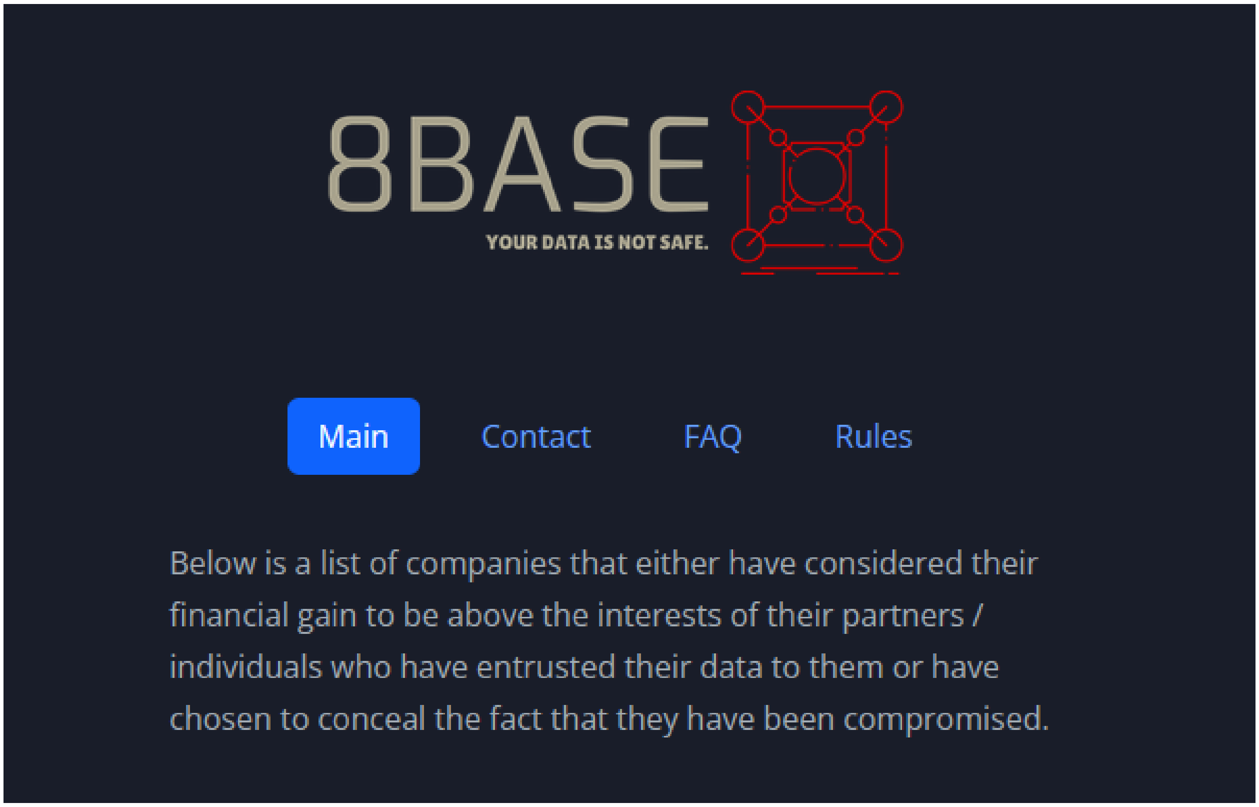
Who’s Behind the 8Base Ransomware Website?

krebsonsecurity.com/2023/09/whos-behind-the-8base-ransomware-website/

The victim shaming website operated by the cybercriminals behind **8Base** — currently one of the more active ransomware groups — was until earlier today leaking quite a bit of information that the crime group probably did not intend to be made public. The leaked data suggests that at least some of website’s code was written by a 36-year-old programmer residing in the capital city of Moldova.



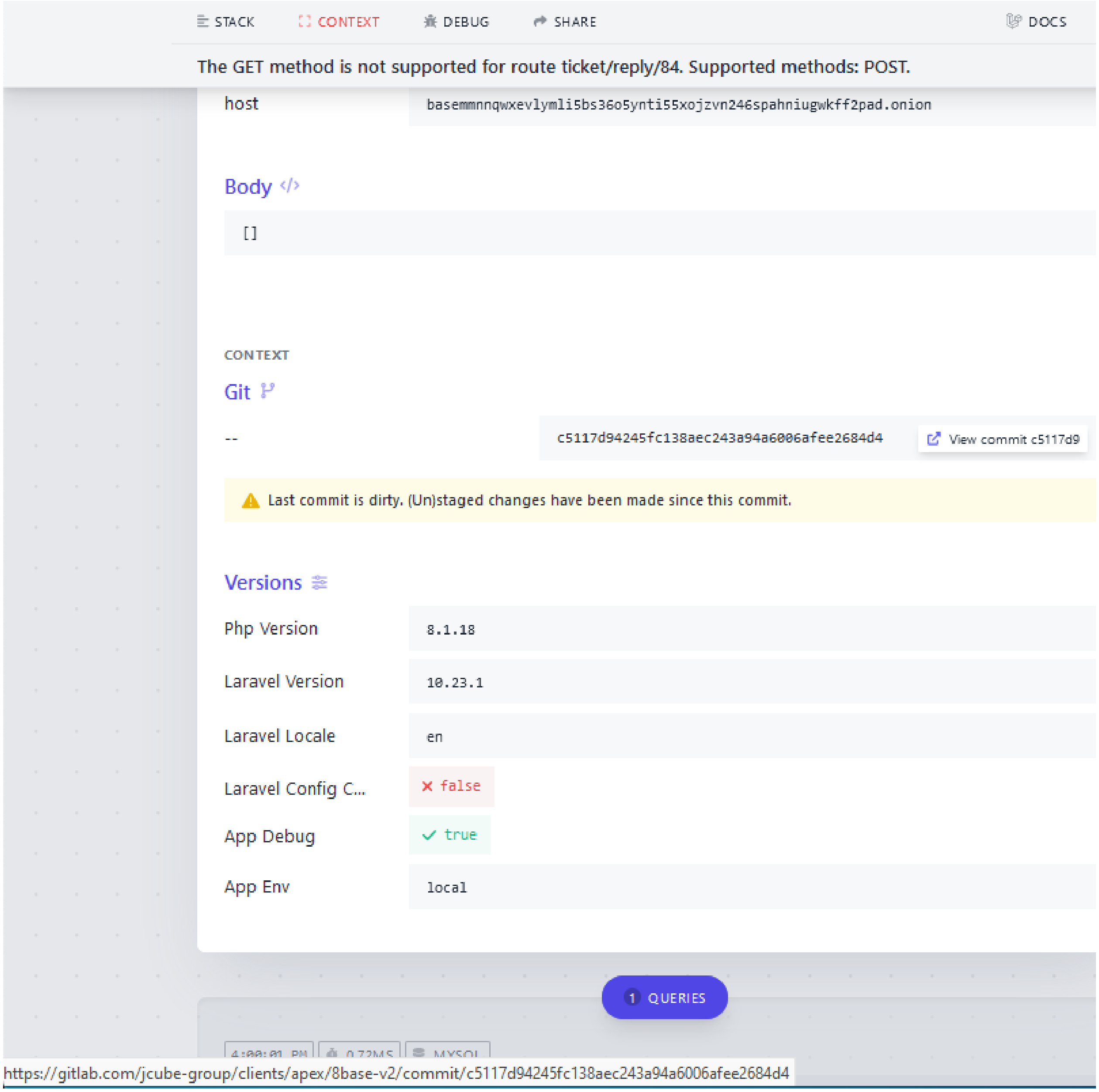
Below is a list of companies that either have considered their financial gain to be above the interests of their partners / individuals who have entrusted their data to them or have chosen to conceal the fact that they have been compromised.

The 8Base ransomware group’s victim shaming website on the darknet.

8Base maintains a darknet website that is only reachable via Tor, a freely available global anonymity network. The site lists hundreds of victim organizations and companies — all allegedly hacking victims that refused to pay a ransom to keep their stolen data from being published.

The 8Base darknet site also has a built-in chat feature, presumably so that 8Base victims can communicate and negotiate with their extortionists. This chat feature, which runs on the Laravel web application framework, works fine as long as you are *sending* information to the site (i.e., by making a “POST” request).

However, if one were to try to fetch data from the same chat service (i.e., by making a “GET” request), the website until quite recently generated an extremely verbose error message:



The GET method is not supported for route ticket/reply/84. Supported methods: POST.

host basemmnnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad.onion

Body

```
[]
```

CONTEXT

Git

-- c5117d94245fc138aec243a94a6006afee2684d4 View commit c5117d9

Last commit is dirty. (Un)staged changes have been made since this commit.

Versions

Php Version 8.1.18

Laravel Version 10.23.1

Laravel Locale en

Laravel Config C... ✗ false

App Debug ✓ true

App Env local

https://gitlab.com/jcube-group/clients/apex/8base-v2/commit/c5117d94245fc138aec243a94a6006afee2684d4

The verbose error message when one tries to pull data from 8Base's darknet site. Notice the link at the bottom of this image, which is generated when one hovers over the "View commit" message under the "Git" heading.

That error page revealed the true Internet address of the Tor hidden service that houses the 8Base website: 95.216.51[.]74, which according to DomainTools.com is a server in Finland that is tied to the Germany-based hosting giant Hetzner.

But that's not the interesting part: Scrolling down the lengthy error message, we can see a link to a private Gitlab server called Jcube-group: **gitlab[.]com/jcube-group/clients/apex/8base-v2**. Digging further into this Gitlab account, we can find some curious data points available in the JCube Group's public code repository.

For example, this “status.php” page, which was committed to JCube Group’s Gitlab repository roughly one month ago, includes code that makes several mentions of the term “KYC” (e.g. KYC_UNVERIFIED, KYC_VERIFIED, and KYC_PENDING).

This is curious because a FAQ on the 8Base darknet site includes a section on “special offers for journalists and reporters,” which says the crime group is open to interviews but that journalists will need to prove their identity before any interview can take place. The 8base FAQ refers to this vetting process as “KYC,” which typically stands for “Know Your Customer.”

“We highly respect the work of journalists and consider information to be our priority,” the 8Base FAQ reads. “We have a special program for journalists which includes sharing information a few hours or even days before it is officially published on our news website and Telegram channel: you would need to go through a KYC procedure to apply. Journalists and reporters can contact us via our PR Telegram channel with any questions.”

basemmnnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad.onion/faq/44
gitlab.com/jcubegroup/jcube-core-v2/-/blob/main/src/Constants/Status.ph

The 8Base FAQ (left) and the KYC code in Kolev’s Gitlab account (right)

The 8Base darknet site also has a publicly accessible “admin” login page, which features an image of a commercial passenger plane parked at what appears to be an airport. Next to the airplane photo is a message that reads, “Welcome to 8Base. Admin Login to 8Base dashboard.”

The login page on the 8Base ransomware group's darknet website.

Right-clicking on the 8Base admin page and selecting "View Source" produces the page's HTML code. That code is virtually identical to a "login.blade.php" page that was authored and committed to JCube Group's Gitlab repository roughly three weeks ago.

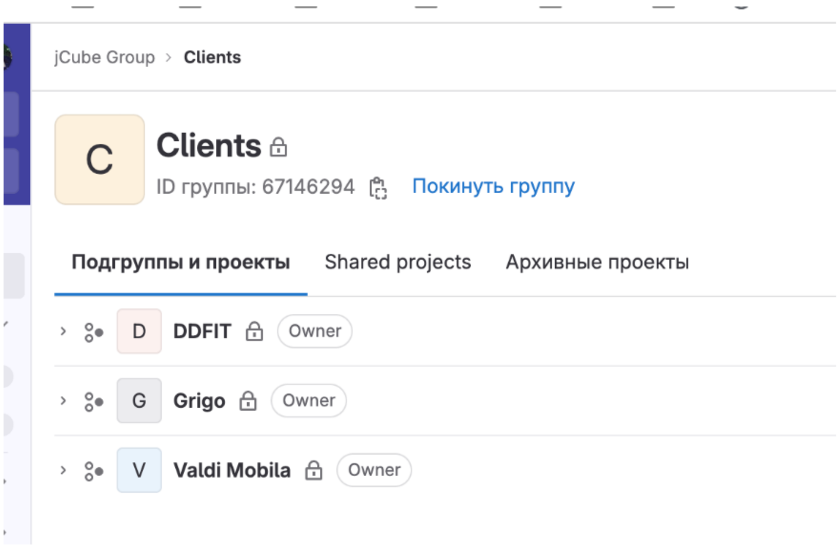
It appears the person responsible for the JCube Group's code is a 36-year-old developer from Chisinau, Moldova named **Andrei Kolev**. Mr. Kolev's LinkedIn page says he's a full-stack developer at JCube Group, and that he's currently looking for work. The homepage for Jcubegroup[.]com lists an address and phone number that Moldovan business records confirm is tied to Mr. Kolev.

The posts on the Twitter account for Mr. Kolev (@andrewkolev) are all written in Russian, and reference several now-defunct online businesses, including pluginspro[.]ru.

Reached for comment via LinkedIn, Mr. Kolev said he had no idea why the 8Base darknet site was pulling code from the "clients" directory of his private JCube Group Gitlab repository, or how the 8Base name was even included.

"I [don't have] a clue, I don't have that project in my repo," Kolev explained. "They [aren't] my clients. Actually we currently have just our own projects."

Mr. Kolev shared a screenshot of his current projects, but very quickly after that deleted it. However, KrebsOnSecurity captured a copy of the image before it was removed:



jCube Group › Clients

C

Clients

ID группы: 67146294

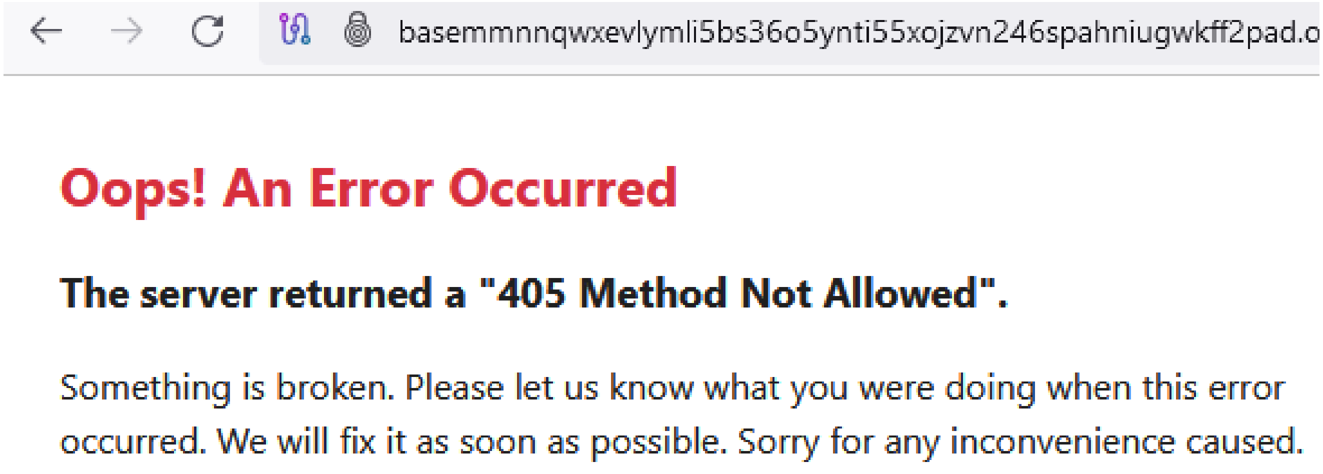
Покинуть группу

Подгруппы и проекты | Shared projects | Архивные проекты

- D DDFIT Owner
- G Grigo Owner
- V Valdi Mobila Owner

A screenshot of Mr. Kolev's current projects that he quickly deleted.

Within minutes of explaining why I was reaching out to Mr. Kolev and walking him through the process of finding this connection, the 8Base website was changed, and the error message that linked to the JCube Group private Gitlab repository no longer appeared. Instead, trying the same "GET" method described above caused the 8Base website to return a "405 Method Not Allowed" error page:



basemmnnqwxevlymli5bs36o5ynti55xojzvn246spahniugwkff2pad.o

Oops! An Error Occurred

The server returned a "405 Method Not Allowed".

Something is broken. Please let us know what you were doing when this error occurred. We will fix it as soon as possible. Sorry for any inconvenience caused.

Mr. Kolev claimed he didn't know anything about the now-removed error page on 8Base's site that referenced his private Gitlab repo, and said he deleted the screenshot from our LinkedIn chat because it contained private information.

Ransomware groups are known to remotely hire developers for specific projects without disclosing exactly who they are or how the new hire's code is intended to be used, and it is possible that one of Mr. Kolev's clients is merely a front for 8Base. But despite 8Base's statement that they are happy to correspond with journalists, KrebsOnSecurity is still waiting for a reply from the group via their Telegram channel.

The tip about the leaky 8Base website was provided by a reader who asked to remain anonymous. That reader, a legitimate security professional and researcher who goes by the handle @htmalgae on Twitter, said it is likely that whoever developed the 8Base website inadvertently left it in "development mode," which is what caused the site to be so verbose with its error messages.

"If 8Base was running the app in production mode instead of development mode, this Tor de-anonymization would have never been possible," @htmalgae said.

A recent blog post from **VMware/Carbon Black** called the 8Base ransomware group "a heavy hitter" that has remained relatively unknown despite the massive spike in activity in Summer of 2023.

"8Base is a Ransomware group that has been active since March 2022 with a significant spike in activity in June of 2023," Carbon Black researchers wrote. "Describing themselves as 'simple pen testers,' their leak site provided victim details through Frequently Asked Questions and Rules sections as well as multiple ways to contact them. "

According to VMware, what's particularly interesting about 8Base's communication style is the use of verbiage that is strikingly familiar to another known cybercriminal group: RansomHouse.

"The group utilizes encryption paired with 'name-and-shame' techniques to compel their victims to pay their ransoms," VMware researchers wrote. "8Base has an opportunistic pattern of compromise with recent victims spanning across varied industries. Despite the high amount of compromises, the information regarding identities, methodology, and underlying motivation behind these incidents still remains a mystery."

Update, Sept. 21, 10:43 a.m. ET: The author of Databreaches.net was lurking in the 8Base Telegram channel when I popped in to ask the crime group a question, and reports that 8Base did eventually reply: ""hi at the moment we r not doing interviews. we have nothing to say. we r a little busy."