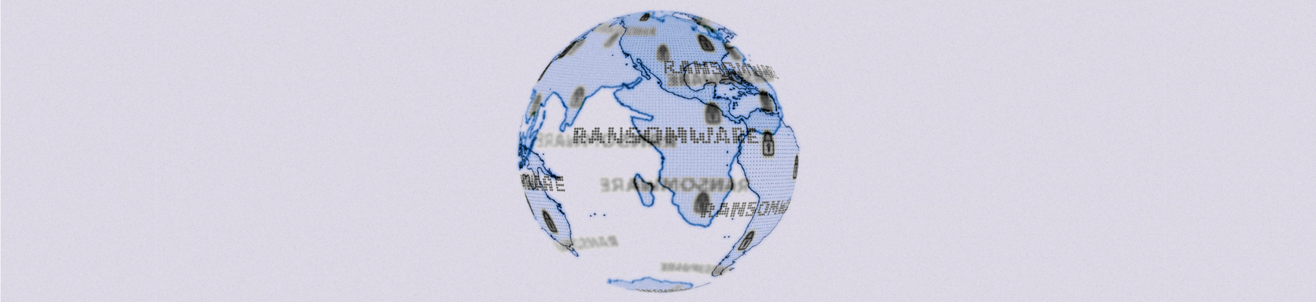
BlackMatter Ransomware Emerges As Successor to DarkSide, REvil

recordedfuture.com/blackmatter-ransomware-successor-darkside-revil/



Insikt Group

BlackMatter is a new ransomware-as-service (RaaS) affiliate program that was founded in July 2021. According to BlackMatter, “The project has incorporated in itself the best features of DarkSide, REvil, and LockBit”.

According to their public blog, below, the threat actor group does not conduct attacks against organizations in several industries, including healthcare, critical infrastructure, oil and gas, defense, non-profit, and government.

Figure 1: *Public extortion blog (Source: BlackMatter Ransomware)*

BlackMatter, a member of the top-tier forum Exploit and likely an operator of BlackMatter ransomware, is currently advertising the purchase of access to corporate networks in the US, Canada, Australia, and the UK. The threat actor is interested in all industries, except healthcare and governments, and has the following requirements for targets:

- Revenue of $100 million and more
- 500-15,000 hosts in the network

Figure 2: *Public Advertisement (Source: Forum Exploit)*

BlackMatter offers a $3,000-$100,000 price range for network access, as well as the share from the potential ransom amount. BlackMatter has a deposit of 4 bitcoins ($110,000) on the forum Exploit.

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). 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.

Recorded Future is following the ongoing developments associated with BlackMatter ransomware.