BlackMatter ransomware moves victims to LockBit after shutdown

bleepingcomputer.com/news/security/blackmatter-ransomware-moves-victims-to-lockbit-after-shutdown/

Lawrence Abrams

By
Lawrence Abrams

- November 3, 2021
- 12:47 PM
- 0

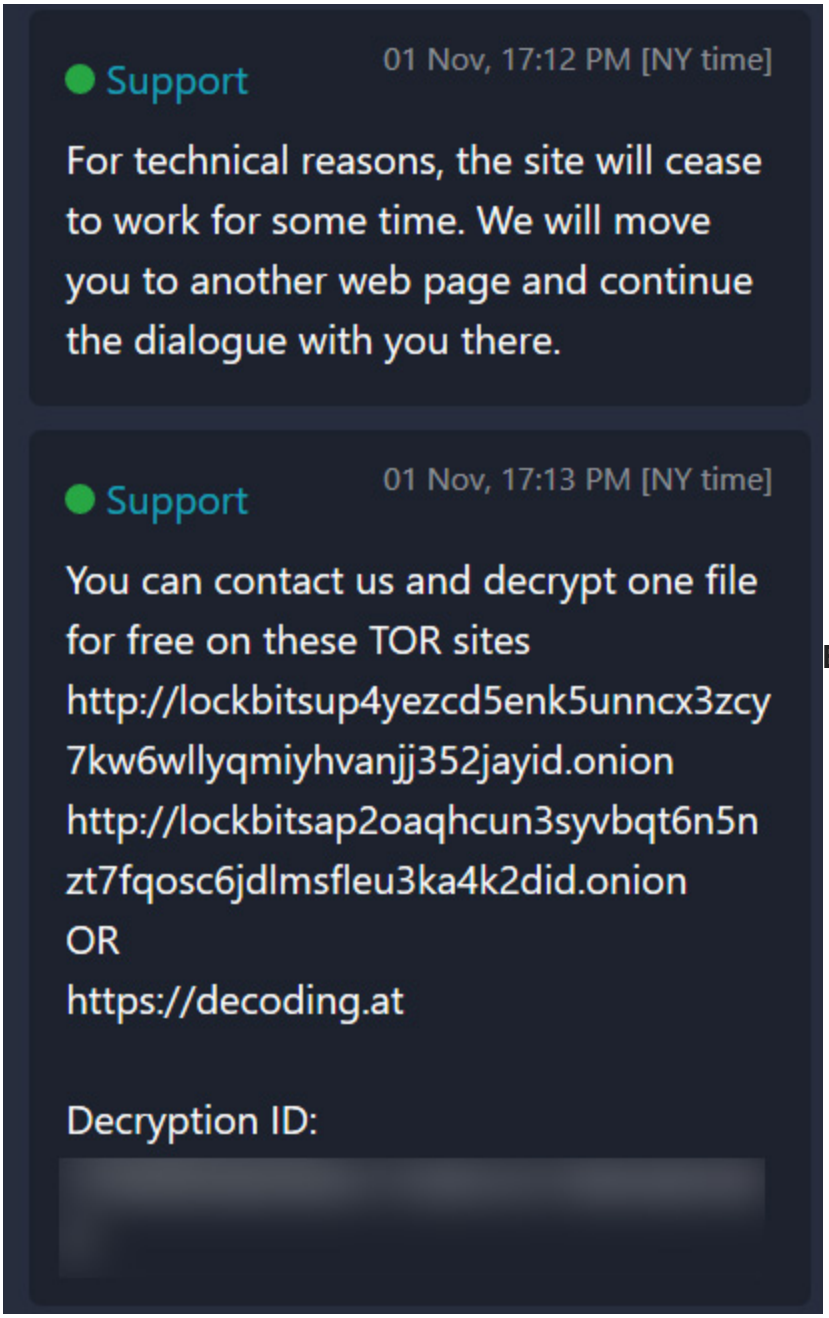
With the BlackMatter ransomware operation shutting down, existing affiliates are moving their victims to the competing LockBit ransomware site for continued extortion.

This morning, news broke that the BlackMatter ransomware gang is shutting down after members have gone missing and increased pressure by law enforcement.

As part of this shutdown, the ransomware operators are allowing affiliates to receive decryptors for existing negotiations so that they can continue extorting victims.

While BlackMatter's infrastructure is still live, BleepingCompuer has learned that affiliates are moving existing victims to the LockBit ransomware negotiation site.

In existing BlackMatter negotiation chats, affiliates are providing victims links to LockBit's Tor sites where new negotiation pages have been setup for them.



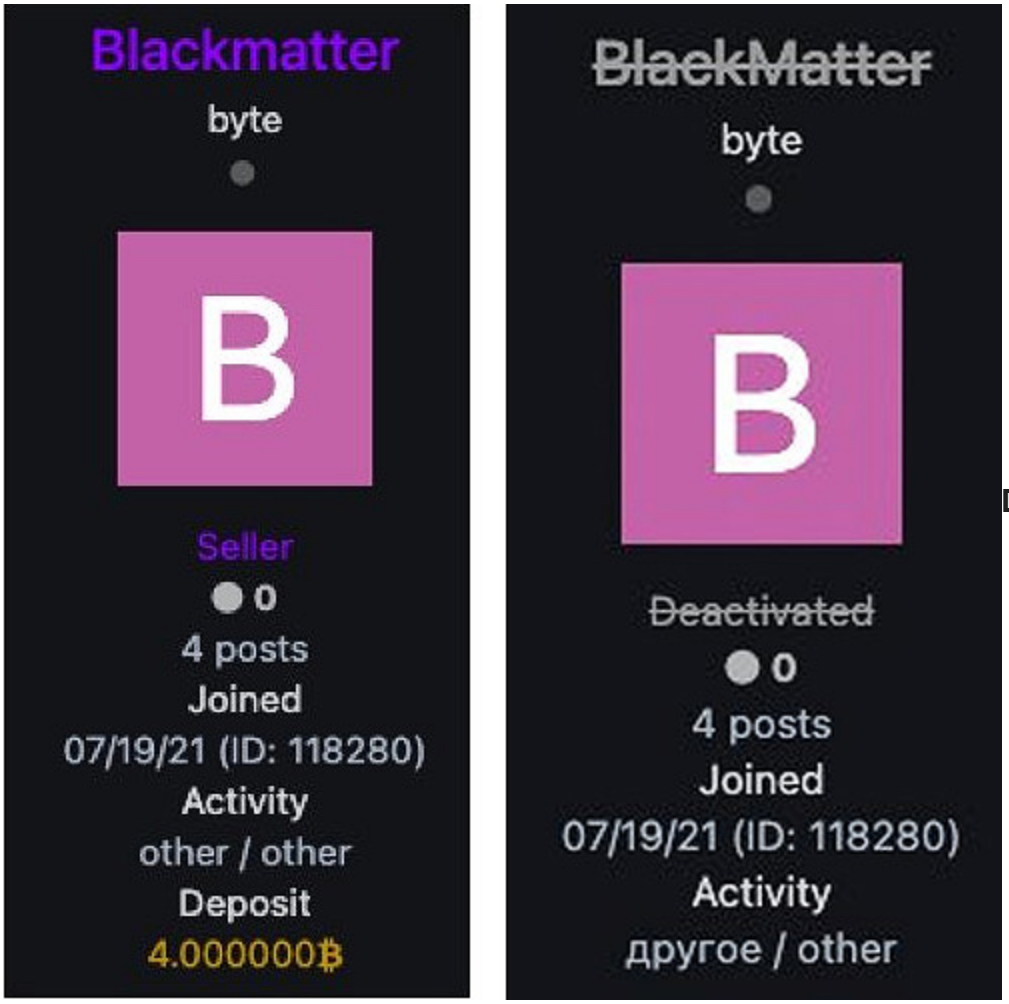
BlackMatter affiliate transfering victim to LockBit site

Source: BleepingComputer

At these LockBit negotiation pages, the BlackMatter affiliates continue to negotiate with victims to receive a ransom payment.

As for BlackMatter, they are continuing their shut down, with today's activities being to delete their presence from Russian-speaking hacking forums.

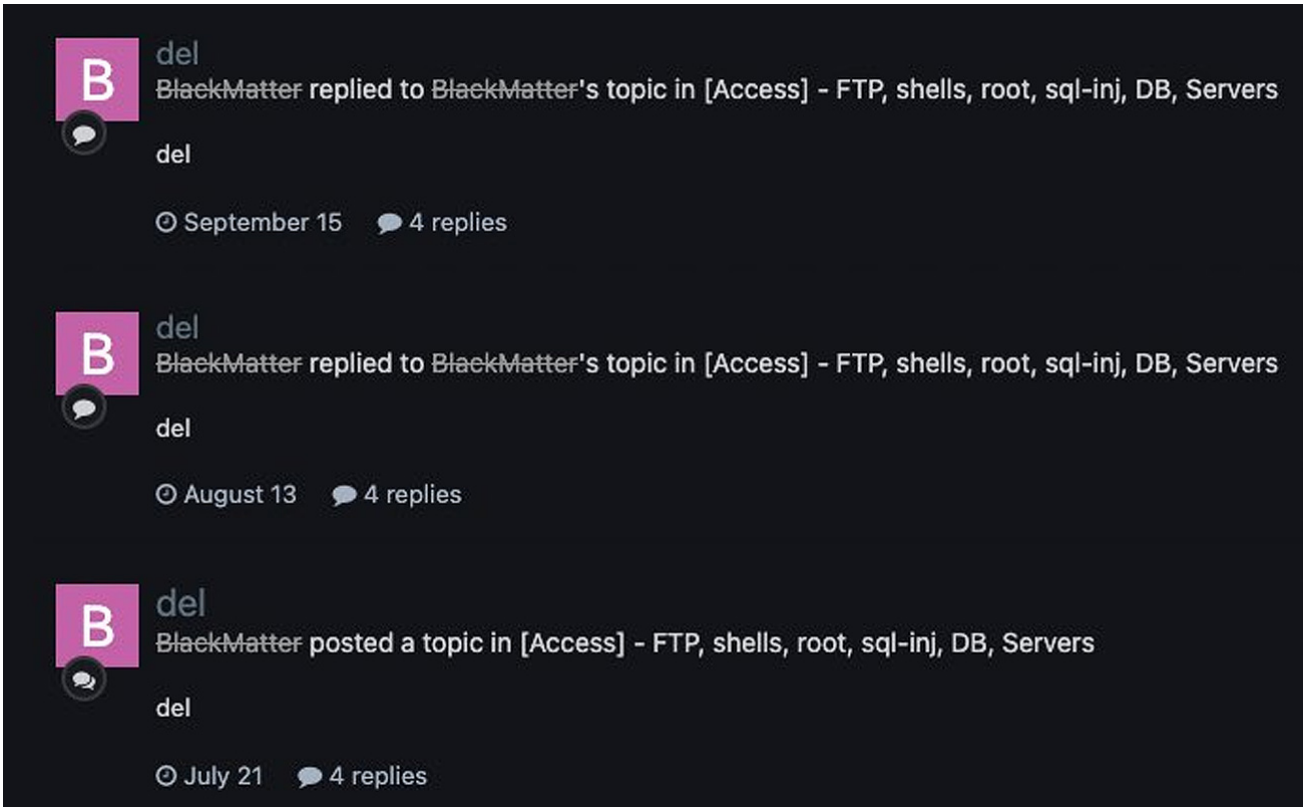
Security researcher pancak3lullz has been following BlackMatter's cleanup activities, showing that the gang withdrew 4 Bitcoins (~$250,000) today from the Exploit hacking forum and deactivated their account.



Deactivating accounts on hacking forums

Source: pancak3lullz

The gang has also been editing their existing posts on forums and asking moderators to delete them.



BlackMatter deleting posts on hacking forums

Source: pancak3lullz

With REvil and BlackMatter now shut down, LockBit has become one of the largest and most successful ransomware operations running today.

The LockBit representative known as 'LockbitSupp' has shown to be a savvy threat actor who constantly adjusts tactics to recruit new affiliates, especially as established operations shut down.

While BlackMatter will likely rebrand and return as a new ransomware operation, their partnership with LockBit may hurt them in the long run as they lose experienced affiliates.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

New RansomHouse group sets up extortion market, adds first victims

Conti ransomware shuts down operation, rebrands into smaller units

The Week in Ransomware - May 6th 2022 - An evolving landscape

Conti, REvil, LockBit ransomware bugs exploited to block encryption

- BlackMatter
- Decryptor
- Extortion

- LockBit
- Ransomware
- Shutdown

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.

- Previous Article
- Next Article

You may also like: