

Meet DarkSide and Their Ransomware – SentinelOne Customers Protected

 sentinelone.com/blog/meet-darkside-and-their-ransomware-sentinelone-customers-protected/

May 10, 2021



The recent campaign targeting Colonial Pipeline in the United States is a sobering example of the extent to which cybersecurity – specifically ransomware – threatens everyday life. There is a lot more to this than encrypted or stolen data. It's hard to understand the economic reverberations of a disruptive attack on critical infrastructure, whether for financial gain or otherwise. With the pipeline being proactively shut down as of Sunday, May 9th, there are concerns around how this outage will affect ongoing fuel prices and for how long. How the coming weeks and months play out may serve as a template for predicting impact and risk associated with similar attacks that will inevitably follow.

SentinelOne detects and protects against DarkSide ransomware. No action is required for our customers.

SentinelOne Protects from DarkSide Ransomware

[Watch Demo](#)

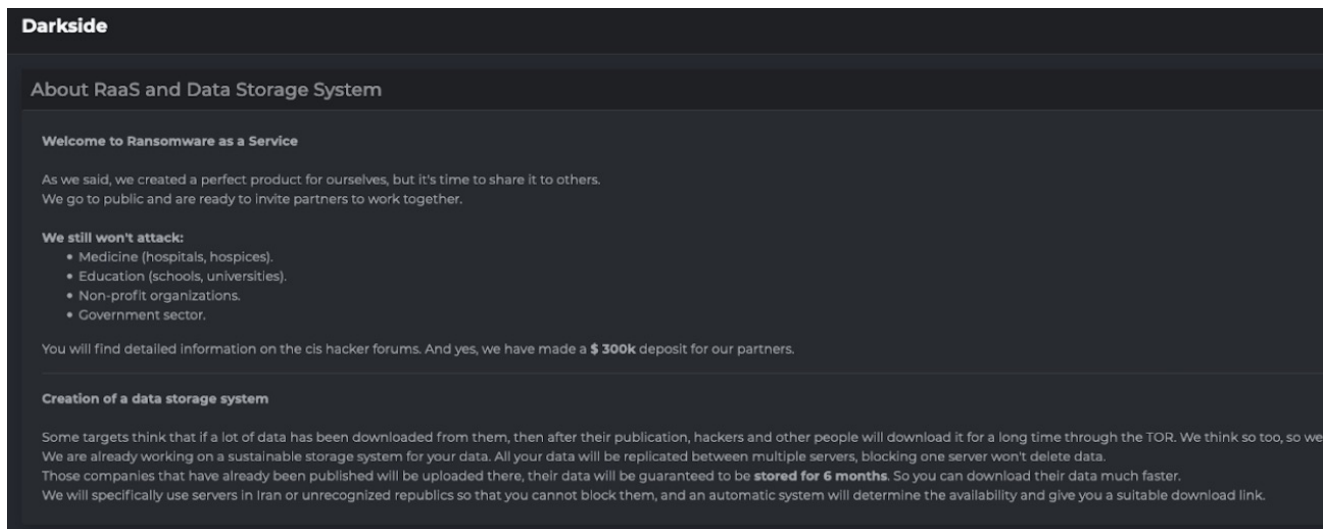
In this post, we discuss the evolution of the DarkSide malware and affiliate networks, including the evolution of their feature sets and recruitment areas.

Watch How SentinelOne Mitigates DarkSide Ransomware

Beyond Protection, it's important that your security tool can mitigate and rollback in the case of a Ransomware attack

Who is DarkSide?

The attack on Colonial Pipeline has been attributed to DarkSide, a relatively new ransomware family that emerged on the crimeware market in November 2020.



DarkSide claims not to attack Medical, Educational, Non-Profit, or Government sectors. DarkSide launched as a RaaS (Ransomware-as-a-Service) with the stated goal of only targeting 'large corporations.' They are primarily focused on recruiting Russian (CIS) affiliates, and are very skeptical of partnerships or interactions outside of that region. From the onset, DarkSide was focused on choosing the 'right' targets and identifying their most valuable data. This speaks to their efficiency and discernment when choosing where to focus their efforts. From their inception, DarkSide claimed they'd avoid attacking the medical, educational, non-profit, or government sectors.

Who are we looking for?

A limited number of stable and adequate partners who understand why you need to upload data, what backups are and how to delete them, Russian-speaking , with average payouts of **400k** .

Who are we NOT looking for?

- English speaking personalities.
- Doubtful personalities, employees of the secret service and analysts of information security companies.
- Those who install Dedicated servers and engage in activities different from the supply of networks.
- Any topics and suggestions different from this post.
- Those who want to learn pentesting and earn millions.
- Those who like to bet 100kk ransom for 3.5 servers.

About software?

We are ready to provide partners with:

- **Windows** [full ASM, salsa20 + rsa 1024, i / o, own implementation of salsa and rsa, fast / auto (improved space) / full, token impersonalization for working with balls, slave table, freeing busy files, changing file permissions, arp scanner, process termination, service termination, drag-and-drop and much more].
- **Linux** [C ++, chacha20 + rsa 4096, multithreading (including Hyper-threading, analog of i / o on windows), support for truncated OS assemblies (esxi 5.0+), fast / space, directory configuration and much more].
- **Admin panel** [full ajax, automatic acceptance of Bitcoin, Monero, generation of win / lin builds with indication of all parameters (processes, services, folders, extensions ...), bots reporting and detailed statistics on the company's performance, automatic distribution and withdrawal of funds, sub - accounts, online chat and many others].
- **Leak site** [hidden posts, phased publication of target data and many more functionality].
- **CDN system for data storage** [Receiving quotas, fast data loading, storage 6m from the moment of loading].

DarkSide affiliate recruitment post

At the time of launch, the features offered by DarkSide were fairly standard. They emphasized their speed of encryption and a wealth of options for dealing with anything that may inhibit the encryption process (i.e., security software). They also advertised a Linux variant with comparable features. Following in the footsteps of recently successful ransomware families like Maze and ClOp, DarkSide established a victim data leaks blog as further leverage to encourage ransom payouts.

The original DarkSide 1.0 Feature set was advertised as follows:

Windows [
full ASM, salsa20 + rsa 1024,
i / o, own implementation of salsa and rsa,
fast / auto (improved space) / full,
token impersonalization for working with balls,
slave table, freeing busy files,
changing file permissions,
arp scanner,
process termination,
service termination,
drag-and-drop and much more].

Linux [
C ++, chacha20 + rsa 4096,
multithreading (including Hyper-threading, analog of i / o on windows),
support for truncated OS assemblies (esxi 5.0+),
fast / space,
directory configuration and much more].

Admin panel [
full ajax,
automatic acceptance of Bitcoin, Monero,
generation of win / lin builds with indication of all parameters (processes,
services, folders, extensions ...),
bots reporting and detailed statistics on the company's performance,
automatic distribution and withdrawal of funds,
sub -accounts,
online chat and many others].

Leak site [
hidden posts,
phased publication of target data and many more functionality].


CDN system for data storage [
Receiving quotas,
fast data loading,
storage 6m from the moment of loading].

A Well-Organized Affiliate Network

Hopeful affiliates are subject to DarkSide's rigorous vetting process, which examines the candidate's 'work history,' areas of expertise, and past profits among other things. To get started, affiliates were required to deposit 20 BTC (at the time, that amounted to around \$300,000 USD).

darksupp Posted 56 minutes ago

byte



Seller

3 posts
Joined
11/03/20 (ID: 110360)
Activity
virology / malware

We launched a CDN system. Now loading and storing target data has become even more convenient. Next in line:

- The second version of windows locker.
- Ability to generate a locker in the form of DLL.
- Ability to generate a locker in the form of a PS1 file (ps1 morfer + dll inject).

+ Quote

DarkSide announces improved CDN

Over the following months, DarkSide continued to improve its services, while also expanding its affiliate network. By late November 2020, DarkSide launched a more advanced Content Delivery Network (CDN) that allowed their operators to more efficiently store and distribute stolen victim data. Many of their high-value targets found themselves listed on the victim blog, including a number of financial, accounting, and legal firms, as well as technology companies.

Initial access can take many forms depending on the affiliate involved, their needs, and timeline. A majority of the campaigns observed were initiated only after the enterprise had been thoroughly scouted via Cobalt Strike beacon infections. After the initial reconnaissance phase, the operators would deploy the DarkSide ransomware wherever it would cause the greatest disruption.

DarkSide Decryption Tool – Is it Working?

In January 2021, [Bitdefender](#) released a DarkSide decryption tool. This tool was also posted to the NoMoreRansom project website. The tool had a reportedly high success rate.

* - According to comparative tests among other projects that are presented on the forum:

- **DarkSide v.1.0** , jap: **ASM** , weight: **59.5 KB** , encryption time: **04:20** .
- **DarkSide v.2.1** , jap: **ASM** , weight: **53 KB** , encryption time: **02:04** (current version, which is in deployment).
- **Competitor** , jap: **S** , weight: **114 KB** , encryption time: **02:48** .
- **Competitor** , jap: **C** , weight: **147 KB** , encryption time: **04:49** .

We will not publish the names of competitors, the testing was carried out in equal conditions, without odds, there are proofs.

DarkSide 2.0 performance comparisons

By March, the group announced the launch of the new and improved DarkSide 2.0. The new iteration included many improvements for both their Windows and Linux variants and is no longer subject to the decryption tool. DarkSide 2.0 reportedly encrypts data on disk twice as fast as the original.

Other updated features include:

- Expanded multi-processor support (parallel/simultaneous encryption across volumes)

- EXE and DLL-based payloads
- Updated SALSA20+RSA1024 implementation with “proprietary acceleration”
- New operating modes (Fast / Full / Auto)
- 19 total build settings
- Active account impersonation
- Active Directory support (discovery and traversal)
- New CMD-line parameter support

On the Linux side, DarkSide 2.0 offers the following updates:

- Updated multithreading support
- Updated CHACHA20 + RSA 4096 implementation
- 2 new operating modes (Fast / Space)
- 14 Total build settings
- Support for all major ESXi versions
- NAS support (Synology, OMV)

Along with this expanded feature set, SentinelLabs researchers have seen a shift in the deployment of the DarkSide ransomware, from standard packers like VMProtect and UPX to a custom packer internally referred to as ‘encryptor2.’

A Battle for Territory

With the release of DarkSide 2.0, the group has continued to increase its footprint in the Ransomware landscape. Along with their territorial expansion throughout 2021, DarkSide also increased their ‘pressure campaigns’ on victims to include DDoS attacks along with the threat of data leakage. They are able to invoke L3/L7 DDoS attacks if their victims choose to resist ‘cooperation’.

More recently, DarkSide operators have been attempting to attract more expertise around assessing data and network value, along with seeking others to provide existing access or newer methods of initial access. These efforts are meant to make operations more streamlined and increase efficiency.

Next updates:

- Automatic test decrypts. From that moment on, the whole process from cryptographing the target to the withdrawal of funds is automated and does not require the participation of a support.
- DDOS targets (L3, L7) are available, at our expense, we hold for a long time until the target goes online.

Now about the important thing, we have grown enough both in terms of the client base and in relation to other projects (based on the analysis of public information) and are ready to expand our and partner teams in two directions:

- **Pentesting networks.**
We are looking for one person or a team, integrate into the work environment and provide employment. A high percentage, the ability to make networks that cannot be realized alone. New experience and stable income.
- **Supply of networks.**
Working both with us and with partners, before issuing networks, we will provide statistics of partner payments (as agreed). When delivering on our product and paying the ransom, we will guarantee an honest distribution of funds. Dashboard for monitoring the results for your target. We only accept networks where you run our payload.

In the two directions above, you need to write in the LAN with the topic "Penetration Testing" or "Networks" and pass an interview.

New methods and talent areas

The Colonial Pipeline attack is only the latest in a slew of increasingly daring ransomware attacks. The absolute best defense against a severe ransomware attack (and the nightmare that follows) is preparation and prevention. Technology is a huge part of that, but one must not discount user hygiene and education. It is vital to keep end users up to date on what threats are out there and how to spot them. Vigilant users, along with robust preventative controls are key. Business continuity planning and disaster recovery drills are not fun, but they are critical and necessary to ensure readiness and resilience against these threats.

The SentinelOne platform is fully capable of preventing and detecting the malware and artifacts associated with DarkSide ransomware. We hope that the pipeline starts flowing again soon; our society depends on it to live.

Indicators of Compromise

SHA256

156335b95ba216456f1ac0894b7b9d6ad95404ac7df447940f21646ca0090673
4d9432e8a0ceb64c34b13d550251b8d9478ca784e50105dc0d729490fb861d1a
61ca175c2f04cb5279f8507e69385577cf04e4e896a01d0b5357746a241c7846
bfb31c96f9e6285f5bb60433f2e45898b8a7183a2591157dc1d766be16c29893
a11cc5051e3a88428db495f6d8e4b6381a1cb3fa5946a525ef5c00bfc44e210
2dcac9f48c3989619e0abd200beaae901852f751c239006886ac3ec56d89e3ef
243dff06fc80a049f4fb37292f8b8def0fce29768f345c88ee10699e22b0ae60
12ee27f56ec8a2a3eb2fe69179be3f7a7193ce2b92963ad33356ed299f7ed975
9cee5522a7ca2bfc7cd3d9daba23e9a30deb6205f56c12045839075f7627297
5860f2415aa9a30c045099e3071f099313f653ae1806d6bcdb5f47d5da96c6d7
78782fd324bc98a57274bd3fff8f756217c011484ebf6b614060115a699ee134
dc4b8dff72ff08ec4daa8db4c096a350a9a1bf5434ba7796ab10ec1322ac38c
8cfd28911878af048fb96b6cc0b9da770542576d5c2b20b193c3cfc4bde4d3bc
4edb883d1ac97824ee42d9f92917cc84b52995abcd17b2852a7e3d5bb567ffbe
e9417cb1baec2826e3f5a6f64ade26c1374d74d8aa41bfabd29ea20ea5894b14
fb76b4a667c6d790c39fcc93a3aac8cd2a224f0eb9ece4ecfd7825f606c2a8b6

SHA1

2715340f82426f840cf7e460f53a36fc3aad52aa
86ca4973a98072c32db97c9433c16d405e4154ac
7944ae1d281bbeeb6f317e2ecec6b4c83e63a06
a4e2deb65f97f657b50e48707b883ce2b138e787
f90f83c3dbcbe9b5437316a67a8abe6a101ef4c3
483c894ee5786704019873b0fc99080fdf1a0976
7ae73b5e1622049380c9b615ce3b7f636665584b
2fc8514367d4799d90311b1b1f277b3fca5ca731
d1dfe82775c1d698dd7861d6dfa1352a74551d35
d3495ac3b708caeceffab59949dbf8a9fa24ccef
7a29a8f5e14da1ce40365849eb59487dbb389d08
1f90eb879580faef3c37e10d0a0345465eebd4ee
88fc623483f7ffe57f986ed10789e6723083fcd8
996567f5e84b7666ff3182699da0de894e7ea662
21145fd2cc8767878edbd7d1900c4c4f926a6d5b
076d0d8d07368ef680aeb0c08f7f2e624c46cbc5

MITRE ATT&CK

[T1112](#) Modify Registry

[T1012](#) Query Registry

[T1082](#) System Information Discovery

[T1120](#) Peripheral Device Discovery

[T1005](#) Data from Local System

[T1486](#) Data Encrypted for Impact

[T1543.003](#) Create or Modify System Process: Windows Service

T1490 Inhibit System Recovery

T1553.004 Subvert Trust Controls: Install Root Certificate

T1078 Valid Accounts