DarkSide ransomware gang returns as new BlackMatter operation

bleepingcomputer.com/news/security/darkside-ransomware-gang-returns-as-new-blackmatter-operation/

Lawrence Abrams

By
Lawrence Abrams

- July 31, 2021
- 03:13 PM
- 1

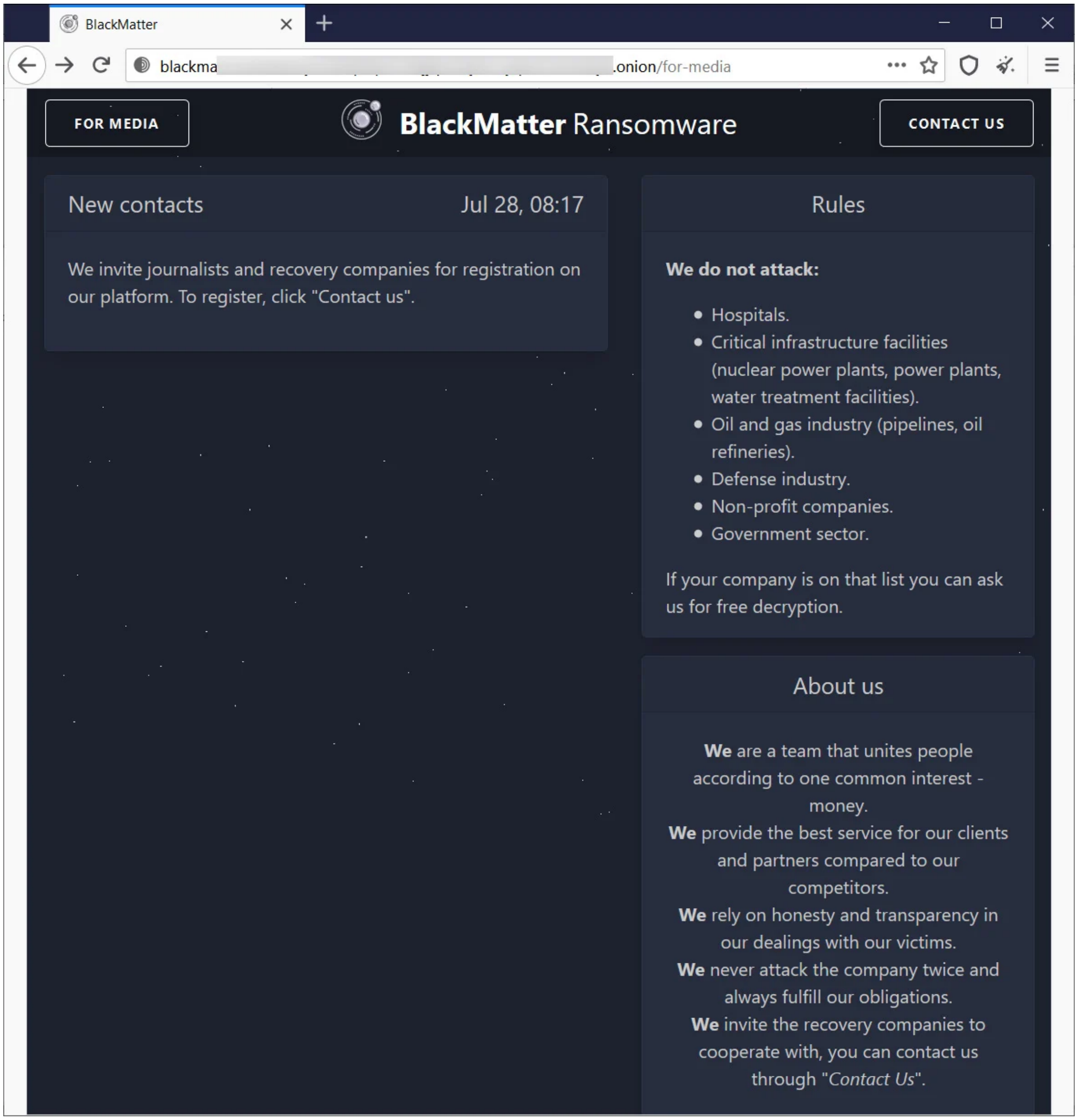
Encryption algorithms found in a decryptor show that the notorious DarkSide ransomware gang has rebranded as a new BlackMatter ransomware operation and is actively performing attacks on corporate entities.

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.

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.



New contacts Jul 28, 08:17

We invite journalists and recovery companies for registration on our platform. To register, click "Contact us".

Rules

We do not attack:

- Hospitals.
- Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).
- Oil and gas industry (pipelines, oil refineries).
- Defense industry.
- Non-profit companies.
- Government sector.

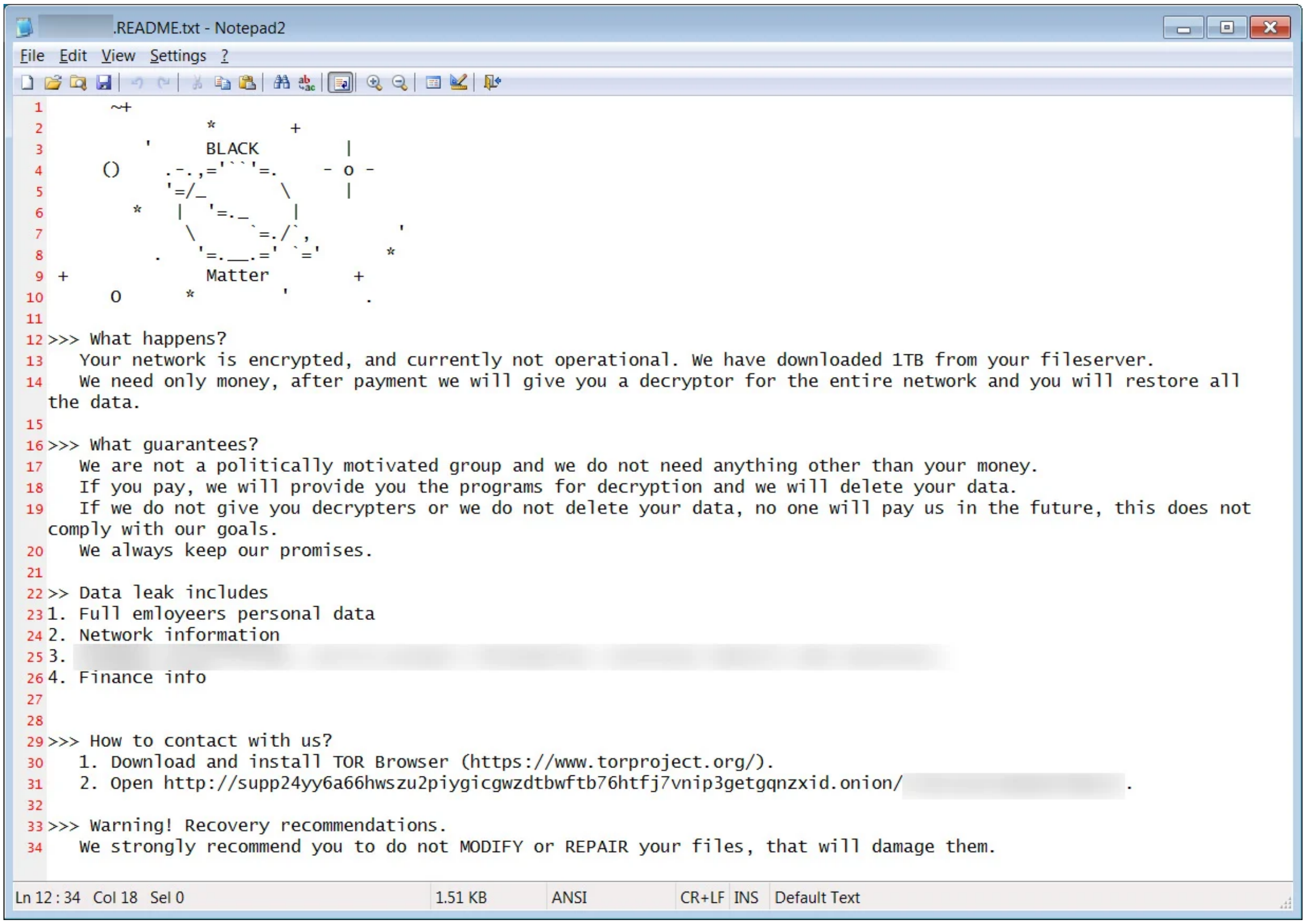
If your company is on that list you can ask us for free decryption.

About us

We are a team that unites people according to one common interest - money.
We provide the best service for our clients and partners compared to our competitors.
We rely on honesty and transparency in our dealings with our victims.
We never attack the company twice and always fulfill our obligations.
We invite the recovery companies to cooperate with, you can contact us through "*Contact Us*".

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.



```
      ~+
               *       +
         '     BLACK        |
     ()    .-.,='``'=.    - o -
           '=/_       \     |
        *   |  '=._    |
             \      `=./`,        '
          .   '=.__.=' `='       *
 +             Matter        +
      O      *        '       .

>>> What happens?
   Your network is encrypted, and currently not operational. We have downloaded 1TB from your fileserver.
   We need only money, after payment we will give you a decryptor for the entire network and you will restore all
the data.

>>> What guarantees?
   We are not a politically motivated group and we do not need anything other than your money.
   If you pay, we will provide you the programs for decryption and we will delete your data.
   If we do not give you decrypters or we do not delete your data, no one will pay us in the future, this does not
comply with our goals.
   We always keep our promises.

>> Data leak includes
1. Full emloyeers personal data
2. Network information
3. [redacted]
4. Finance info


>>> How to contact with us?
   1. Download and install TOR Browser (https://www.torproject.org/).
   2. Open http://supp24yy6a66hwszu2piygicgwzdtbwftb76htfj7vnip3getgqnzxid.onion/[redacted].

>>> Warning! Recovery recommendations.
   We strongly recommend you to do not MODIFY or REPAIR your files, that will damage them.
```

BlackMatter ransom note

BlackMatter's encryption routines match DarkSide

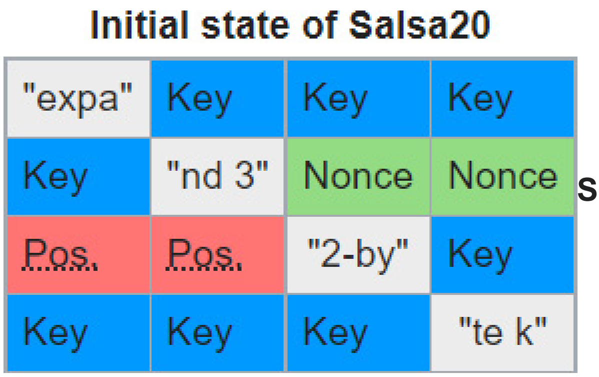
While researching the new ransomware group, BleepingComputer found a decryptor from a BlackMatter victim and shared it with Emisosft CTO and ransomware expert Fabian Wosar.

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.

> After looking into a leaked BlackMatter decryptor binary I am convinced that we are dealing with a Darkside rebrand here. Crypto routines are an exact copy pretty much for both their RSA and Salsa20 implementation including their usage of a custom matrix.
>
> — Fabian Wosar (@fwosar) July 31, 2021

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
Pos.	Pos.	"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 like 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.

Related Articles:

Conti ransomware shuts down operation, rebrands into smaller units

REvil ransomware returns: New malware sample confirms gang is back

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.