BlackMatter & Haron: Evil Ransomware Newborns or Rebirths

By Lisa Vaas

Published: 2021-07-28 · Archived: 2026-04-05 20:00:39 UTC

They're either new or old REvil & DarkSide wine in new bottles. Both have a taste for deep-pocketed targets and DarkSide-esque virtue-signaling.

So much for darkened servers at the headquarters of DarkSide or REvil ransomware groups. Turns out, we've got either their rebranded versions or two new ransomware gangs to contend with.

The first new group to appear this month was Haron, and the second is named BlackMatter. As Ars Technica's Dan Goodin points out, there may be more still out there.

They're both claiming to be focused on targets with deep pockets that can pay ransoms in the millions of dollars. They're also virtue-signaling a la DarkSide, with similar language about sparing hospitals, critical infrastructure, nonprofits, etc.

BlackMatter also promised free decryption if its affiliates screw up and kill kittens or freeze files at, say, pipeline companies, as happened when Colonial Pipeline was attacked by DarkSide in May.

Haron & Its Cut-and-Paste Ransom Note

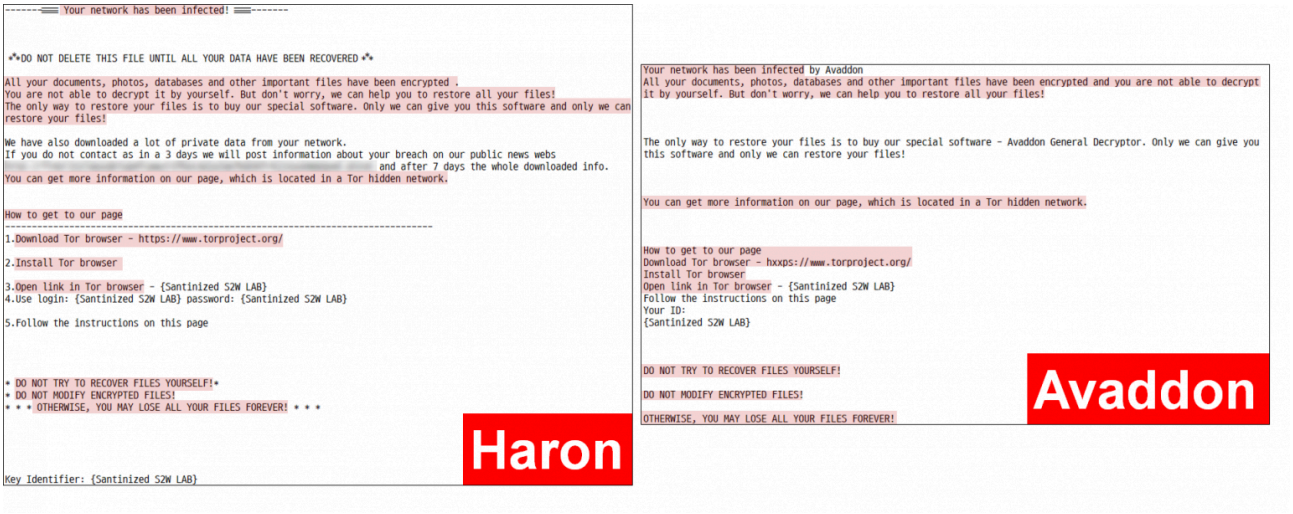
The first sample of the Haron malware was submitted to VirusTotal on July 19. Three days later, the South Korean security firm S2W Lab reported on the group in a post that laid out similarities between Haron and Avaddon.

Avaddon is yet another prolific ransomware-as-a-service (RaaS) provider that evaporated in June rather than face the legal heat that followed Colonial Pipeline and other big ransomware attacks. At the time, Avaddon released its decryption keys to BleepingComputer – 2,934 in total – with each key belonging to an individual victim. According to law enforcement, the average extortion fee Avaddon demanded was about $40,000, meaning the ransomware operators and their affiliates quit and walked away from millions.

Or Did They?

In its July 22 post, S2W Lab said that when infected with Haron ransomware, "the extension of the encrypted file is changed to the victim's name." Haron is also similar to Avaddon ransomware in that its operators are using a ransom note and operating their own leak site. In its post, S2W provided side-by-side images of ransom notes from the two gangs.

As you can see below, the two ransom notes read like a cut-and-paste job. S2W Lab noted that the main difference is that Haron suggests a specific ID and Password for victims to log in to the negotiation site.



Ransom notes from Avaddon and Haron. Source: S2W Lab.

There are loads of other similarities between Haron and Avaddon, including:

- Yet more cut-and-paste verbiage on the two negotiation sites.
- Nearly identical appearances of the negotiation sites, besides the ransomware name of “Avaddon” being swapped for “Haron.”
- Identical chunks of open-source JavaScript code used for chat that was previously published on a Russian developer forum.
- The two leak sites share the same structure.

If Haron is Avaddon reborn, the new bottles for the old wine include a strategy to induce negotiations by setting a time for the next data update. Another difference: no triple-threat play to be seen from Haron, at least not yet. In triple-threat attacks, not only is data encrypted locally and exfiltrated before the ransom demand is made, but recalcitrant victims are also subjected to threats of distributed denial-of-service (DDoS) attack until they yield.

Also, Haron has shrunk the negotiation time to six days, whereas Avaddon allotted 10 days for negotiation. Another difference is in the engines running the two ransomwares: S2W Lab said that Haron is running on the Thanos ransomware – a “Ransomware Affiliate Program,” similar to a ransomware-as-a-service (RaaS), that’s been sold since 2019 – whereas Avaddon was written in C++.

None of the similarities are solid proof of Avaddon having risen from the ashes like a ransomware phoenix: They could simply point to one or more threat actors from Avaddon working on a reboot, or they could point to nothing at all.

“It is difficult to conclude that Haron is a re-emergence of Avaddon based on our analysis,” according to S2W’s writeup, which pointed out that “Avaddon developed and used their own C++ based ransomware,” whereas the publicly available Thanos ransomware that Haron is using is baked on C#.

SentinelOne's Jim Walter told Ars that he's seen what look like similarities between Avaddon and Haron samples, but he'll know more soon.

As of July 22, Haron's leak site had only disclosed one victim.

BlackMatter

The second ransomware newbie calls itself BlackMatter. News about the new network was reported on Tuesday by security firm Recorded Future – which labeled it a successor to DarkSide and REvil – and by its news arm, The Record. Risk intelligence firm Flashpoint also spotted the newcomer, noting that BlackMatter registered an account on the Russian-language underground forums XSS and Exploit on July 19 and deposited 4 bitcoins (approximately $150,000 USD as of Wednesday afternoon) into its Expoit escrow account.

Both of those forums banned ransomware discussion in May, following DarkSide's attack on Colonial Pipeline. In the wake of that catastrophic shutdown, which sparked gas hoarding along the East coast and an emergency order from the federal government, REvil instituted pre-moderation for its partner network, saying that it would ban any attempt to attack any government, public, educational or healthcare organizations.

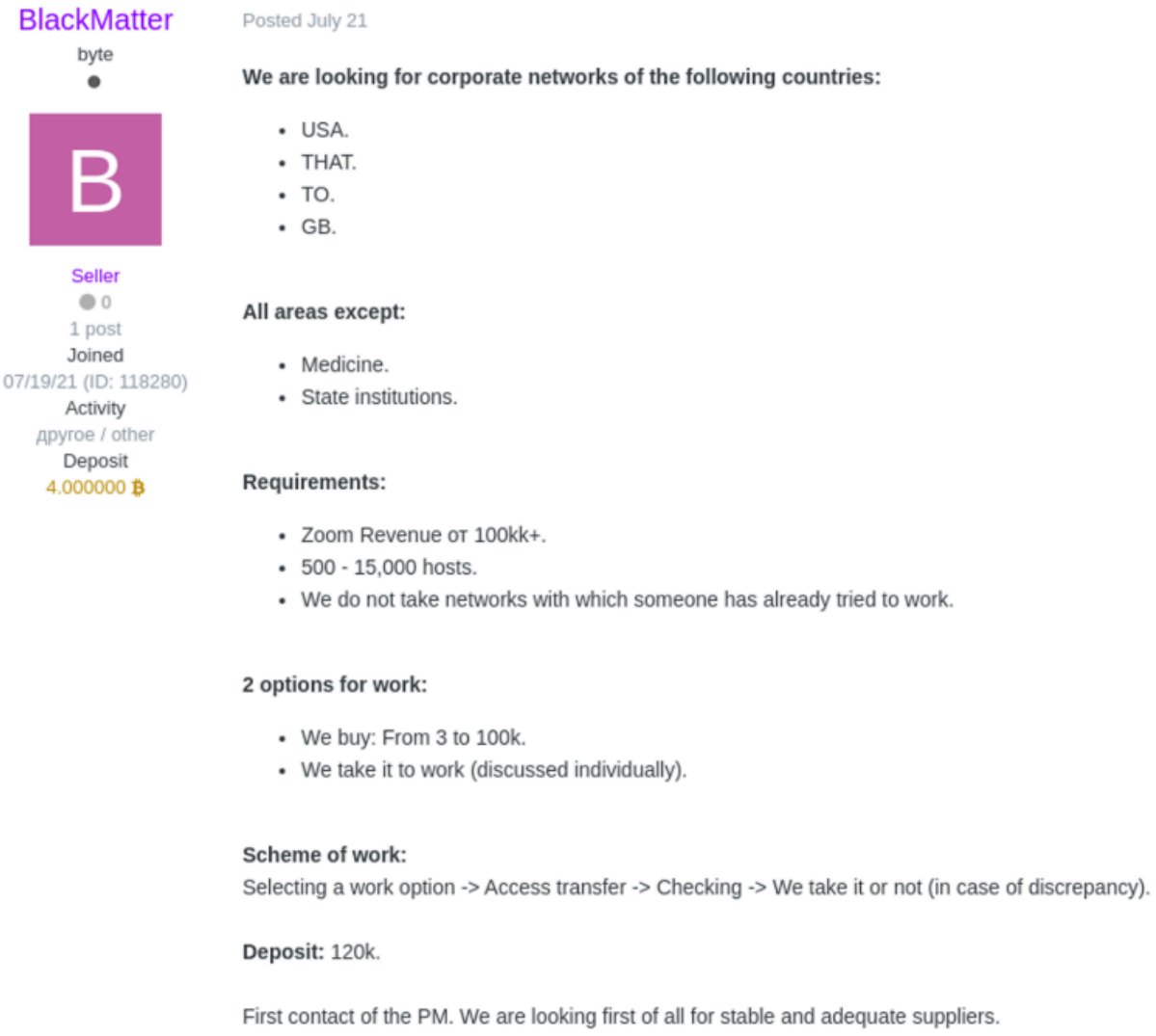
Referring to DarkSide's experience, REvil's backers said that the group was "forced to introduce" these "significant new restrictions," promising that affiliates that violated the new rules would be kicked out and that it would give out decryption tools for free.

Flashpoint noted that the large deposit on the Exploit forum shows that BlackMatter is serious.

On July 21, the threat actor said that the network is looking to buy access to affected networks in the U.S., Canada, Australia, and the UK, presumably for ransomware operations. It's offering up to $100,000 for network access, as well as a cut of the ransom take.

Putting Up Big Money for Big Fish

BlackMatter is putting up big money because it's after big fish. The group said that it was looking for deep-pocketed organizations with revenues of more than $100 million: the size of organizations that could be expected to pay big ransoms. The threat actor is also requiring that targets have 500-15,000 hosts in their networks. It's also up for all industries, except for healthcare and governments.



BlackMatter
byte
B
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 от 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.

BlackMatter ad on the Exploit underground forum. Source: Recorded Future.

‘We Are Ethical Blood Suckers’

That’s where the virtual signaling comes in. The Record reports that BlackMatter’s leak site is currently empty, which means that BlackMatter only launched this week and hasn’t yet carried out any network penetrations.

When it does go after victims, the list won’t include a roster of target types that is currently, supposedly, taboo to target. A section of BlackMatter’s leak site lists the type of targets that are off-limits, including:

- 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

Sound familiar? That's because it's a dead ringer for a list formerly provided on the leak site of the DarkSide gang before it supposedly went belly-up following the Colonial attack. Promises not to attack these types of organizations aren't always adhered to by these gangs' affiliates, but BlackMatter has promised that if victims from those industries are attacked, the operators will decrypt their data for free.

Buying Legitimacy

Mike Fowler, vice president of intelligence services at GroupSense – a firm that offers threat intelligence and ransom negotiation – has been keeping an eye on BlackMatter. He told Threatpost on Wednesday that lately, there's been an evolution in tactics, techniques and processes (TTP) used by emerging RaaS cartels such as Hive, Grief and, most recently, BlackMatter: an evolution reminiscent of the 2020 shift to double extortion pioneered by Maze.

"GroupSense has witnessed an expected jockeying for position and brand awareness within the RaaS cartels," Fowler said in an email. "This was clearly evidenced by BlackMatter's account registration on the top two cybercrime forums. Their deposit of 4 Bitcoins into their escrow account on the largest Russian cybercrime forum, Exploit, is clearly an attempt to purchase legitimacy."

Careful Victim Targeting

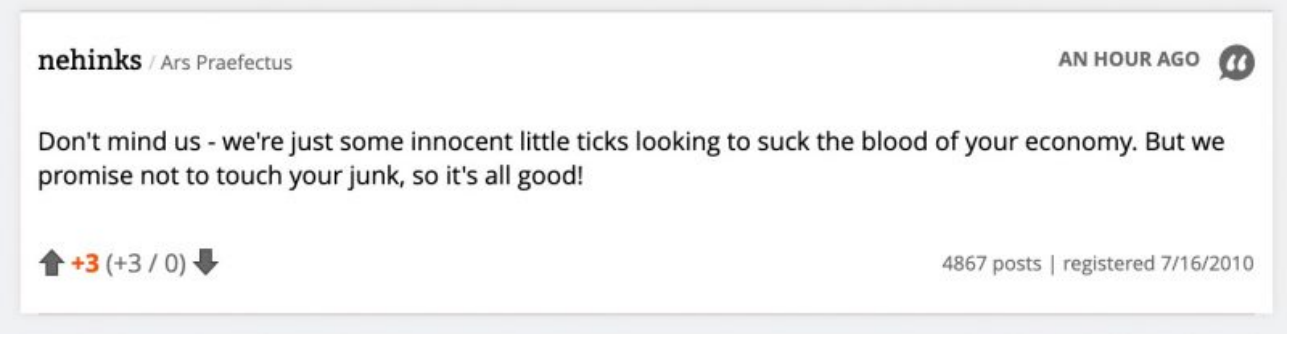
Digital Shadows' Sean Nikkel told Threatpost on Wednesday that the careful selection of big companies reflects the increasing number of threat actors that are "doing their due diligence" when it comes to selecting victims.

"We've seen time and again when they have some knowledge around key personalities within an organization, revenue, size, and even customers, so the idea of big game hunting seems to be in line with observed ransomware trends," Nikkel said via email.

He called the virtue signaling and promise to do right by the exempted industries an "interesting twist."

"While REvil had publicly stated that everything was fair game previously, maybe this cooling-off period from previous attention has forced a change of heart, if it is indeed them coming back," Nikkel added.

"Interesting" is one way to frame it. Another way to look at it is as squeaking from blood-sucking parasites, as a commenter on Ars' coverage suggested:



Neither was GroupSense's Fowler impressed by BlackMatter's "pinky promise" not to victimize certain business segments. He said it rings particularly hollow "given their rise to prominence as REvil's standing as the #2 RaaS

fades into obscurity."

Still, to put it all into perspective, while BlackMatter is "the flavor of the day," Fowler says that other RaaS services, such as Conti, Grief, Hive and LockBit, are "just as big a threat."

Ransomware Phoenixes or New Ratbags? Time Will Tell

Dirk Schrader, global vice president of security research at New Net Technologies (NNT), told Threatpost on Wednesday that anybody who didn't see REvil or DarkSide re-emerging might not have their head screwed on right. There's a "good chance" that REvil decided proactively "to take down everything and to re-emerge, just to make tracking and tracing even more difficult," he added in an email.

Meanwhile, whatever sabre-rattling the Biden administration has been doing at Russia or China about kinetic responses and hack-backs won't change the situation, Schrader predicted. As it is, the threat actors are refining their approaches to look at targets that have "a higher motivation" to pay ransom, cases in point being Kaseya and SolarWinds.

"Ransomware groups will continue to look for attack vectors that are likely to have a higher motivation for payment, and that is the next evolution in this business," Schrader said via email. "We already see the early effects. Kaseya, SolarWinds, tools that promise access to high-value assets, where an organization's revenue stream and reputation depends on."

Schrader thinks that VMware's recently added capability of encrypting EXSi servers is "a harbinger of what will come," pointing to CISA's recent alert about the top routinely exploited vulnerabilities, which included a warning about CVE-2021-21985: the critical remote code execution (RCE) vulnerability in VMware vCenter Server and VMware Cloud Foundation.

"In essence, not paying a ransom is the only angle that will – over time – eradicate ransomware," Schrader said. "And to be positioned for that, companies will have to minimize and protect their attack surface, harden their systems and infrastructure, manage existing accounts properly and delete old ones, patch vulnerabilities according to risks, and be able to operate in a cyber-resilient manner when under attack."

Where's the MBA Coursework About Ransomware?

GroupSense's Fowler said that the focus has to be on prevention and mitigation before ransomware is deployed. But what about after? "Ransomware attacks are a cyber issue up to the point that the ransomware is executed," he pointed out. "Then it becomes a business issue, and this presents business considerations and continuity hurdles not part of the curriculum on any MBA course I'm familiar with currently."

072821 16:28 UPDATE: Added input from Mike Fowler.

first. Join host Becky Bracken and Uptycs researchers Amit Malik and Ashwin Vamshi on **Aug. 17 at 11 AM EST for this LIVE discussion**.
