Servers of Colonial Pipeline hacker Darkside forced down: security firm

May 14 2021, by Paul Handley

After a cyber attack, Colonial said it was moving toward a partial reopening of its pipeline system—the largest fuel network between Texas and New York

Servers for Darkside were taken down by unknown actors Friday, a week after the cyber extortionist forced the shutdown of a large US oil

pipeline in a ransomware scam, a US cyber security firm said.

Recorded Future, the security firm, said in a post that the allegedly Russia-based Darkside had admitted in a web post that it lost access to certain servers used for its web blog and for payments.

Accessed via TOR on the dark web, the Darkside site address showed a notice saying it could not be found.

Recorded Future threat intelligence analyst Dmitry Smilyanets said he found a Russian language comment on a ransomware website ostensibly from "Darksupp", described as the operator of Darkside.

"A few hours ago, we lost access to the public part of our infrastructure, namely: Blog. Payment server. DOS servers," Darksupp wrote.

"The Darkside operator also reported that cryptocurrency funds were also withdrawn from the gang's payment server, which was hosting ransom payments made by victims," said Recorded Future.

While there was no evidence of who might have forced down Darkside's website, the twitter account of a US military cyber warfare group, the 780th Military Intelligence Brigade, retweeted the Recorded Future report on Friday.

Darkside, which only surfaced online late last year, was behind the attack on Colonial Pipeline that forced the shutdown of its network shipping gasoline, diesel and aviation fuel across much of the eastern half of the United States.

After Darkside froze Colonial's computer systems last week and demanded millions in ransom to unlock them, Colonial shut down its pipeline, sparking fuel shortages and long lines at gas stations across

much of the southeast.

On Thursday Colonial said it had resumed fuel deliveries along its 5,500 mile (8,850 kilometers) pipeline amid unconfirmed reports it had paid Darkside $5 million to end the cyber-siege.

The attention that the Colonial shutdown brought to Darkside and the apparent attack to shut it down appeared to spark turmoil in the flourishing ransomware "industry," in which hackers and owners of the ransomware software and payment operations openly collaborate on mainly Russian language forums.

US President Joe Biden said that even though US intelligence did not link the Russia-based hackers to the Russian government, he would nevertheless bring up the issue with President Vladimir Putin in a summit tentatively planned in the coming months.

One such forum, XSS, announced Thursday a ban on sales and rentals of ransomware, according to Digital Shadows, a cyber security firm.

Nevertheless, ransomware extortion continued to proliferate. Various groups, including Darkside before it was shut down, posted fresh information on companies whose data had been hacked and was being held for payments that can run into the millions of dollars.

Ireland's health authority said Friday it had shut down its computer systems after experiencing a "significant ransomware attack."

And another extortionist group, Babuk, continued to release sensitive online files stolen from the Washington metropolitan police department as it continued to demand a seven-figure payout from the main security body of the US capital city.