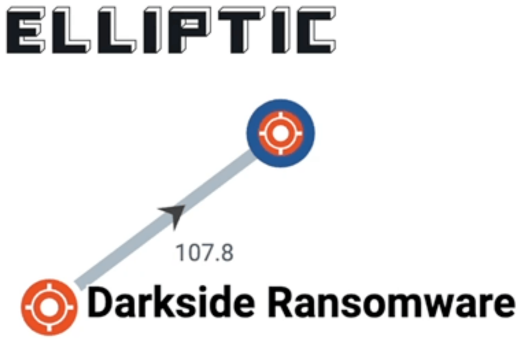
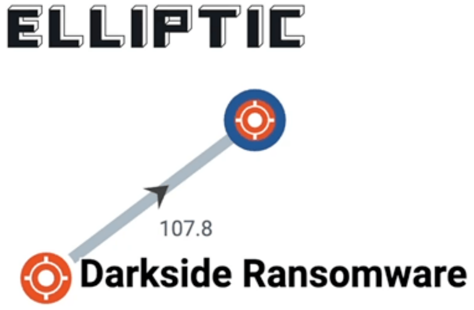
DarkSide bitcoins on the move following government cyberattack against REvil ransomware group

elliptic.co/blog/darkside-bitcoins-on-the-move-following-government-cyberattack-against-revil-ransomware-group





Elliptic Intel

$7 million in bitcoin held by the DarkSide ransomware group is on the move, five months after the attack on Colonial Pipeline that crippled fuel supplies along the US East coast. These funds had remained dormant since the group shut down on May 13.

DarkSide received just over $90 million in bitcoin ransom payments from around 50 victims, before shutting down shortly after the Colonial Pipeline attack. The following month US authorities seized 63.7 bitcoins that made up the affiliate's share of the 75 BTC Colonial Pipeline ransom payment.

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.

The DarkSide developer maintained a wallet to hold its share of the ransom payments — including 11.3 bitcoins from the Colonial payment. On May 13, DarkSide claimed that its infrastructure, including the wallet, had been seized by an unknown third party. On the same day the wallet was emptied, with 107.8 bitcoins (then worth $5.3 million) being sent to a new bitcoin address.

These funds remained dormant until yesterday (October 21). Beginning at 7am GMT, the funds, now worth $7 million, were moved through a series of new wallets over the course of several hours, with small amounts being "peeled" off at each step. This is a common money laundering technique, used to attempt to make the funds more difficult to track and to aid their conversion into fiat currency through exchanges. The process is ongoing, but small amounts of the funds have already been sent to known exchanges.

The movement of the dormant DarkSide funds comes on the same day that it was reported that the REvil ransomware group had been hacked and forced online in a government-led operation. DarkSide has been strongly linked to REvil, with the ransomware groups sharing similarly structured ransom notes and using the same code.

Elliptic's clients, including financial institutions and cryptocurrency exchanges can be alerted to any client deposits that originate from the DarkSide wallet, by using our transaction and wallet screening solutions.

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.