Chatter Indicates BlackMatter as REvil Successor

flashpoint-intel.com/blog/chatter-indicates-blackmatter-as-revil-successor/

July 27, 2021

Blogs

Blog

On July 19, 2021, a threat actor operating under the alias “BlackMatter” registered an account on the high-tier Russian-language illicit forums XSS and Exploit. The actor deposited 4 BTC (approximately $150,000 USD) into their escrow account. Large deposits on the forum indicate the seriousness of the threat actor.

BlackMatter Registration

On July 19, 2021, a threat actor operating under the alias “BlackMatter” registered an account on the high-tier Russian-language illicit forums XSS and Exploit. The actor deposited 4 BTC (approximately $150,000 USD) into their escrow account. Large deposits on the forum indicate the seriousness of the threat actor. On July 21, the threat actor posted a notice on the forums, stating they are looking to purchase access to infected corporate networks in the US, Canada, Australia, and the UK, presumably for ransomware operations. The threat actor said they are looking for larger corporate networks with revenues of over US $100 million.

While the inclusion of Five Eyes countries is notable, it is likely more financially-motivated than strategic. US, Canada, Australia, and the UK are ranked among the top 10 most-targeted countries for publicly-reported incidents on ransomware blogs and, further, the April 2021 paper from the Institute for Security and Technology Ransomware Task Force highlighted that White House and DNI would coordinate with Five Eyes on a number of action items for combating ransomware.[1] Recent reports highlight intelligence sharing with partner countries on suspicious cryptocurrency transactions in foreign exchanges.[2]

Re-emergence?

The timing of the post is interesting in that it occurred two months after XSS, Exploit, and Raid Forums banished the DarkSide ransomware group, and forbade the discussion and solicitation of ransomware with the forums. DarkSide ransomware group was responsible for extorting Colonial Pipeline, resulting in a disruption in one of the largest oil pipelines in the United States. Shortly after the incident, DarkSide's blog was offline and the Justice Department claimed that they recovered $2.3 million from Colonial's ransomware payment.[3] "UNKN" (aka "Unknown") a representative of REvil, relayed DarkSide's shutdown through a forum post.

[1] *https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf*
[2] *https://edition.cnn.com/2021/07/06/politics/white-house-ransomware-strategy/index.html*
[3] *https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside*

On July 13, 2021, REvil abruptly shut down their ransomware blog. On the same day, XSS banned REvil's spokesperson UNKN. The shutdown followed REvil's high-profile ransomware attack against the technology provider, Kaseya.

BlackMatter does not openly state that they are a ransomware collective operator, which technically doesn't break the rules of the forums, though the language of their post, as well as their goals clearly indicate that they are a ransomware collective operator.

Re-branding?

The emergence of a new group following the closure of DarkSide and REvil leaves threat actors questioning their origins, and if this is a possible rebranding. Both BlackMatter and UNKN appear to have similar rules around targeting. For example, both BlackMatter and UNKN explicitly say they will not target medical and government institutions. Regarding tactics, both groups use the same public corporate databases to research possible victims. Furthermore, Flashpoint analysts note that REvil previously labeled their Windows Registry key "BlackLivesMatter."

While the information may not be a smoking gun, it may indicate that REvil has not gone totally offline, but merely took a small hiatus following some high-profile breaches. It is also important to note that two posts and a large escrow account do not make a ransomware group. It is possible that copycats are intentionally mimicking the behavior of REvil to gain immediate credibility for allegedly being the reincarnation of REvil.

Ran Somewhere? No, Still Here

While recent bans on forums made it significantly harder for ransomware collectives to recruit partners, nevertheless ransomware collectives are finding new creative avenues to attract threat actors, who would be interested in working with them.

For instance, on July 22, 2021, Flashpoint observed an advertisement of the partner program of the AvosLocker Ransomware collective. The advertisement was distributed on Jabber via a service called “HQ Advert Services,” which specializes in mass spam campaigns via Jabber and Telegram. HQ Advert and other similar services maintain a list of Jabber and Telegram handles and are able to distribute the advertisements of interest for a fee.

Prior to that, ransomware actors have also maintained communications on a number of other platforms. Some, such as Black Shadow, maintain Telegram accounts, others, such as LockBit 2.0, run ransomware-as-a-service (RaaS) recruitment on their forums, and still others have moved to new forums for RaaS recruitment such as Babuk’s RAMP forum.

At this time, we can only assess the possible origins and intentions of BlackMatter. Their presence on XSS and Exploit highlights the increasing importance of those forums in ransomware recruitment, despite the apparent bans in May 2021.

Re-recruitment

On July 27, the group began recruiting potential partners and affiliates via IM protocol, Jabber. Notably, the group is using Exploit’s Jabber server to send out their recruitment message, again showing ransomware groups utilizing Exploit’s infrastructure to forward their nefarious agenda despite an alleged ban.

In the advertisement, BlackMatter announced they were looking for experienced penetration testers who work with Windows and Linux systems and initial access suppliers, who would either sell their access or work for a percentage of the profits. The group listed their Jabber handle and Tox ID, and asked interested parties to contact them.

Remodel? Who Wore it Best?

Flashpoint analysts also discovered a leaks site on an onion domain run by the group, in which BlackMatter expands its rules on targeting to include restrictions on targeting the oil and gas sector and the defense and CI sector. The leaks site currently does not list any victims.

After the discovery of the site, rumors again abounded claiming that BlackMatter is a rebranding of the group DarkSide, which went offline after losing control of their infrastructure in May 2021. These rumors are based on the design of the BlackMatter leaks site, which is similar to the now-defunct DarkSide leaks site, and by the fact that BlackMatter explicitly stated they would not target the oil and gas industry — a nod to the Colonial Pipeline breach which proved DarkSide's demise. At this time, there is no concrete evidence connecting the two and

When DarkSide went offline and their alias “darksupp” was banned from the Russian-language illicit forum XSS, the administrators seized the group's sizable deposit of 23 BTC (approximately US $911,000) and distributed it among former DarkSide partners. This is notable because such a move might have discouraged any former members of DarkSide to make substantial deposits on illicit forums, as BlackMatter did when making a BTC 4 deposit on Exploit.

blackmatter-ransomware

Image 1: Screenshot of the BlackMatter leaks site, which bares a resemblance to DarkSide’s now-defunct leaks site.

Track Ransomware Activity With Flashpoint

The data above was discovered directly through analyst research in the Flashpoint platform. Sign up for a free trial, and see firsthand how Flashpoint can help you and your organization access the most critical information affecting your industry and the security community.