Darkside gang estimated to have made over $90 million from ransomware attacks

therecord.media/darkside-gang-estimated-to-have-made-over-90-million-from-ransomware-attacks/

May 18, 2021

The operators of the Darkside ransomware are believed to have made at least $90 million from ransom payments over the past nine months, since October 2020.

“In total, just over $90 million in Bitcoin ransom payments were made to DarkSide, originating from 47 distinct wallets,” blockchain analysis firm Elliptic said in a report published earlier today.

Citing data shared by dark web intelligence platform DarkTrace, Elliptic said the Darkside group appears to have made at least 99 victims, of which approximately 47% paid their ransom demands.

“**The average payment was $1.9 million**,” said Elliptic co-founder and chief scientist Dr. Tom Robinson.

“May was set to be a record month, until DarkSide reportedly shut down its operations on May 13, and its Bitcoin wallet was emptied.”

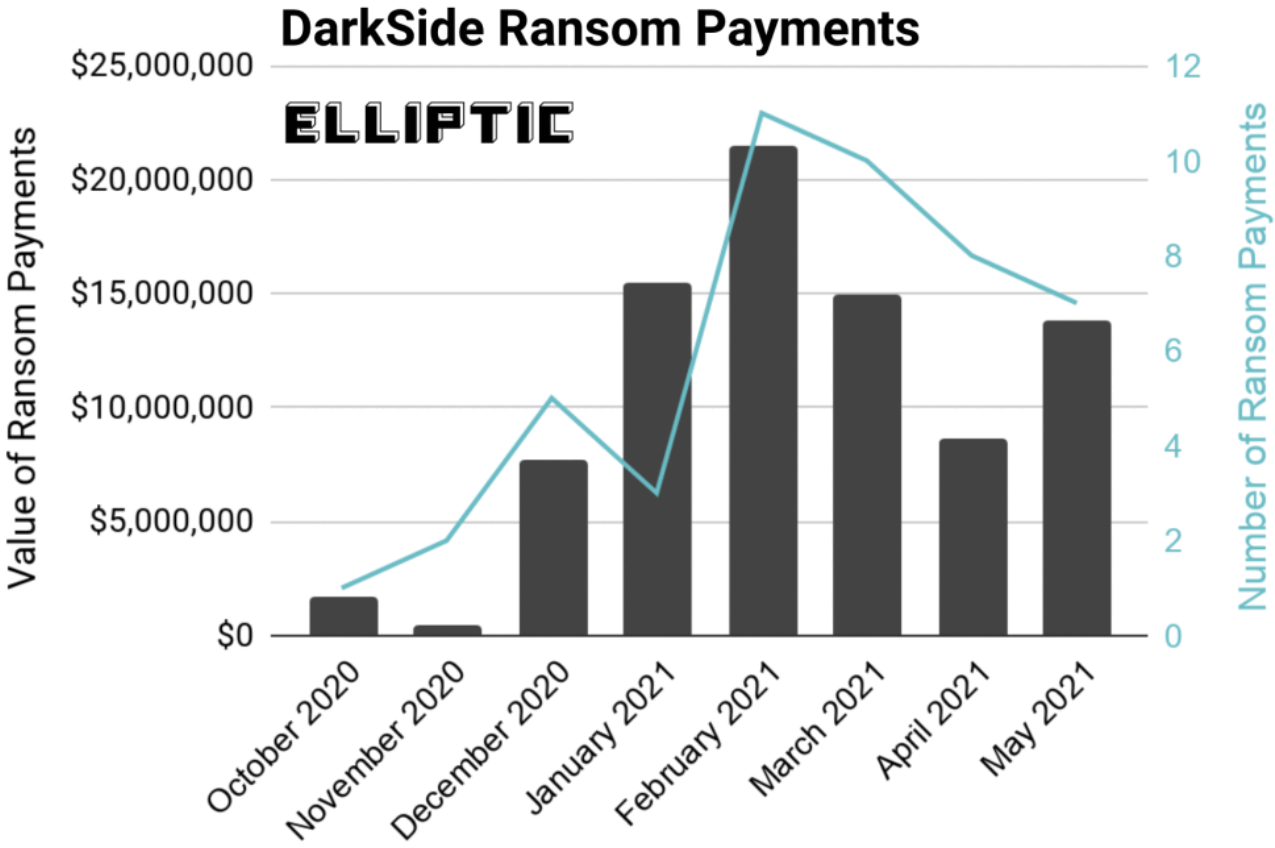

Image: Elliptic

Elliptic's report comes after previous studies have put the estimated earnings of gangs like Maze/Egregor at $75 million, Ryuk at $150 million, REvil at $100 million (threat actor's own claims), and Netwalker at $25 million (for a period of 3 months only).

While estimating a ransomware gang's earnings is not an exact science, as investigators never have a full picture of a gang's operations, Elliptic's findings firmly put the Darkside group in the upper echelon of ransomware operations.

Since Darkside is provided through a ransomware-as-a-service (RaaS) model, which allows the Darkside coders to keep 25% of the paid ransoms, or 10% if the ransom is larger than $5 million, Elliptic believes that **the actual Darkside group made roughly $15.5 million**, while the rest of the funds were transferred to Darkside's affiliates—the group who rented the ransomware and then deployed it inside the hacked companies.

Bot knowing how much money a ransomware gang made is a rather useless stat that does nothing but promotes the profitability of the ransomware criminal ecosystem.

In an email today, Dr. Robinson told *The Record* that they weren't only able to estimate the group's earnings, but they were also able to track down how the Darkside payments moved across the blockchain to cash-out points, information which the Elliptic exec said is available to the law enforcement agencies that use its platform and "which provides investigators with important leads."

Tags

- Bitcoin
- blockchain
- Darkside
- Elliptic
- extortion
- profits
- RaaS
- Ransomware

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.