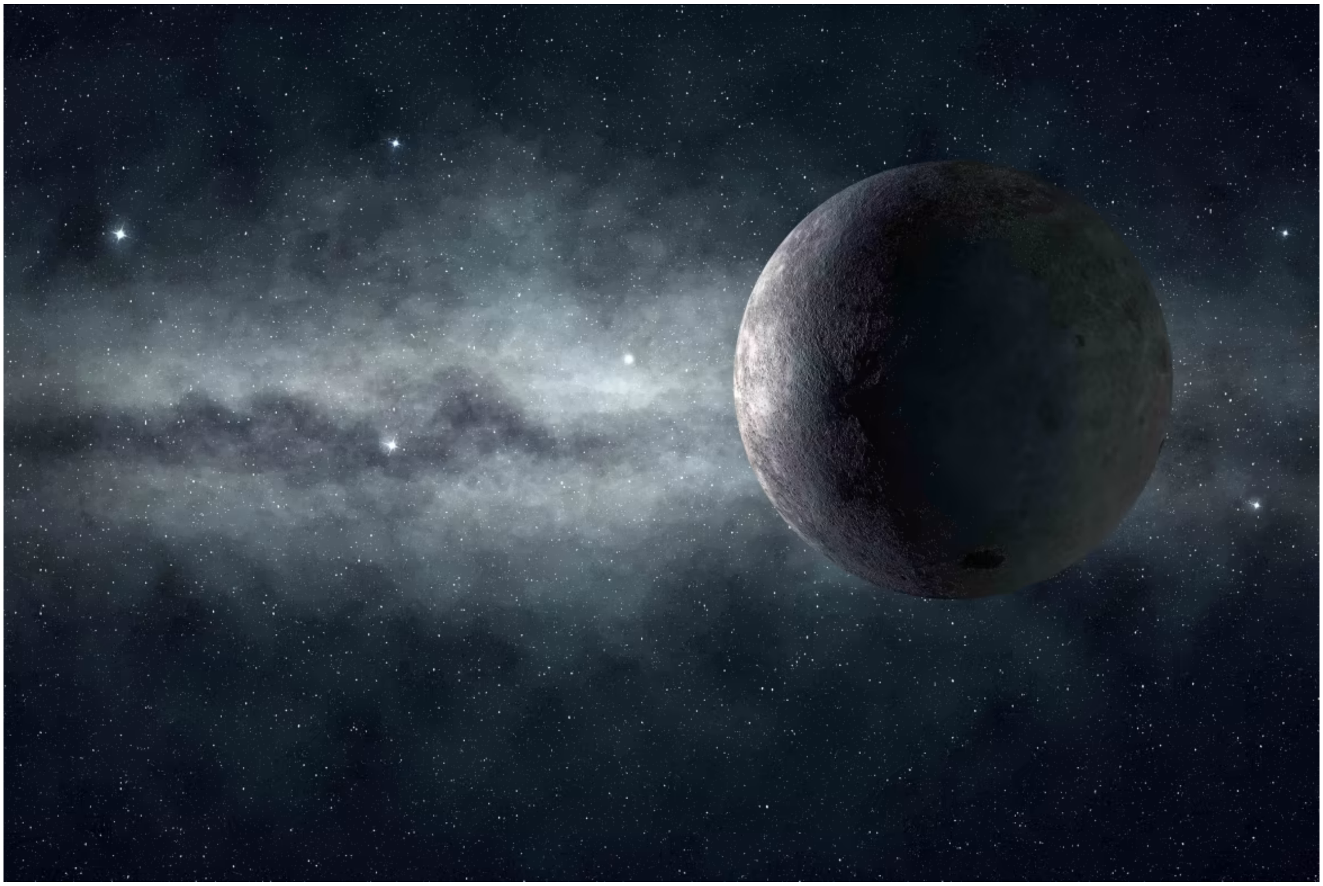
Download the Darkside Ransomware Analysis Report

brandefense.io/darkside-ransomware-analysis-report/

February 21, 2022



The DarkSide ransomware has been identified as a cybercrime gang thought to be based in Russia especially targeting the US and Eastern Europe corporations. Also, they leverage ransomware in their campaign. They had targeted energy, financial, and so on sectors. But targets do not include hospitals, government institutions, schools, non-profit organizations DarkSide that has first seen in August 2020. Also, their loudest operation is known as Colonial Pipeline in the US.

The DarkSide threat group also has been using the Double Extortion attack model. It is standardized between ransomware gangs to enforce organizations that have disaster recovery plans and refuse to pay the ransom. Therefore, if the victim accomplishes to recover encrypted data, they still have to pay to avoid publicly sharing data.

The DarkSide exhibits aggressive behavior for their targets to pay the ransom, dispositions to send emails to the employee if they think to get ignored or their victims did not respond themselves in 2-3 days. If this method is not working, they will not hesitate to tell by calling high-level executives. In this way, threat actors will notify the victim customers or press about the ransomware attack.

The DarkSide ransomware gang has been sold ransomware as RaaS modeling in underground cybercrime forums. This situation enables to conduct of campaigns without technical requirements.

As a result of the DarkSide ransomware campaigns, obtained ransom was $312.000 in 2020, while it rose approximately three times by reaching $800.000 in 2021. According to posts username darksupp believed to have belonged DarkSide in underground forums DarkSide developers get a share %25 for $500.000 and below ransom and for 5 Million $ and above also %10.

BRANDEFENSE
CYBER THREAT INTELLIGENCE

DarkSide Ransomware
Analysis Report

Author: Threat Intelligence Team
Release Date: [illegible]
Report ID: [illegible]

Brandefense
Digital Risk Protection Platform | info@brandefense.com | [illegible]