

BlackMatter ransomware gang rises from the ashes of DarkSide, REvil

bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/

Lawrence Abrams

By

[Lawrence Abrams](#)


- July 31, 2021
- 11:12 AM
- 3



A new ransomware gang named BlackMatter is purchasing access to corporate networks while claiming to include the best features from the notorious and now-defunct REvil and DarkSide operations.

Last week, both [Recorded Future](#) and security researcher [pancak3](#) shared that a new threat actor named 'BlackMatter' had posted to hacking forums where they want to purchase access to corporate networks.

BlackMatter
byte
●



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

Posted July 21

We are looking for corporate networks of the following countries:

- USA.
- THAT.
- TO.
- GB.

All areas except:

- Medicine.
- State institutions.

Requirements:

- Zoom Revenue or 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.

Forum post by BlackMatter to the Exploit forum

In the post, the threat actor stated that they want to buy access to networks in the USA, Canada, Australia, and Great Britain, except for networks associated with medical and government entities.

They further shared that they were willing to spend \$3,000 to \$100,000 per network that had the following criteria:

- Revenue of \$100 million or more.
- The network should contain 500-15,000 devices.
- It should be a new network that other threat actors have not already targeted.

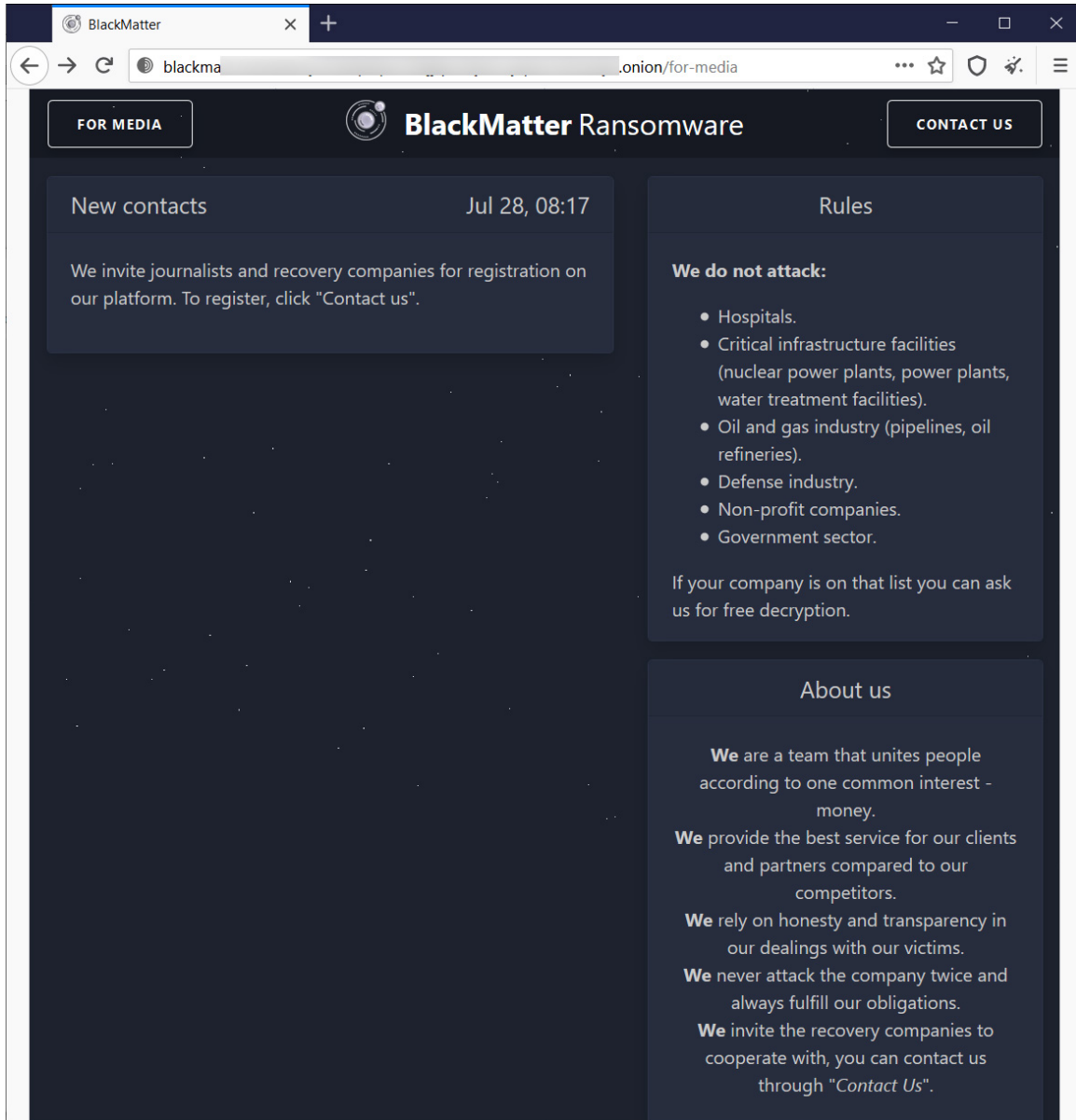
To show that they were serious, the threat actor deposited four bitcoins (\$120,000) in the Exile hacking forum's cryptocurrency wallet to show that they mean business and were a serious player.

As forums promoting ransomware are now banned on the XSS and Exploit forums, the threat actor did not indicate how they would use the network access.

BlackMatter ransomware gang emerges

That same day, researchers from Recorded Future revealed that a new Tor data leak site for a 'BlackMatter' ransomware operation appeared on the dark web last week.

The name indicates that the BlackMatter threat actor is the public-facing representative for the ransomware operation under the same name.



New

BlackMatter data leak site

In addition to posting information about themselves their operation, BlackMatter states that they will not target entities in the following industries:

- 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.

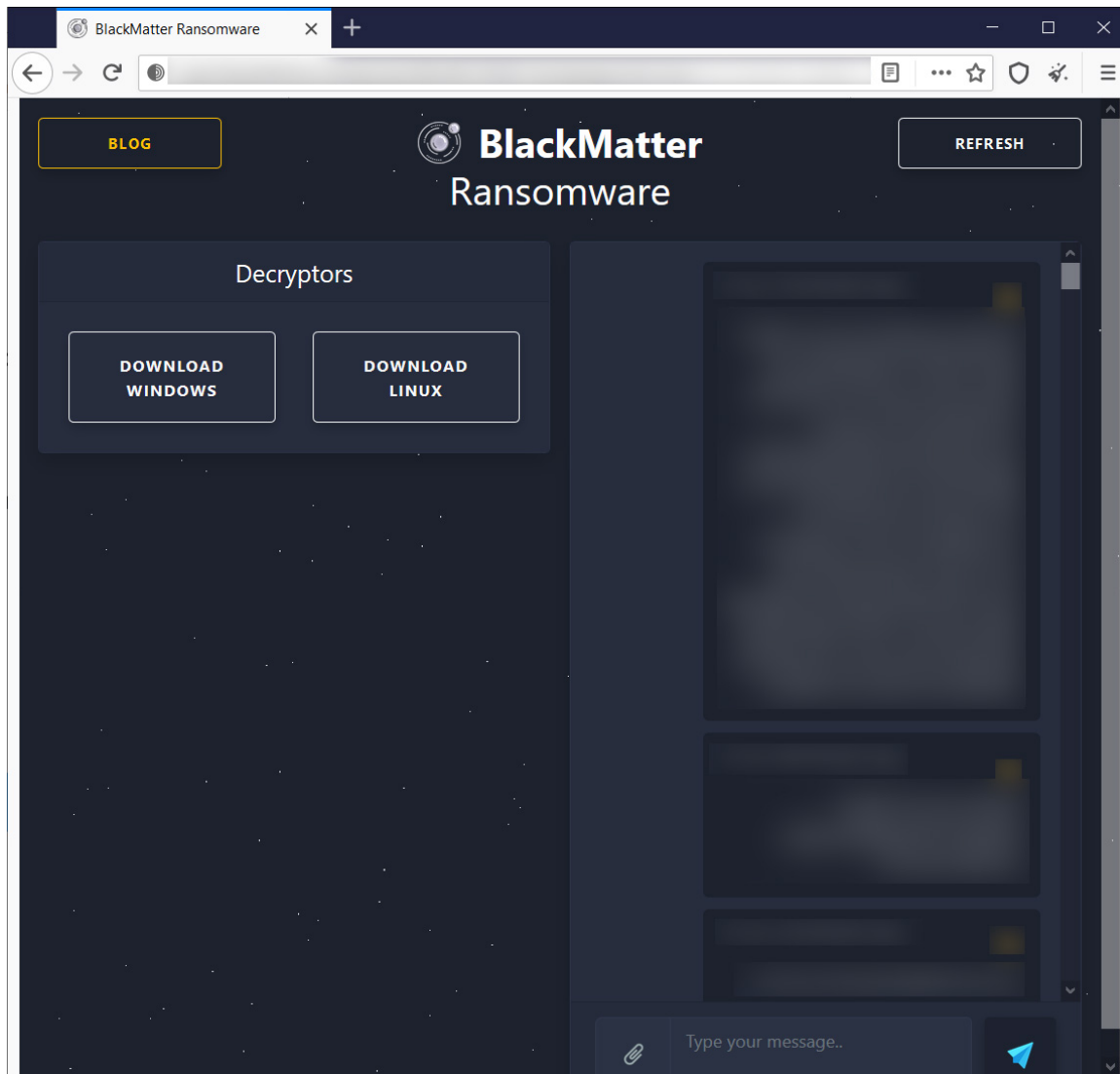
Recorded Future says the gang's ransomware executables come in various formats so that they can encrypt different operating systems and device architecture.

"The ransomware is provided for several different operating systems versions and architectures and is deliverable in a variety of formats, including a Windows variant with SafeMode support (EXE / Reflective DLL / PowerShell) and a Linux variant with NAS support: Synology, OpenMediaVault, FreeNAS (TrueNAS)," reported Recorded Future.

"According to BlackMatter, the Windows ransomware variant was successfully tested on Windows Server 2003+ x86/x64 and Windows 7+ x64 / x86. The Linux ransomware variant was successfully tested on ESXI 5+, Ubuntu, Debian, and CentOS. Supported file systems for Linux include VMFS, VFFS, NFS, VSAN."

At this time, there are no victims listed on the site. However, the ransomware gang states that "all blogs hidden for now. For a very short time," indicating that they are actively attacking victims.

BleepingComputer has been able to confirm that there are active attacks underway and that at least one victim paid \$4 million to the threat actors this week.



BlackMatter Tor negotiation site

Source: BleepingComputer

Based on the negotiation chat, this is a veteran ransomware operation and most likely a rebrand of one of the larger and now-defunct groups that recently shut down.

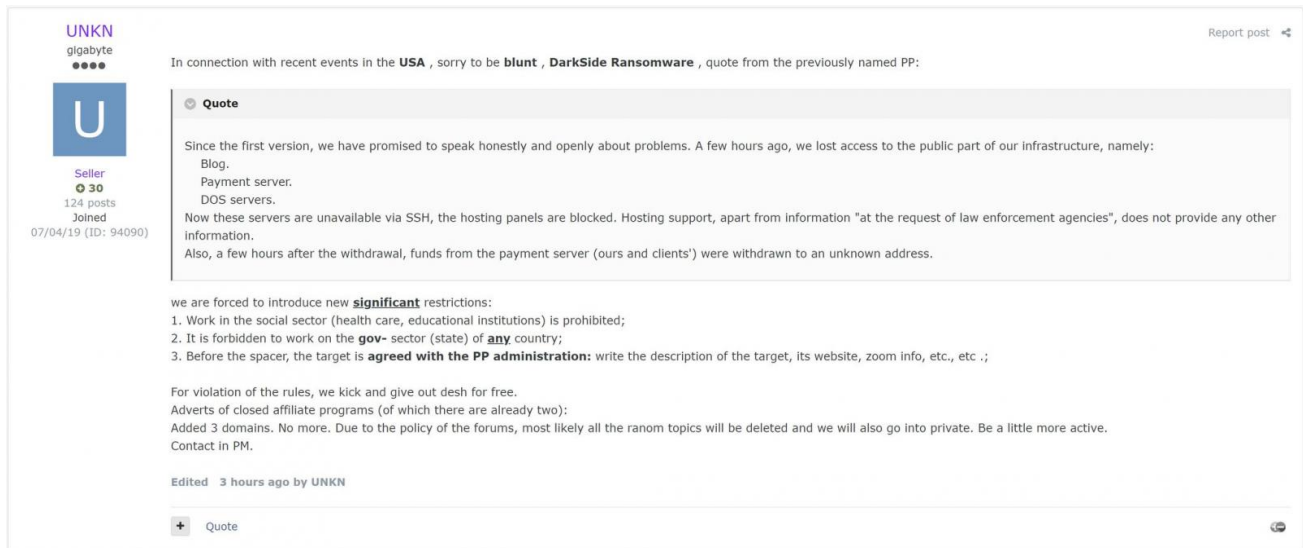
Rising from the ashes of DarkSide and REvil?

Information discovered by security researchers as well as the similarities in web sites and partners may indicate that BlackMatter has recruited or was created by threat actors that were previously with the DarkSide and the REvil ransomware operations.

As ransomware gangs commonly rebrand to evade law enforcement, when we first reported on DarkSide in August 2020, some security researchers and law enforcement believed REvil was rebranding as the new DarkSide operation.

However, both gangs continued operating side-by-side for almost a year until DarkSide attacked Colonial Pipeline. Feeling the full pressure of the US government and law enforcement, DarkSide shut down its operation in May.

The shut down of DarkSide was first reported by REvil's public-facing representative, Unknown, who posted about it on a hacking forum.



The screenshot shows a forum post by a user named UNKN. The user's profile information includes a blue 'U' avatar, the name 'UNKN', a bio 'gigabyte', and a 'Seller' status with '30' items and '124 posts'. The post content begins with a quote: 'In connection with recent events in the USA, sorry to be blunt, DarkSide Ransomware, quote from the previously named PP:'. The quoted text lists infrastructure components lost: 'Blog, Payment server, DOS servers.' and states that servers are unavailable via SSH and hosting support is limited. It also mentions that funds from a payment server were withdrawn to an unknown address. The main post text continues with a list of 'significant' restrictions: 1. Work in the social sector (health care, educational institutions) is prohibited; 2. It is forbidden to work on the gov- sector (state) of any country; 3. Before the spacer, the target is agreed with the PP administration: write the description of the target, its website, zoom info, etc., etc. ;. It also mentions that for rule violations, users are kicked and given a 'desh' for free, and that closed affiliate programs will be deleted. The post was edited 3 hours ago by UNKN.

Forum post by UNKN about DarkSide seizure

Two months later, it was REvil's turn to shut down after conducting a massive attack on managed service providers worldwide through a zero-day Kaseya VSA vulnerability.

Like DarkSide, REvil was feeling massive pressure from the US government and international law enforcement. It is widely speculated that the Russian government told them to shut down and disappear for a while.

After seeing the BlackMatter Tor site, security researchers found that it showed a strong resemblance to the now-defunct DarkSide ransomware's Tor site.

Both pages share a similar color theme, similar language, a similar way of referring to themselves, and also included a list of targets they would not attack.

Recorded Future also reported that BlackMatter said, "The project has incorporated in itself the best features of DarkSide, REvil, and LockBit."

Finally, cybersecurity firm Mandiant has seen indicators suggesting that an actor previously connected to DarkSide is now partnering with BlackMatter.

"We have seen some indication that currently suggests that at least one actor connected to some DARKSIDE ransomware operations is aligning themselves with BLACKMATTER," Kimberly Goody, Mandiant Director of Financial Crime Analysis, told BleepingComputer.

"This isn't necessarily surprising as we commonly see ransomware affiliates partnering with multiple providers."

While many clues indicate that this may be a rebrand of DarkSide, or possibly created by actors from both groups, we will not know for sure until a sample of the ransomware is analyzed for code similarities.

As BlackMatter attacks are ongoing, researchers will likely find a sample soon.

Related Articles:

[REvil ransomware returns: New malware sample confirms gang is back](#)

[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](#)

[REvil's TOR sites come alive to redirect to new ransomware operation](#)

- [BlackMatter](#)
- [DarkSide](#)
- [Ransomware](#)
- [Rebrand](#)
- [REvil](#)

[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](#)

Comments



Amigo-A - 9 months ago

-
-

""BlackMatter said, "The project has incorporated in itself the best features of DarkSide, REvil, and LockBit.""

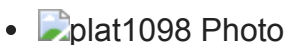
This confession is the best proof, not even a sample is needed to tie together the extortionists behind it. They are not connected with Russia, they are by themselves, outside the area of responsibility.



Some-Other-Guy - 9 months ago

-
-

A confession is not proof



plat1098 - 9 months ago

-
-

A Twitter post via BC suggests this gang will not attack oil and pipeline infrastructure-- to me, another clue that this BlackMatter gang is a re-do of REvil.

I see Biden's threats aren't having the desired effects at the moment. Let's try yet again, sir. Or is it a waste of time?

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
