BlackMatter Under the Lens: An Emerging Ransomware Group Looking for Affiliates

blog.cyble.com/2021/08/05/blackmatter-under-the-lens-an-emerging-ransomware-group-looking-for-affiliates/

August 5, 2021

A new ransomware group is emerging on the darkweb, looking for affiliates to start its operations. This group calls itself BlackMatter and has posted ads on two cybercrime forums named Exploit[.]in, and XSS[.]is. The BlackMatter ransomware group is seeking cybercriminals already having access to the potential target's networks. In RaaS, the ransomware group creates ransomware and a platform to manage the possible targets and victims.

Category	Surface Web
Risk Score	High
TLP Rating	White
APT Group	N/A
Threat Name	BlackMatter
Target	Firms with revenue of $100 Million and more
Affected Region	United States of America, Canada, Australia, and Great Britain.
Threat Description	New ransomware group looking for affiliates for ransomware operations.

BlackMatter Threat Summary (Available to enterprise customers since July 21)

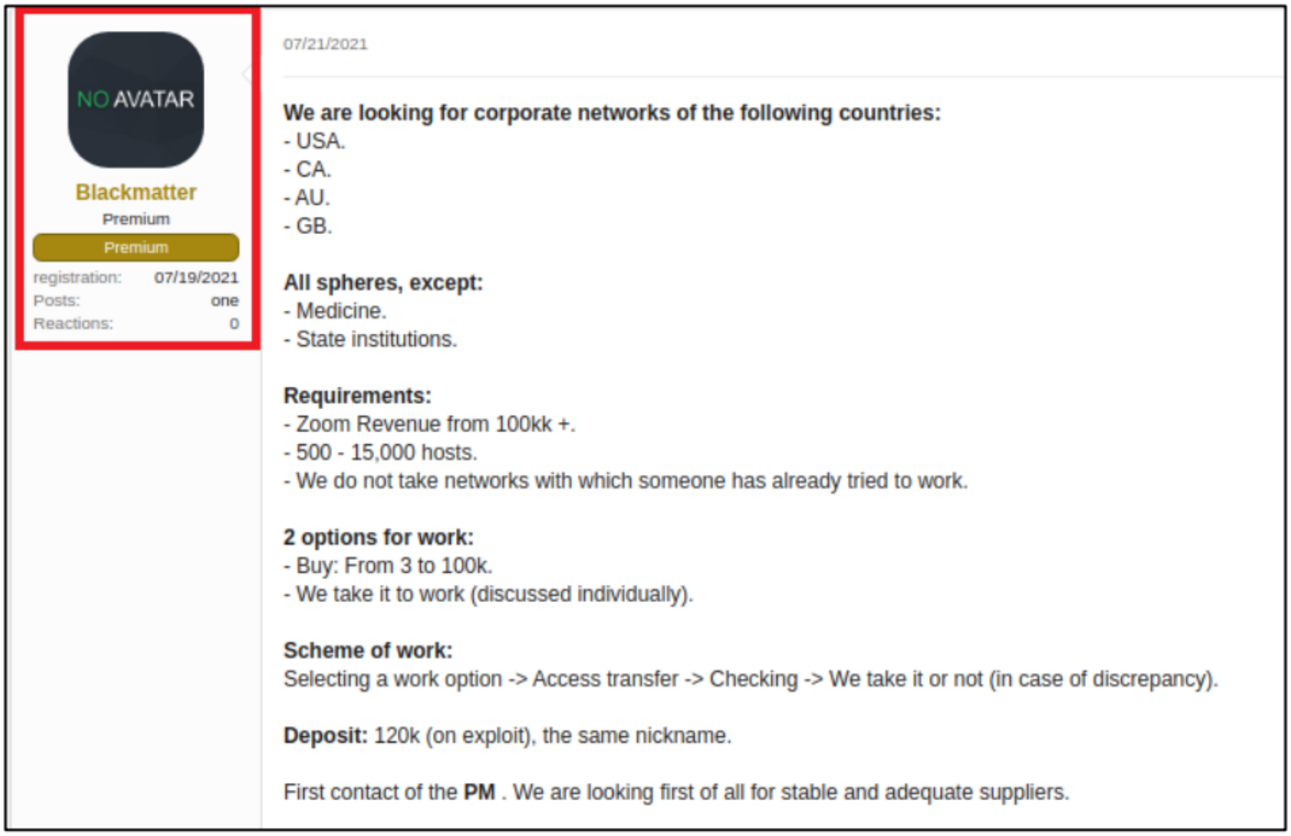
Technical Analysis:

Cyble Research Labs found the post on XSS[.]is by the threat actor named BlackMatter, as shown in Figure 1. In the post, the TA has mentioned the conditions required for affiliates to join them, which are as follows:

> Corporate Networks should be from one of the following countries: the United States of America, Canada, Australia, and Great Britain.
>
> They are targeting all organizations except the medical industry and government institutions.

The revenue of the target organization should be more than $100 million and should be having 500-1500 hosts.

The networks on which other actors have already tried attacks are excluded from the target list.



Blackmatter
Premium
Premium

registration:	07/19/2021
Posts:	one
Reactions:	0

07/21/2021

We are looking for corporate networks of the following countries:
- USA.
- CA.
- AU.
- GB.

All spheres, except:
- Medicine.
- State institutions.

Requirements:
- Zoom Revenue from 100kk +.
- 500 - 15,000 hosts.
- We do not take networks with which someone has already tried to work.

2 options for work:
- 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).

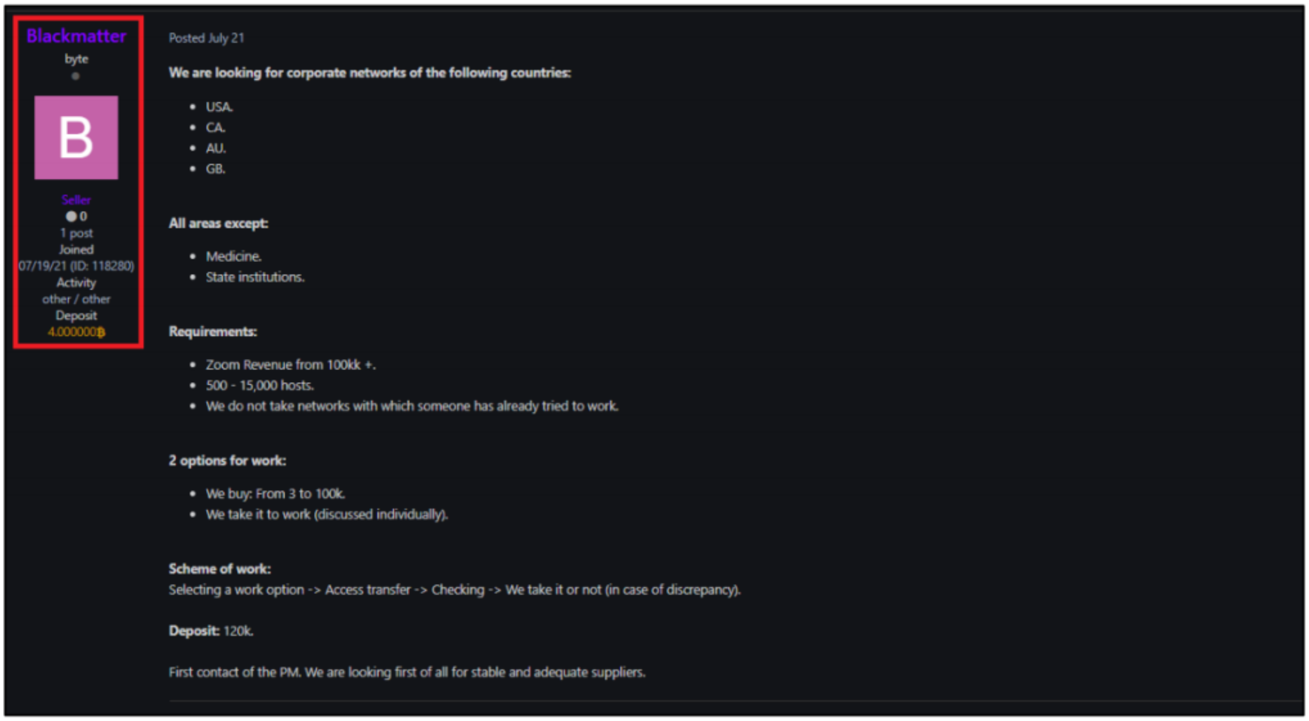
Deposit: 120k (on exploit), the same nickname.

First contact of the **PM** . We are looking first of all for stable and adequate suppliers.

Figure 1 BlackMatter group posted an ad for affiliates posted on XSS.is

The TA has given two options for affiliation. The first option offers to buy network access for an amount ranging from $3k to $100k. In the second option, affiliates may work with the group in place of a percentage in ransom. Once the affiliates are selected, they need to deposit $120,000 to the group to participate in their ransomware activity.

The TA has posted a similar threat post on another cybercrime forum named Exploit[.]in. The TA post is shown in Figure 2.



Blackmatter
byte

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

Posted July 21

We are looking for corporate networks of the following countries:

- USA.
- CA.
- AU.
- GB.

All areas except:

- Medicine.
- State institutions.

Requirements:

- Zoom Revenue from 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).

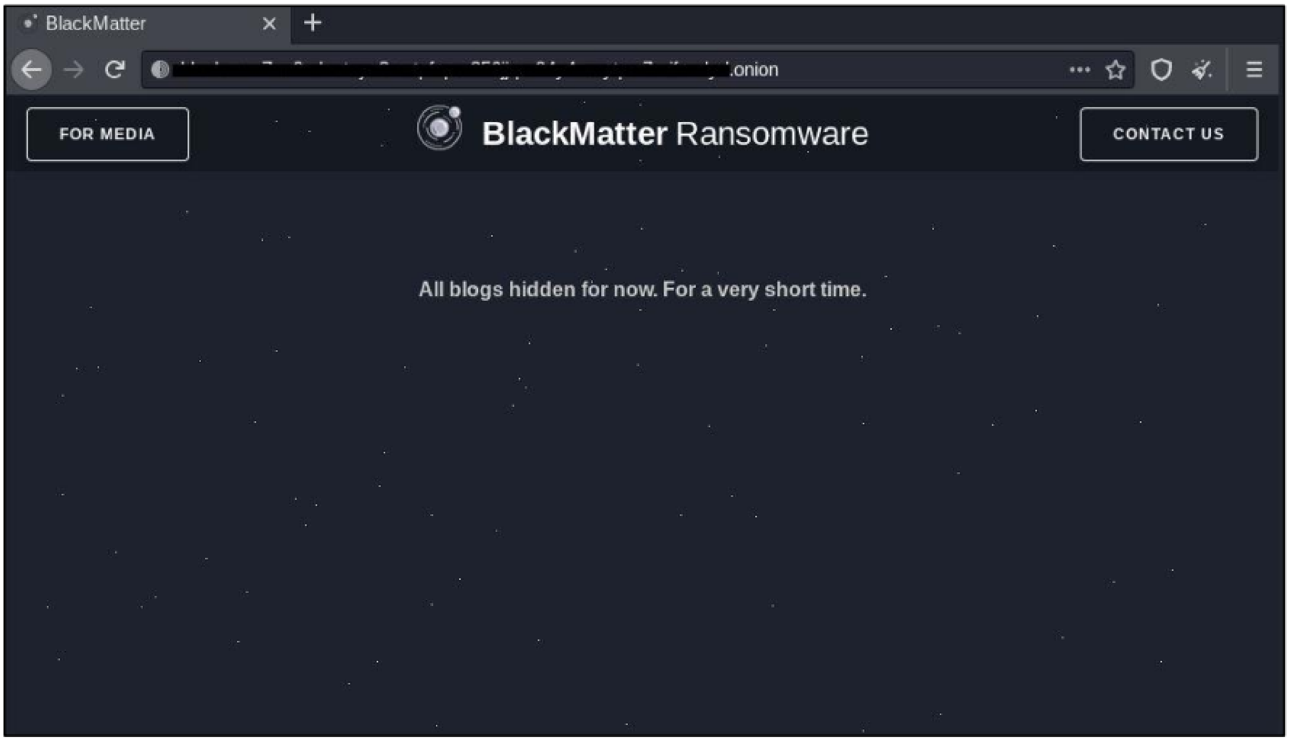
Scheme of work:
Selecting a work option -> Access transfer -> Checking -> We take it or not (in case of discrepancy).

Deposit: 120k.

First contact of the PM. We are looking first of all for stable and adequate suppliers.

Figure 2 BlackMatter group posted an ad for affiliates posted on Exploit[.]in

We found that the leak website of the BlackMatter ransomware group is hosted in the TOR network (Figure 3). The Home page shows buttons for media updates and contact. The Home page displays the message, “All blogs hidden for now. For a very short time.” It indicates that the group has started its operations.



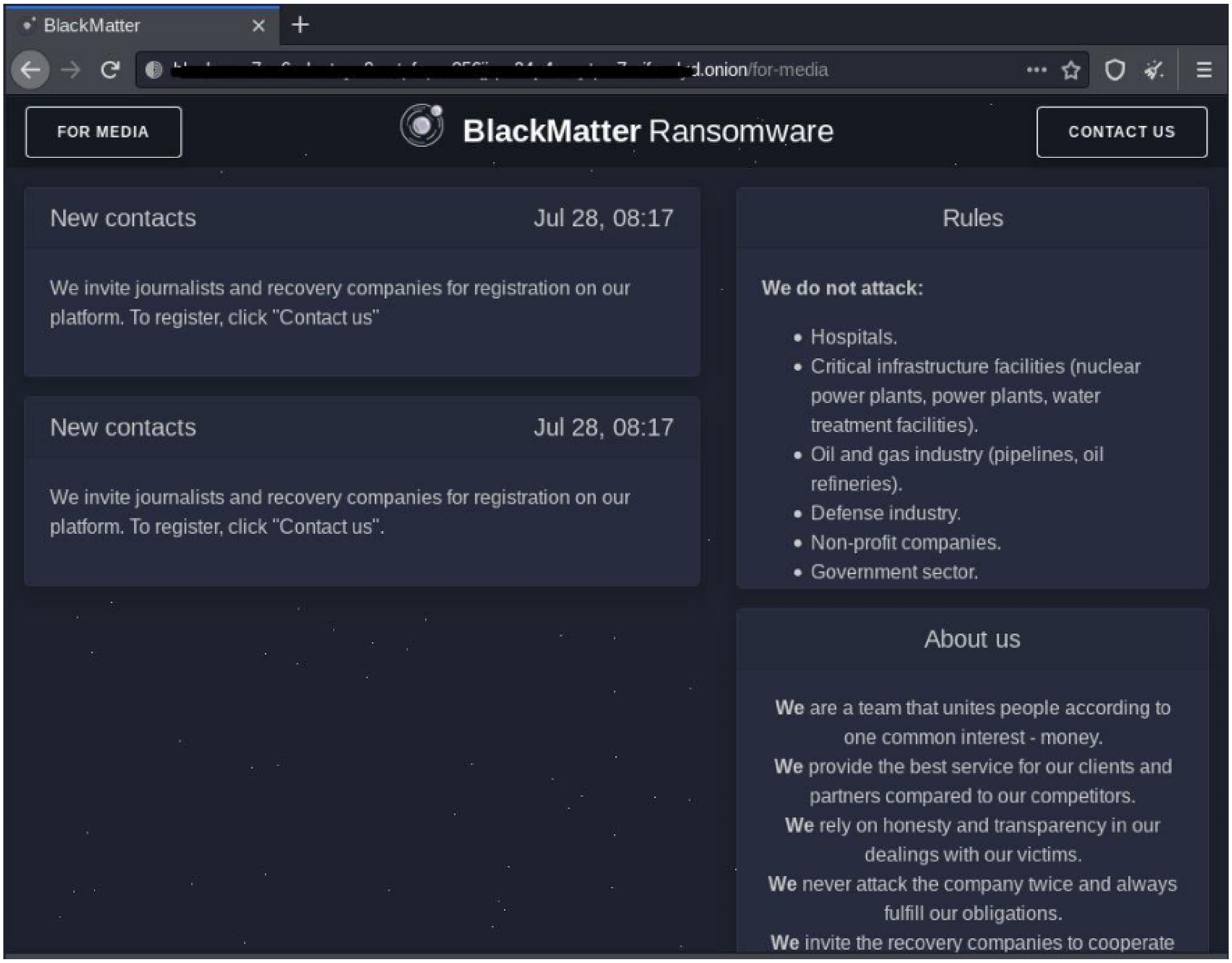
All blogs hidden for now. For a very short time.

Figure 3: Home page of the BlackMatter Ransomware.

When we clicked on the button for media updates, we were redirected to the Media page, as shown in Figure 4. It also displays information such as excluded targets and messages to the media. Following is the list of excluded targets:

- 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.

Referring to the above list, we can say that the ransomware group is targeting private organizations so that they can continue their operations without getting media attention. We can imply that attackers are aware of the consequences of compromising highly sensitive targets. Based on rules and about us information given on the BlackMatter ransomware leak website, we suspect that this group has close connections with the DarkSide ransomware group. We presume that the group is only interested in the money.



New contacts Jul 28, 08:17

We invite journalists and recovery companies for registration on our platform. To register, click "Contact us"

New contacts Jul 28, 08:17

We invite journalists and recovery companies for registration on our platform. To register, click "Contact us".

Rules

We do not attack:

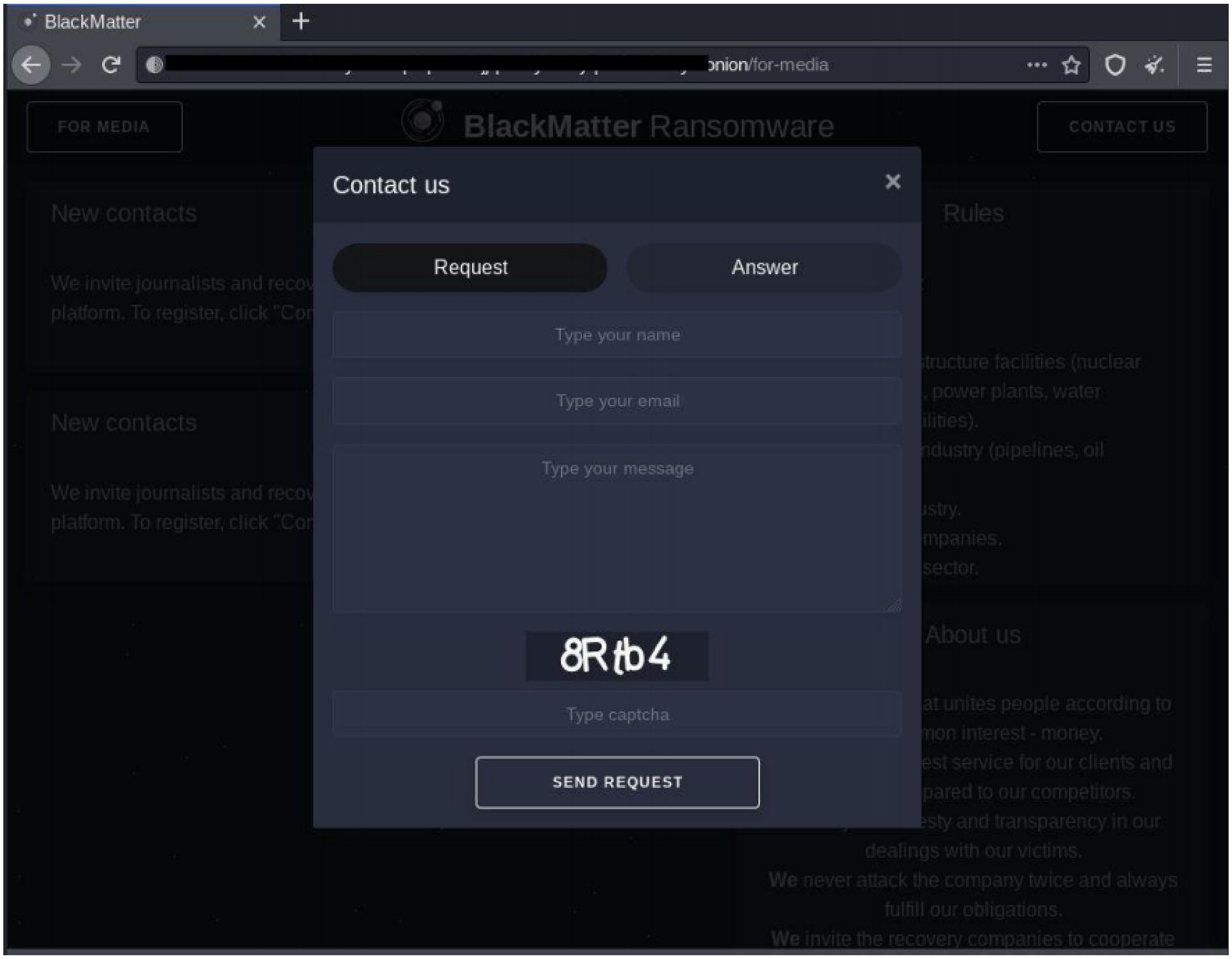
- Hospitals.
- Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities).
- Oil and gas industry (pipelines, oil refineries).
- Defense industry.
- Non-profit companies.
- Government sector.

About us

We are a team that unites people according to one common interest - money.
We provide the best service for our clients and partners compared to our competitors.
We rely on honesty and transparency in our dealings with our victims.
We never attack the company twice and always fulfill our obligations.
We invite the recovery companies to cooperate

Figure 4 Media page of the BlackMatter Ransomware group.

Figure 4 shows the contact page of the BlackMatter Ransomware through which people can contact the ransomware group.



We invite journalists and recov
platform. To register, click "Co

We invite journalists and recov
platform. To register, click "Co

tructure facilities (nuclear
, power plants, water
ilities).
ndustry (pipelines, oil

istry.
mpanies.
sector.

at unites people according to
mon interest - money.
est service for our clients and
pared to our competitors.
esty and transparency in our
dealings with our victims.
We never attack the company twice and always
fulfill our obligations.
We invite the recovery companies to cooperate

Figure 5 Contact page of the BlackMatter Ransomware.

Conclusion:

The BlackMatter ransomware group tries to gain access to critical servers from other threat actors in order to launch its campaign. Organizations should perform security scanning and immediate patching of known vulnerabilities using various processes such as Vulnerability Assessment and Penetration Testing (VAPT), Red teaming, and Purple teaming.

Cyble Research Labs is continuously monitoring BlackMatter activities. We will keep informing our clients with recent updates about this campaign.

Our Recommendations:

Use strong passwords and enforce multi-factor authentication wherever possible.

Turn on the automatic software update feature on your computer, mobile, and other connected devices wherever possible and pragmatic.

Use a reputed anti-virus and internet security software package on your connected devices, including PC, laptop, and mobile.

Refrain from opening untrusted links and email attachments without verifying their authenticity.

About Us

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups To Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com.