

## DarkSide ransomware gang returns as new BlackMatter operation

By Lawrence Abrams

Published: 2021-07-31 · Archived: 2026-04-05 13:39:22 UTC



Encryption algorithms found in a decryptor show that the notorious DarkSide ransomware gang has rebranded as a new BlackMatter ransomware operation and is actively performing attacks on corporate entities.

After conducting an [attack on Colonial Pipeline](#), the US's largest fuel pipeline, and causing fuel shortages in the southeast of the USA, the DarkSide ransomware group faced [increased scrutiny](#) by international law enforcement and the US government.

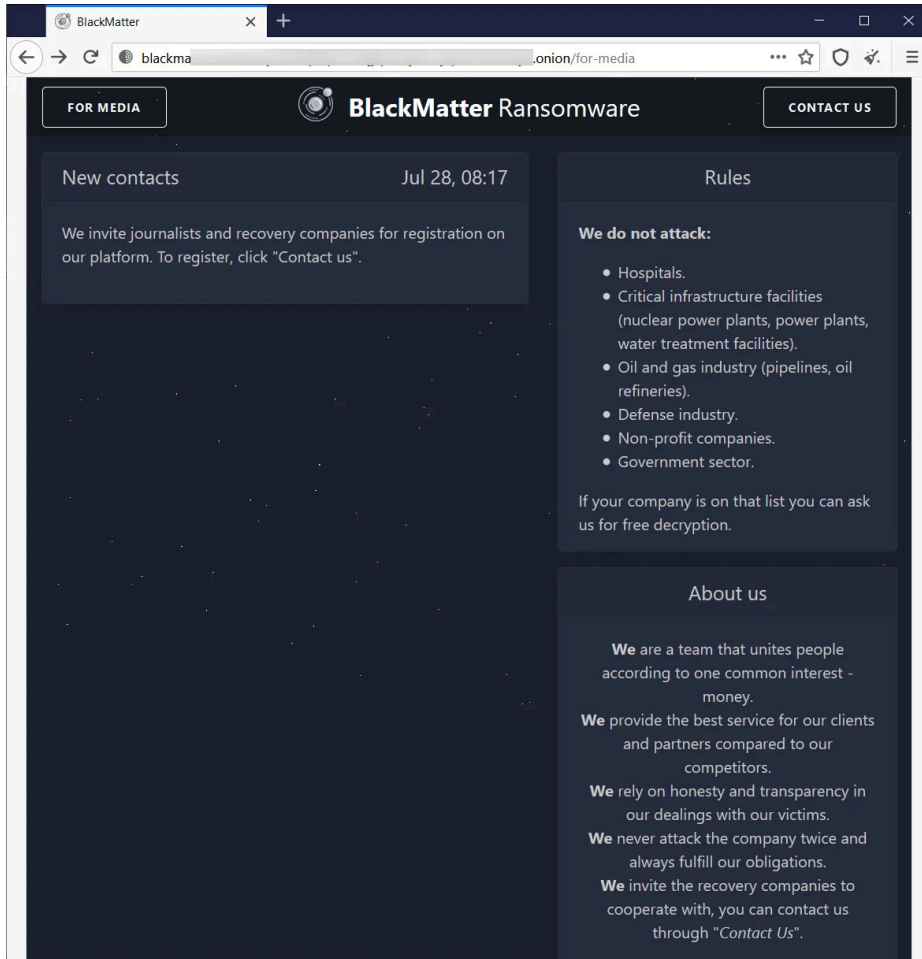
In May, the [DarkSide ransomware operation suddenly shut down](#) after losing access to their servers and cryptocurrency was seized by an unknown third-party.



Visit Advertiser website [GO TO PAGE](#)

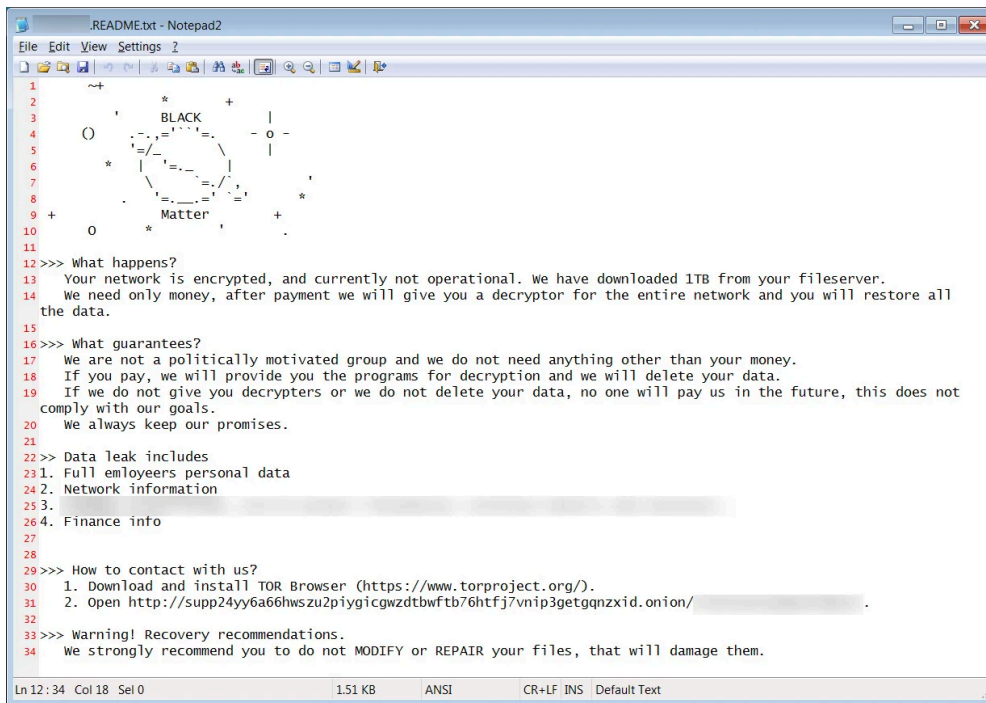
It was later learned that the [FBI recovered 63.7 Bitcoins](#) of the approximately 75 Bitcoin (\$4 million) ransom payment made by Colonial Pipeline.

This week, a [new ransomware operation known as BlackMatter emerged](#) that is actively attacking victims and purchasing network access from other threat actors to launch new attacks.



**BlackMatter data leak site**

BleepingComputer is aware of multiple victims targeted by BlackMatter with ransom demands ranging from \$3 to \$4 million. One victim has already paid a \$4 million ransom to BlackMatter this week to delete stolen data and receive both a Windows and Linux ESXi decryptor.



### BlackMatter ransom note

## BlackMatter's encryption routines match DarkSide

While researching the new ransomware group, BleepingComputer found a decryptor from a BlackMatter victim and shared it with Emissoft CTO and ransomware expert [Fabian Wosar](#).

After analyzing the decryptor, Wosar confirmed that the new BlackMatter group is using the same unique encryption methods that DarkSide had used in their attacks.

Wosar told BleepingComputer that the encryption routines used by BlackMatter are pretty much the same, including a custom Salsa20 matrix unique to DarkSide.

When encrypting data using the [Salsa20 encryption algorithm](#), a developer provides an initial matrix consisting of sixteen 32-bit words.

### Initial state of Salsa20

"expa"	Key	Key	Key
Key	"nd 3"	Nonce	Nonce
P.os.	P.os.	"2-by"	Key
Key	Key	Key	"te k"

### Salsa20 matrix

Source: Wikipedia

When encrypting files, Fabian told BleepingComputer that instead of using constant strings, a position, nonce, and key, for each encrypted file, DarkSide fills the words with random data.

This matrix is then encrypted with a public RSA key and stored in the footer of the encrypted file.

Fabian says this Salsa20 implementation was previously only used by DarkSide, and now BlackMatter.

BleepingComputer was also told that DarkSide used an RSA-1024 implementation unique to their encryptor, which BlackMatter also uses.

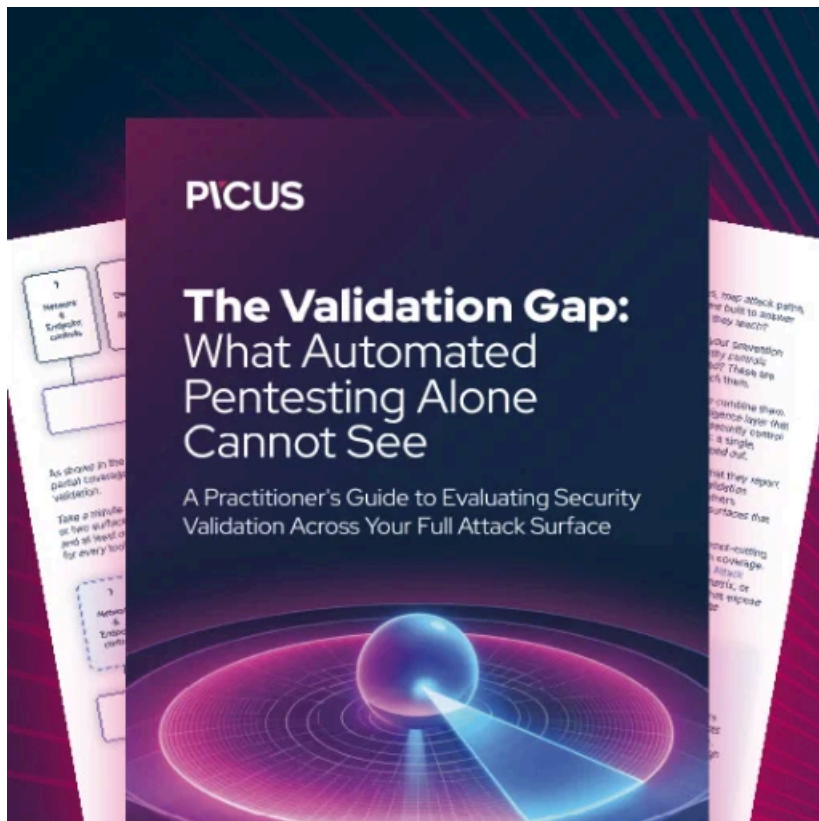
While there is not 100% proof that BlackMatter is a rebrand of the DarkSide operation, many similar characteristics make it hard to believe this is not the case.

When we take the same encryption algorithms, the similar language used on the BlackMatter sites, similar craving of media attention, and similar color themes for their TOR sites, it is highly likely that BlackMatter is the new DarkSide.

A rebrand from DarkSide also explains the reason the new BlackMatter group won't target the "Oil and Gas industry (pipelines, oil refineries)," which led to their previous downfall.

Unfortunately, this is a highly skilled group that targets multiple device architectures, including Windows, Linux, and ESXi servers.

Due to this, we will need to keep an eye on this new group as they will surely perform attacks on well-known targets in the future.



### **Automated Pentesting Covers Only 1 of 6 Surfaces.**

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---

Source: <https://www.bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/>