

## Hitting the BlackMatter gang where it hurts: In the wallet

- [FABIAN WOSAR](#)
- OCTOBER 24, 2021



*Earlier this year, Emsisoft researchers discovered a critical flaw in the [BlackMatter](#) ransomware that allowed them to help victims recover their files without paying a ransom, preventing millions of dollars falling into the hands of cybercriminals. The work has been conducted quietly and privately so as not to alert the BlackMatter operators to the flaw. For the reasons discussed below, we believe it is now safe to share the story without jeopardizing the operation.*

Over the past decade, Emsisoft has dedicated itself to the global fight against ransomware. Not only have we built decryption tools which have helped more than 6 million victims recover their data without paying a ransom, but we've also created a [unique service that helps ransomware victims who paid ransoms to recover more efficiently](#).

During this time, we have seen numerous ransomware gangs come and go. The exact motivations for their disappearance are often unclear, but we can make some well-educated guesses.

Perhaps the most common reason is financial fulfillment. Threat actors run a successful campaign, generate enough money for their participants to retire comfortably and choose to cease operations. In other situations, retirement is more about self-preservation, with threat actors withdrawing from the ransomware game after attracting too much unwanted attention.

For [BlackMatter's predecessor, DarkSide](#), it was very much a case of the latter.

## A brief history

DarkSide had been a major player in the ransomware-as-a-service landscape since August 2020, and generally targeted large private sector organizations that could afford seven-figure ransom demands. It had been one of the most active groups until early May 2021, when the gang bit off more than it could chew by attacking the largest pipeline system for refined oil products in the U.S.: Colonial Pipeline. The attack, which caused fuel shortages and forced some airlines to reschedule flights, impacted the daily lives of millions of people on the Eastern seaboard, drawing a large amount of attention from the press – as well as the ire of the U.S. authorities.

The U.S.' retaliation was swift. Within days, DarkSide had lost control over some of its critical infrastructure, including bitcoin wallets that contained the \$4.4 million ransom Colonial Pipeline had hastily paid in the hopes of quickly getting back to an operational state. Feeling the pressure, DarkSide went dark – until, that was, late July 2021.

On July 21, 2021, a new post made by the user account “BlackMatter” appeared on a popular underground forum:

**B** **Purchase / implementation of your access to corporate networks**  
 By BlackMatter , Wednesday at 08:50 AMin [Access] - FTP, shells, root, sql-inj, DB, Servers

**Blackmatter**  
 byte

**B**

**Seller**  
 ● 0  
 1 post  
 Joined  
 07/19/21 (ID: 118280)  
 Activity  
 other / other  
 Deposit  
 4.000000฿

Posted Wednesday at 08:50 AM

**We are looking for corporate networks of the following countries:**

- USA.
- CA.
- AU.
- GB.

**All areas except:**

- Medicine.
- State institutions.

**Requirements:**

- Zoom Revenue from 100kk +.
- 500 - 15,000 hosts.
- We do not take networks with which someone has already tried to work.

**2 options for work:**

- We buy: From 3 to 100k.
- We take it to work (discussed individually).

**Scheme of work:**  
 Selecting a work option -> Access transfer -> Checking -> We take it or not (in case of discrepancy).

**Deposit: 120k.**

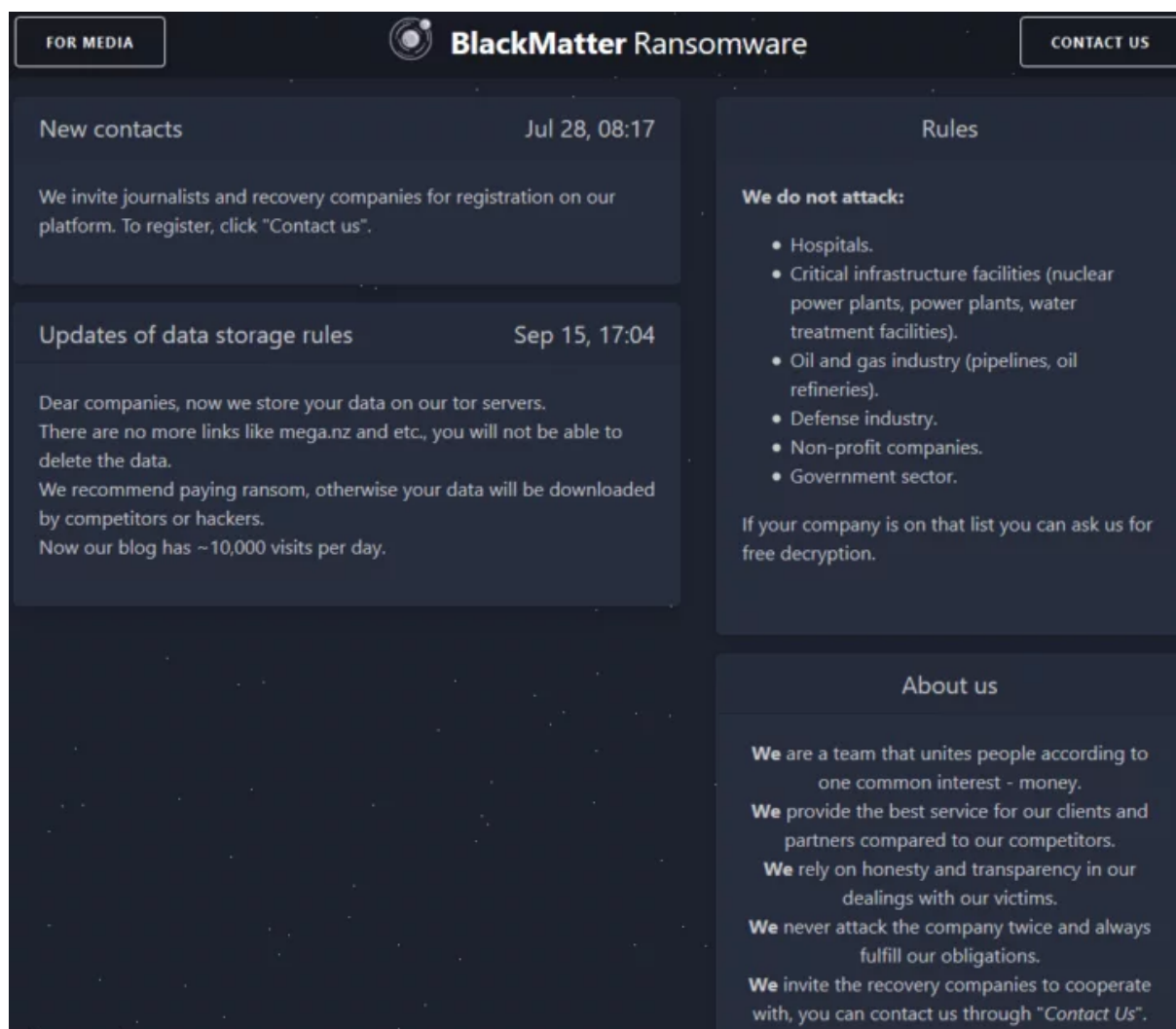
First contact of the PM. We are looking first of all for stable and adequate suppliers.

+ Quote

*Machine translation of an advertisement post looking for access to corporate networks, courtesy of our friends at Curated Intelligence*

The advertiser was looking to recruit parties who could provide access to corporate networks of companies with more than \$100,000,000 yearly revenue. This is a common practice for ransomware-as-a-service operations, where the different aspects of an attack are usually outsourced to other, more specialized groups or individuals. In this particular case, the BlackMatter user was looking to recruit initial access providers and brokers.

Shortly after, on July 27, 2021, it became apparent who this mysterious poster was and why they were willing to purchase access to company networks when a new leak site was discovered on the dark web: BlackMatter Ransomware.



*BlackMatter ransomware leak website*

One of the most interesting aspects of the BlackMatter leak site is the list of prohibited targets that must not be attacked by any BlackMatter affiliate. The industries on this list very much reflect the industries that the [U.S. designates as critical infrastructure](#) – the same industries that got DarkSide into trouble in the first place, and the same industries that U.S. President Joe Biden declared as off-limits to malicious cyber activity in a private meeting with Russian President Vladimir Putin in June 2021. But BlackMatter had and has no intention of adhering to its own rules. Since the leak site was launched, the gang has attacked U.S. critical infrastructure entities including blood testing facilities and organizations in the food and agriculture sector.

When we first got our hands on an actual BlackMatter payload on July 31st, 2021, the initial rumors that BlackMatter could be a repaint of the DarkSide operation were quickly confirmed. The very first BlackMatter version turned out to be almost identical to the last DarkSide version, with the only difference being minor incremental improvements. This first version was

quickly followed up with multiple new iterations of the BlackMatter payload and, at the time of writing, the latest internal version number of the payload has reached 2.0.

## Repeating past mistakes

DarkSide's original run wasn't flawless. For example, on December 12, 2020, Emsisoft researchers noticed a mistake the DarkSide operators had made that allowed us to decrypt the data encrypted by the Windows version of the ransomware without the need for a ransom to be paid. The gang fixed this flaw on January 12, 2021.

Publicly disclosing the existence of a flaw in ransomware can alert the threat actors to its existence, resulting in them immediately fixing the problem. Consequently, in the case of gangs that we believe to be technically sophisticated – such as DarkSide/BlackMatter – we do not publicly announce or disclose the existence of vulnerabilities. Instead, we communicate our decryption capabilities in private via a network of law enforcement agencies and trusted parties. In our opinion, this approach enables us to help as many victims for as long as possible. Additionally, it creates an incentive for victims to report ransomware incidents to local authorities as they may, in return, be able to provide crucial intelligence from third parties such as us which avoids the need for ransom demands to be paid.

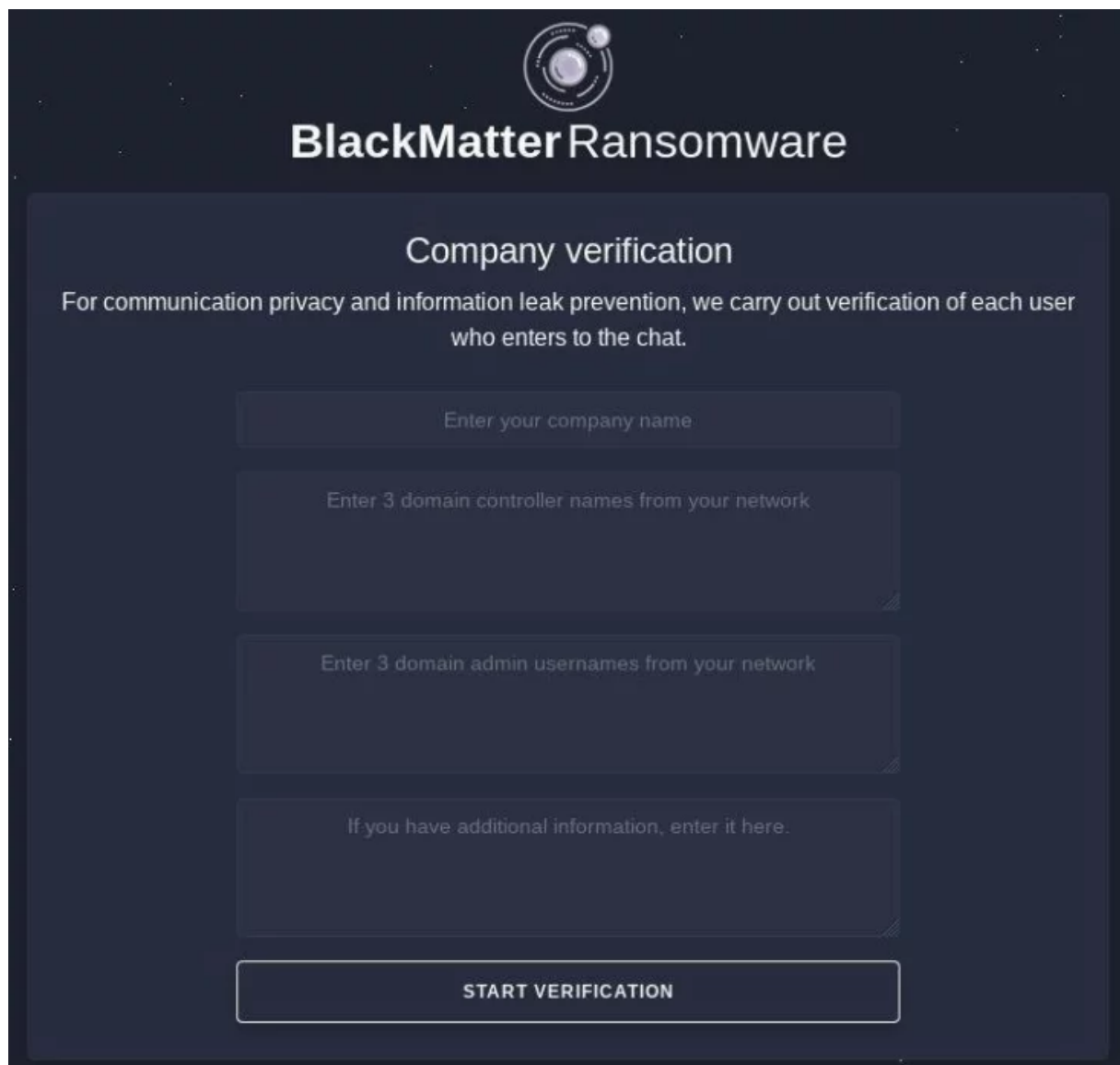
Knowing DarkSide's past mistakes, we were surprised when BlackMatter introduced a change to their ransomware payload that allowed us to once again recover victims' data without the need for a ransom to be paid. As soon as we became aware of the gang's error, we quietly reached out to our partners, who then assisted us in reaching as many victims as possible before they paid BlackMatter's ransom.

Since then, we have been busy helping BlackMatter victims recover their data. With the help of law enforcement agencies, CERTs and private sector partners in multiple countries, we were able to reach numerous victims, helping them avoid tens of millions of dollars in demands.

However, it wasn't all smooth sailing. One of the biggest challenges we faced during the operation related to social media, and Twitter in particular. During one of the more high profile BlackMatter incidents in September 2021, the ransom note was leaked. Ransom notes, including BlackMatter's, contain critical information intended for the victim only, including instructions on

how to reach out and communicate with the threat actor. Consequently, anybody who has access to a note can interact with the gang as though they were the victim.

The broad Twitter infosec community quickly picked up on the leak, got their hands on the private link intended for the victim only, and started to hijack the negotiations being held on the BlackMatter communication platform. Soon, both the victim and the BlackMatter operators were confronted with an onslaught of insults and trolling behavior. In addition, screenshots of the conversations were taken and circulated within the Twitter community, which caused even more people to join the “fun”, quickly derailing any sort of intelligence gathering by law enforcement and security researchers in the process.



The image shows a dark-themed web interface for BlackMatter Ransomware. At the top center is a circular logo with a globe and the text 'BLACK MATTER RANSOMWARE'. Below the logo, the text 'BlackMatter Ransomware' is displayed in a large, white, sans-serif font. Underneath, the heading 'Company verification' is centered. A paragraph of text reads: 'For communication privacy and information leak prevention, we carry out verification of each user who enters to the chat.' Below this text are four input fields, each with a light gray border and placeholder text: 'Enter your company name', 'Enter 3 domain controller names from your network', 'Enter 3 domain admin usernames from your network', and 'If you have additional information, enter it here.'. At the bottom of the form is a prominent white button with the text 'START VERIFICATION' in all caps.

*Extended verification introduced as a consequence of extensive trolling*

We have been fighting ransomware for more than ten years, so we understand the frustration the infosec community feels towards ransomware threat actors better than anyone. However, as cathartic as throwing expletives might have felt, it resulted in BlackMatter locking down their platform, and locking us and everyone else out in the process. Unfortunately, that meant one of the most valuable tools we had to reach victims disappeared literally overnight, leading to missed victims who may have unnecessarily paid ransoms.

## The inevitable end

While reading this post, you might have had a hunch where all of this was heading. After all, if BlackMatter hadn't figured out that something was wrong on their own, we would have continued our work in silence. But, unfortunately, BlackMatter released an update several weeks ago that fixed the flaw we were using to help victims.

However, just because this specific vulnerability has run its course doesn't mean our work is done. While we are confident that we managed to reach many BlackMatter victims, there are still some victims that we haven't been able to contact. We are now urging these victims to [reach out to us](#), as we can likely help them recover their data without paying the criminals.

Beyond BlackMatter, our team has identified vulnerabilities in about a dozen active ransomware families. In these cases, we can recover the vast majority of victims' encrypted data without a ransom payment. As with BlackMatter, we aren't making the list of families public until the vulnerability has been found and fixed by their respective operators. This is why we encourage victims to report incidents to law enforcement, as they may be able to direct them to us or other companies that can help.

Victims can also [reach out to us directly for a free evaluation](#). Even if we cannot help them avoid paying a ransom, our battle-earned expertise and world-class tools can often allow them to recover much faster, frequently shaving days or even weeks off the recovery time.

Last but not least, we are also issuing an open invitation to all law enforcement agencies, governmental institutions, and CERTs, as well as all insurance and digital forensic and incident response providers. We are constantly expanding both our capabilities and network to reach and help more victims. If you are interested in what we can do for you, your clients, or even your citizens, [don't hesitate to reach out](#).