# An interview with BlackMatter: A new ransomware group that's learning from the mistakes of DarkSide and REvil

By Dmitry Smilyanets

Published: 2023-01-04 · Archived: 2026-04-05 13:01:22 UTC

Editor’s Note: In July, a new ransomware gang started posting advertisements on various cybercrime forums announcing that it was seeking to recruit partners and claiming that it combined the features of notorious groups like REvil and DarkSide.

Named BlackMatter, the gang said it was specifically interested in targeting large companies with annual revenues of more than $100 million. However, the group said some industries were off limits: It would not extort healthcare, critical infrastructure, oil and gas, defense, non-profit, and government organizations.

A representative from the group talked to Recorded Future expert threat intelligence analyst Dmitry Smilyanets recently about how BlackMatter is learning from the mistakes of other ransomware groups, what they look for when they recruit partners, and why they avoid certain targets. The interview was conducted in Russian and translated to English with the help of a professional translator, and has been edited for clarity.

**Dmitry Smilyanets: Your product appeared quite recently and as far as we know, there have been no public attacks using BlackMatter yet. How long ago did you start developing it?**

**BlackMatter:** There haven't been any attacks yet if you are judging by the public blog. In fact, there have been, and the companies we attacked are already communicating with us. As long as the negotiations are successful we do not publish a blog post on the main page of the blog.

The product has been in development for the last six months. Perhaps it seems simple (judging by the blog or the communication page), but it is not—what users see publicly is the tip of the iceberg.

Before starting the project, we studied the following products in detail:

- LockBit has a good codebase, but a skimpy and non-functional panel (at the time we used their product). If you compare it to a car, you can say that this is a Japanese car production line with good engines but an empty and non-functional interior. You can ride one, but with little pleasure.
- REvil is a good project on the whole, time-tested software (since GandCrab, they haven't made any significant edits since that time), a fairly functional panel, but focused more on the overall number of successful "loads" as opposed to specific targeted cryptography.
- Darkside is a relatively new software with a good codebase (partly problematic, but the ideas themselves deserve notice) and an interesting web part compared to other RaaS.

The executable itself has incorporated the ideas of LockBit, REvil, and partly DarkSide. The web part has incorporated the technical approach of DarkSide since we consider it the most structurally correct (separate companies for each target, and so on).

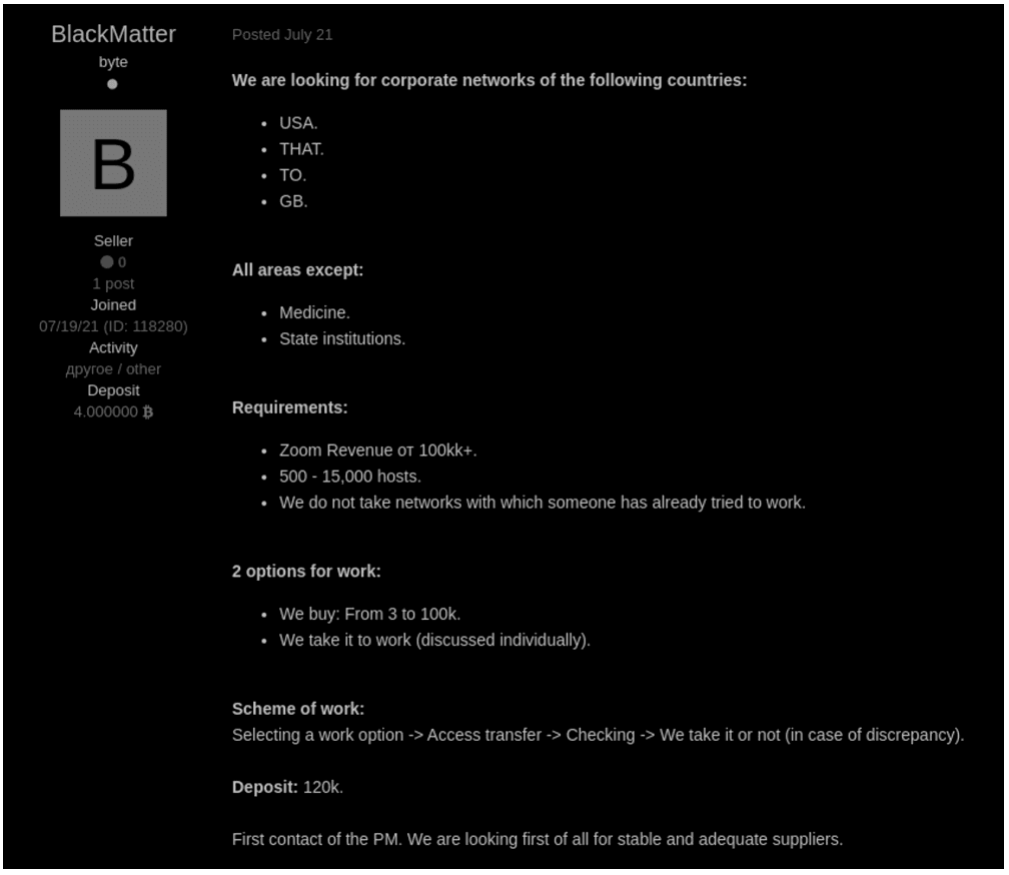


Image: The Record

**DS: How difficult is it to organize an affiliate program (also known as ransomware-as-a-service)?**

**BM:** On the whole, less difficult than not. The level is important, RaaS can also be offline (when builds are issued via jabber/tox), but there is no market demand for this and current customers, after using REvil and DarkSide, are not ready to take such affiliate programs seriously. We created a project and brought it to the market exactly at a time when the niche is vacant and the project fully meets the market demands, therefore its success is inevitable.

**DS: Most recently, the largest groups—DarkSide, REvil, Avaddon, BABUK—have disappeared from the scene. Many researchers believe that this was due to the attention of the top leadership of the United States and Russia to the situation with ransomware attacks. Is it true? Do you think your product will have the same fate?**

**BM:** Yes, we believe that to a large extent their exit from the market was associated with the geopolitical situation on the world stage. First of all, this is the fear of the United States and its planning of offensive cyber operations, as well as a bilateral working group on cyber extortion. We are monitoring the political situation, as well as receiving information from other sources. When designing our infrastructure, we took into account all these factors and we can say that we can withstand the offensive cyber capabilities of the United States. For how long? Time will tell. For now, we are focusing on long-term work. We also moderate the targets and will not allow our project to be used to encrypt critical infrastructure, which will attract unwanted attention to us.

**DS: You mentioned that your product brings together the very best of DarkSide, REvil, and LockBit. What are their strengths?**

**BM:** Our project has incorporated the strengths of each of the partner programs:

- From REvil—SafeMode, their implementation was weak and not well thought out, we developed the idea and thoroughly implemented it. We also implemented the PowerShell version of the ransomware variant given the REvil implementation.
- From LockBit—an approach to the implementation of the codebase, we took some things from there, mostly little things.
- From DarkSide—first of all, this is the idea of impersonation (the ability of the encryptor to use the domain administrator account to encrypt the shared drives with maximum rights), we also borrowed the structure of the admin panel from there.

**DS: Based on the latest reports published this week, BlackMatter is visually very similar to DarkSide. Can you confirm that your infrastructure is based on DarkSide?**

**BM:** We can confidently say that we are fans of dark mode in design, we are familiar with the DarkSide team from working together in the past but we are not them, although we are intimate with their ideas.

**DS: LockBit 2.0 is considered the fastest locker at the moment. What is the encryption/decryption speed of your variant?**

**BM:** This is not true. After reading the question - we decided to prepare ourselves by downloading the latest publicly available version of LockBit (end 06.21) and conducting tests, we can state the following:

- BlackMatter: 2.22
- LockBit: 02.59

The tests were carried out under the same conditions. Moreover, LockBit encrypts the first 256 kb of the file (which is pretty bad from the point of view of cryptographic strength). We, on the other hand, encrypt 1 MB. Essentially, that's the secret to their speed.

**DS: Are you planning to add new features to the product, following the example of StealBit?**

**BM:** Yes, the software is constantly being improved, in terms of the new functions that will appear in the near future—printing the text of the note on all available printers. We also watch our competitors and always implement what we consider promising and in demand by our clients.

**DS: I have already seen several recruiting announcements for your team. How many penetration testers would you like to recruit? Is it easier to work with a small but strong team, or with an army of script kiddies?**

**BM:** We are geared at strong, self-sufficient teams with experience, their own technical solutions, and a real desire to make money, not someone who wants to try the business out. We usually filter out script kiddies before they get access to our admin panel.

**DS: Obviously, there are many talented professionals on your team. Why is it that this talent is aimed at destructive activities? Have you tried legal penetration testing?**

**BM:** We do not deny that business is destructive, but if we look deeper—as a result of these problems new technologies are developed and created. If everything was good everywhere there would be no room for new development.

There is one life and we take everything from it, our business does not harm individuals and is aimed only at companies, and the company always has the ability to pay funds and restore all its data.

We have not been involved in legal pentesting and we believe that this could not bring the proper material reward.

**DS: What do you think about the attacks carried out against Colonial Pipeline's infrastructure or JBS? Does it make sense to attack such large networks?**

**BM:** We think that this was a key factor for the closure of REvil and DarkSide, we have forbidden that type of targeting and we see no sense in attacking them.

**DS: The US Department of Justice said they were able to recover some of the bitcoins paid by Colonial. How do you think this has happened?**

**BM:** We think that the DarkSide team or their partners transferred bitcoins to web wallets, which led to the seizure of private keys.

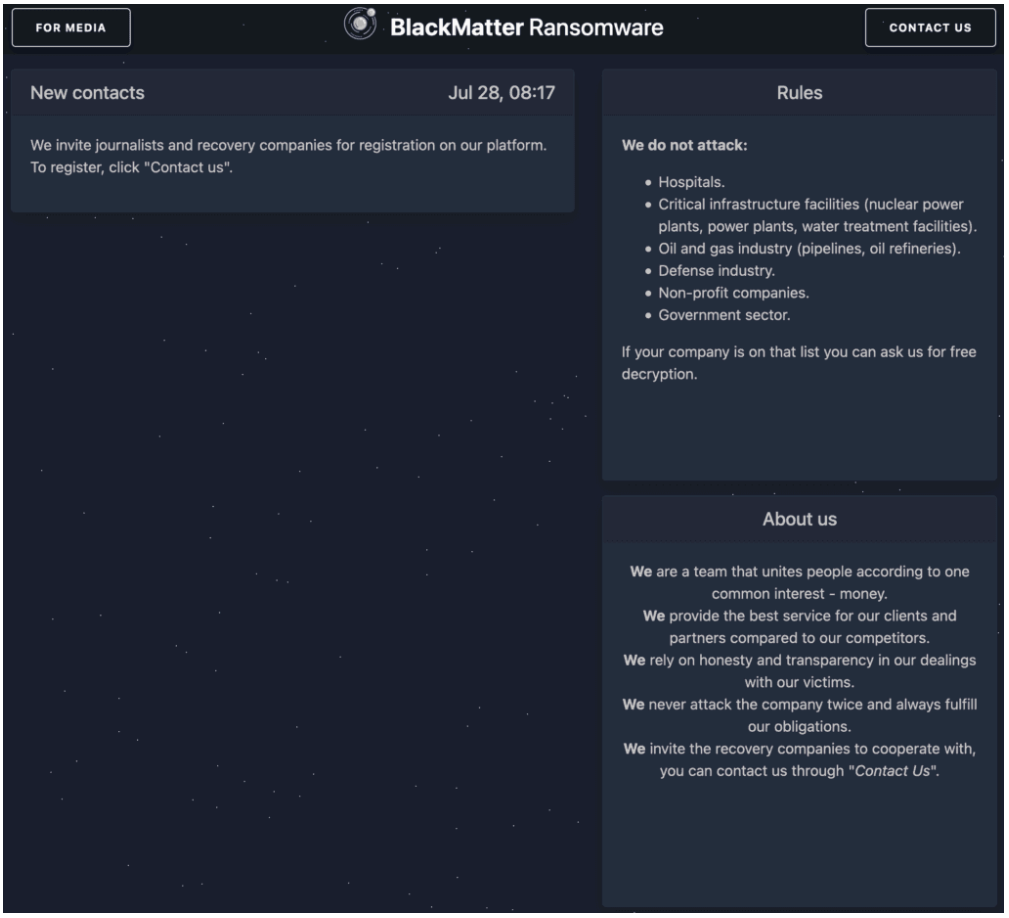


Image: The Record

**DS: You are actively buying access to the networks and declare that you are NOT interested in government and medical institutions. At the same time, you stated that you will not encrypt a wider range of industries, including critical infrastructure, defense, non-profit, and oil. Who has the last word to encrypt the network or not?**

**BM:** The last word is ours. We check each target and decide if it has potential negative consequences for us. The discrepancy between the industries in the blog and on the forum is related to marketing. In personal correspondence we filter out those which we are not interested in.

**DS: What type of primary network access is the easiest in 2021 in your opinion?**

**BM:** We do not work with VPN and other time-consuming types of initial access but are focused on getting direct access to the network immediately.

**DS: What carries more effect motivating the company to pay: The infrastructure being unavailable, or the fear of a data leak?**

**BM:** It varies from company to company. For some it is important to maintain confidentiality, and for others it's restoring infrastructure. If the network is completely encrypted and there is also a risk of data being published, the company will most likely pay.

**DS: Unknown spoke about a special outlook towards insurance companies. Do you think that if insurance companies abruptly stop covering ransomware incidents it will change your interest in ransomware?**

**BM:** It will not change, the companies will continue to pay money regardless. It is possible that the amount being paid will decrease.

Now the insurance fees have increased, but fearing that they will be left alone in the situation everyone will continue buying the insurance.

**DS: What's happened with Unknown? There are a lot of rumors, can you clarify the situation?**

**BM:** We do not know. Most likely, after the last payment, he went on vacation or is preparing a rebranding of their project.

**DS: Tell me a secret.**

**BM:** There are no secrets, but we believe in our motherland, we love our families, and we earn money for our children.

Dmitry Smilyanets

Mission-driven and Russian-speaking intelligence analyst with type A personality. Dmitry has twenty years of experience and expertise in cybercrime activity that includes being a former member of an elite Russian-based hacking organization.

---