BlackMatter ransomware says its shutting down due to pressure from local authorities

therecord.media/blackmatter-ransomware-says-its-shutting-down-due-to-pressure-from-local-authorities/

November 3, 2021

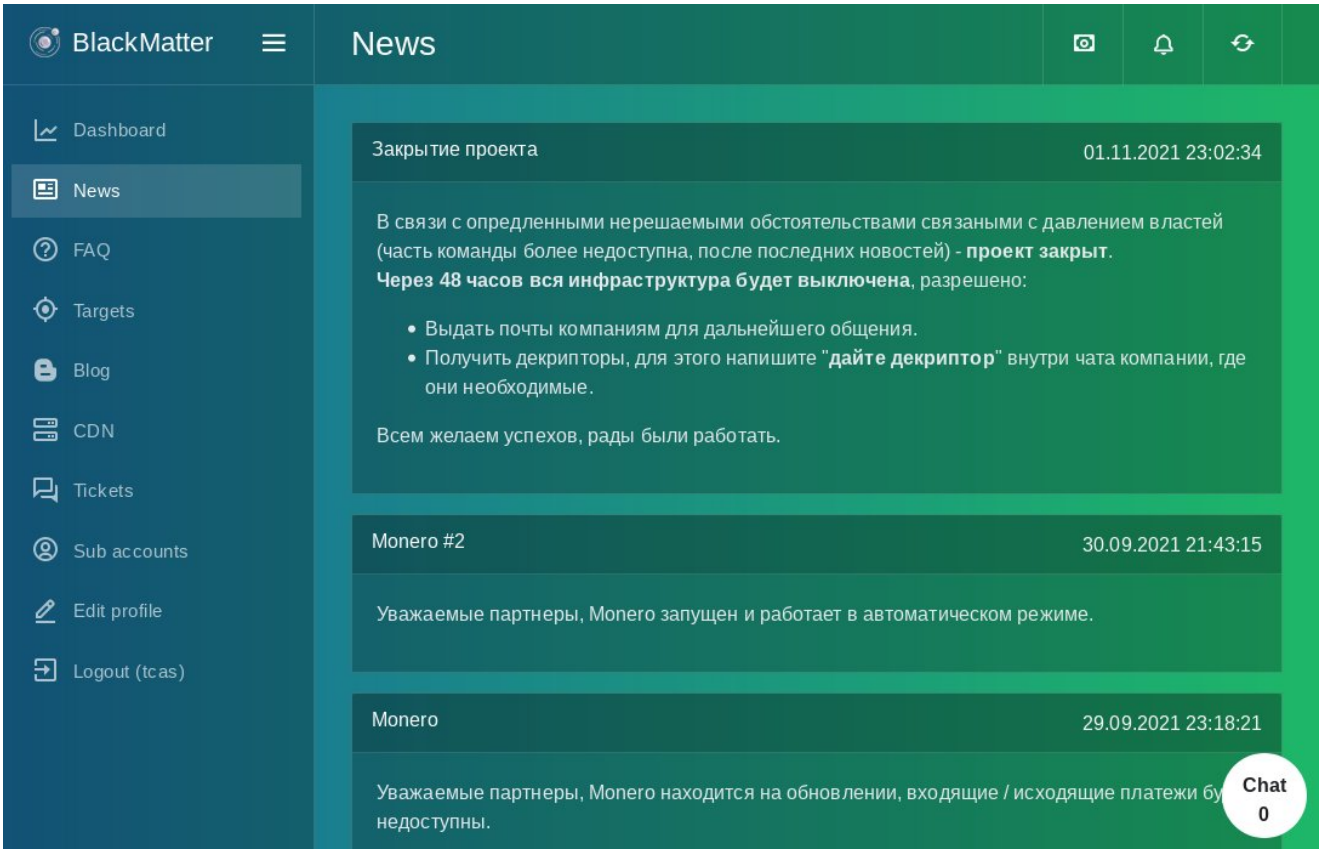

Image: vx-underground

The criminal group behind the BlackMatter ransomware have announced plans today to shut down their operation, citing pressure from local authorities.

The group announced its plan in a message posted in the backend of their Ransomware-as-a-Service portal, where other criminal groups typically register in order to get access to the BlackMatter ransomware strain.

The message, dated to Monday, November 1, 2021, and obtained by a member of the vx-underground infosec group, is pictured above and translated below:

> Due to certain unsolvable circumstances associated with pressure from the authorities (part of the team is no longer available, after the latest news) – the project is closed. After 48 hours, the entire infrastructure will be turned off, it is allowed to:
>
> -Issue mail to companies for further communication.
> -Get decryptors, for this write “give a decryptor” inside the company chat where they are needed.
>
> We wish you all success, we were glad to work.

While the group did not explain the “latest news” that led to its decision to shut down, their announcement comes after three major events that have taken place over the past two weeks.

The first of these were reports from Microsoft and Gemini Advisory that linked the FIN7 cybercrime group, considered the creators of the Darkside and BlackMatter strains, to a public cybersecurity firm named Bastion Secure, through which they allegedly recruited unwitting collaborators.

The second was the fact that security Emsisoft had secretly developed a decryption utility for the BlackMatter ransomware strain, which the company had been secretly offering to victims in order to avoid them paying the group’s ransom demands, putting a dent in its profits.

The third was a report from the New York Times this Sunday that announced that the US and Russia had started a closer collaboration aimed at cracking down on Russia-based cybercrime and ransomware gangs, among others. This is of importance because the FIN7 group has been historically believed to operate out of Russia.

Political pressure mounting on ransomware gangs

FIN7’s recent announcement also comes after the operators and members of multiple ransomware operations have been hunted and arrested all over the world this summer.

For example, in their previous incarnation as the Darkside ransomware, the FIN7 group had to pull the plug on their operation after their servers were hacked and cryptocurrency funds were stolen, following a suspected law enforcement action.

In addition, rival ransomware gang REvil shut down not once, but twice, with the second time in October, after law enforcement backdoored and hijacked their dark web servers.

Furthermore, just last week, Europol detained a Ukrainian group who orchestrated more than 1,800 ransomware attacks with strains such as LockerGoga, MegaCortex, and Dharma, including the devastating attack on aluminum producer Norsk Hydro in early 2019.

This period of intense pressure on ransomware gangs comes after attacks have reached an all-time high this year, with some attacks causing major issues across the world. Examples here include the Darkside ransomware attack on Colonial Pipeline (caused fuel supply issues for the US East Coast), the REvil attack on JBS Foods (disrupted meat supply across the US), and the REvil attack on Kaseya (disrupted thousands of companies across the globe).

As Jeff Moss, founder of the Black Hat and DEF CON security conferences, said earlier today on Twitter, law enforcement agencies have typically known the identities of most ransomware operators but have also known they couldn't go after some groups because of Russia's uncooperative behavior, something that appears to be changing – based on BlackMatter's statement.

> Suggests the authorities have known all along and only once the pressure increased did they act. It's examples like that that convinced me that ransomware is at least 50% a political problem. https://t.co/1Yi6KxriMD
>
> — Jeff Moss (@thedarktangent) November 3, 2021

Tags

- BlackMatter
- Darkside
- RaaS
- Ransomware
- Russia
- shutdown

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.