DarkSide ransomware servers reportedly seized, operation shuts down

bleepingcomputer.com/news/security/darkside-ransomware-servers-reportedly-seized-revil-restricts-targets/

Lawrence Abrams

By
Lawrence Abrams

- May 14, 2021
- 10:37 AM
- 2

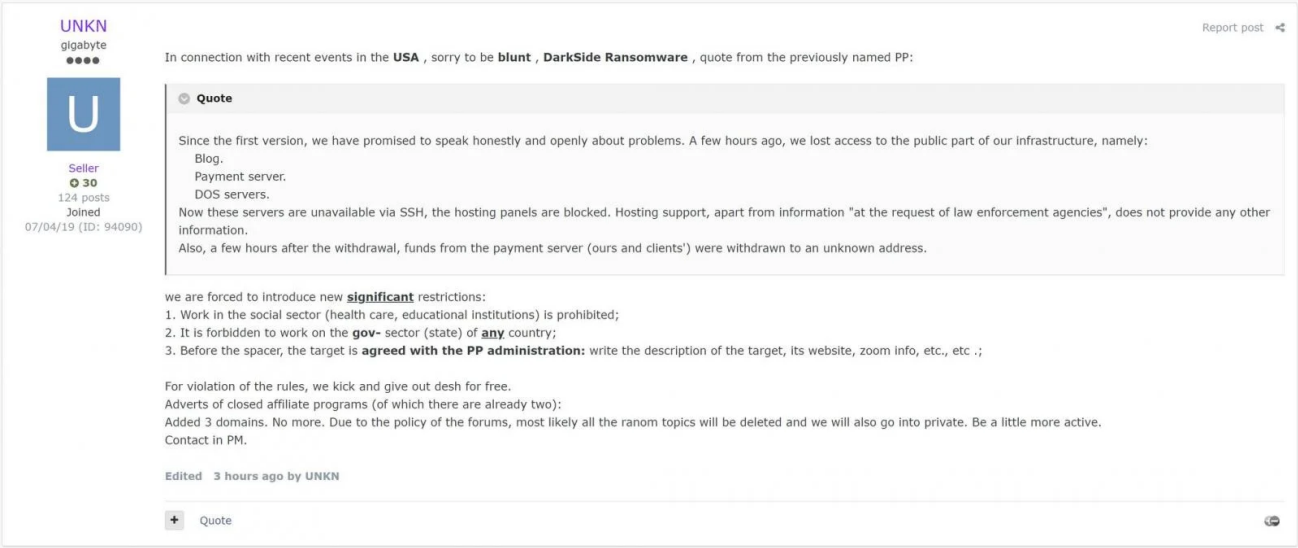
The DarkSide ransomware operation has allegedly shut down after the threat actors lost access to servers and their cryptocurrency was transferred to an unknown wallet.

This news was shared by a threat actor known as 'UNKN', the public-facing representative of the rival REvil ransomware gang, in a forum post first discovered by Recorded Future researcher Dmitry Smilyanets on the Exploit hacking forum.

In the post, 'Unkn' shared a message allegedly from DarkSide explaining how the threat actors lost access to their public data leak site, payment servers, and CDN servers due to law enforcement action.

"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," reads the forum post from UNKN.

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



Forum post by UKNK about DarkSide seizure

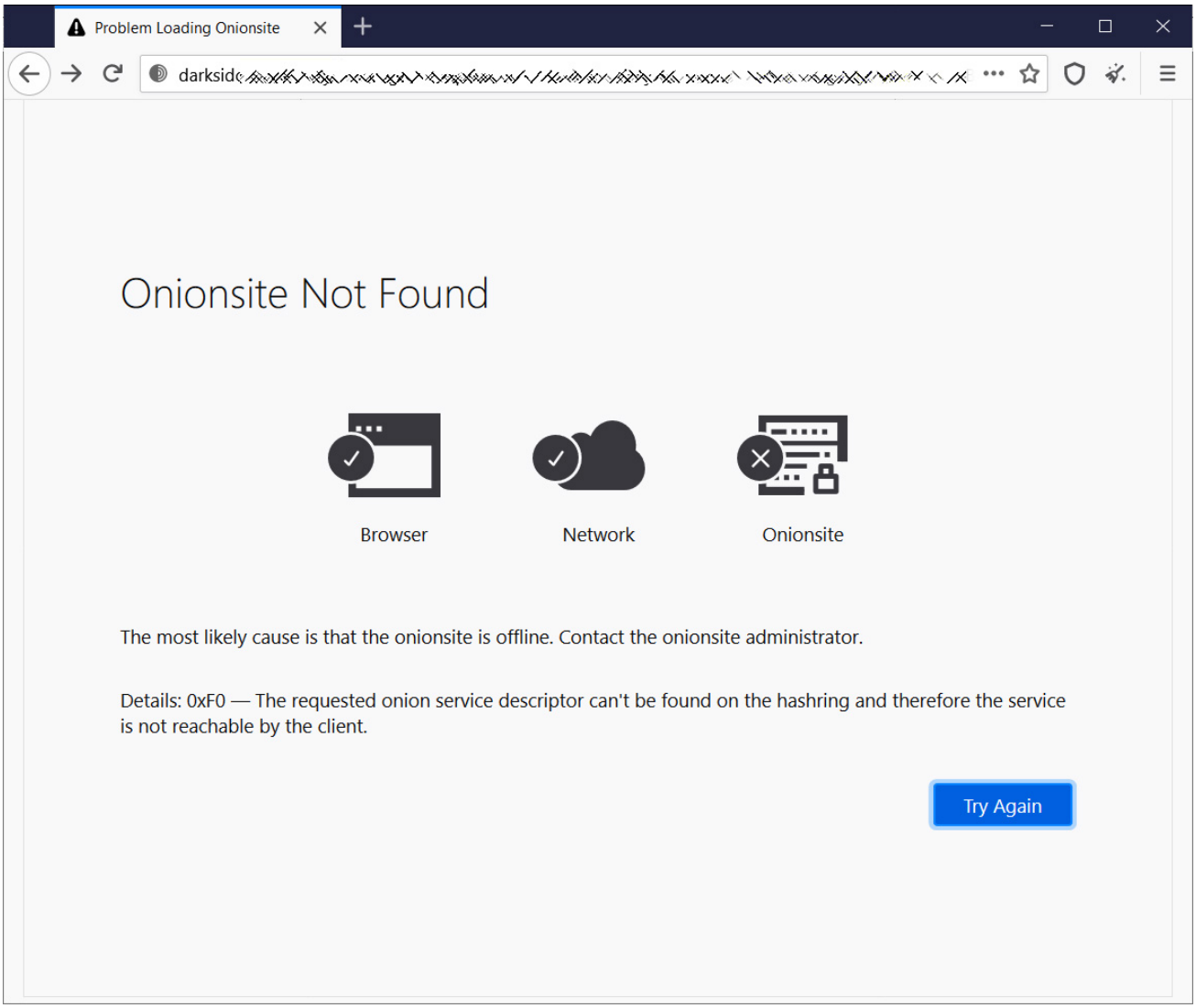
Source: Dmitry Smilyanet

This news comes a day after President Biden said in a White House press conference that countries harboring ransomware networks must take action to shut them down.

"We do not believe — I emphasize, we do not believe the Russian government was involved in this attack. But we do have strong reason to believe that criminals who did the attack are living in Russia. That's where it came from — were from Russia," Biden said in a press conference about the Colonial Pipeline attack.

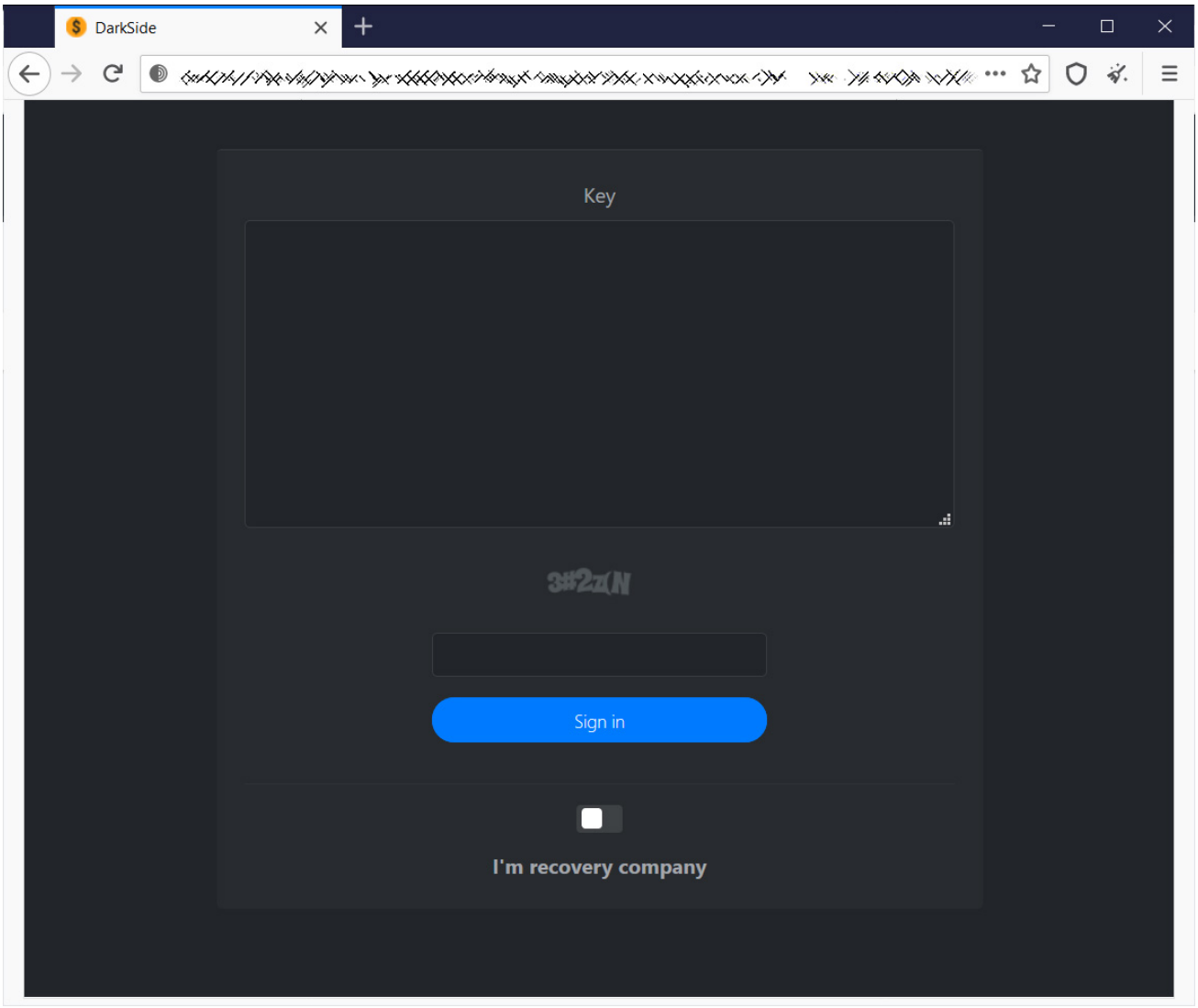
"We have been in direct communication with Moscow about the imperative for responsible countries to take decisive action against these ransomware networks."

Starting yesterday, security researchers and journalists noted that the DarkSide data leak site was no longer accessible, and it was speculated that law enforcement had seized the server.



Offline DarkSide data leak site

However, BleepingComputer has confirmed that the DarkSide Tor payment server is still operational at the time of this writing. If law enforcement seized the server, they might have kept it running to allow victims to access their decryptors.



DarkSide Tor payment live at the time of writing

Feeling the heat from law enforcement, it has also been speculated that the DarkSide ransomware gang may be pulling an exit scam.

After pulling in $9.4 million in ransom payments this week between Brenntag and Colonial Pipeline, they may be stealing the money, so they do not have to pay affiliates and to blame it on a law enforcement operation.

DarkSide shuts down affiliate program

After we published our story, Intel471 gained access to the full message sent to affiliates of the DarkSide ransomware-as-a-service operation.

According to this message, DarkSide decided to close their operation "due to the pressure from the US" and after losing access to their public-facing servers.

The full translated message acquired by Intel471 is below:

> Starting from version one, we promised to speak about problems honestly and openly. A couple of hours ago, we lost access to the public part of our infrastructure, in particular to the
>
> blog
>
> payment server
>
> CDN servers
>
> At the moment, these servers cannot be accessed via SSH, and the hosting panels have been blocked.
>
> The hosting support service doesn't provide any information except "at the request of law enforcement authorities." In addition, a couple of hours after the seizure, funds from the payment server (belonging to us and our clients) were withdrawn to an unknown account.
>
> The following actions will be taken to solve the current issue: You will be given decryption tools for all the companies that haven't paid yet.
>
> After that, you will be free to communicate with them wherever you want in any way you want. Contact the support service. We will withdraw the deposit to resolve the issues with all the affected users.
>
> The approximate date of compensation is May 23 (due to the fact that the deposit is to be put on hold for 10 days on XSS).
>
> In view of the above and due to the pressure from the US, the affiliate program is closed. Stay safe and good luck.
>
> The landing page, servers, and other resources will be taken down within 48 hours.

An interesting point in this message is that the affiliates will be provided decryptors for their victims. These decryptors will allow the affiliates to extort those victims on their own without any affiliation with DarkSide.

REvil ransomware adds new restrictions

Historically, the REvil ransomware gang has shown no scruples regarding who they attack.

However, after the DarkSide's reported **takedown**, REvil has now begun to impose new restrictions on who can be encrypted.

REvil's representative, UNKN, states that affiliates are now required first to gain permission to target an organization and that they can no longer target the following entities:

> 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;

Ransomware-as-a-Service (RaaS) operations have historically run as a free-for-all, where affiliates encrypt any victim they want without gaining prior approval.

It will be interesting to see if these new rules will lead affiliates to move to other RaaS operations with fewer restrictions.

Update 5/14/21: Added full message sent to affiliates about DarkSide closing down. Changed DoS to CDN (thx Evgueni).

Related Articles:

US Senate: Govt's ransomware fight hindered by limited reporting

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

REvil ransomware returns: New malware sample confirms gang is back

REvil's TOR sites come alive to redirect to new ransomware operation

- CryptoCurrency
- DarkSide
- Law Enforcement
- Ransomware
- REvil

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Comments

- 
  Citadel - 1 year ago
  -
  -
  There needs to be more severe repercussions. I know everyone's focus is on prevention. But full-circle prevention has to include repercussions. At this point, the word 'hitmen' comes to mind.

- 
  jacosa13 - 1 year ago
  -
  -
  My nightmare isa gigantic book deal the criminal[s]

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: