US offers $10 million reward for info on Darkside ransomware group

By Catalin Cimpanu

Published: 2022-12-19 · Archived: 2026-04-05 17:21:16 UTC

The US government has offered today a $10 million reward for any information that may lead to the identification and/or arrest of members of the Darkside ransomware group.

The State Department said the reward is eligible for any information on Darkside members with a key leadership position inside the group's operations.

Tips that lead to the arrest of Darkside affiliates, which might help the group carry out an attack once in a while, can also bring in up to $5 million, the State Department said in a press release today.

US government cites Colonial Pipeline attack as reason

Officials said they are offering these large rewards because of the group's attack on Colonial Pipeline, one of the largest fuel pipeline operators in North America.

Carried out in May 2021, the attack had a huge impact on the United State's economy, crippling 45% of the fuel supply for the US East Coast, disrupting businesses and regular consumers alike.

Following several veiled threats from the White House in the aftermath of the attack, the Darkside gang shut down its operations a week later, citing a mysterious cyberattack following which they said they lost control over servers and some of their funds.

The group attempted a comeback over the summer, rebranding as BlackMatter and relaunching in July, but earlier this week, the group said they are shutting down for a second time, citing pressure from local authorities and the disappearance of some of its members.

Darkside group members have a long history of cybercrime

All in all, the chances that security researchers will send tips about the gang's members and their real identities are very high.

The cybersecurity community has been tracking the group since the early 2010s, typically under the codename of FIN7, when the group was primarily involved in carrying out attacks on point-of-sale systems.

Some of these early FIN7 members were charged and subsequently arrested in 2018, a good indicator that the group may not live as deep in the shadows as they think they do.

The rewards offered today are not the first that the US government has offered for information on foreign hackers. Previous cases include:

- **July 2021** - a $10 million reward or any information that helps US authorities identify and locate threat actors "acting at the direction or under the control of a foreign government" that carry out malicious cyber activities against US critical infrastructure.
- **August 2020** - a $10 million reward for information on any person who works with or for a foreign government for the purpose of interfering with US elections through "illegal cyber activities."
- **April 2020** - a $5 million reward for information on North Korea's hackers and their ongoing hacking operations.

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
