Who is DarkSide – The Group Behind the Colonial Pipeline Breach?

Published: 2021-05-19 · Archived: 2026-04-05 19:52:41 UTC

Key Findings

- The “DarkSide” ransomware group has made the news in 2021 due to its high-value targets such as the Colonial Pipeline and its high ransom amounts. It is considered to be one of the most prolific ransomware groups in the field. In August 2020, the DarkSide team launched its own public blog, “DarkSide Leaks”, to intimidate victims, boast about its attacks, and post stolen information from victims who did not pay the ransom.
- The group established criteria for whom it partners with (experienced Russian-speaking hackers) and who it allows partners to target (former Soviet states and certain industries are off-limits).
- DarkSide has recently reached widespread notoriety as the suspected culprit behind the Colonial Pipeline ransomware attack. While DarkSide’s blog is down as of this writing, it released a statement in which it claimed to be apolitical, uninterested in “creating problems for society”, and unaffiliated with any governments.
- The DarkSide ransomware group is notable for its professionalism, including its attention to its product, customer service, and “code of ethics”. This professionalism makes DarkSide a particularly dangerous and capable ransomware group, although the full fallout from a highly public attack on critical American infrastructure remains to be seen.

Analysis

Gemini Advisory has previously written a public report that describes the operations and tactics of ransomware teams. The “DarkSide” ransomware group recently reached widespread notoriety as the suspected culprit behind the Colonial Pipeline ransomware attack. This attack disrupted the largest pipeline for refined oil products in the United States and has led to ongoing gas shortages, with the pipeline’s systems beginning to restart on Wednesday, May 12. DarkSide is also known for high ransom demands and is considered to be one of the most prolific ransomware groups in the field. According to multiple sources, the group first appeared in August 2020 and remains active as of this writing. The group also provides Ransomware-as-a-Service (RaaS), which is an essential malware rental service in which other cybercriminals can rent out DarkSide’s malware to conduct ransomware attacks.

Public Blog

In August 2020, the DarkSide team launched its own public blog, “DarkSide Leaks” on the Tor network. Like other teams, DarkSide uses its blog to intimidate victims, boast about its attacks, and post victims’ stolen

information if they did not pay the ransom.

Image 1: DarkSide Leaks home page.

Dark Web Activity

In November 2020, the actor “darksupp” created threads on two top-tier dark web forums in which they announced the launch of DarkSide’s partner program. This program is effectively RaaS; partners rent DarkSide’s ransomware to attack victims and DarkSide offers its partners 75% to 90% of the ransom money. In March 2021, the same actor created a new thread announcing the launch of DarkSide Ransomware v.2.0.

darksupp appears to be the public face of the organization and frequently publishes up-to-date information about the team and ransomware updates. As of this writing, darksupp’s threads advertising DarkSide’s RaaS still remain on two dark web forums. In addition, darksupp made a deposit of 23 Bitcoin (~$1.3 million USD as of this writing) on one of these forums to signal that the group is serious and trustworthy. The security deposit is intended to remedy issues arising with its partners by allowing the forum administrators to act as mediators and an escrow service.

One of darksupp’s updates referenced a new DarkSide policy. If a victim company does not contact DarkSide to pay its ransom, the criminal group offers to launch distributed denial-of-service (DDoS) attacks against the company to put even more pressure on it to contact DarkSide. While other ransomware groups may use similar tactics, they often do not advertise their use of DDoS, so this disclosure sets DarkSide apart.

Rules of Engagement

In the March 2021 forum post, darksupp outlined the group’s criteria for whom it partners with and who it allows partners to target. darksupp specified that DarkSide exclusively seeks experienced, Russian-speaking partners and does not wish to work with English-speaking individuals or individuals linked to security services or cybersecurity companies. Additionally, the group stated its service is aimed at targeting only large corporations and listed the criteria for the types of entities that partners should not target. The criteria include:

- Hospitals, nursing homes, hospices, and medical organizations producing and distributing COVID-19 vaccines
- Organizations and businesses providing funeral services
- Government and public sector bodies
- Non-governmental organizations

DarkSide also stated that partners should not target any entity in the former Soviet Union (FSU), which is common for threat actors located in the FSU. The group stipulated that partners should not conduct any activity that could harm the reputation of DarkSide. While DarkSide’s blog is down as of this writing, it released a statement after news of the Colonial Pipeline hack broke in which it claimed to be apolitical, uninterested in “creating problems for society”, and unaffiliated with any governments. The RaaS model makes it difficult for

groups like DarkSide to predict their cybercriminal clients' ransomware targets, and this statement indicates DarkSide's aversion to the attention of such a high-profile attack. It remains unclear if the group will release the database of its latest victim or if it will attempt to backtrack, given the disturbingly high-profile nature of its recent attack.

Additionally, the actor has indicated that its ransomware can work with Windows and Linux OS and has a convenient admin panel with various functions, including managing the distribution and withdrawal of funds via BTC or XMR (Bitcoin or Monero), generating builds and decryptors, online chat, and more.


Darksupp advertising private cryptolocker

Image 2: "darksupp" advertising private cryptolocker.

Attack Vectors

Since the DarkSide ransomware is advertised as a RaaS, actors renting the ransomware could use various attack vectors, ranging from phishing campaigns to exploiting vulnerable internet-facing applications. After gaining access to a victim's internal network, DarkSide operators establish an RDP connection with its command-and-control server through port 443 (HTTPS), routing internet traffic through the Tor anonymous network. In addition, DarkSide uses one of Cobalt Strike's payload generation mechanisms called "Beacon" to establish a command-and-control mechanism as an additional backdoor on internal hosts.

To conduct reconnaissance on the internal network, run commands, dump processes, and steal credentials, attackers use tools such as Advanced IP Scanner, PSExec, Mimikatz, but are not limited to these alone.

With a complete understanding of the network and internal resources, the DarkSide ransomware operators inject a malicious ransomware executable into an existing system process via CMD commands, after which several preparatory procedures take place: detecting the presence of anti-forensics and anti-debugging mechanisms, removing Shadow Volume Copies and stopping system processes that can interfere with encryption. After that encryption is performed using the Salsa20 + RSA1024 for Windows OS and ChaCha20 + RSA4096 for Linux OS cryptographic algorithms by adding an 8-character extension to the encrypted files and leaving a ransom note titled "REDME.victimsID.text".

Extortion Tactics

DarkSide uses "double extortion" tactics, a method in which attackers first download the victim's database and then encrypt all of the data on the victim's network. The team uses the DarkSide Leaks blog to intimidate companies that refused to pay the ransom by threatening to make the database publicly available. According to the message generated by the ransomware on victim computers, DarkSide's data leaks site creates a unique link for each victim along with a unique key. Upon entering the key in the required field, the ransom amount and BTC/XMR wallets appear for the victims, who also have an online chat feature for support and possible negotiations.

In a creative nascent scheme, DarkSide offered to notify stock market investors before leaking confidential stolen data. These investors could then short the target company's stock in anticipation of a drop in its share price following publicity about the breach and leaked data. While the risks to participating investors running afoul of the Securities and Exchange Commission (SEC) would be high and the rewards likely low, this scheme demonstrates DarkSide's innovative nature. It also demonstrates DarkSide's aggressive exploitation of the same target, first encrypting a victim's data, then threatening to publicly release that data, then deploying DDoS attacks, and finally attempting to exploit the victim's stock prices.

Victims

As of this writing, the home page of DarkSide Leaks contains news about more than 80 entities that have become victims of the ransomware, although the true number is likely greater. Below are some of the most notable victims referenced on DarkSide Leaks:

- August 2020 – Brookfield Asset Management Inc.
- October 2020 – Mestek
- November 2020 – Automation Personnel Services, Forbes Energy Services
- January 2021 – Aaronson Rappaport Feinstein & Deutsch, LLP
- February 2021 – Oak Valley Community Bank, Centrais Eletricas Brasileiras, Companhia Paranaense de Energia
- March 2021 – Indonesia Eximbank
- May 2021 – Colonial Pipeline

The Colonial Pipeline is DarkSide's most notable target, given the highly public nature of the hack's damages and the effect on critical US infrastructure. While many hacking groups (including DarkSide) have been wary of attracting US law enforcement's attention in attacks as brazen as this one, the US response to this attack will likely signal the severity of the consequences to hacking groups across the dark web. This may serve as either a deterrent or an incentive to attempting similar attacks of this scale.

Conclusion

The DarkSide ransomware group is notable for its professionalism. While many other RaaS groups exist, DarkSide stands out for its attention to its product, including consistent modifications and quality upgrades. Its customer service feature for hacking victims is intended to allow ransom transactions to resolve as smoothly as possible, which is a far cry from the gloating and insulting ransom messages in the early days of ransomware. DarkSide's "code of ethics" designating certain industries off-limits also demonstrates closer attention to the group's clients than many of its peer gangs. Its ability to cover its tracks through sophisticated tactics, techniques, and procedures (TTPs) has allowed it to maintain a relatively opaque presence until recently, when the Colonial Pipeline attack brought it into the news. This professionalism makes DarkSide a particularly dangerous and capable ransomware group, although the full fallout from a highly public attack on critical American infrastructure remains to be seen.

Update 05/14/2021

As of May 14, several credible underground sources have claimed that the DarkSide ransomware group no longer has a presence on the dark web. It purportedly no longer has access to its servers and control panel. Additionally, one of the top-tier forums on which DarkSide operated has imposed sanctions against all ransomware groups, banning them from the forum entirely. The other top-tier forum deleted the account darksupp and two threads about its ransomware. Two unrelated ransomware groups, “Avaddon” and “REvil”, have additionally included new conditions for their RaaS clients that forbid them from targeting certain entities. These developments suggest that the consequences for hitting such a high-profile target may be uncharacteristically severe.

Gemini Advisory Mission Statement

Gemini Advisory provides actionable fraud intelligence to the largest financial organizations in an effort to mitigate ever-growing cyber risks. Our proprietary software utilizes asymmetrical solutions in order to help identify and isolate assets targeted by fraudsters and online criminals in real-time.
