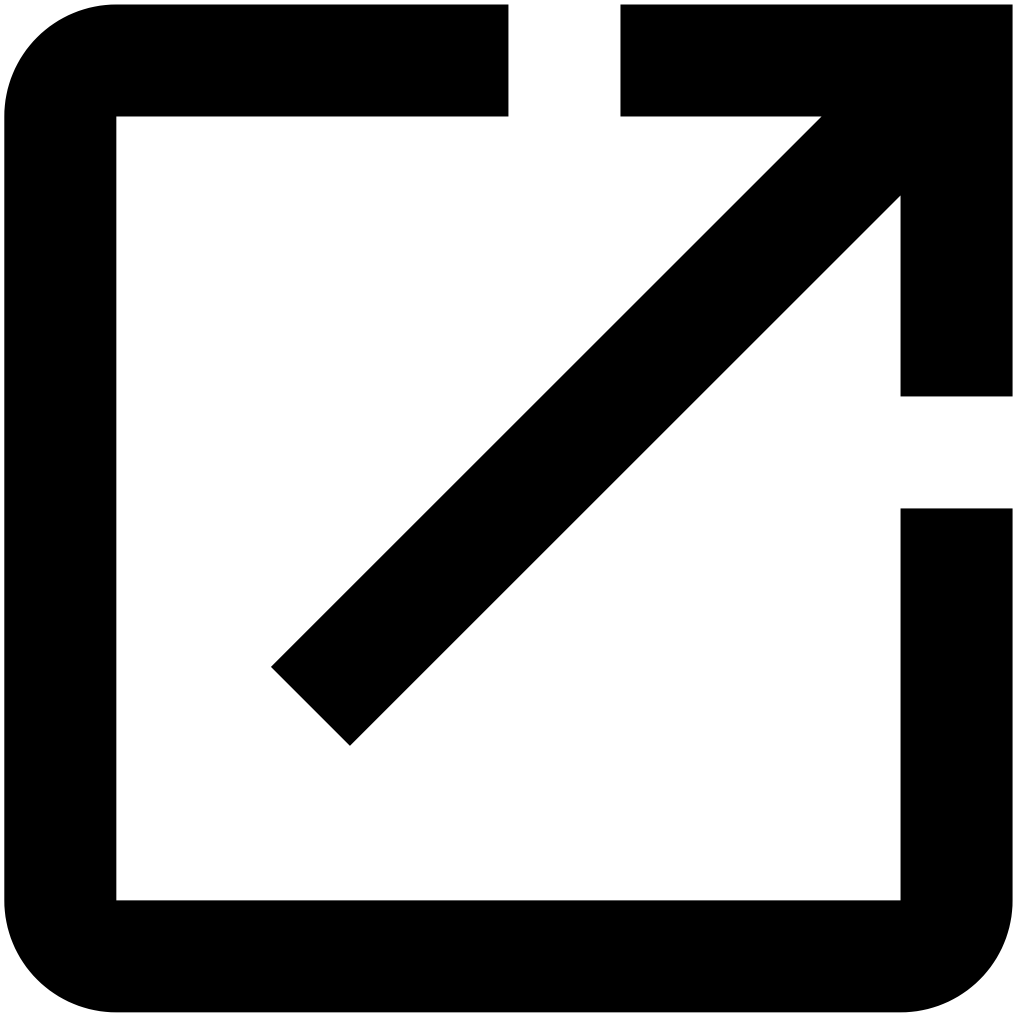
Published: 2024-12-20 · Archived: 2026-04-05 19:48:13 UTC

Daniel Christian Hulea, a Romanian man charged for his involvement in NetWalker ransomware attacks, was sentenced to 20 years in prison after pleading guilty to computer fraud conspiracy and wire fraud conspiracy in June.

Hulea was extradited to the United States after being arrested by Romanian police in Cluj in July 2023 at a request from U.S. law enforcement authorities.

According to court documents, Hulea admitted to participating in a conspiracy to use NetWalker ransomware. Affiliates of the NetWalker cybercrime gang have deployed this malware in attacks against hundreds of victims worldwide, including hospitals, law enforcement, emergency services, companies, municipalities, school districts, colleges, and universities.


0:00



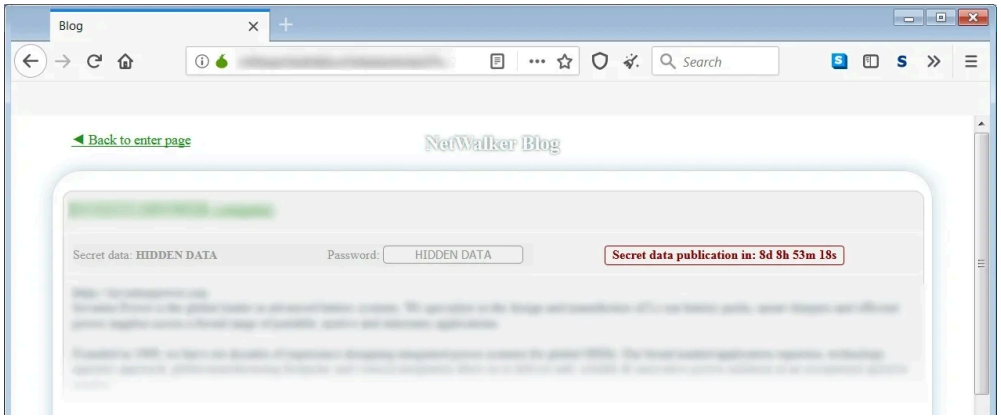
The group's attacks have also taken advantage of the global crisis triggered by the COVID-19 pandemic to target healthcare organizations and extort victims.

As part of his plea agreement, Hulea said he obtained approximately 1,595 bitcoins from NetWalker ransomware victims for himself and a co-conspirator, worth roughly $21.5 million at the time of the ransom payments.

In addition to his 20 years in prison, he was ordered to pay $14,991,580.01 in restitution and forfeit $21,500,000. He must also relinquish his interests in an Indonesian company and a luxury resort property currently under construction in Bali, Indonesia, financed using proceeds from the ransomware attacks.

Two years ago, in October 2022, the United States also sentenced Canadian man Sebastien Vachon-Desjardins to 20 years in prison, another Netwalker ransomware affiliate who orchestrated attacks on multiple U.S. companies and at least 17 Canadian entities, leading to tens of millions in dollars.

When the U.S. DOJ charged Desjardins on January 27th, 2021, an international law enforcement operation also seized all Netwalker websites, including their Tor payment and data leak sites.



Netwalker ransomware leak site (BleepingComputer)

Netwalker was a Ransomware-as-a-Service (RaaS) operation active since 2019 that recruited affiliates to deploy the ransomware for a 60-75% share of all ransom payments.

According to an August 2020 report, the threat actors involved in the cybercrime group collected $25 million from victims within just five months.

During the attacks, the ransomware affiliates stole data from compromised systems and encrypted the devices. They then asked victims to pay ransoms ranging from hundreds of thousands to millions of dollars to recover files and prevent their stolen data from being leaked online.

Earlier this year, security researchers analyzing Alpha ransomware payloads and modus operandi in February found strong links with the now-defunct Netwalker ransomware operation, hinting at the Netwalker code repurposed for new attacks by other threat actors or a NetWalker rebrand.
