Darkside Ransomware Technical Analysis - Open Report - Brandefense

Published: 2023-11-29 · Archived: 2026-04-05 14:40:13 UTC

(…) The DarkSide ransomware has been identified as a cybercrime gang thought to be based in Russia, especially targeting the US and Eastern European 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, or non-profit organizations. DarkSide was first seen in August 2020. Also, their loudest operation is known as Colonial Pipeline in the US.

The DarkSie threat group has also been using the Double Extortion attack model. It is standardized between ransomware gangs to enforce organizations with disaster recovery plans that refuse to pay the ransom. Therefore, if the victim accomplishes recovering 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(…)
