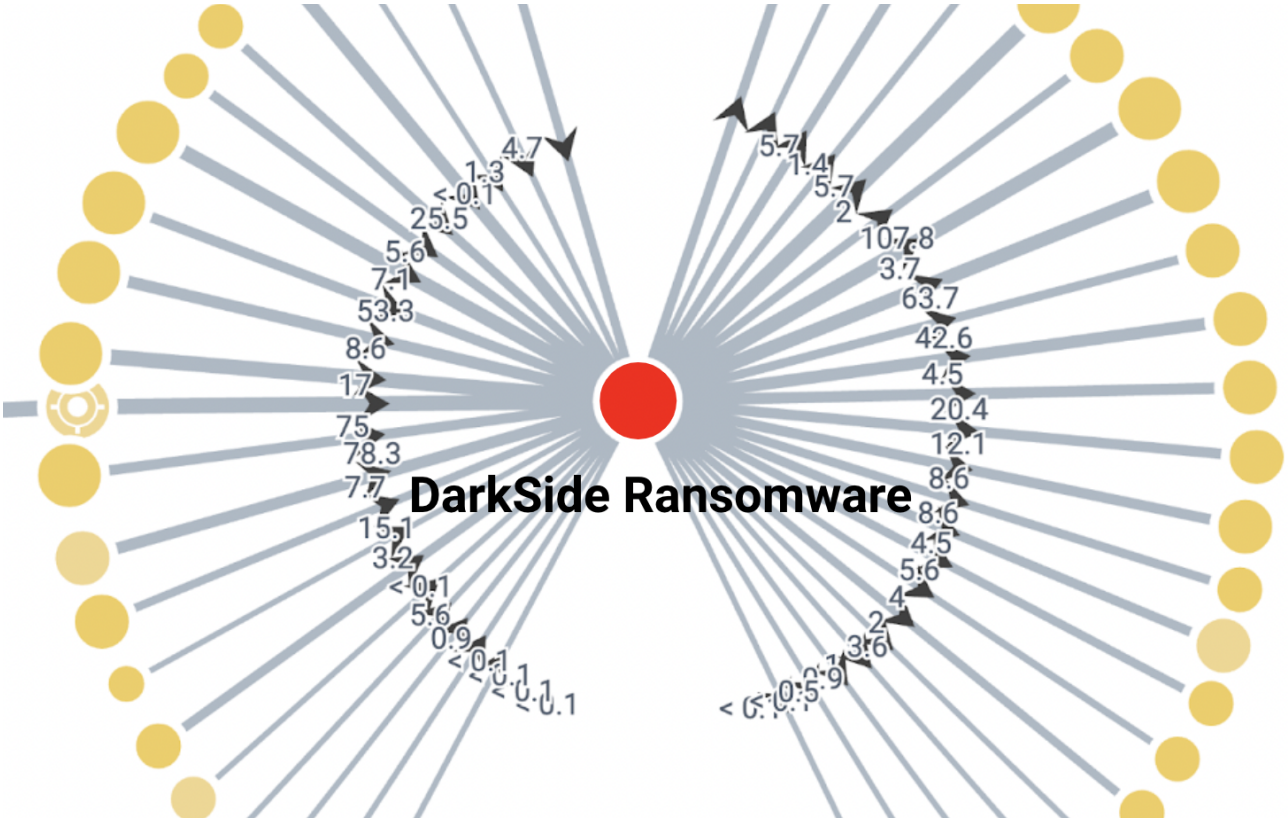
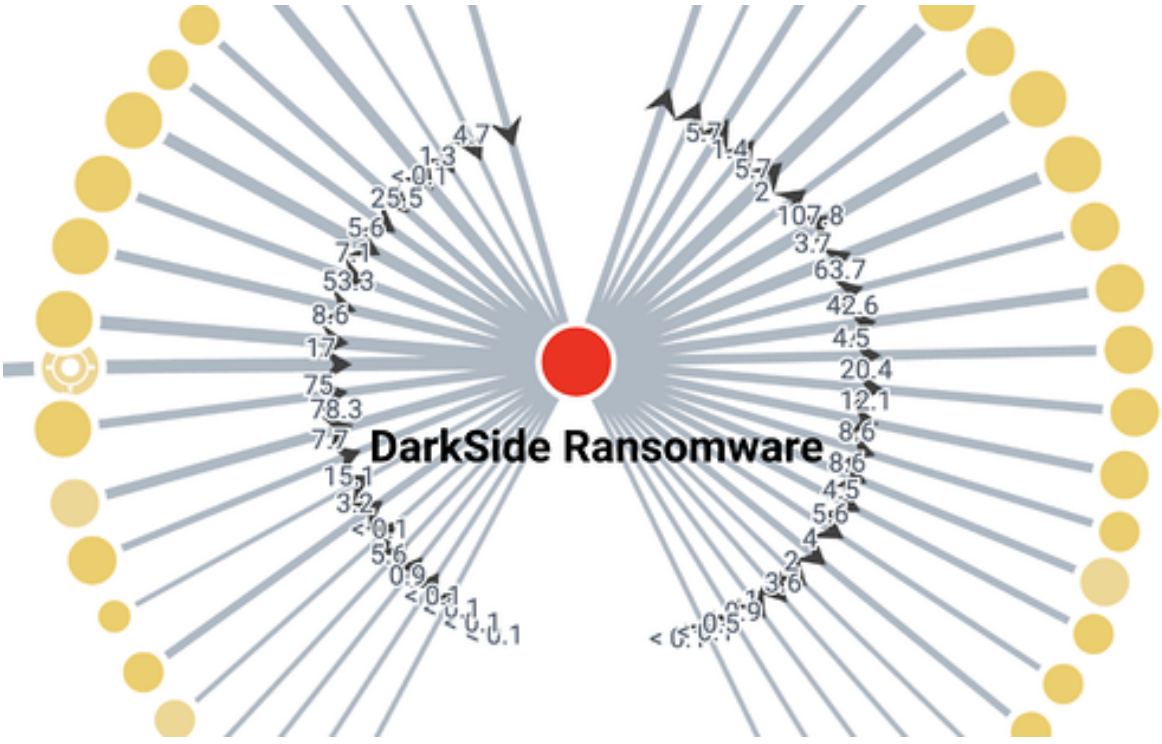
Elliptic Follows the Bitcoin Ransoms Paid by Colonial Pipeline and Other DarkSide Ransomware Victims

elliptic.co/blog/elliptic-follows-bitcoin-ransoms-paid-by-darkside-ransomware-victims





Dr. Tom Robinson

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

What does Elliptic's analysis tell us about DarkSide, the cybercrime group that held the US's energy infrastructure to ransom this week?

Updated: 15 May 2021

Elliptic clients can now use our transaction screening software to screen deposits for links to this high-profile incident.

Elliptic has identified the Bitcoin wallet used by the DarkSide ransomware group to receive ransom payments from its victims, based on our intelligence collection and analysis of blockchain transactions. This wallet received the 75 BTC payment (worth $4.4 million at the time of the transaction) made by Colonial Pipeline on May 8, following the crippling cyberattack on its operations - leading to widespread fuel shortages in the US.

Our analysis shows that the wallet has been active since 4th March 2021 and has received 57 payments from 21 different wallets. Some of these payments directly match ransoms known to have been paid to DarkSide by other victims, such as 78.29 BTC (also worth $4.4 million at the time of the transaction) sent by chemical distribution company Brenntag on May 11.

In fact the affiliate's share (the part of the ransom that goes to the deployer of the malware) of both the Colonial Pipeline and Brenntag ransom payments were sent to the same Bitcoin address, suggesting that the same party was responsible for infecting both of these businesses.

In addition, our analysis shows that a previously unreported ransom payment for ~$320,000 was made to DarkSide on the 10th May: the bitcoins originated from the same exchange used by Colonial Pipeline.

In total, the DarkSide wallet has received Bitcoin transactions since March with a total value of $17.5 million. Ransoms associated with previous attacks were paid to other wallets.

Where is Darkside sending the bitcoins?

We can also use blockchain analysis to follow the money trail and determine where DarkSide is sending its ransomware proceeds, to launder them or convert them to cash.

It has been reported within the past hours that DarkSide itself has ceased operations and has had its funds seized - and indeed their wallet was emptied of the $5 million in Bitcoin it contained on Thursday afternoon. There has been speculation that the bitcoins were seized by the US government - if that is the case they didn't actually seize most of Colonial Pipeline's ransom payment - the majority of that was moved out of the wallet on the 9th May.

But by tracing previous outflows from the wallet, we can gain insights into how DarkSide and its affiliates were laundering their previous proceeds. What we find is that 18% of the Bitcoin was sent to a small group of exchanges. This information will provide law enforcement with critical leads to identify the perpetrators of these attacks.

An additional 4% has been sent to Hydra, the world's largest darknet marketplace, servicing customers in Russia and neighboring countries. As we revealed in previous research, Hydra offers cash-out services alongside narcotics, hacking tools and fake IDs. These allow Bitcoin to be converted into gift vouchers, prepaid debit cards or cash Rubles. If you're a Russian cybercriminal and you want to cash-out your crypto, then Hydra is an attractive option.

What can be done about this?

By identifying this wallet, Elliptic's clients, including financial institutions, crypto exchanges and fintechs will now be alerted to any client deposits that originate from the DarkSide wallet. By using our transaction and wallet screening tools they can ensure that DarkSide and other ransomware operators cannot cash-out or exchange their Bitcoin proceeds, disincentivizing this activity.

Elliptic's law enforcement clients can also use our software to trace these funds and seek to identify those responsible for these crippling cyber attacks.

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

If you don't already have Elliptic backing up your crypto AML compliance operations already, you can schedule a demo today:

SCHEDULE A DEMO

Disclaimer

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.