DarkSide ransomware made $90 million in just nine months

bleepingcomputer.com/news/security/darkside-ransomware-made-90-million-in-just-nine-months/

Ionut Ilascu

By
Ionut Ilascu

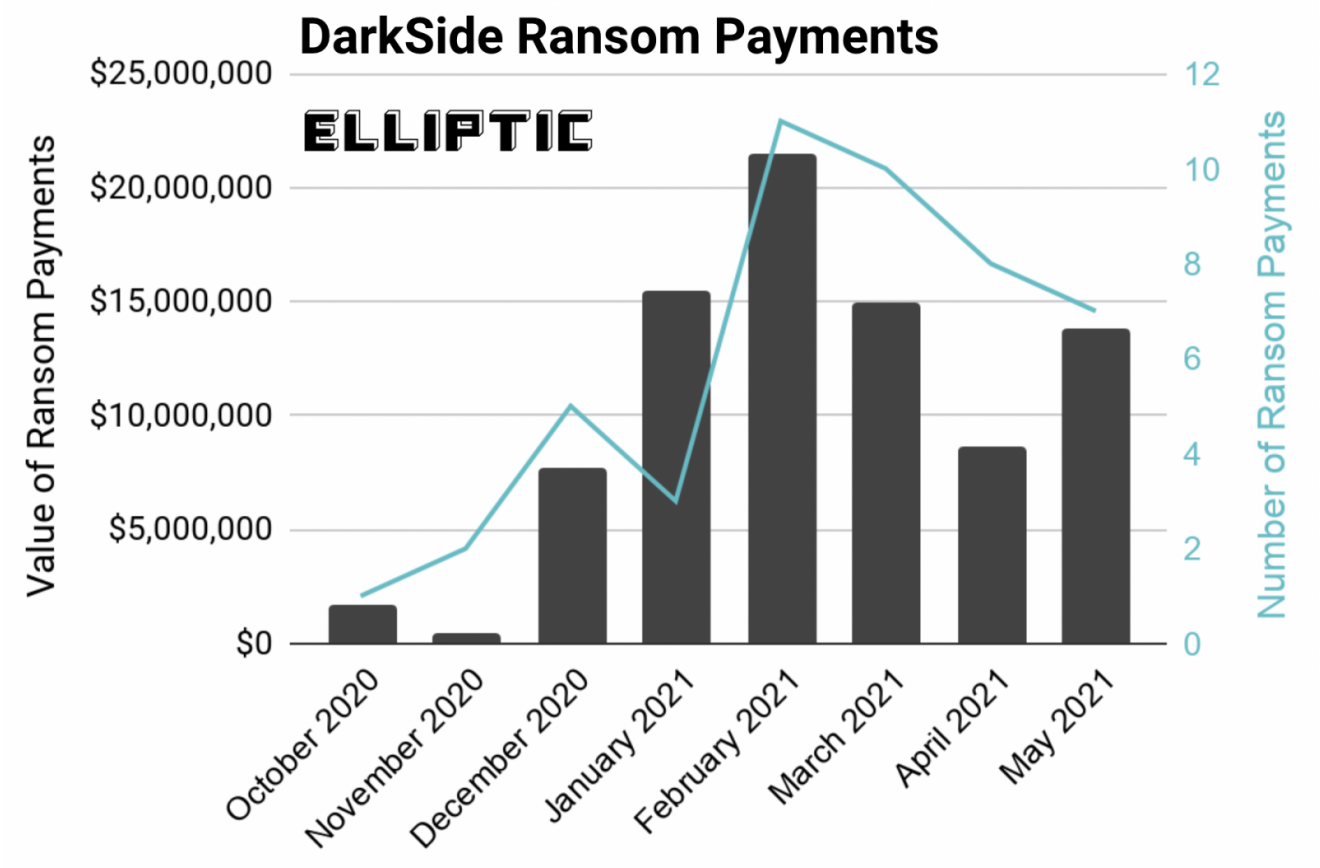
- May 18, 2021
- 12:33 PM
- 0

The DarkSide ransomware gang has collected at least $90 million in ransoms paid by its victims over the past nine months to multiple Bitcoin wallets.

Around 10% of the profit came in one week from attacking just two companies: Colonial Pipeline, the largest oil pipeline system in the United States, and Brenntag, a large chemical distribution company in Germany.

Huge ransom payments

Blockchain analysis company Elliptic found and analyzed ransom payments made to DarkSide from 47 distinct Bitcoin wallets. The transactions totaled just over $90 million since October 2020.



source: Elliptic

Assuming these are all the payments that DarkSide received from its victims, the group's average ransom would be $1.9 million, making the threat actor one of the greediest in the ransomware business.

A blog post from Managed Detection and Response (MDR) service provider eSentire on May 12, a day before DarkSide operations closed, counted 59 victims listed on the gang's leak site, which would add to the 47 associated with the Bitcoin wallets that Elliptic analyzed.

Although DarkSide launched in August 2020, the gang became a prolific actor on the ransomware scene and saw a significant surge in profits lately.

Elliptic notes in a report last week that the operation made $17.5 million, which is around 20% of its known total profits, only in the past three months.

Attacks on Colonial Pipeline and Brenntag chemical distribution company brought the cybercriminals about $10 million, as the former paid nearly $5 million and the latter paid a $4.4 million ransom.

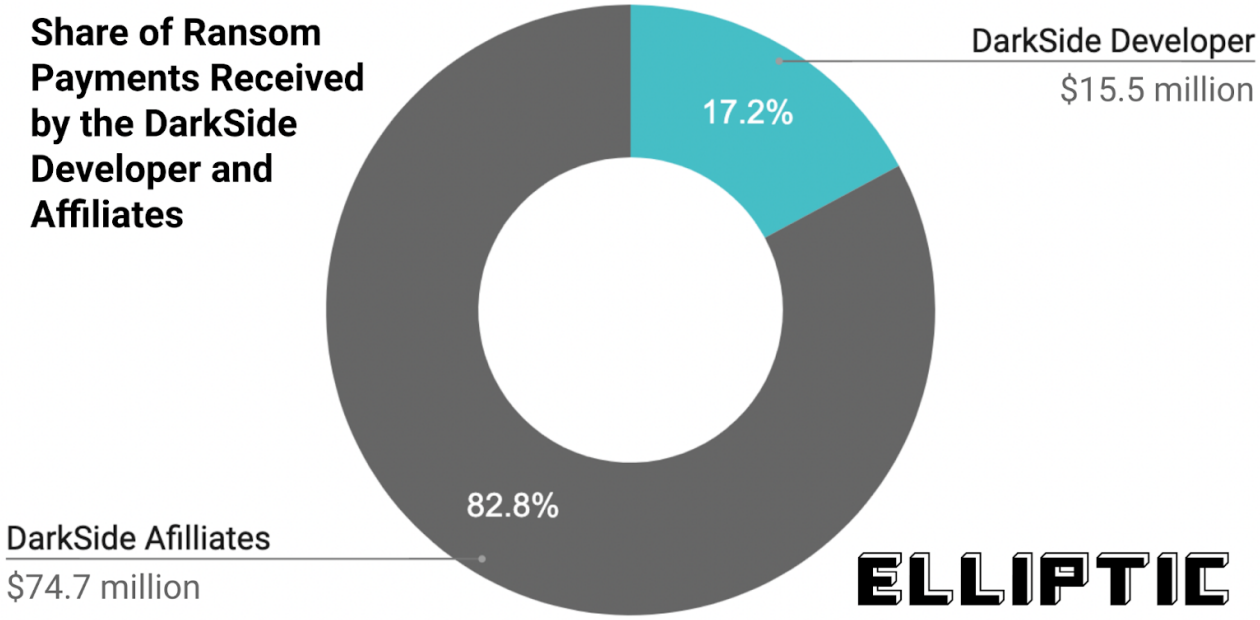
Splitting the profit

Being a ransomware-as-a-service (RaaS) operation, the DarkSide profits were split between the developers of the malware and the affiliates that breached victim networks, stole data, and deployed the file-encrypting malware.

Affiliates, or partners, typically get the lion's share of the money because they do most of the work. In the case of DarkSide, they got between 75% and 90% of the profit, depending on the size of the ransom.

For ransoms smaller than $500,000, the DarkSide developers would take 25%; the share decreased to 10% for larger payments of more than $5 million.

Elliptic co-founder and chief scientist Dr. Tom Robinson says that the "split of the ransom payment is very clear to see on the blockchain" and that the malware developer received $15.5 million worth of bitcoins from the total profits.



source: Elliptic
Following the transactions from wallets belonging to DarkSide affiliates, Robinson found that 18% of the proceeds were sent to some exchange services and 4% went to a large dark market that provides, among others, cash-out services.

With $90 million from ransoms over a period of nine months, DarkSide sits among the most profitable ransomware groups:

- Ryuk - at least $150 million
- GandCrab - $150 million (self-claim) in one year and a half
- REvil - $100 million (self-claim) in one year
- Maze/Egregor - over $63 million received to one Bitcoin address in four months (between August 2020 and the end of the year)
- Netwalker - $25 million in five months
- Qlocker - $260,000 in 5 days

Related Articles:

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

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

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.