BlackMatter ransomware targets companies with revenue of $100 million and more

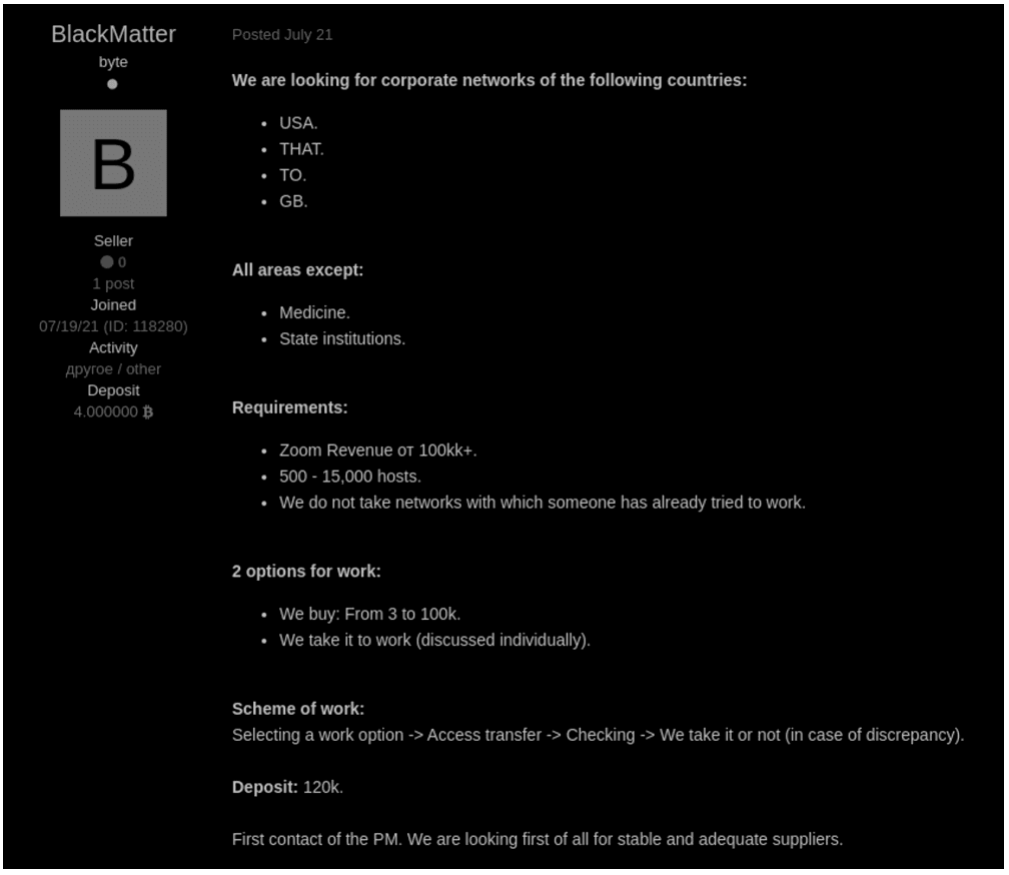
By Catalin Cimpanu

Published: 2022-12-12 · Archived: 2026-04-05 15:54:22 UTC

A new ransomware gang launched into operation this week, claiming to combine the best features of the now-defunct Darkside and REvil ransomware groups, Recorded Future analysts have discovered.

Named **BlackMatter**, the group is currently recruiting affiliates (collaborators) through ads posted on two cybercrime forums named Exploit and XSS.

Although ads for ransomware operations have been banned on the two forums since May, the BlackMatter group is not advertising its Ransomware-as-a-Service (RaaS) offering directly but has posted ads for recruiting "initial access brokers," a term used to describe individuals with access to hacked enterprise networks.



According to the gang's ads, BlackMatter is interested in working with brokers who can grant it access to apex corporate networks—for companies that have revenues of $100 million/year or larger.

Per the BlackMatter gang, the networks need to have between 500 and 15,000 hosts and be located in the US, the UK, Canada, or Australia.

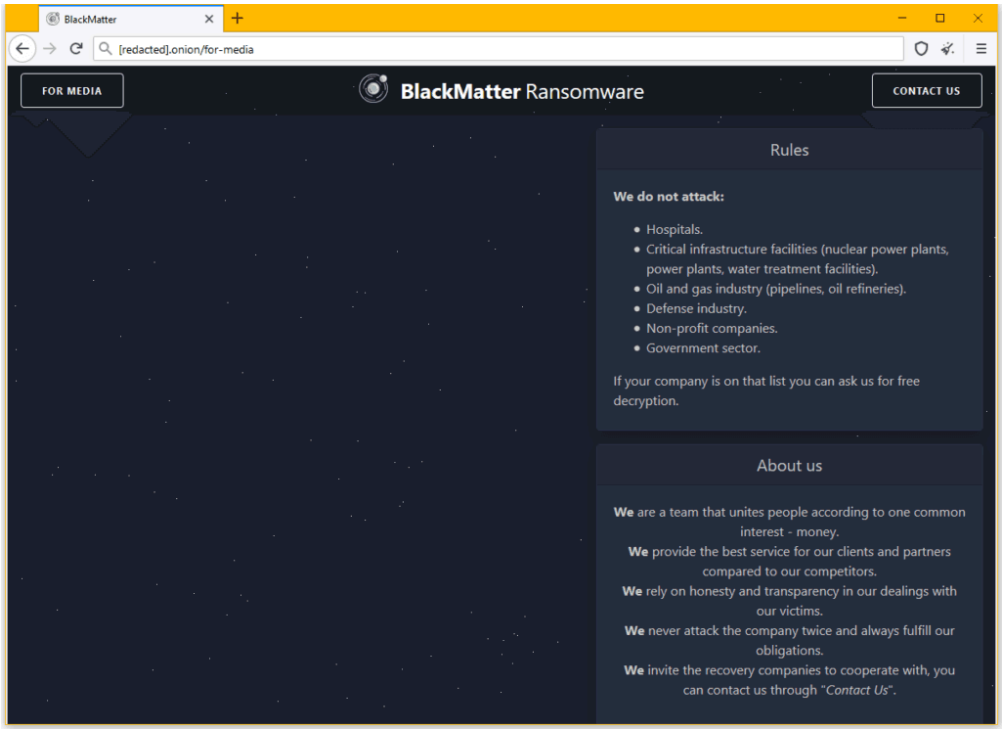
The BlackMatter group says it is willing to pay up to $100,000 for exclusive access to any of these high-value networks.

Once the group finds a suitable target, they will use the access granted by the broker to deploy tools that take over a company's internal systems and then deploy their file-encrypting payload.

The group boasted about having the ability to encrypt different operating system versions and architectures. This includes the likes of Windows systems (via SafeMode), Linux (Ubuntu, Debian, CentOS), VMWare ESXi 5+ virtual endpoints, and network-attached storage (NAS) devices (such as Synology, OpenMediaVault, FreeNAS, and TrueNAS).

BlackMatter also operates a dark web leak site

Just like most top-tier ransomware gangs today, BlackMatter also operates a website on the dark web—called a **leak site**—where it intends to publish data they steal from their victims if the hacked company does not agree to pay to decrypt their files.



This site is currently empty, confirming that the BlackMatter group only launched this week and did not carry out any intrusions just yet.

In a section of this website, the BlackMatter group also lists a spectrum of targets that they do not intend to attack. This includes [sic]:

- 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.

The BlackMatter gang claims that if a victim from these industry verticals is infected, they plan to decrypt their data for free.

This section is eerily similar to a section that was previously available on the leak site of the Darkside gang, which ceased operations after an attack on US pipeline operator Colonial.

Recorded Future analysts, who spotted this new group's infrastructure earlier this week, told *The Record* that based on the observed evidence so far, they believe that there is a connection between BlackMatter and the former Darkside group, although this connection is still under investigation.

No previous article

No new articles

Catalin Cimpanu

is a cybersecurity reporter who 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.
