DarkSide ransomware rushes to cash out $7 million in Bitcoin

Ionut Ilascu

By
Ionut Ilascu

- October 22, 2021
- 02:02 PM
- 0

Almost $7 million worth of Bitcoin in a wallet controlled by DarkSide ransomware operators has been moved in what looks like a money laundering rollercoaster.

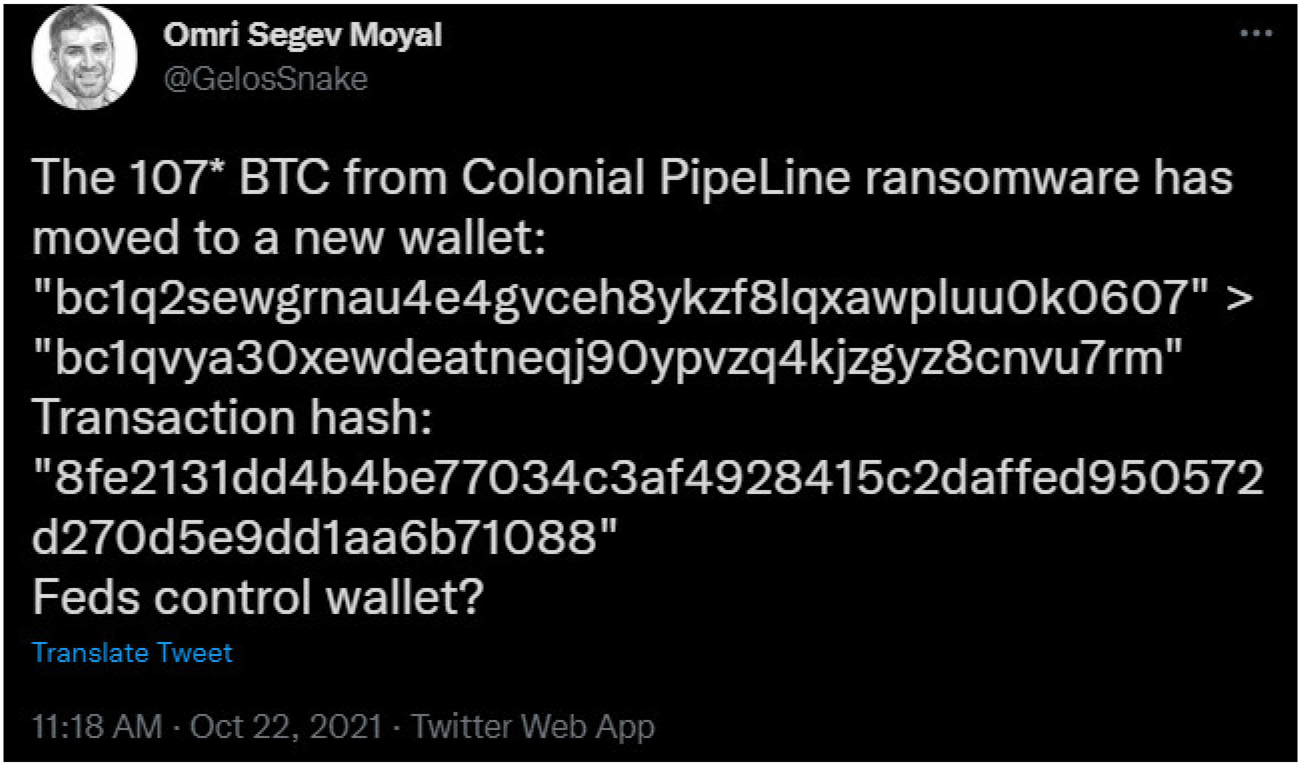
The funds have been moving to multiple new wallets since yesterday, a smaller amount being transferred with each transaction to make the money more difficult to track.

The timing aligns with the takedown of REvil ransomware infrastructure after hijacking the gang's Tor hidden service as a result of an international law enforcement operation.

The money laundering flow

The DarkSide ransomware gang has extorted dozens of victims of tens of millions of U.S. dollars, their most famous attack being on May 7, against the largest fuel pipeline in the United States, Colonial Pipeline.

Omri Segev Moyal, the CEO and co-founder of cybersecurity company Profero, tweeted today that 107 bitcoins from a DarkSide wallet were moved to a new wallet.



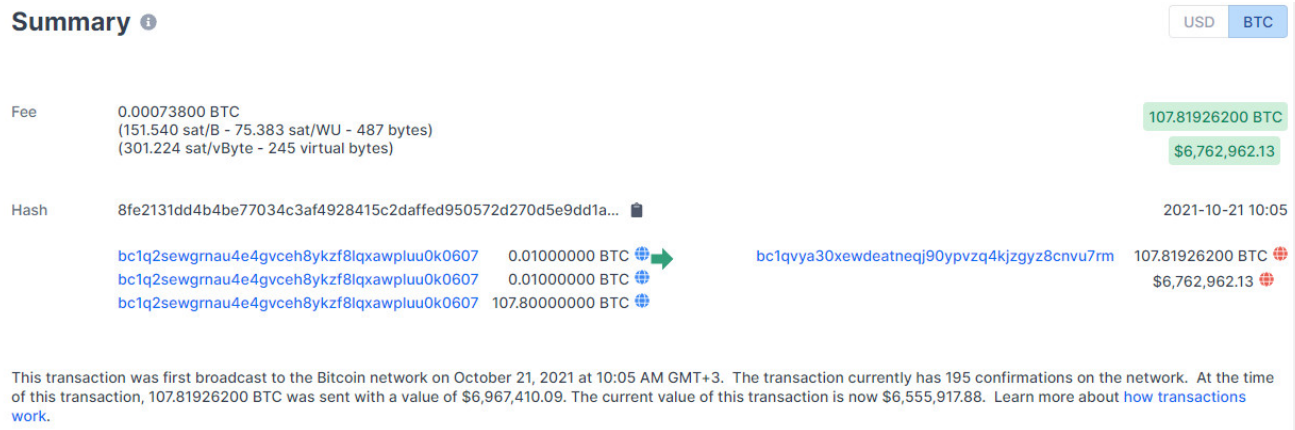
Omri Segev Moyal
@GelosSnake

The 107* BTC from Colonial PipeLine ransomware has moved to a new wallet:
"bc1q2sewgrnau4e4gvceh8ykzf8lqxawpluu0k0607" >
"bc1qvya30xewdeatneqj90ypvzq4kjzgyz8cnvu7rm"
Transaction hash:
"8fe2131dd4b4be77034c3af4928415c2daffed950572d270d5e9dd1aa6b71088"
Feds control wallet?

11:18 AM · Oct 22, 2021 · Twitter Web App

source: Omri Segev Moyal, co-founder and CEO of Profero

Looking at the transaction hash, the move started on October 21, 2021, at 7:05 AM (GMT) and the initial value was a little under $7 million.



Summary

Fee: 0.00073800 BTC
(151.540 sat/B - 75.383 sat/WU - 487 bytes)
(301.224 sat/vByte - 245 virtual bytes)

107.81926200 BTC
$6,762,962.13

Hash: 8fe2131dd4b4be77034c3af4928415c2daffed950572d270d5e9dd1a...

2021-10-21 10:05

bc1q2sewgrnau4e4gvceh8ykzf8lqxawpluu0k0607 0.01000000 BTC
bc1q2sewgrnau4e4gvceh8ykzf8lqxawpluu0k0607 0.01000000 BTC
bc1q2sewgrnau4e4gvceh8ykzf8lqxawpluu0k0607 107.80000000 BTC

bc1qvya30xewdeatneqj90ypvzq4kjzgyz8cnvu7rm 107.81926200 BTC
$6,762,962.13

This transaction was first broadcast to the Bitcoin network on October 21, 2021 at 10:05 AM GMT+3. The transaction currently has 195 confirmations on the network. At the time of this transaction, 107.81926200 BTC was sent with a value of $6,967,410.09. The current value of this transaction is now $6,555,917.88. Learn more about how transactions work.

In a blog post today, blockchain analysis company Elliptic shows how DarkSide's cryptocurrency flowed through different wallets, shrinking from 107.8 BTC to 38.1 BTC.

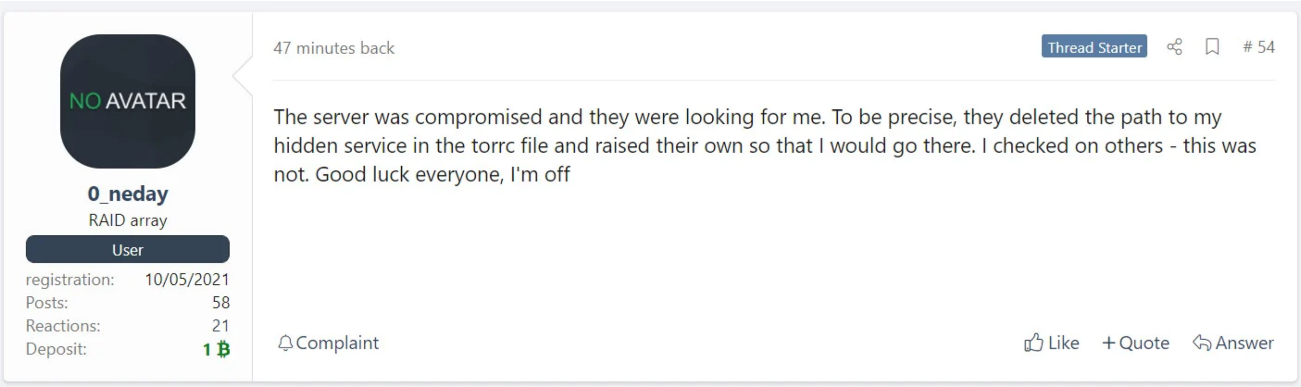
ELLIPTIC
107.8
Darkside Ransomware

The money-laundering process

Moving the funds this way is a typical money laundering technique that hinders tracing and helps cybercriminals convert the cryptocurrency to fiat money.

Elliptic says that the process continues still and that small amounts of the money have already been transferred to known exchanges.

Moving the money at this time may be a result of what happened to the REvil ransomware operation, which shut down for a second time this year after finding that its services had been compromised by a third-party.



The server was compromised and they were looking for me. To be precise, they deleted the path to my hidden service in the torrc file and raised their own so that I would go there. I checked on others - this was not. Good luck everyone, I'm off

The hacking occurred after REvil attacked the Kaseya MSP platform that served more than 1,000 companies across the globe. While the FBI was on the verge of disrupting REvil, the cybercriminals shut down their operation.

When REvil restarted its business, they restored from the backups that had been infiltrated by the FBI before the gang closed shop.

DarkSide money recovered by the FBI

DarkSide's attack on Colonial Pipeline was the last one from DarkSide under this name. Until then, the ransomware gang had collected at least $90 million from its victims.

However, they chose their last target poorly, since its operations supplied petroleum products to markets and refineries on the U.S. East Coast accounting for 45% of all fuel consumed in the region.

Even if Colonial Pipeline paid the 75 BTC (around $5 million at the time) ransom, the consequences of the attack were too much for the DoJ not to treat it with top priority.

On June 7, the DoJ announced that it recovered 63.7 bitcoins of the ransom Colonial Pipeline paid to DarkSide to recover their systems as fast as possible.

DarkSide then exited the ransomware business only to emerge as BlackMatter. In July, the rebranded threat actor was looking to buy access to corporate networks.

Recorded Future announced at the time BlackMatter saying that it "incorporated in itself the best features of DarkSide, REvil, and LockBit."

Under the new name, the ransomware actors continued to hit large companies such as medical technology giant Olympus, the New Cooperative farmers organization in the U.S., or Marketron provider of marketing services.

In a joint advisory released recently, CISA, the FBI, and the NSA provide mitigation information that can help organizations defend against BlackMatter ransomware attacks.

Related Articles:

US Senate: Govt’s ransomware fight hindered by limited reporting

Fake crypto giveaways steal millions using Elon Musk Ark Invest video

US sanctions Bitcoin laundering service used by North Korean hackers

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Windows 11 KB5014019 breaks Trend Micro ransomware protection

- Bitcoin
- BlackMatter
- CryptoCurrency
- DarkSide
- Ransomware

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: