DarkSide ransomware gang moves some of its Bitcoin after REvil got hit by law enforcement

By Catalin Cimpanu

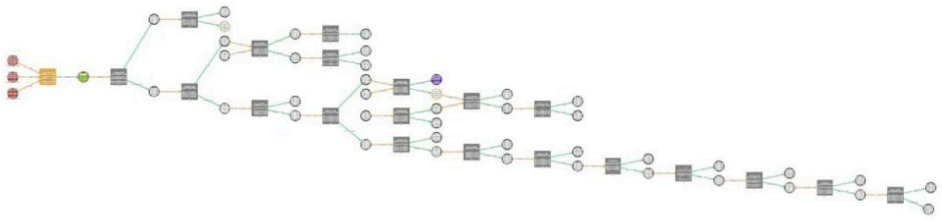
Published: 2022-12-18 · Archived: 2026-04-05 22:55:04 UTC

The operators of the Darkside and BlackMatter ransomware strains have moved a large chunk of their Bitcoin reserves after news broke that fellow ransomware gang REvil had its servers taken over by a coalition of law enforcement agencies.

Approximately 107 BTC ($6.8 million) were moved earlier today, according to Omri Segev Moyal, CEO and co-founder of security firm Profero.

"Basically, since 2AM UTC whoever controlled the wallet started to break the BTC into small chunks," Moyal told *The Record*.

"At the time of this writing, the attackers split the funds into 7 wallets of 7-8 BTC and the rest (38BTC) is stored in the following wallet: bc1q9jy4pq5su9slh56gryydwkk0qjnqxvfwzm7xl6."



Moyal said he believed the funds were still controlled by the Darkside/BlackMatter gang and were being prepared to be laundered or cashed out.

He said that law enforcement agencies typically move seized assets to a new wallet under their control and wouldn't need to break the funds into smaller chunks, a step typical in money laundering operations.

Darkside moves $6.8 million, fearing a repeat

The funds were moved roughly six hours after Reuters reported that a coalition of law enforcement agencies from several countries was responsible for hijacking the servers of fellow ransomware group REvil over the weekend.

The Darkside group's quick reaction to move funds and re-asses control is justifiable in light of the gang's history and past attacks.

Darkside was the ransomware strain used in the incident that crippled the operations of Colonial Pipeline in May, an attack that indirectly caused fuel supply outages across the US East Coast.

In light of the attack and its political repercussions, the Darkside gang shut down its operations a week later. At the time, the gang claimed they shut down after they lost control over some servers and some cryptocurrency wallets (money).

Nevertheless, the gang re-launched in July with new infrastructure and under the new name of BlackMatter.

Moving some of its funds shortly after the REvil takedown news makes sense since the gang would like to make sure they don't lose funds for a second time, during another law enforcement crackdown. Furthermore, the gang was most likely spooked already after the US government published a security advisory about its activities four days before.

Moyal has now notified and asked cryptocurrency exchanges to block the Darkside/BlackMatter wallets holding their new funds, but the fractured cryptocurrency exchange landscape still leaves many ways for the group to launder its profits.

> Dear #bitcoin exchange platform, please block the following wallets from the incoming transactions: https://t.co/NwNiIno5mX
>
> Attackers have split the BTC into 7 wallets with what looks like preparation to convert to other exchange or cashout somehow.
>
> — Omri Segev Moyal (@GelosSnake) October 22, 2021

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who 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.
