Hacker group, Darkside, allegedly received Bitcoin worth $90 million from the Colonial Pipeline cyberattack

DarkSide, the hacker group who perpetrated the recent Colonial Pipeline cyberattack, reportedly received bitcoin amounting to $90 million as ransom payments last week before the pipeline system ceased its operation.

London-based blockchain firm Elliptic reported that it had traced DarkSide's bitcoin wallet used for the collection of ransom payments from its victims.

The statement was released on Friday, and on the same day, security researchers Intel 471 added that DarkSide closed down after its servers became inaccessible and it emptied its cryptocurrency wallets completely.

The Colonial Pipeline ransomware attack

Colonial Pipeline dealt with a ransomware attack that blew out of proportion giving the company no choice but to slow down and then halt the operation of its almost 5,500 miles pipeline in the US.

As a result, the gas delivery system in the Southeastern states was significantly interrupted, causing consumers to go as far as hoard gas unsafely.

After initial investigations, the FBI attributed the crime to the cybercriminal gang, DarkSide. The said group is speculated to have been operating in Eastern Europe. It was allegedly divulged that Colonial paid $5 million worth of ransom to DarkSide.

DarkSide earned its reputation for using ransomware as a service business model. The idea is that they develop and sell ransomware tools to other criminals capable of carrying out cyberattacks.

Bitcoin under scrutiny again

Ransomware, a malicious software, blocks access to any computer system. Hackers will demand a ransom payment in exchange for the restoration of the access.

Ransom payments in this type of illegal activity are often asked to be in the form of cryptocurrency like bitcoin. Part of the reason is that people may choose not to reveal their identity and still successfully transact using cryptocurrency.

In turn, bitcoin has gained a bad reputation for its use in criminal activity. However, the digital ledger that bolsters bitcoin is open, meaning researchers can track where funds are being sent.

In the report provided by Elliptic, the hackers and their associates gained bitcoin with a value of $90 million as payments for the last nine months. The majority of the complete haul is subjected to crypto conversions, where they are withdrawn into actual money.

The ransom payoff came from a total of 47 victims with an average payment of about $1.9 million.

Elliptic's analysis encompasses all payments directed to DarkSide. However, as mentioned by Elliptic's co-founder and chief scientist, Tom Robinson, "further transactions may not yet be uncovered, and the figures here should be considered a lower bound."

Furthermore, according to Elliptic, from the $90 million hauls, the hacker group's developer took $15.5 million while $74.7 million went to its associates.

The DarkSide's bitcoin wallet was believed to contain $5.3 million worth of cryptocurrency before they were withdrawn entirely last week.

While some may assume that the hackers are currently enjoying their dirty money, it is also generally speculated that the US government had confiscated this bitcoin.