

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

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:

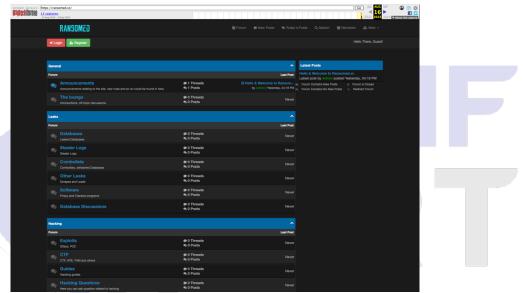


Figure 1 https://web.archive.org/web/20230816134436/https://ransomed.vc/

llo & Welcome to Ransomed.vc	Threaded Mod
Admin •	

Hello!	
A message no one has expected. We are finally opening our doors and presenting you a brand new forum. Over 70 Hours a week are being put on into this project.	
Before your think "Bruh, just another board" let me explain you what makes us better from the others. Our goal is to make the ultimate, place for sellingbuying or just chilling within a safe forum. We will listen to any of our users wishes as long as it is possible to be done.	
In the upcoming week, you will be able to enjoy,	
"[1 Credit System 2. Custom made shoutbox 3. More Awards 4. Staff Applications	
Ransomed.vc Administrators & Staff Members	
	55 Re

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.

-					
WayBackMachine	https://ransomed.vc/ 13 captures 15 Aug 2023 - 6 Sep 2023			Go JUL AUG SEP	e 3
	13 mg euto-13 mg edil	RANSOMED Continue arrange (In 115 Incidence (Contract) (In put) contractions continue arrange (In 115 Incidence (Contract) (In put) contractions continue loss of the relations		aues urs 202	About this capture }
	Online a	gency that is looking forward to put canctions on the less that dared a			
		Pending/Canceled Payments			
		(A1 Data Provider) {1&G Broker House} {Censored}{Censored}			
		<u>{Censored}</u>			
		<a< td=""><td></td><td></td><td></td></a<>			
	Figure 3 <u>https://we</u>	b.archive.org/web/20230821202610/H	https://ransomed.vc/		

The first victims, the people behind ransomed[.]vc were the companies: - A1 Data Provider:

Updated Non-Stop)	IENT			
A1 Data Provide	•			
Austria (MAin Country of O Serbia Bulgaria Croatia N. Macedonia BLD COMPANIES AFFECTED: BoB	sed. Our group was able to gather access to multip rator))le control panels. In the following countries:		
Yessai Red Bull Mobile PLOYES AFFECTED: erage: 18,000 STOMERS AFFECTED: ound 11M				
te payment is due until 9/	VIP Clients rangomed.vc		ŵ	ම ප් ඩ
٨	Location:015 Total: 45 980	ransomed.vc		

Figure 4 https://ransomed[.]vc/a1.html (no longer active)



- I&G; Broker House:

JACC; Broker Hourse Comment from the suther the of the biggest Broker house in the bilkes and central europe. Provide strate Provide strate Wreesges: The payment is due until 905/2023 Clients <	PENDING PAYMENT (Updated Non-Stop)		
Che of the biggest Broker house in the balkans and central europe.	I&G Broker Hourse		
Average 1 % COSCOMER AFFECTED; Around 1 JM The payment is due until 9/05/2023			
Image: Second and Seco	Average: 4k CUSTOMERS AFFECTED:		
Clients	The payment is due until 9/05/2023		
Clients CONSULTATION OF CONSUL			
Image: State of the state o		EGNBULSTAT	
		Agents Agents	
	ned.vc anone		
General Control General Control General Control Figure 5 https://ransomed[.]vc/ig.html (ho longer active)	P anazon van		

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:

Current Progress of payment:
1/4 partial payments have been paid. expecting second payment by 8/25/2023 (EDITED)
Figure 6 Status of ransom payment by A1

Or have paid them in full:

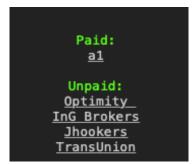


Figure 7 Status of ransom payment by A1



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.

Ransoned Group Pain	
Pilds Mella and witcome it one of the most particular affiliate program is if an end of the most is the inter of the most is the most	
Pick and base	
Territer SC nutries SC nutri	Arra va Mars va Mars

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

FAQ NEWS TOR SSN Lookup		
RANSOMED.VC		
We offer a secure solution for addressing data security vulnerabilities within companies. As penetration testers, we seek compensation for our professional services. Our operations are conducted in strict compliance with GDPR and Data Privacy Laws. In cases where payment is not received, we are obligated to report a Data Privacy Law violation to the GDPR agency!		
News: Our Telegram Got Banned, Follow us on twitter for latest news. @RansomedVC		
Data For Sale We are now selling some data from 1 who did not wanna pay, MetroCLub, I am sorry)		
Buy MatoricCub Data		
Join Our Affiliale Program		
wantager.com / Post Date: 9.7.2023		
Revenue: \$9.9M		
we have access everything on their servers, including the Database,Customers Chats, Bank Transfer Documents		
Archive Snapshot		
We require a ransom of \$10,000		
Pay		
nucleus.live / Post Date: 9.7.2023		
Revenue: \$9.9M		
we have access everything on their servers, including the Database, Customers Chats, Bank Transfer Documents		
Archive Snapshot	100 million (1997)	
We require a ransom of \$18,000		
Pay		
makflix.eu / Post Date: 9.6.2023		
Revenue: <\$5M		
we have access everything on their servers, including the Database,Customers Chats, and other non public documents.		
We require a ransom of \$10,000 \$9,000		
Per c		
medcenter-tambov.ru / Post Date: 9.6.2023 Revenue: \$13.3M		
 we have access everything on their servers, including the Database, and other non public documents.We are not going to make them public unless we get paid. We require a ransom of \$25,000 		
Pay		

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:

	style.css	*\
*-	-	*/
/**		
* /	copyright 2023 alphaot	tuken
/*-		*\
	CUSTOM PROPERTY	
٠+		+/

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

🚯 alphaotuken Add files via upload 🗸		f82010f - 5 month
	Cosmic Nova About Santase Reg Contacts	an tau
Our Specialliza		
	We be being a first set	Dur Fetures
Strategy & Research Web Development	That Users Love Write the are real to be legal of the memory field. Newsear	Development
Marca of deal in order and a short order. Marca of deal and a short of deal and an and a short order and a short of deal and a short order and a sh		Paring & Lucobing manan and angust
Our Fetures	Why Our Agency	r Blog & News
Kes & Analysis Mana & Manager and and Manager Manager and and Manager Manager and and Manager Manager and and Manager Manager and		Strangen huld
Designing Transit Strategies and all	winnershut mice Share shapement between and a shapement between and a share shapement between and a share shapement between and a share shapement between a share	Allowed and a second and a second a se
ave fino, menuge	9875 7894	
Our Blog & Ne		Service Servic
Theffielden Bassa area, consecting pellonitages		n c Presis. (D News, NEW C N
Extension of the second	Our Speciallization	
Figure 12 Gro	aphic from user template alph	naotuken

Index of /assets

<u>js/</u>

Name	Last modified	Size Description
Parent Director	<u>y</u>	-
css/	2023-08-17 11:03	-
images/	2023-08-17 11:03	-

Apache/2.4.41 (U	Ubuntu) Server at	t 179.43.142.108 P	ort 443
------------------	-------------------	--------------------	---------

2023-08-17 11:03

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

-

🚯 alphaotuken Update script.js		
	Last commit message	
•		
CSS		
images		
🖿 js	Update script.js	

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="R ansomed.vc - Digital Peace Tax Agency">\n<meta name="description" content="Ransome d.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 R ansomed. We provide a stable and safe-to-use place for companies' data leaks. We are si mple pentesters who want to be paid for the job they have done.">\n <meta name="keywor ds" 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

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.

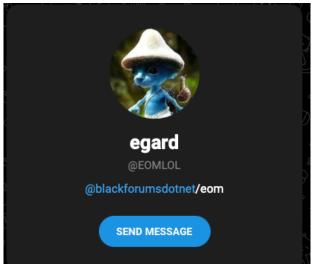


Figure 17 https://t[.]me/EOMLOL

[TLP:CLEAR]



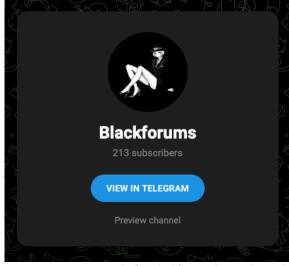


Figure 18 Business card of @Blackforumsdotnet channel

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

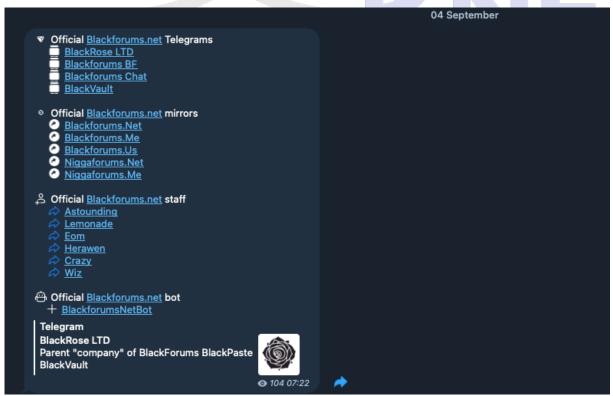


Figure 19 Message on @Blackforumsdotnet channel

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



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

Whois DNS Records Diagnostics ccache 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			
Registrar Info Name TUCOWS, INC. Whois Server whois.tucows.com Referral URL http://tucowsdomains.com Status clientTransferProhibited https://icann.org/epp#clientTransferProhibited			
Name TUCOWS, INC. Whois Server whois.tucows.com Referral URL http://tucowsdomains.com Status clientTransferProhibited https://icann.org/epp#clientTransferProhibited			
Whois Server whois.tucows.com Referral URL http://tucowsdomains.com Status clientTransferProhibited https://icann.org/epp#clientTransferProhibited			
Referral URL http://tucowsdomains.com Status clientTransferProhibited https://icann.org/epp#clientTransferProhibited			
Status clientTransferProhibited https://icann.org/epp#clientTransferProhibited			
clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited			
Important Dates			
res On 2025-04-09			
Registered On 2023-04-09			
Updated On 2023-09-02			
Figure 20 <u>https://who.is/whois/blackforums.net</u>			

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

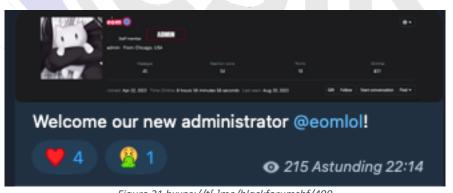


Figure 21 hxxps://t[.]me/blackforumsbf/499

[TLP:CLEAR]



Listed as the BlackForums administration team are users such as:

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



◇ Official Blackforums.net staff
 ◇ 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

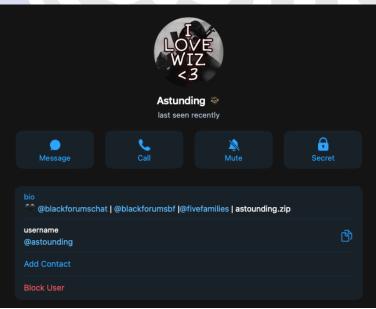


Figure 23 @Astounding



<u>Name:</u> @lemonade_got_banned

Description:

Co-Owner of BlackForums.net

	LEMON. last seen rec			
Message	Call	Uideo		
bio Co-Owner of BlackFo	orums.net			
username @lemonade_got_ban	nned		ඵ	
Add Contact				
Block User				
Figu	ure 24 @lemonad	le_got_banned	d	

<u>Name:</u> @Mulicious

Description:

Vulnerability is the birthplace of Innovation

PORTLORDS Alex Terrible last seen recently							
Message	Call	Mute					
bio Vulnerability is the bir	thplace of Innovation						
username @Mulicious			ற				
Add Contact							
Block User							

Figure 25 @Mulicious



Name: @LoaderCrazy

Description:

@blackforumschat | @blackforumsbf | https://Developent.co

		Anonym Jast seen rec				
M	essage	Call	Video			
bio 🏷 @l	blackforumschat @b	lackforumsbf https:	://Developent.co			
userna @Load	ime derCrazy			ற	_	
Add C	ontact					
Block	User					
	F	Figure 26 @Loo	aderCrazy			

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.



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

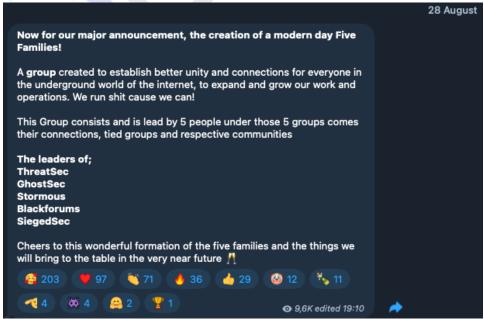


Figure 29 hxxps://t[.]me/FiveFamilies/9



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

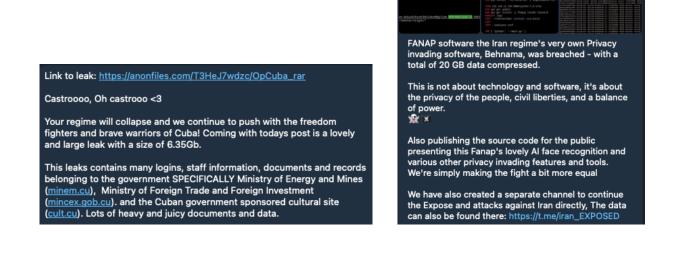
- ThreatSec - date of creation: 22.05.2023

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



- GhostSec - date of creation: 25.10.2020

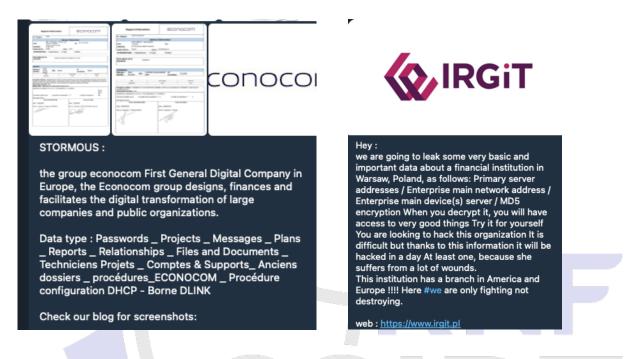
The group is responsible for attacks on Iran and Cuba, among others:





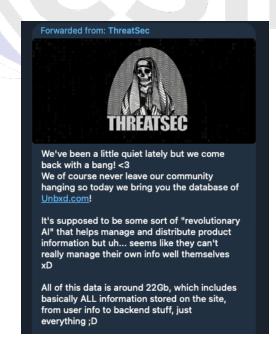
- Stormous - date of creation: 30.04.2021

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:



- 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:

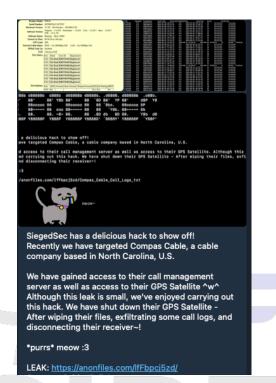




- SiegedSec - date of creation: 03.04.2022

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



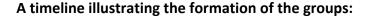


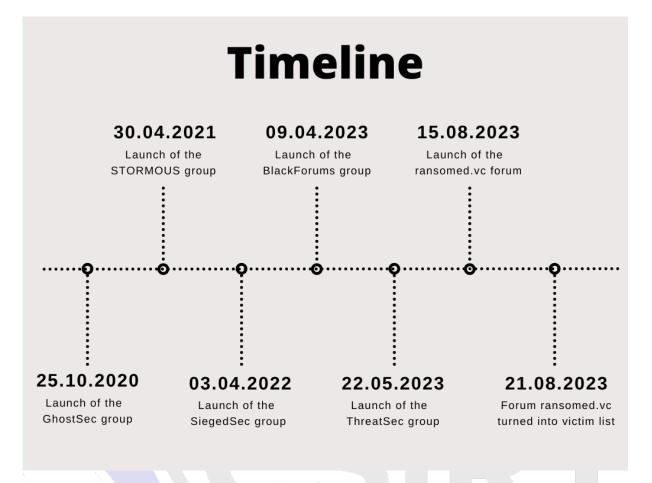
We have also created an account on <u>blackforums.net</u>, where we will also post our work :D <u>https://blackforums.net/SiegedSec</u>

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



[TLP:CLEAR]





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.
- 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.