

# Darkside ransomware gang says it lost control of its servers & money a day after Biden threat

R. [therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/](https://therecord.media/darkside-ransomware-gang-says-it-lost-control-of-its-servers-money-a-day-after-biden-threat/)

May 14, 2021



A day after US President Joe Biden said the US plans to disrupt the hackers behind the Colonial Pipeline cyberattack, the operator of the Darkside ransomware said the group lost control of its web servers and some of the funds it made from ransom payments.

“A few hours ago, we lost access to the public part of our infrastructure, namely: Blog. Payment server. CDN servers,” said **Darksupp**, the operator of the Darkside ransomware, in a post spotted by Recorded Future threat intelligence analyst [Dmitry Smilyanets](#).

“Now these servers are unavailable via SSH, and the hosting panels are blocked,” said the Darkside operator while also complaining that the web hosting provider refused to cooperate.

In addition, the Darkside operator also reported that cryptocurrency funds were also withdrawn from the gang’s payment server, which was hosting ransom payments made by victims.

The funds, which the Darkside gang was supposed to split between itself and its affiliates (the threat actors who breach networks and deploy the ransomware), were transferred to an unknown wallet, Darksupp said.

## Takedown?

---

This sudden development comes after US authorities announced their intention to go after the gang.

In two conferences this week, on Monday and Thursday, US President Biden himself came out and said the US would go after the group after one of its attacks crippled a major fuel transport pipeline that impacted half of the US East Coast, leading the US to declare a state of national emergency in order to ensure gasoline was delivered to impacted regions.

“We have been in direct communication with Moscow about the imperative for responsible countries to take decisive action against these ransomware networks,” President Biden said in a press conference on Thursday.

“We are also going to pursue a measure to disrupt their ability to operate,” he added [see *video below*].

Pres. Biden on Colonial Pipeline hack: "We do not believe the Russian government was involved in this attack—but we do have strong reason to believe that the criminals who did the attack are living in Russia." <https://t.co/CAHmsNFmcf>  
[pic.twitter.com/ex8AfuwIPX](https://t.co/ex8AfuwIPX)

— ABC News (@ABC) [May 13, 2021](#)

President Biden’s statement also came after Bill Evanina, former Director of the US National Counterintelligence and Security Center (NCSC), also said last week that the US intelligence community was very likely respond to respond to the brazen Colonial attack in a disruptive manner.

Darkside attribution is a good move by the FBI. I fully expect Darkside to shortly experience the full extent of IC and DoD precision tactical deterrent capabilities.  
<https://t.co/YsHFi0h2TY>

— William Evanina (@BillEvanina) [May 10, 2021](#)

## Or exit scam?

---

But Smilyanets warns that the group’s announcement could also be a ruse, as no announcement has yet been made by US officials.

The group could be taking advantage of President Biden’s statements as cover to shut down its infrastructure and run away with its affiliate’s money without paying their cuts—a tactic known as an “exit scam” on the cybercriminal underground.

According to #REvil #ransomware operator Unknown (possible false flag), #DarkSide – No More. Servers are seized. Money is gone 🗑️

— Dmitry Smirnovets (@ddd1ms) May 14, 2021

Reached out for comment, a spokesperson for the Justice Department said the department does not comment on active investigations and could not confirm a coordinated action from any US entity.

## REvil and Avaddon gangs announce changes too

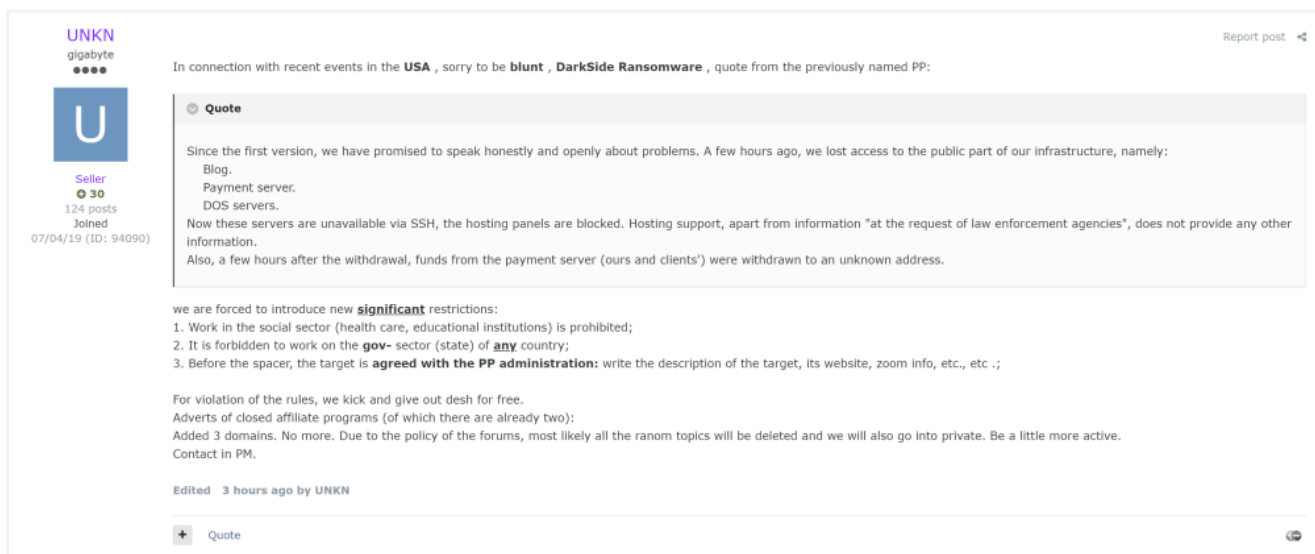
But it's been a busy past 24 hours for ransomware gangs.

The news that Darkside lost control of its servers and that a major cybercrime forum was banning ransomware ads, all happening within a span of hours of each other, also had an effect on REvil, arguably considered today's biggest ransomware operation.

In a post quoting Darkside's (now-deleted) statement, REvil spokesperson Unknown made an announcement of their own and said they also plan to stop advertising their Ransomware-as-a-Service platform and "go private"—a term used by cybercrime gangs to describe their intention to work with a small group of known and trusted collaborators only.

Additionally, the REvil group also said that it plans to stop attacking sensitive social sectors like healthcare, educational institutes, and the government networks of any country, which it believes could draw unwanted attention to its operation, such as the attention Darkside is getting right now.

In the case of any of such attacks carried out by any of its collaborators, REvil said they plan to provide a free decryption key to victims and stop working with the misbehaving affiliate.



The screenshot shows a forum post by a user named UNKN. The user's profile information includes the name UNKN, a gigabyte icon, four stars, a blue square with a white 'U', the role 'Seller', a 30-day icon, 124 posts, and a 'Joined' date of 07/04/19 (ID: 94090). The post content is as follows:

In connection with recent events in the USA, sorry to be blunt, DarkSide Ransomware, quote from the previously named PP:

**Quote**

Since the first version, we have promised to speak honestly and openly about problems. A few hours ago, we lost access to the public part of our infrastructure, namely:

- Blog.
- Payment server.
- DOS servers.

Now these servers are unavailable via SSH, the hosting panels are blocked. Hosting support, apart from information "at the request of law enforcement agencies", does not provide any other information.

Also, a few hours after the withdrawal, funds from the payment server (ours and clients') were withdrawn to an unknown address.

we are forced to introduce new **significant** restrictions:

1. Work in the social sector (health care, educational institutions) is prohibited;
2. It is forbidden to work on the **gov-**sector (state) of **any** country;
3. Before the spacer, the target is **agreed with the PP administration**: write the description of the target, its website, zoom info, etc., etc. ;

For violation of the rules, we kick and give out desh for free.

Adverts of closed affiliate programs (of which there are already two):

Added 3 domains. No more. Due to the policy of the forums, most likely all the ranom topics will be deleted and we will also go into private. Be a little more active.

Contact in PM.

Edited 3 hours ago by UNKN

Quote

Image: Recorded Future

Furthermore, hours after REvil's announcement, the operators of the Avaddon ransomware also announced similar updates to their program, with the same clause barring ransomware groups from attacking government entities, healthcare orgs, and educational institutes.

While we may never know who or what is driving these changes among ransomware gangs, it is pretty clear that the Colonial Pipeline attack and its aftermath appears to have broken the camel's back, and US authorities have started applying some sort of pressure on these groups.

[@ddd1ms](#) & [@campuscodi](#) Some change is happening.... [@Raj\\_Samani](#)  
[@ChristiaanBeek](#) [@McAfee\\_Labs](#) [pic.twitter.com/SIgNW3V2Df](https://pic.twitter.com/SIgNW3V2Df)

— John Fokker ([@John\\_Fokker](#)) [May 14, 2021](#)

## Tags

- [Biden](#)
- [Colonial Pipeline](#)
- [cybercrime](#)
- [Darkside](#)
- [Exploit forum](#)
- [hacking forum](#)
- [Ransomware](#)
- [US government](#)

Catalin Cimpanu is a cybersecurity reporter for The Record. He 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.