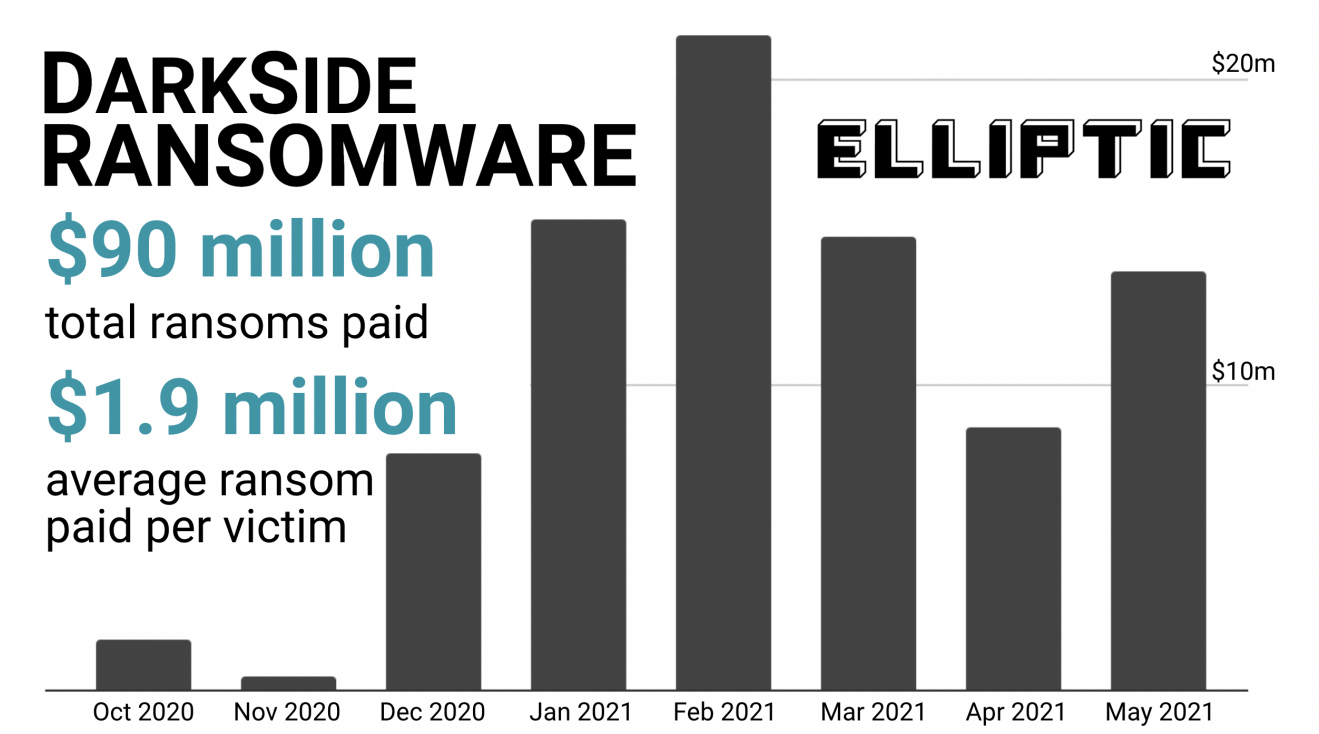
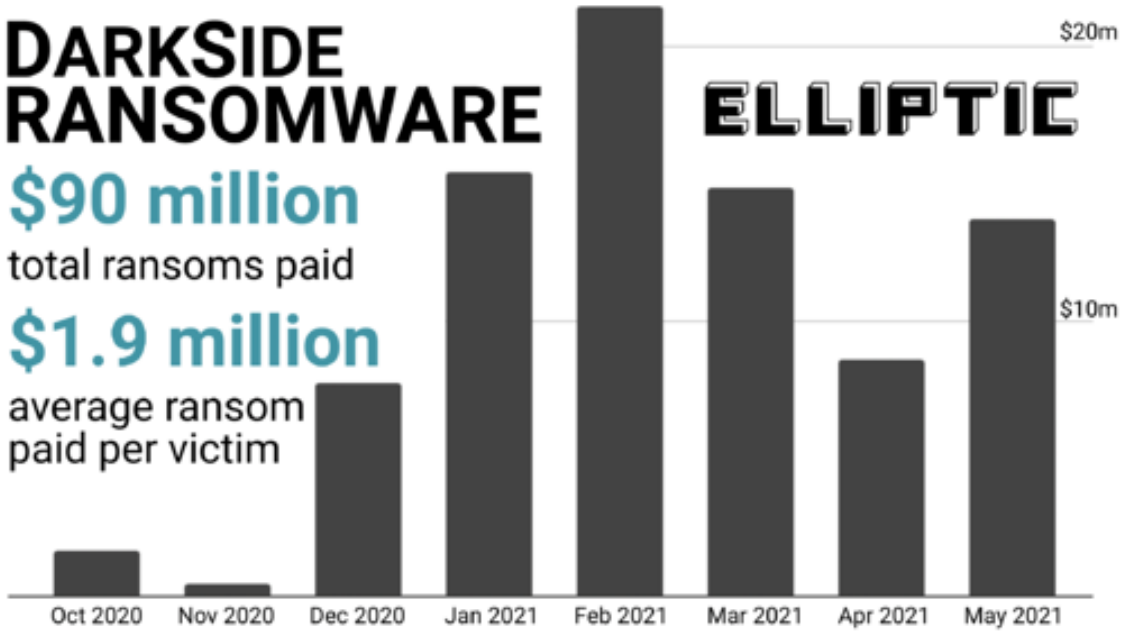
# DarkSide Ransomware has Netted Over $90 million in Bitcoin

elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin



**Dr. Tom Robinson**

Elliptic's Co-founder and Chief Scientist discusses cryptocurrency forensics, investigations, compliance, and sanctions.

Elliptic was first to identify the Bitcoin wallet used by the DarkSide ransomware group to receive a 75 Bitcoin ransom payment from Colonial Pipeline.

Colonial was the victim of a ransomware attack on May 7, 2021, which led to a voluntary shutdown of the main pipeline supplying 45% of fuel to the East Coast of the United States. The attack was described as the worst cyberattack to date on U.S. critical infrastructure.

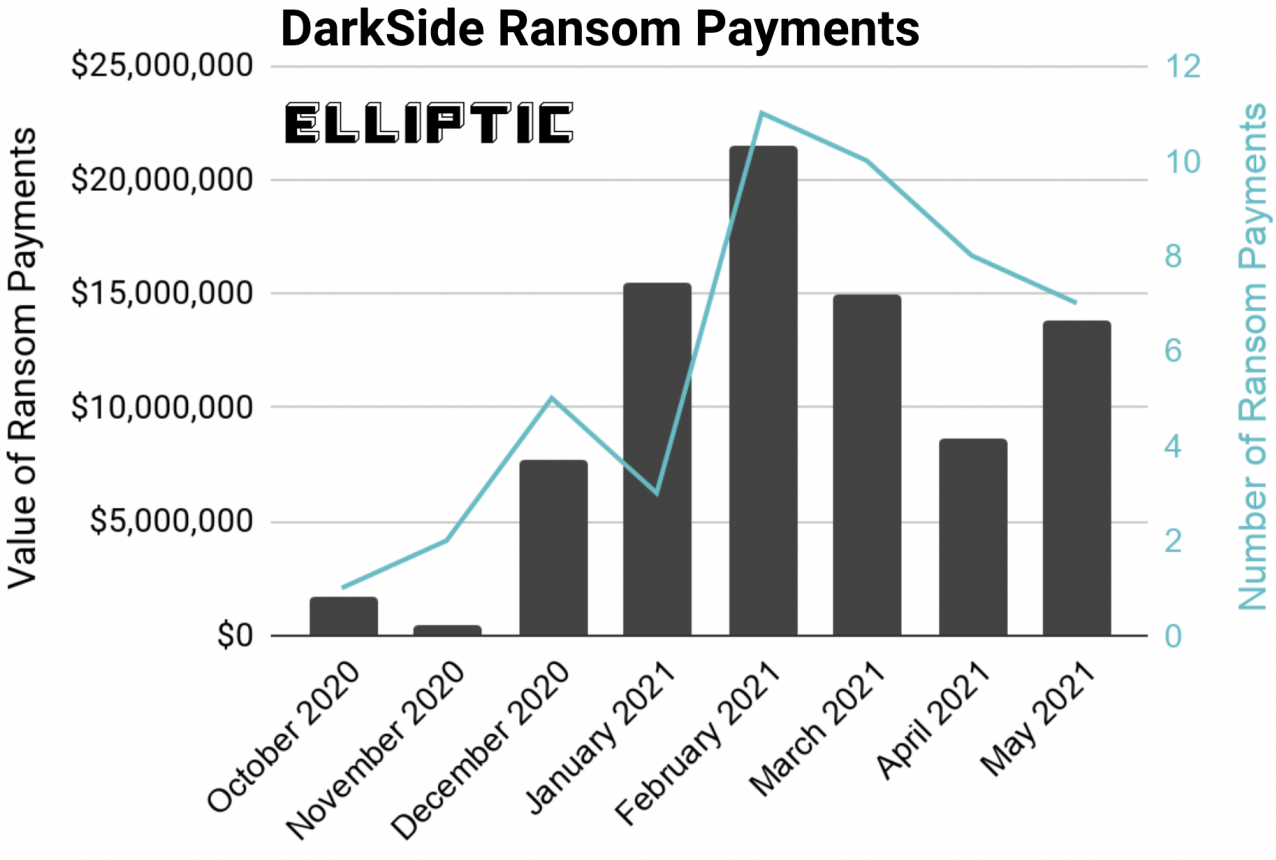
In this new report we expand our original analysis to examine all of the wallets used by DarkSide to receive Bitcoin ransoms from victims over the past nine months.

This relies on Elliptic's sophisticated blockchain analysis platform, combined with open source intelligence gathered by our team of analysts. To our knowledge, this analysis includes all payments made to DarkSide, however further transactions may yet be uncovered, and the figures here should be considered a lower bound.

**Over $90 million extracted from 47 victims**

In total, just over $90 million in Bitcoin ransom payments were made to DarkSide, originating from 47 distinct wallets. According to DarkTracer, 99 organisations have been infected with the DarkSide malware - suggesting that approximately 47% of victims paid a ransom, and that the average payment was $1.9 million.

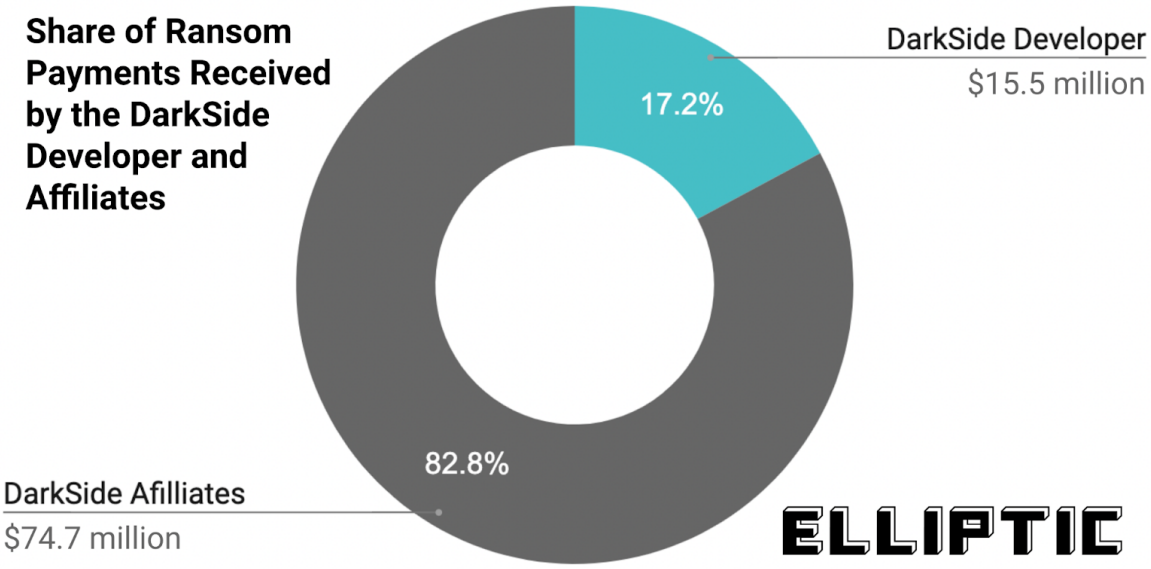
The chart below shows the total value and number of ransom payments made to DarkSide over the past nine months. May was set to be a record month, until DarkSide reportedly shut down its operations on May 13, and its Bitcoin wallet was emptied.




**Sharing the spoils**

DarkSide is an example of “Ransomware as a Service” (RaaS). In this operating model, the malware is created by the *ransomware developer*, while the *ransomware affiliate* is responsible for infecting the target computer system and negotiating the ransom payment with the victim organisation. This new business model has revolutionised ransomware, opening it up to those who do not have the technical capability to create malware, but are willing and able to infiltrate a target organisation.

Any ransom payment made by a victim is then split between the affiliate and the developer. In the case of DarkSide, the developer reportedly takes 25% for ransoms less than $500,000, but this decreases to 10% for ransoms greater than $5 million. This split of the ransom payment is very clear to see on the blockchain, with the different shares going to separate Bitcoin wallets controlled by the affiliate and developer. In total, the DarkSide developer has received bitcoins worth $15.5 million (17%), with the remaining $74.7 million (83%) going to the various affiliates.




In fact the affiliate's share of both the Colonial Pipeline and Brenntag ransom payments were sent to the same Bitcoin wallet, suggesting that the same party was responsible for infecting both of these businesses.

**Following the money**

Using Elliptic's blockchain analytics we can follow the ransom payments and see where the bitcoins are being spent or exchanged. What we find is that the majority of the funds are being sent to cryptoasset exchanges, where they can be swapped for other cryptoassets, or fiat currency.

The majority of cryptoasset exchanges comply with anti money laundering regulations. They verify their customers' identity and report suspicious activity. They also use blockchain analytics tools such as those offered by Elliptic, to check customer deposits for links to illicit activity such as ransomware.

However some jurisdictions do not enforce these regulations, and it is to exchanges in these locations that much of the DarkSide ransomware proceeds are being sent. Regulated cryptoasset businesses should perform careful due diligence on the virtual asset service providers (VASPs) that they transact with. Elliptic Discovery provides risk profiles of all major global VASPs - enabling you to to take a risk-based approach to your crypto counterparties.

Learn more about how Elliptic helps crypto businesses and financial institutions manage their cryptoasset risk.

## Disclaimer

This blog is provided for general informational purposes only. By using the blog, you agree that the information on this blog does not constitute legal, financial or any other form of professional advice. No relationship is created with you, nor any duty of care assumed to

you, when you use this blog. The blog is not a substitute for obtaining any legal, financial or any other form of professional advice from a suitably qualified and licensed advisor. The information on this blog may be changed without notice and is not guaranteed to be complete, accurate, correct or up-to-date.