DarkSide Ransomware Links to REvil Group Difficult to Dismiss

flashpoint-intel.com/blog/darkside-ransomware-links-to-revil-difficult-to-dismiss/

May 11, 2021

Blogs

Blog

The first report of a DarkSide ransomware attack came on August 10, 2020, with even early reports finding the ransomware to be highly customized with lucrative, million-dollar payouts from large corporate targets in finance, technology, and manufacturing industries. On that same day, August 10th, the DarkSide actors launched their associated DarkSide website on Tor.

Key Takeaways from Recent DarkSide Ransomware Events:

1. On May 10, 2021, the U.S. Federal Bureau of Investigation (FBI) issued a statement confirming that "the DarkSide ransomware is responsible for the compromise of the Colonial Pipeline networks," with its pipeline systems taken offline since Friday, May 7, 2021.
2. "DarkSide" is a ransomware strain that was originally developed by Russian-speaking threat actors and has been active since August 2020. The ransomware is highly customized, designed to target large corporations in select industry verticals, particularly those in finance, technology, and manufacturing.

3. Flashpoint assesses with moderate confidence that the ransomware is a variant of “REvil” ransomware and is based on its code.
4. DarkSide ransom payment demands range widely from $200,000 to $2,000,000, depending on the size and possibly other associated characteristics of the targeted organization.
5. When DarkSide victims refuse to pay the ransom demand, the ransomware group follows through on its threat, releasing victims’ sensitive data on publicly visible websites

What Is DarkSide Ransomware and Where Did It Come From?

The first report of a DarkSide ransomware attack came on August 10, 2020, with even early reports finding the ransomware to be highly customized with lucrative, million-dollar payouts from large corporate targets in finance, technology, and manufacturing industries. On that

same day, August 10th, the DarkSide actors launched their associated DarkSide website on Tor.

DarkSide uses Salsa20 and RSA-1024 to encrypt victims' files on Windows OS. It also allegedly comes in a version for Linux, although no samples are publicly available. The Linux version is said to be written in C++ and to use ChaCha20 and RSA-4096 for file encryption.

Various industry reports suggest that the ransomware not only encrypts victims data, but also propagates laterally on the network and steals sensitive information from affected machines. If victims refuse to pay, their data is posted publicly on the DarkSide Tor website and offered for download. Although there is no publicly available information about the infection vector, because the attacks are highly specific, compromised Remote Desktop Protocol (RDP) servers and custom phishing attacks are two highly plausible options.

Learn more about **Flashpoint Threat Response and Readiness** offerings and how Flashpoint prepares and actively supports organizations to respond to any ransomware attack.

Operators Quickly Expand DarkSide to Ransomware-as-a-Service (RaaS) Model

The first DarkSide ransomware attacks were all owner-operated, but after a few successful months, the owners began to expand their operations. On November 10, DarkSide operators announced on Russian-language forums XSS and Exploit the formation of their new DarkSide affiliate program providing partners with a modified form of their DarkSide ransomware to make use in their own operations.

It's worth noting that DarkSide actors have pledged in the past to not attack organizations in the medical, education, nonprofit, or government sectors. At one point, they also advertised that they donate a portion of their profit to charities. However, neither claim has been verified and should be met with a heightened degree of scrutiny; these DarkSide operators would be far from the first cybercriminals to make such claims and not follow through.

DarkSide Operators Likely Former "REvil" Affiliates

Flashpoint assesses with moderate confidence that the threat actors behind DarkSide ransomware are of Russian origin and are likely former affiliates of the "REvil" RaaS group. Several facts support this attribution:

- Spelling mistakes in the ransom note and grammatical constructs of the sentences suggest that the writers are not native English speakers.
- The malware checks the default language of the system to avoid infecting systems based in the countries of the former Soviet Union.

- The design of the ransom note, wallpaper, file encryption extension and details, and inner workings bear similarities to “REvil” ransomware, which is of Russian origin and has an extensive affiliate program. This shows the evolution path of this ransomware and ties it to other Russian-origin ransomware families.
- The affiliate program is offered on Russian-language forums XSS and Exploit.

Prepare for Ransomware with Flashpoint

Request a demo today and see firsthand how Flashpoint’s Threat Response and Readiness offerings ensure your entire team is prepped and able to respond to any ransomware attack. And when equipped with Flashpoint Intelligence Platform and our dedicated, prebuilt ransomware dashboards, you move a step ahead of ransomware attacks and the cybercriminal groups who use them.