DarkSide ransomware explained: How it works and who is behind it

By by Lucian Constantin CSO Senior Writer

Published: 2021-05-13 · Archived: 2026-04-05 18:27:12 UTC

The Colonial Pipeline attack thrust the DarkSide ransomware into the spotlight. This is what's known about the threat actors and how they operate.

DarkSide is a ransomware threat that has been in operation since at least August 2020 and was used in a cyberattack against Georgia-based Colonial Pipeline, leading to a major fuel supply disruption along the East Coast of the US. The malware is offered as a service to different cybercriminals through an affiliate program and, like other prolific ransomware threats, employs double extortion that combines file encryption with data theft and is deployed on compromised networks using manual hacking techniques.

In a recent report, researchers from threat intelligence firm Flashpoint said they believe "that the threat actors behind DarkSide ransomware are of Russian origin and are likely former affiliates of the REvil RaaS [ransomware-as-a-service] group."

A PR savvy group that claims moral principles

Researchers believe that the DarkSide creators initially ran all their targeted attack campaigns themselves, but after a few months they started making their ransomware available to other groups and marketed it on Russian-language underground forums. In their launch announcement they claimed to have already made millions of dollars in profits by partnering with other well-known cryptolockers (ransomware programs) in the past.

The group encourages news reporters to register on its website to receive advance information about breaches and non-public information and promises fast 24-hour replies to any media questions. They also invited data decryption companies to partner with them to help victims that don't have large IT departments decrypt their data after they pay.

The group also claims that it doesn't attack medical facilities, COVID vaccine research and distribution companies, funeral services, non-profit organizations, educational institutions, or government organizations because of its "principles."

Following the attack on Colonial Pipeline, the group issued a statement saying that going forward it will review victims that its affiliates compromised and whose data they intend to encrypt:

> "We are apolitical, we do not participate in geopolitics, do not need to tie us with a defined government and look for other our motives. Our goal is to make money, and not creating problems for society. From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future." [sic]

In October, the group also claimed that it is donating a portion of the extorted funds to charities and posted proof of two $10,000 donations.

Based on these communications, it's clear that the group wants and knows how to attract attention to itself and its activities, likely in an attempt to gain more affiliates, but researchers warn that their claims have not been proven and are actually deceptive. For example, if it's proven that charities received money obtained from illegal activities, those funds will be seized or returned. Even though the group said it doesn't attack educational institutions, it did attack one company that processed data from schools. When the company declined to pay the ransom, the attackers emailed the impacted schools to put pressure on the victim organization by warning them that the personal information of children and school employees might be leaked.

The claims about donations and not targeting certain types of organizations have not 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," Flashpoint researchers said.

How DarkSide compromises networks

DarkSide and its affiliates follow the same human-operated model of ransomware deployment as other prolific ransomware groups that have plagued businesses in recent years. This means attackers gain access to networks through a variety of methods, including stolen credentials followed by manual hacking techniques and using a variety of system administration or penetration testing tools to perform lateral movement.

The goal is to map the network to identify critical servers, escalate privileges, obtain domain administrative credentials, disable and delete backups, exfiltrate sensitive data and only when the terrain is all set, deploy the ransomware to as many systems as possible in one go. This careful and methodical approach is much more effective and hard to defend against than ransomware programs that propagate automatically through networks by using built-in routines that might fail and trip detection mechanisms.

"With respect to DarkSide's affiliates, there is overlap in how the ransomware was delivered, including affiliates gaining initial network access by exploiting vulnerable software like Citrix, Remote Desktop Web (RDWeb), or remote desktop protocol (RDP), performing lateral movement, and exfiltrating sensitive data before ultimately deploying ransomware," researchers from security firm Intel471 said in a report.

Every DarkSide affiliate could employ different tactics to gain the initial foothold. These are similar to the techniques used by other ransomware groups: buying stolen credentials from underground markets, performing brute-force password guessing or credential stuffing attacks, buying access to machines that are already infected with botnet malware such as Dridex, TrickBot or Zloader, or sending emails with malicious attachments that deploy some type of lightweight malware loader.

One DarkSide actor observed by Intel471 sourced initial access credentials from a network access broker then used the Mega.nz file-sharing service to exfiltrate data, used a PowerShell backdoor to persist in the network and deployed the KPOT information-stealing malware alongside the DarkSide ransomware. Another affiliate openly recruited "penetration testers" to use VPNs and the already-obtained network access to perform lateral movement and deploy the ransomware.

Third-party and open-source tools commonly used for lateral movement activities include PowerShell scripts, the Cobalt Strike and Metasploit penetration testing frameworks, the Mimikatz password dumping tool, and the BloodHound visualization tool that can help attackers discover obscure attack paths and relationships to exploit in Active Directory environments. Tools that are already part of Windows like Certutil.exe and Bitsadmin.exe are also abused.

This living-off-the-land approach that includes the use of valid credentials and tools that are also employed by system admins and network defenders makes these human-operated ransomware attacks hard to detect without advanced network monitoring.

How the DarkSide ransomware routine works

The DarkSide ransomware itself uses Salsa20 and RSA-1024 to encrypt victims' files and reportedly also has a Linux version. When deployed on Windows, the malware first checks the system's language setting and if it's the language of a country located in the former Soviet Bloc or its sphere of influence, it avoids encrypting the data. This is typical of malware created by groups who are based in the region and who want to avoid attracting the attention of local authorities by not hitting local organizations.

According to researchers from Cybereason, the malware then stops services that contain the following terms in their names: vss, sql, svc, memtas, mepocs, sophos, veeam or backup. These are processes related to backup operations, like the Windows Volume Shadow Copy Service (VSS) or security products. It then proceeds to enumerate running processes and terminates them so it can unlock the files they were accessing to encrypt them. It also uses a PowerShell command to delete all volume shadow copies already created and which could be used to restore files.

The DarkSide ransomware creates a unique ID for every victim and adds it to the file extension for the encrypted files. The ransom amounts can vary significantly from a few hundred thousand dollars to millions depending on what the attackers determined is the victim's size and its annual income.

"In March 2021, the developer rolled out a number of new features in an effort to attract new affiliates," researchers from Intel471 said. "These included versions for targeting Microsoft Windows and Linux based systems, enhanced encryption settings, a full-fledged and integrated feature built directly into the management panel that enabled affiliates to arrange calls meant to pressure victims into paying ransoms, and a way to launch a distributed denial-of-service (DDoS)."
