DarkSide ransomware is creating a secure data leak service in Iran

bleepingcomputer.com/news/security/darkside-ransomware-is-creating-a-secure-data-leak-service-in-iran/

Lawrence Abrams

By
Lawrence Abrams

- November 13, 2020
- 03:00 AM
- 0

The DarkSide Ransomware operation claims they are creating a distributed storage system in Iran to store and leak data stolen from victims. To show they mean business, the ransomware gang has deposited $320 thousand on a hacker forum.

DarkSide is run as a Ransomware-as-a-Service (RaaS) where developers are in charge of programming the ransomware software and payment site, and affiliates are recruited to hack businesses and encrypt their devices.

As part of this arrangement, the DarkSide ransomware developers receive a 10-25% cut, and an affiliate gets 75-90% of any ransom payments they generate.

As DarkSide is a private operation, hackers who want to distribute their ransomware must first apply for access.

Distributed storage system to leak data

Yesterday, cybersecurity intelligence firm Kela shared a new topic posted by the DarkSide Ransomware operators on a Russian-speaking hacker forum with BleepingComputer.

In this topic, DarkSide has stated that they are working on a distributed storage system to store and leak victims' stolen data.

Since late 2019, ransomware operations have been actively performing a double-extortion strategy of stealing unencrypted data and then encrypting the victim's computers. The encrypted files and the threat to publicly release data on ransomware data leak sites are used to extort victims into paying the ransom.

To disrupt these extortion demands, law enforcement and cybersecurity firms actively try to take down these data leak sites.

To prevent this, DarkSide states that they plan to create a distributed "sustainable storage system" in Iran to host the victim's stolen data for six months.

"Some targets think that if a lot of data has been downloaded from them, then after their publication, hackers and other people will download it for a long time through the TOR. We think so too, so we will change it."

"We are already working on a sustainable storage system for your data. All your data will be replicated between multiple servers, blocking one server won't delete data."

"Those companies that have already been published will be uploaded there, their data will be guaranteed to be stored for 6 months. So you can download their data much faster."

"We will specifically use servers in Iran or unrecognized republics so that you cannot block them, and an automatic system will determine the availability and give you a suitable download link," the DarkSide operators stated.

They state that all the stolen data will be replicated between the various servers, so if one server is taken down, the data could still be accessed from the others.

DarkSide deposits $320 thousand on a hacker forum

As part of this same forum topic, the DarkSide operation announced that they were looking for new Russian affiliates to join their program, who they claim to earn an average of $400k per victim.

As part of this recruitment drive, affiliates must pass an interview and answer any questions the developers have about their level of experience.

"Pass an interview, show your work and payments, answer the necessary questions." - DarkSide developers.

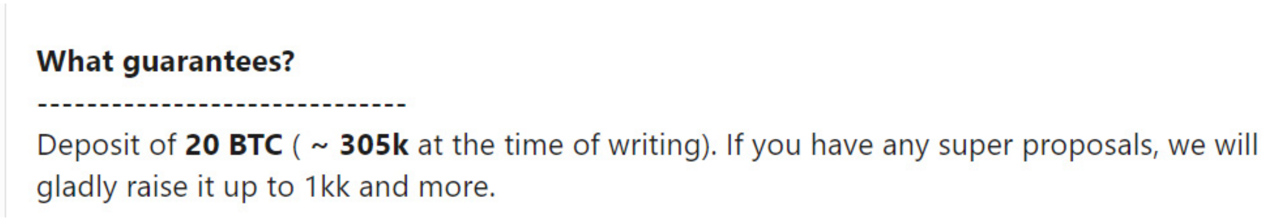
Unlike other ransomware operations, such as Ryuk, Egregor, and others, DarkSide states that do not allow attacks on:

- Medicine (hospitals, hospices).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

It is too soon to tell if DarkSide will keep its promises about not targeting these organizations.

In addition to recruiting affiliates, DarkSide states that they are willing to spend 400K to hackers with access to large companies in the USA that can be encrypted.

To back up their claims, the DarkSide gang deposited 20 bitcoins on the forum, which is worth approximately $320 thousand at today's values.

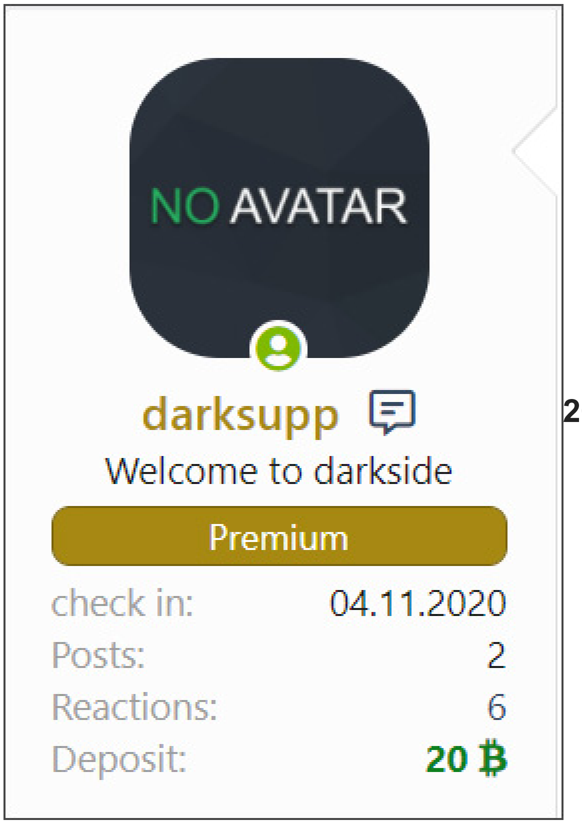


What guarantees?

Deposit of **20 BTC** (**~ 305k** at the time of writing). If you have any super proposals, we will gladly raise it up to 1kk and more.

Deposit of 20 bitcoins

As you can see below, the public-facing representative of DarkSide, known as 'darksupp', now has 20 bitcoins deposited in their account.



darksupp

Welcome to darkside

Premium

check in:	04.11.2020
Posts:	2
Reactions:	6
Deposit:	20 ₿

20 bitcoin deposit

These deposited bitcoins can then be transferred to other members to purchase software, services, or information.

This show of wealth is similar to REvil's recruitment drive in September when they deposited $1 million in bitcoins to the same forum.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

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

- Affiliates
- Bitcoin
- DarkSide
- Hacker Forum
- RaaS
- Ransomware
- Ransomware-as-a-Service

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

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: