DarkSide affiliates claim gang's bitcoin deposit on hacker forum

bleepingcomputer.com/news/security/darkside-affiliates-claim-gangs-bitcoins-in-deposit-on-hacker-forum/

Ionut Ilascu

By
Ionut Ilascu

- May 21, 2021
- 03:29 AM
- 0

Since the DarkSide ransomware operation shut down a week ago, multiple affiliates have complained about not getting paid for past services and issued a claim for bitcoins in escrow at a hacker forum.

Russian-language cybercriminal communities typically have an escrow system to avoid scams between sellers and buyers. For ransomware operations, the deposit is a clear statement that they mean big business.

To gain the trust of potential partners and expand the operation, DarkSide deposited 22 bitcoins on the popular hacker forum XSS. The wallet is managed by the site's administrator, which in this case acts as a guarantor for the gang and an arbitrator if a dispute occurs.

REvil ransomware last year deposited $1 million worth of Bitcoin to a different hacking forum to attract new recruits into the operation. This move showed that they trusted the forum administrator with the money and that there was plenty of money to be made.

Last week, DarkSide closed shop and informed affiliates that the decision came after losing access to their public-facing servers and it was "due to the pressure from the US" after the attack on Colonial Pipeline.

Unpaid debts

DarkSide's dissolving of the ransomware-as-a-service (RaaS) operation was abrupt and clearly left some unfinished business. Five partners have complained that the operators owed them money from paid ransoms or from hacking services:

- The first affiliate asking for claim states that they were the 'pentester' for an attack and was owed 80% of the ransom payment. However, after the victim paid, the DarkSide operators stated they no longer had access to the funds and the affiliate could use the deposit at XSS to receive payment
- The second affiliate states that they had bitcoins left for them on the affiliate portal but had to rush to their relatives before they could claim them
- A third affiliate states that they too were a 'pentester' and had a ransom payment right before the DarkSide operation shut down. This affiliate states they sent proof to the XSS admin
- A fourth affiliate states that they worked on corporate breaches but never received their last $150,000 payment
- The fifth and final affiliate states that there was a $72,000 made to them on the affiliate portal but could not collect it before the operation closed due to health reasons

In the case of the first claim issued on March 14, the forum administrator who is acting as arbitrator, approved compensation from DarkSide's deposit. They also asked others to come forward if they have cause.

Four days later, the second claim appeared, followed by another three on March 19 and 20. None of these received a reply from the forum administrator.

DarkSide became known in August 2020 and became one of the most prolific ransomware groups. In nine months, the operation made at least $90 million from ransoms.

In just one week, the gang collected about $9 million from two attacks: Colonial Pipeline and German chemical distribution company Brenntag.

Even if DarkSide shut down, there are still victims being extorted. Affiliates have received the corresponding decryption keys to continue negotiations with victim companies separately.

h/t 3xp0rt

Related Articles:

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

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

- DarkSide
- Ransomware

Ionut Ilascu

Ionut Ilascu is a technology writer with a focus on all things cybersecurity. The topics he writes about include malware, vulnerabilities, exploits and security defenses, as well as research and innovation in information security. His work has been published by Bitdefender, Netgear, The Security Ledger and Softpedia.

- Previous Article
- Next Article

You may also like: