

RANSOMED[.]VC - forum, ransomware or hackers?

Introduction:

Modern cybercrime is a complex and rapidly growing field that focuses not only on making a profit, but also on influencing politics and promoting ideology. Criminal groups in the cyber sphere are increasingly beginning to operate in a hierarchical manner, forming alliances and using various methods to achieve their goals. The following analysis can help us understand how these organizations are evolving and what strategies they are adopting to achieve their goals.

Description:

Ransomed[.]vc debuted as a forum for cybercriminals on 15.08.2023:

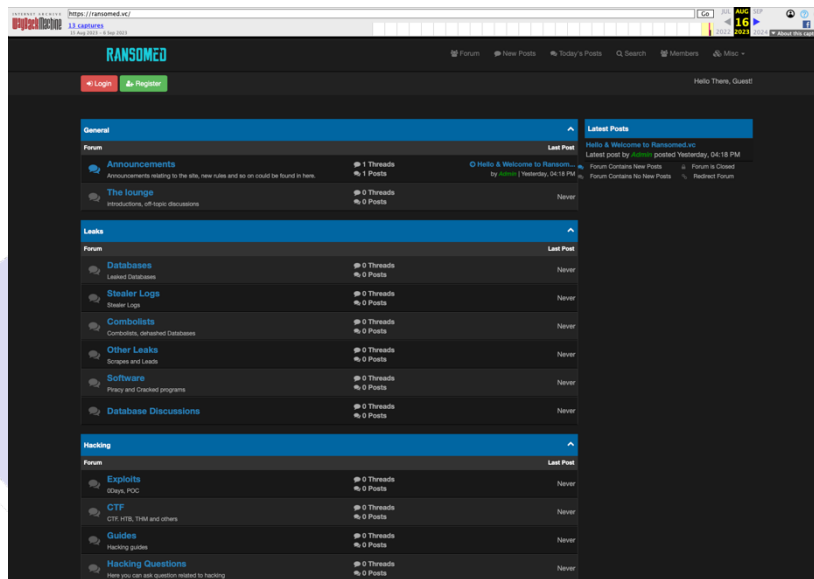


Figure 1 <https://web.archive.org/web/20230816134436/https://ransomed.vc/>

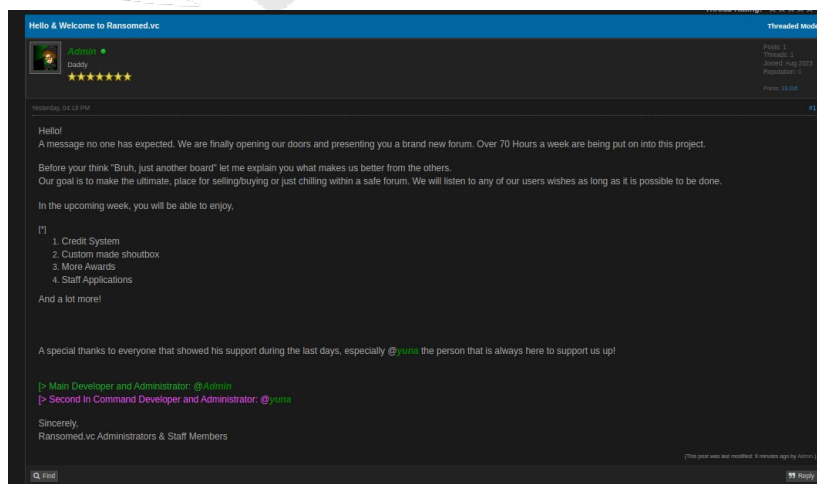


Figure 2 Source: <https://twitter.com/FalconFeedsio/status/1691764241156673677/photo/1>

In just a week (Aug. 21, 2023), the site has turned into a so-called "Victim List" - a list of companies that have fallen victim to ransomware attacks.

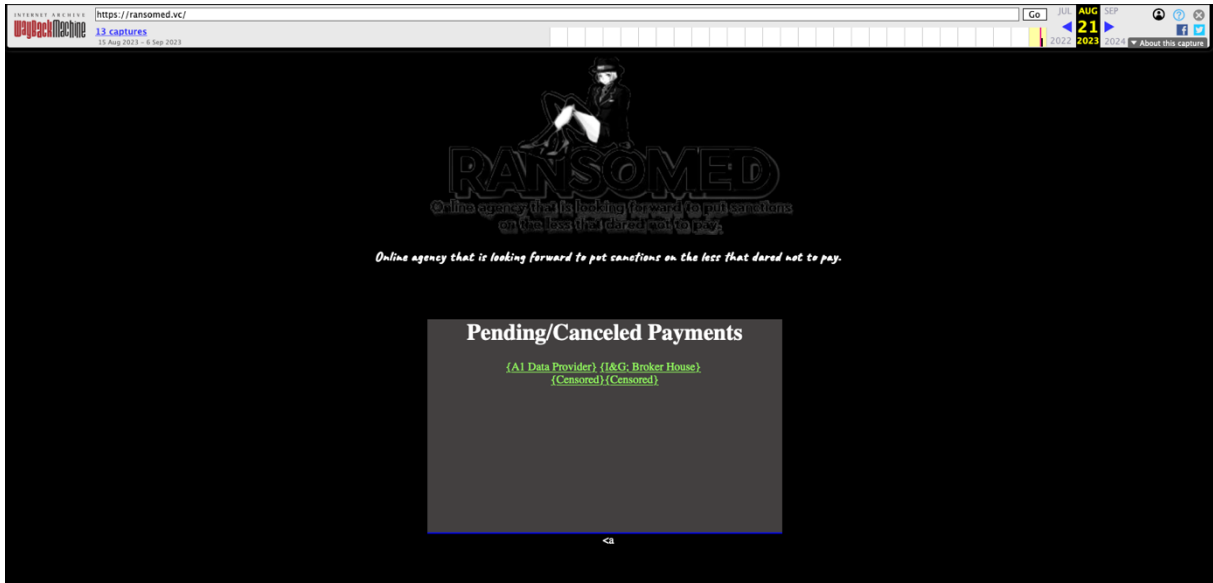


Figure 3 <https://web.archive.org/web/20230821202610/https://ransomed.vc/>

The first victims, the people behind ransommed[.]vc were the companies:

- A1 Data Provider:

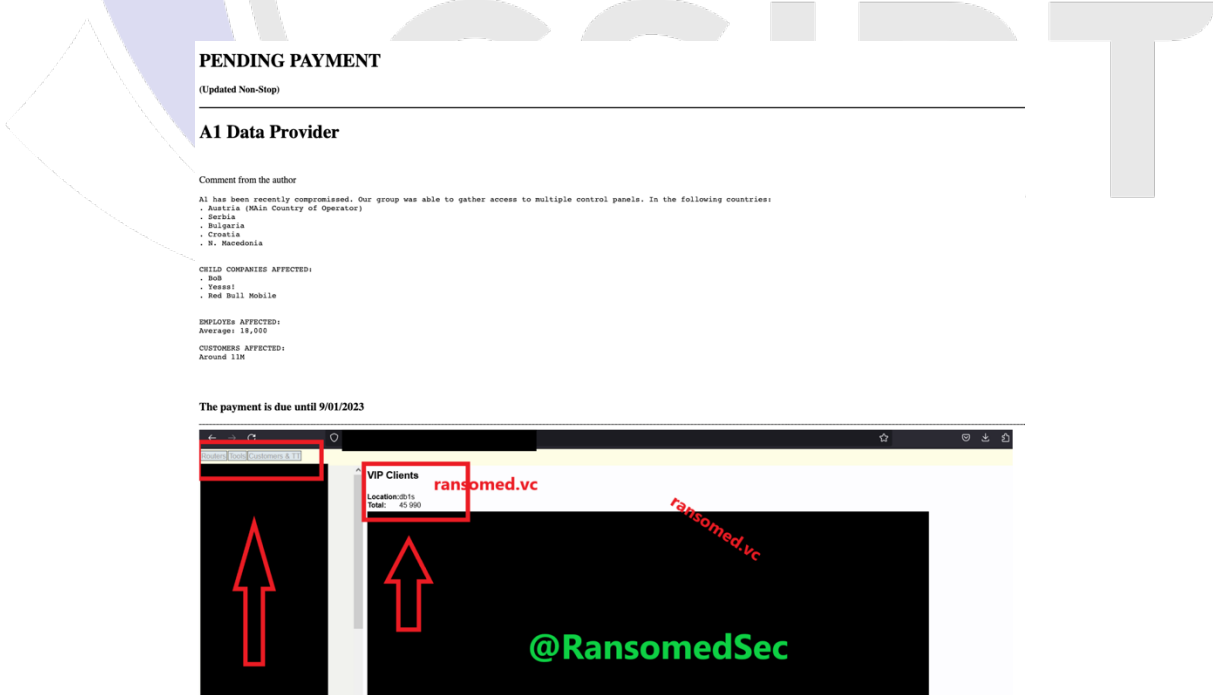


Figure 4 [https://ransomed\[.\]vc/a1.html](https://ransomed[.]vc/a1.html) (no longer active)

- I&G; Broker House:

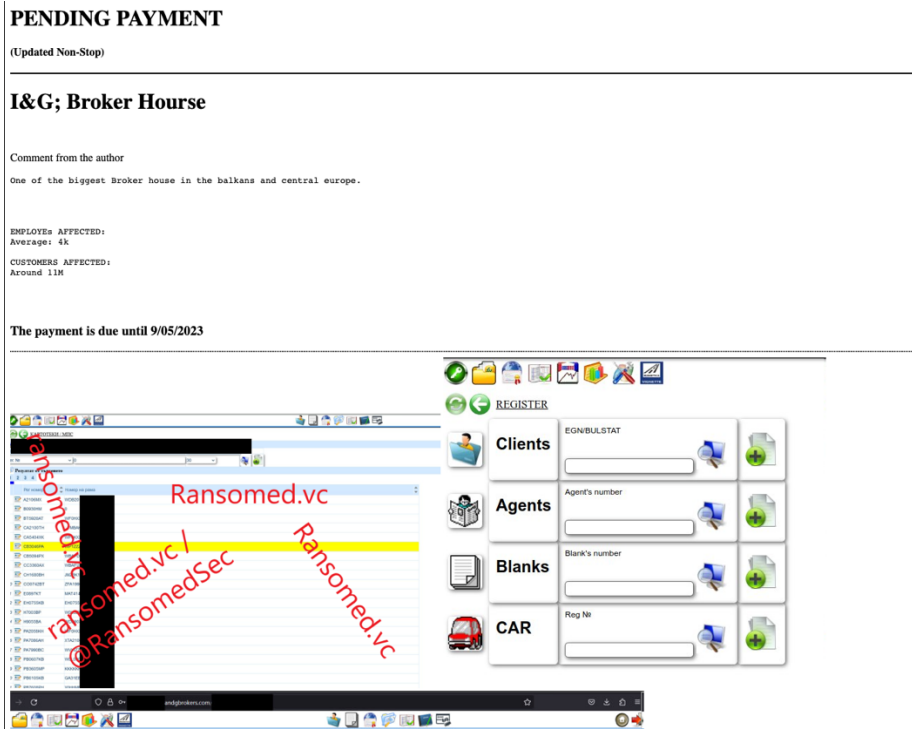


Figure 5 [https://ransomed\[.\]vc/ig.html](https://ransomed[.]vc/ig.html) (no longer active)

Over the next few days, the list of victims grew, and the ransomware group, claimed that companies were already partially paying ransoms to decrypt data:



Figure 6 Status of ransom payment by A1

Or have paid them in full:

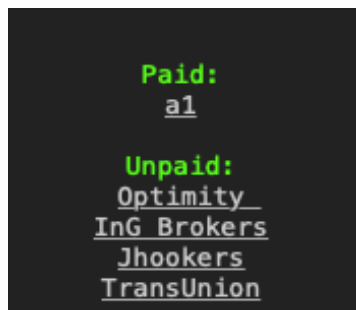


Figure 7 Status of ransom payment by A1

The length of time it took for ransomed[.]vc to transform from a forum into a victim letter suggested that shortcomings on the part of the attackers could be sought. A fuzz'ing of the ransomed[.]vc site was performed on 24.08.2023.



Figure 8 The appearance of the ransomed[.]vc website on 24.08.2023

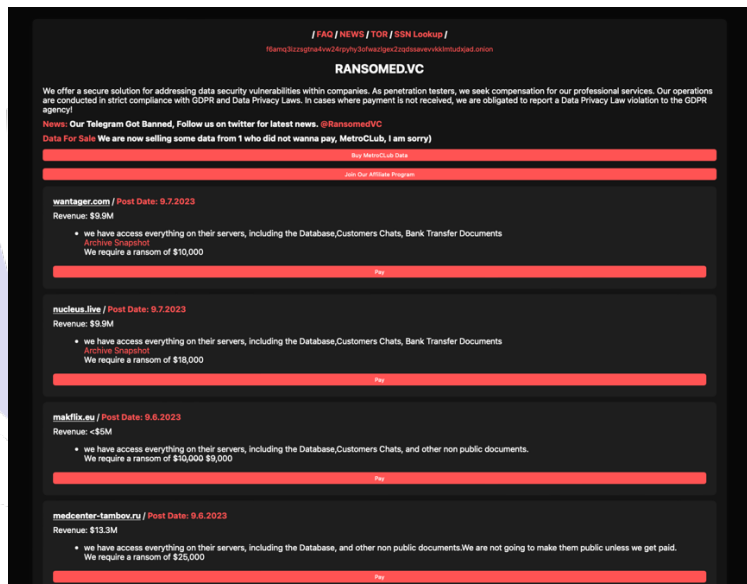


Figure 9 The appearance of the ransomed[.]vc website on 06/09/2023

After a brief analysis of the fuzz'er results, one would conclude that ransomed[.]vc is using pre-made template elements sourced from GitHub (https://github.com/alphaotuken/Cosmic), from the presumably unwitting user @alphaotuken:

```
/*-----*\n#style.css\n/*-----*/\n\n**\n * copyright 2023 alphaotuken\n*/\n\n/*-----*\n#CUSTOM PROPERTY\n/*-----*/
```

Figure 10 Code snippet from the .css file from https://ransomed[.]vc

The files that I was able to get from the ransomed[.]vc server such as graphics and directories from the site template are identical:



Figure 11 Graphics sourced from ransomed[.]vc directories

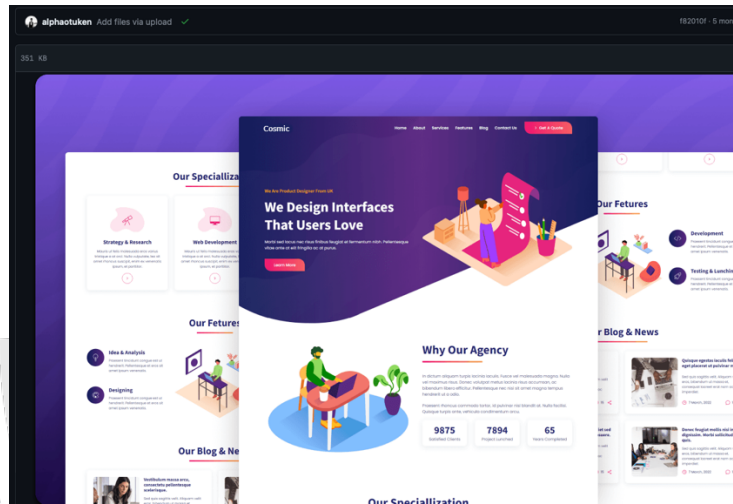


Figure 12 Graphic from user template alphaotuken

Index of /assets

Name	Last modified	Size	Description
Parent Directory		-	
css/	2023-08-17 11:03	-	
images/	2023-08-17 11:03	-	
js/	2023-08-17 11:03	-	

Apache/2.4.41 (Ubuntu) Server at 179.43.142.108 Port 443

Figure 13 Directory /assets/ with ransomed[.]vc

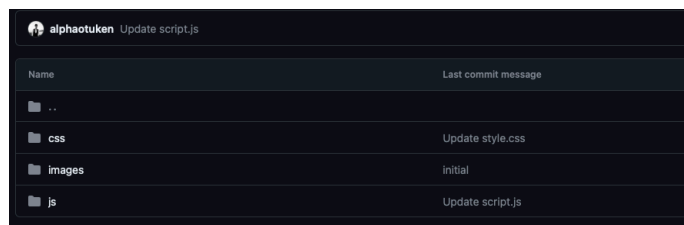


Figure 14 The /assets/ directory from the alphaotuken user template

An examination of the site's metatag data using the Censys Search tool also yielded interesting results.

The results that caught my attention were in the <meta name> field:

```
<!DOCTYPE html>\n<!-- HTML+CSS+JS T.ME/EOMLOL-->\n<meta name="title" content="Ransomed.vc - Digital Peace Tax Agency">\n<meta name="description" content="Ransomed.vc - Digital Peace Tax Agency Online agency that is looking forward to put sanctions on t
```

Figure 15 Meta name from the old version of the ransomed[.]vc website

For comparison <meta name> in the new version of the site: ransomed[.]vc:

```
<!DOCTYPE html>\n<html lang="en">\n <head>\n <meta charset="UTF-8">\n <meta name="viewport" content="width=device-width, initial-scale=1.0">\n <meta name="title" content="Ransomed - If You Pay, You Gain">\n <meta name="description" content="Welcome To Ransomed. We provide a stable and safe-to-use place for companies' data leaks. We are simple pentesters who want to be paid for the job they have done.">\n <meta name="keywords" content="Ransom, Ransomware, Hackers, RansomedVC, Hackers, CyberSecurity">\n <meta name="robots" content="index, follow">\n <style>\n body {\n font-family: system-ui, -
```

Figure 16 Meta name from the latest version of the ransomed[.]vc website (as of 06.09.2023)

In the original version of the ransomed[.]vc website, in the <meta> section, we can find a link to Telegram messenger: [t\[.\]me/EOMLOL](https://t.me/EOMLOL)

After pasting the above address into the browser bar, we will see the Telegram business card of user: egard (@EOMLOL), who links to the channel in his profile description: @blackforumsdotnet.

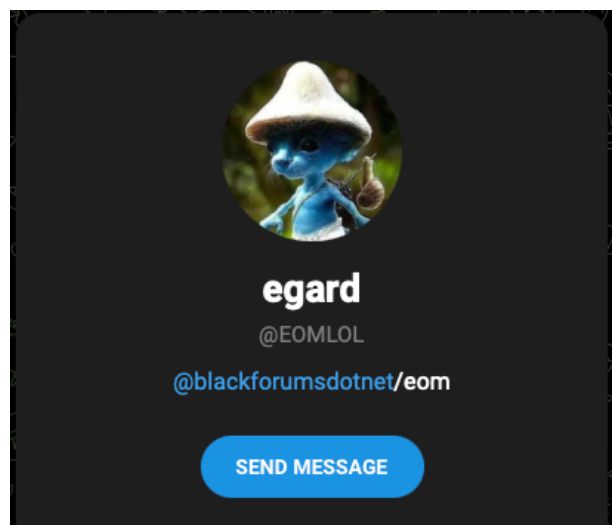


Figure 17 [https://t\[.\]me/EOMLOL](https://t.me/EOMLOL)

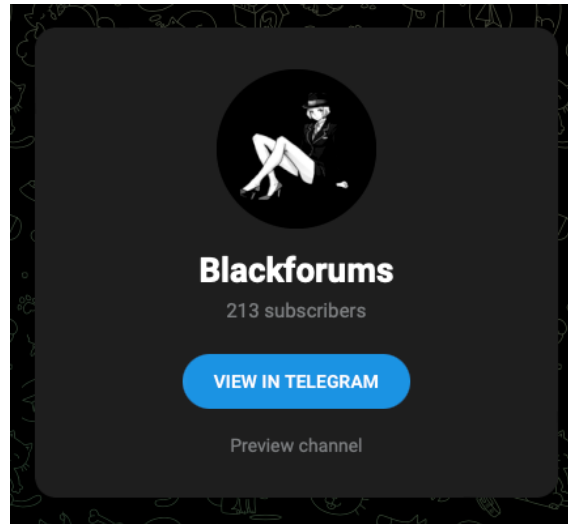


Figure 18 Business card of @Blackforumsdotnet channel

The @Blackforumsdotnet channel was created on 20.07.2023, while the first visible message is dated 04.09.2023:

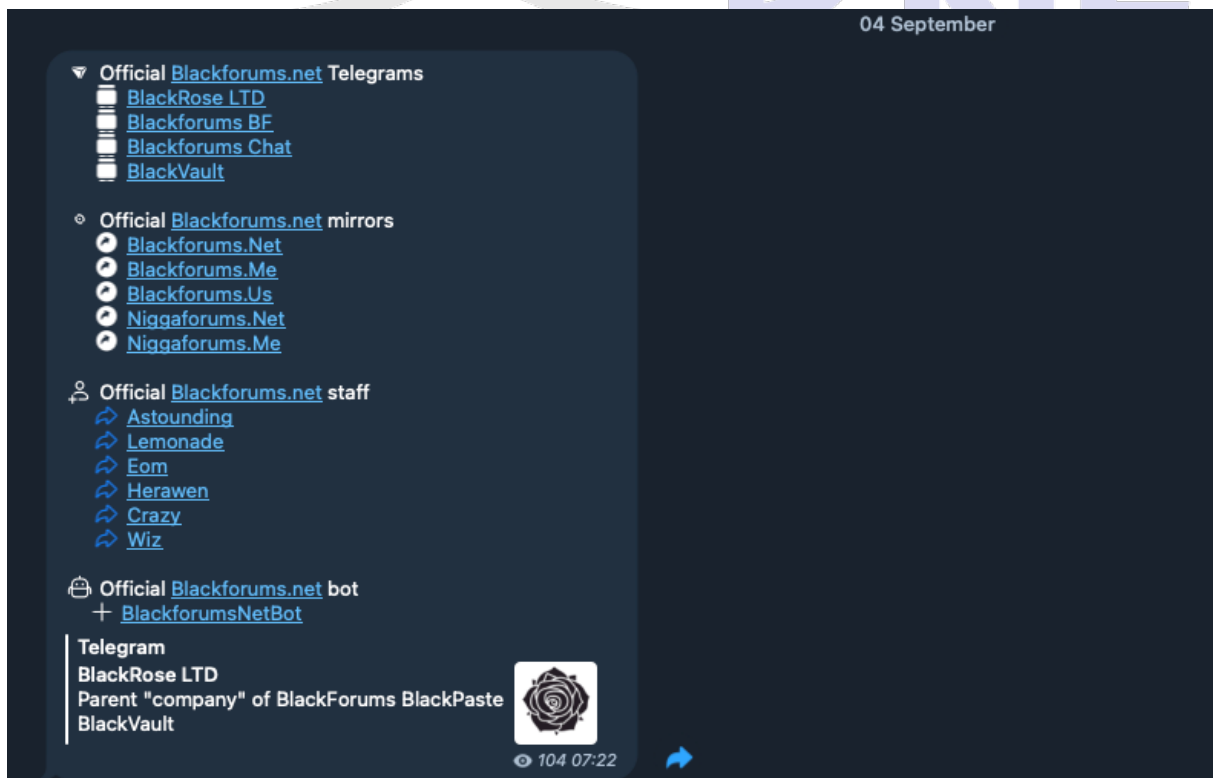
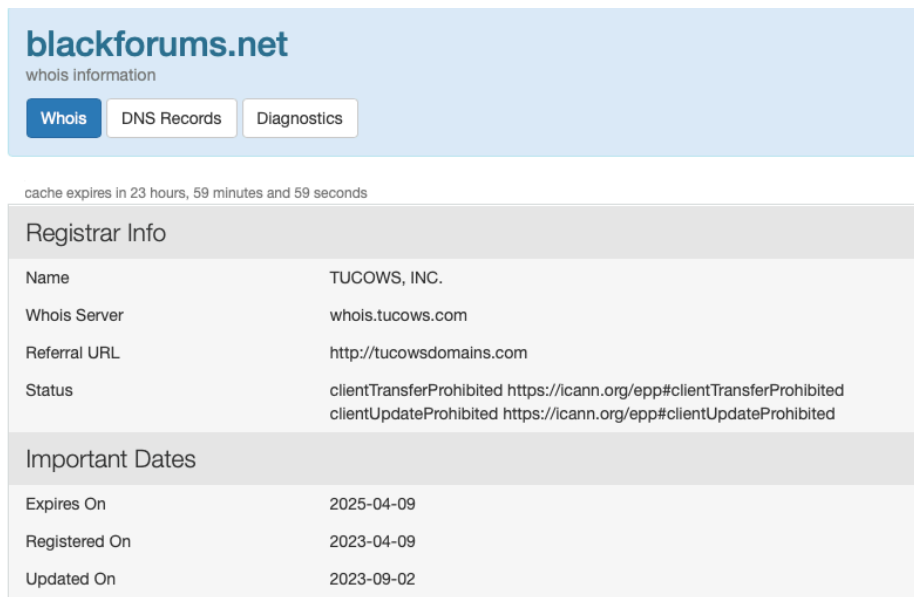


Figure 19 Message on @Blackforumsdotnet channel

In the message we have links to more channels that take you to the forum community chat rooms [https://blackforums\[.\]net](https://blackforums[.]net)

Who.is for the domain blackforums[.]net:



blackforums.net
whois information

Whois DNS Records Diagnostics

cache expires in 23 hours, 59 minutes and 59 seconds

Registrar Info	
Name	TUCOWS, INC.
Whois Server	whois.tucows.com
Referral URL	http://tucowsdomains.com
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited

Important Dates	
Expires On	2025-04-09
Registered On	2023-04-09
Updated On	2023-09-02

Figure 20 <https://who.is/whois/blackforums.net>

Returning to the Telegram channels associated with BlackForums, one of them we can refer to as the "main channel": [hxxps://t.\]me/blackforumsbf](https://t.me/blackforumsbf), where on 05.09.2023 user: @EOMLOL was announced as one of the forum administrators:

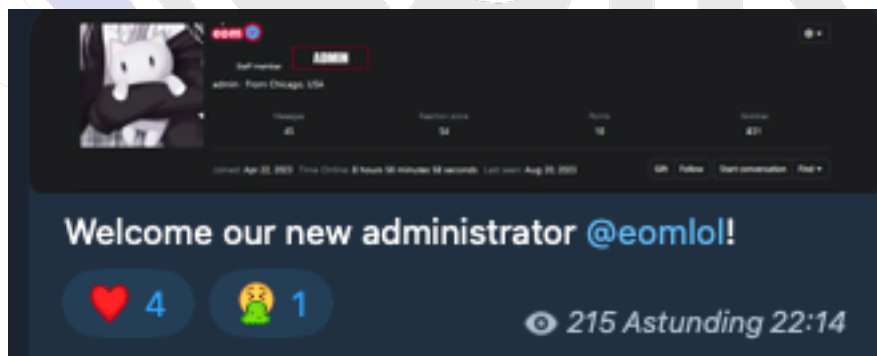


Figure 21 [hxxps://t.\]me/blackforumsbf/499](https://t.me/blackforumsbf/499)

Listed as the BlackForums administration team are users such as:

- @Astounding
- @Lemonade
- @Eom
- @Herawen
- @Crazy
- @Wiz

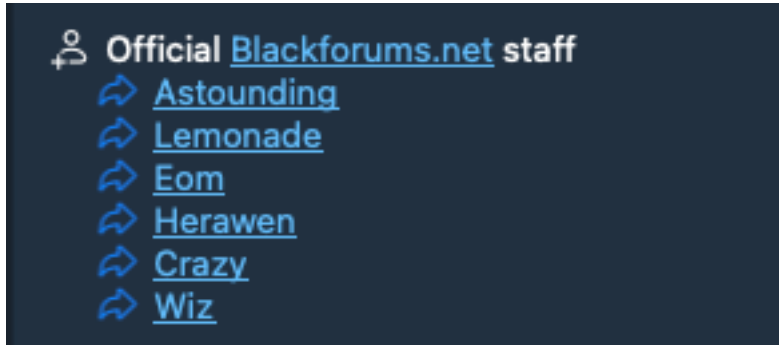


Figure 22 List of administrators

Let's move on to analysis, each account of the above:

Name:

@Astounding

Description:

♥ @blackforumschat | @blackforumsbf | @fivefamilies | astounding.zip

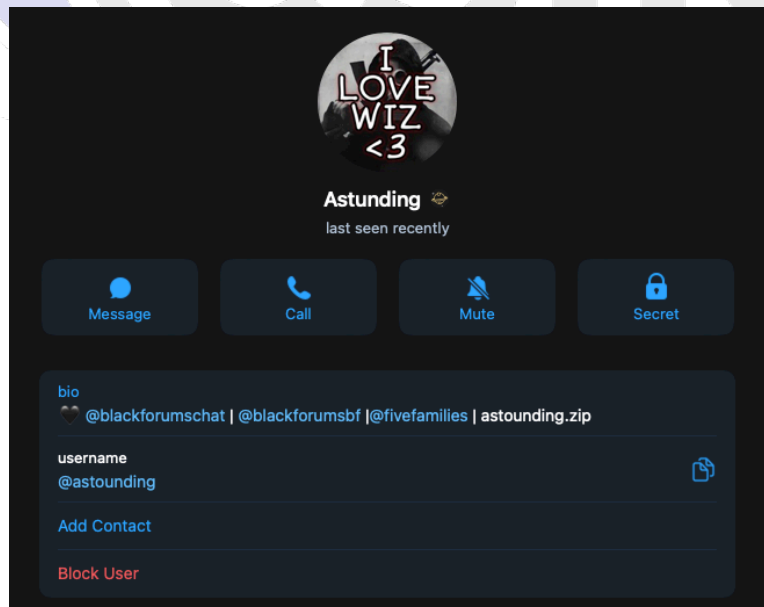


Figure 23 @Astounding

Name:

@lemonade_got_banned

Description:

Co-Owner of BlackForums.net

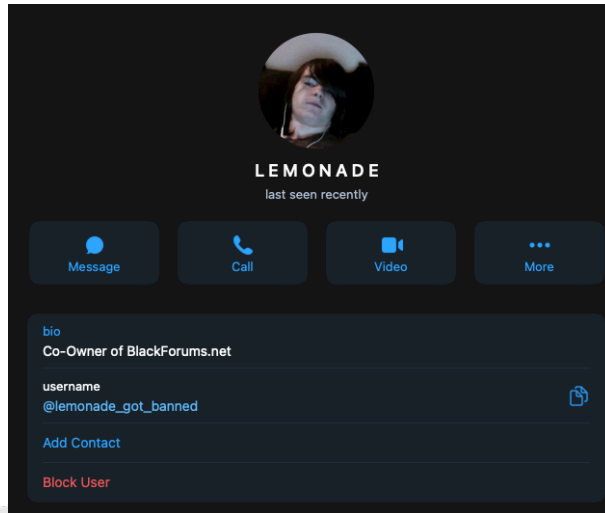


Figure 24 @lemonade_got_banned

Name:

@Mulicious

Description:

Vulnerability is the birthplace of Innovation

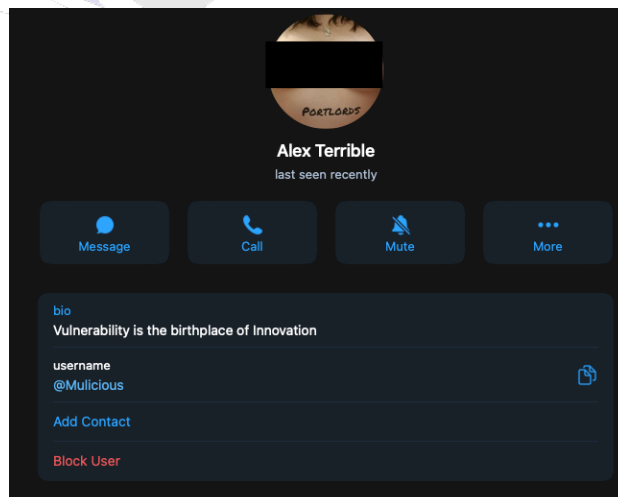


Figure 25 @Mulicious

Name:
@LoaderCrazy

Description:
♥ @blackforumschat | @blackforumsbf | <https://Developent.co>

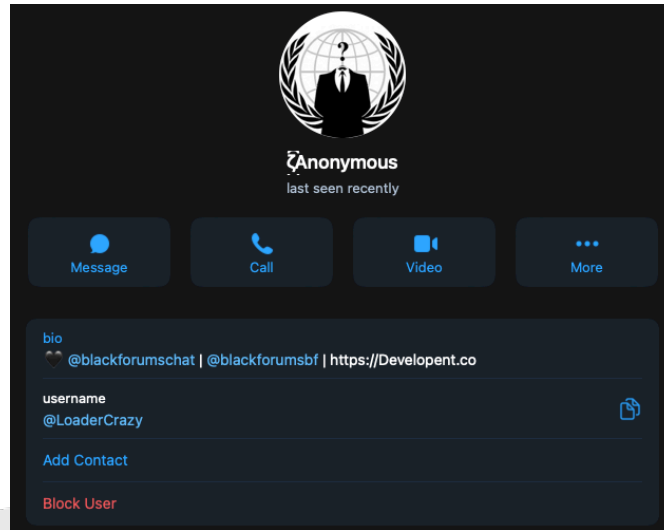


Figure 26 @LoaderCrazy

Name:
@ThreatSecurity

Description:
Founder of @ThreatSec & @FiveFamilies, Twitter: Wizpwn 🤖



Figure 27 @ThreatSecurity

Two accounts (@ThreatSecurity, @Astounding) from the BlackForums team have a sub-linked channel named in their account descriptions: **@FiveFamilies**.

FiveFamilies is a coalition of five cybercrime groups, each specializing in a specific area of activity. Collectively, their activities range from attacks on various countries to the publication of sensitive data.



Figure 28 <https://t.me/FiveFamilies>

On 28.08.2023, the following message appeared on the @FiveFamilies channel:

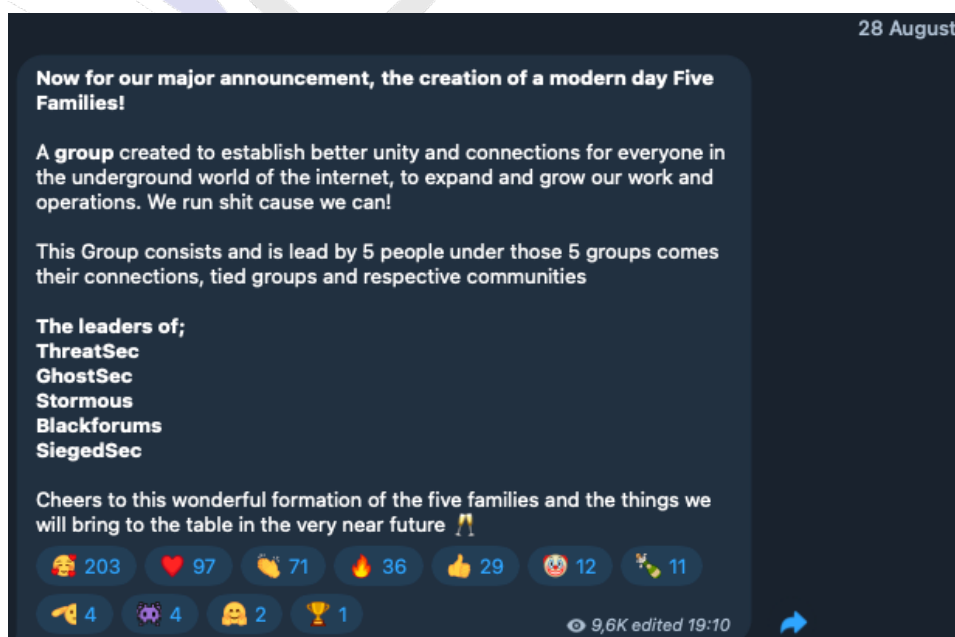
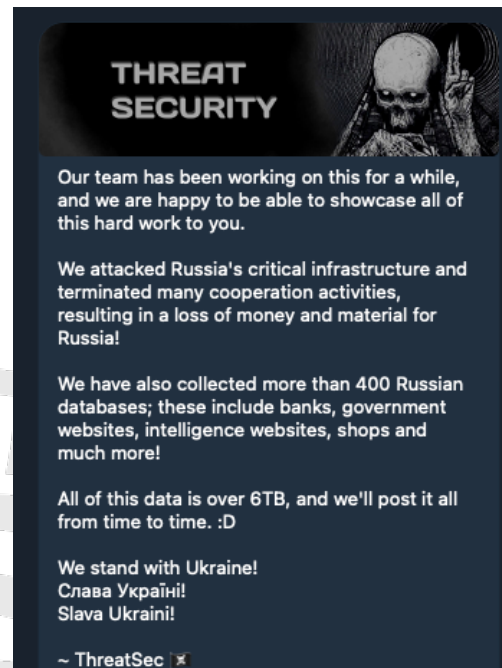
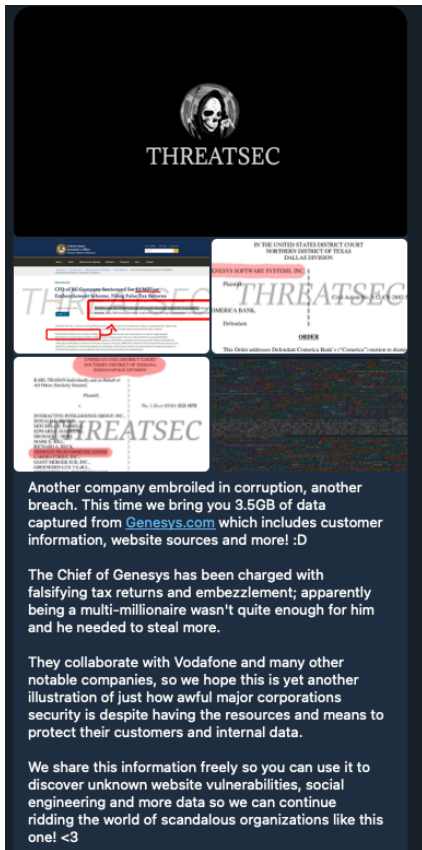


Figure 29 <https://t.me/FiveFamilies/9>

In which we can read that the title **FiveFamilies** includes the following groups:

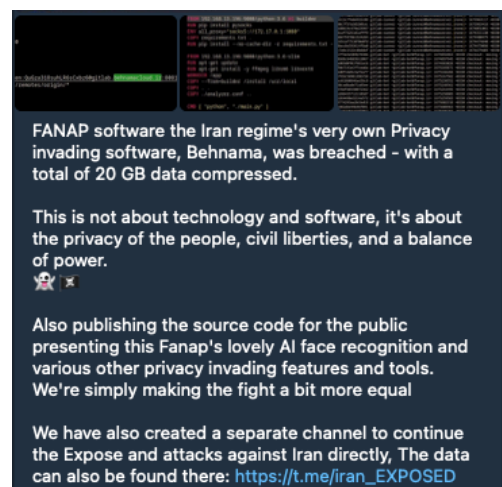
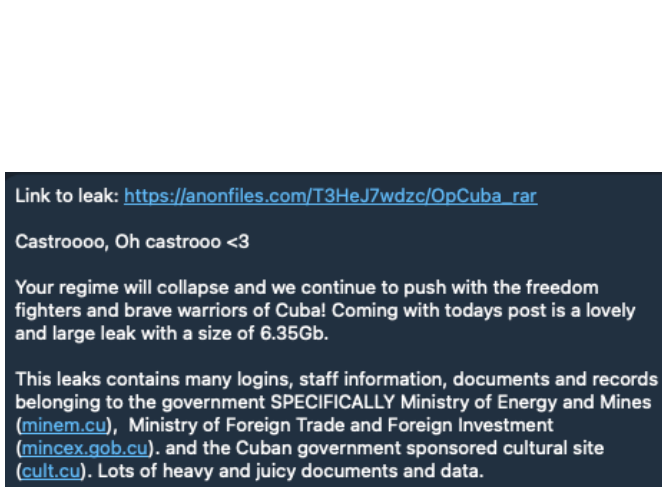
- **ThreatSec** - date of creation: 22.05.2023

The group is responsible for, among other things, attacks on genesys.com and Russia:




- **GhostSec** - date of creation: 25.10.2020

The group is responsible for attacks on Iran and Cuba, among others:



- **Stormous** - date of creation: 30.04.2021

The group is responsible for, among other things, an attempted attack on the Polish Commodity Exchange Clearing House. (the attack did not actually happen, and their published information about the leak turned out to be false) and companies in Europe:



STORMOUS :

the group econocom First General Digital Company in Europe, the Econocom group designs, finances and facilitates the digital transformation of large companies and public organizations.

Data type : Passwords _ Projects _ Messages _ Plans _ Reports _ Relationships _ Files and Documents _ Techniciens Projets _ Comptes & Supports_ Anciens dossiers _ procédures_ECONOCOM _ Procédure configuration DHCP - Borne DLINK

Check our blog for screenshots:

Hey :


we are going to leak some very basic and important data about a financial institution in Warsaw, Poland, as follows: Primary server addresses / Enterprise main network address / Enterprise main device(s) server / MD5 encryption When you decrypt it, you will have access to very good things Try it for yourself You are looking to hack this organization It is difficult but thanks to this information it will be hacked in a day At least one, because she suffers from a lot of wounds. This institution has a branch in America and Europe !!!! Here #we are only fighting not destroying.

web : <https://www.irgit.pl>

- **Blackforums** - date of creation: 09.04.2023

It is up to the group to maintain the forum and do media work such as pasting information from @FiveFamilies into one channel:

Forwarded from: ThreatSec



We've been a little quiet lately but we come back with a bang! <3
We of course never leave our community hanging so today we bring you the database of [Unbx.com](https://unbx.com)!

It's supposed to be some sort of "revolutionary AI" that helps manage and distribute product information but uh... seems like they can't really manage their own info well themselves xD

All of this data is around 22Gb, which includes basically ALL information stored on the site, from user info to backend stuff, just everything ;D

- **SiegedSec** - date of creation: 03.04.2022

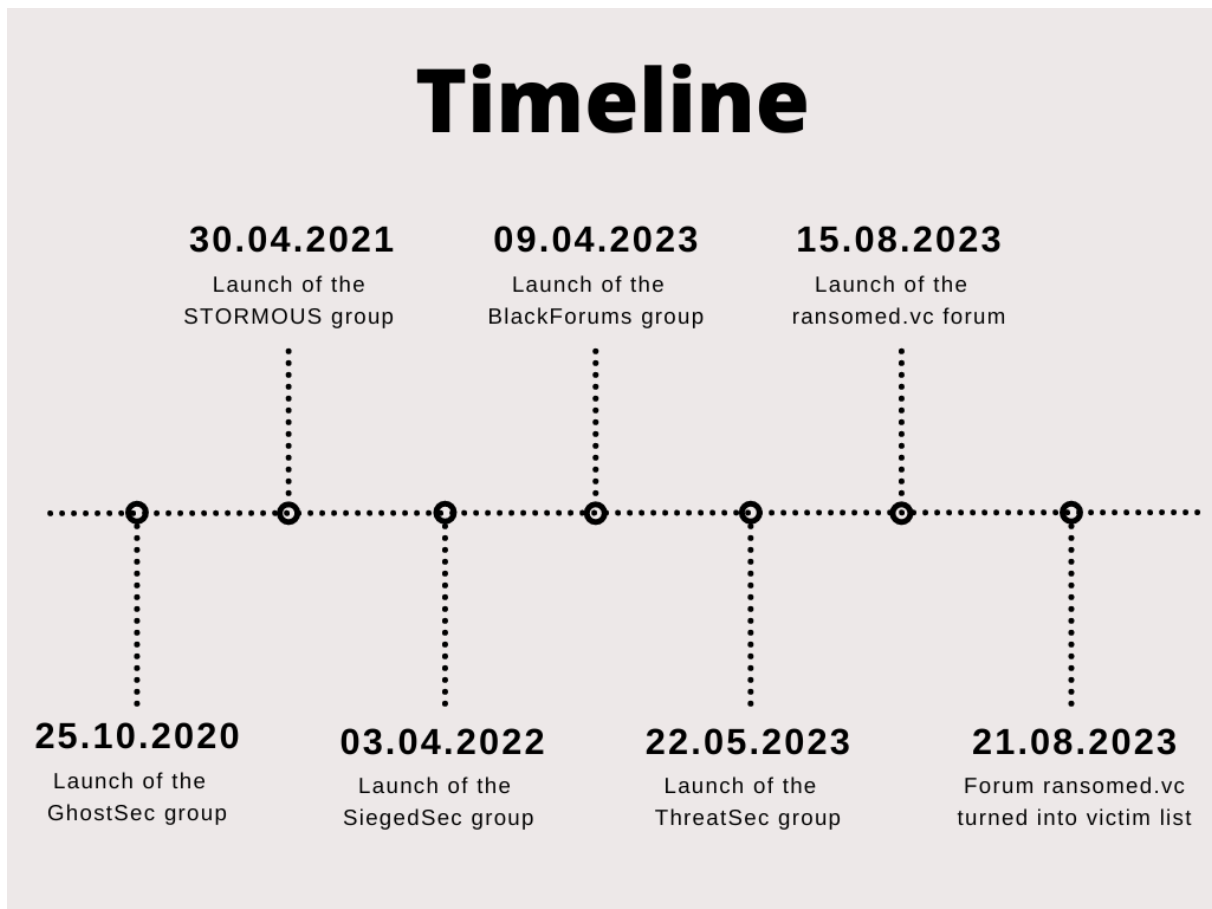
The group is responsible for, among other things, the publication of NATO COI data and attacks on US companies:



We have also created an account on blackforums.net, where we will also post our work :D
<https://blackforums.net/SiegedSec>

While we're here, shoutout to our friends at [@GhostSec](#), [@KittenSec](#), and [@ThreatSec](#)! Go check them out if you haven't already, they do awesome work.

A timeline illustrating the formation of the groups:



Key Findings:

Ransomed[.]vc, at first glance may have appeared to be a standard forum targeting cybercriminals. However, upon closer inspection and examination of the clues hidden in various places on the network, it became clear that this was just the tip of the iceberg in an elaborate network of organized activity in cyberspace.

1. **Evolution of Activity:** The dynamic change in the nature of the ransomed[.]vc site from a forum to a "Victim List" in a short period of time underscores the flexibility and adaptability of cybercriminal groups operating online.
2. **Connections between different groups:** The discovery of links between various users and channels on the Telegram platform, including BlackForums and @FiveFamilies, shows how complex and multi-layered the connections between cyber organizations can be.
3. **Use of ready-made resources:** The use of off-the-shelf templates, such as this one from GitHub, indicates that these groups focus on efficiency, often at the expense of professionalism.

Recommendations:

1. **Continuous Monitoring:** Organizations and individuals must constantly monitor and analyze cybercriminal activity. This will not only allow early detection of potential threats, but also give a better understanding of the criminals' modus operandi and motivations.
2. **Employee Training:** Understanding that cybersecurity is a complex and rapidly evolving field is key. Organizations should invest in regular cybersecurity training for their employees.
3. **Inter-organizational cooperation:** In the face of such complex threats, cooperation between different individuals, countries and private organizations becomes essential. Sharing information about threats, criminals' tactics and best practices can be the key to successfully combating cybercrime.

As a result, this ransomed[.]vc analysis highlights the fact that cybercrime has become more complex, sophisticated and coordinated. Actions taken by organizations and individuals must be equally dynamic and comprehensive to effectively counter these threats in a digital world.

