

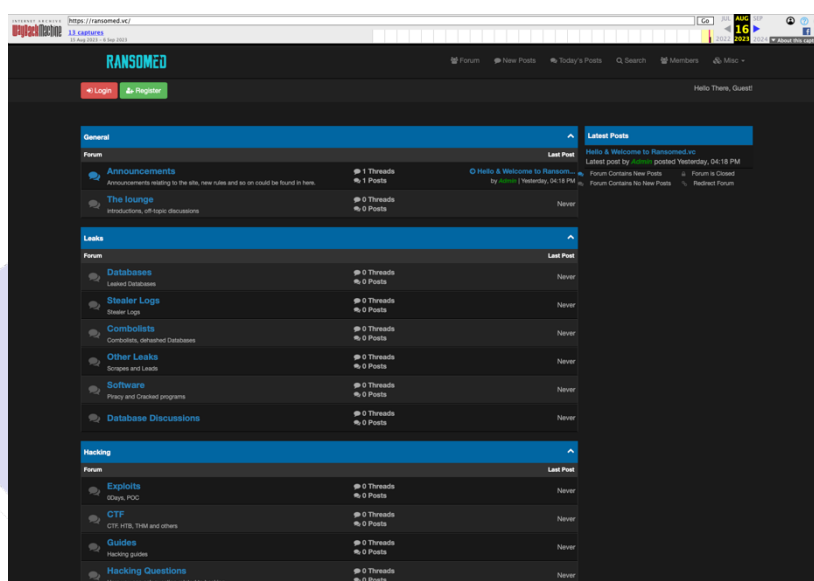
RANSOMED[.]VC – forum, ransomware czy hakywiści?

Wstęp:

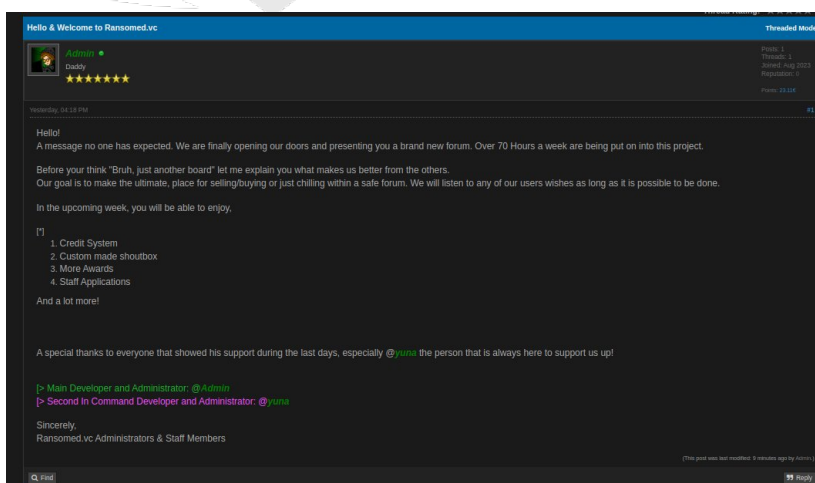
Współczesna cyberprzestępczość jest złożoną i dynamicznie rozwijającą się dziedziną, która koncentruje się nie tylko na osiągnięciu zysku, ale także na wpływniu na politykę oraz promowaniu ideologii. Grupy przestępcze w sferze cyberprzestrzeni coraz częściej zaczynają działać w sposób hierarchiczny, tworząc sojusze i wykorzystując różne metody, aby osiągnąć swoje cele. Poniższa analiza może nam pomóc zrozumieć, jak ewoluują te organizacje i jakie strategie przyjmują w celu osiągnięcia swoich celów.

Opis:

Ransomed[.]vc debiutowało jako forum dla cyberprzestępców 15.08.2023:

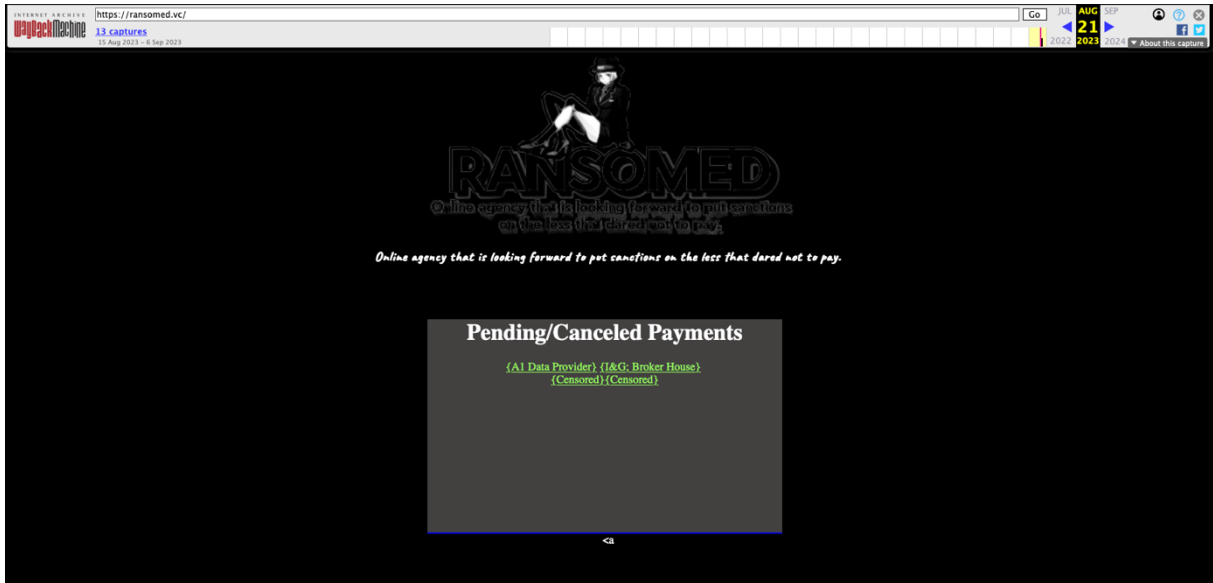


Rysunek 1 <https://web.archive.org/web/20230816134436/https://ransomed.vc/>



Rysunek 2 Źródło: <https://twitter.com/FalconFeedsio/status/1691764241156673677/photo/1>

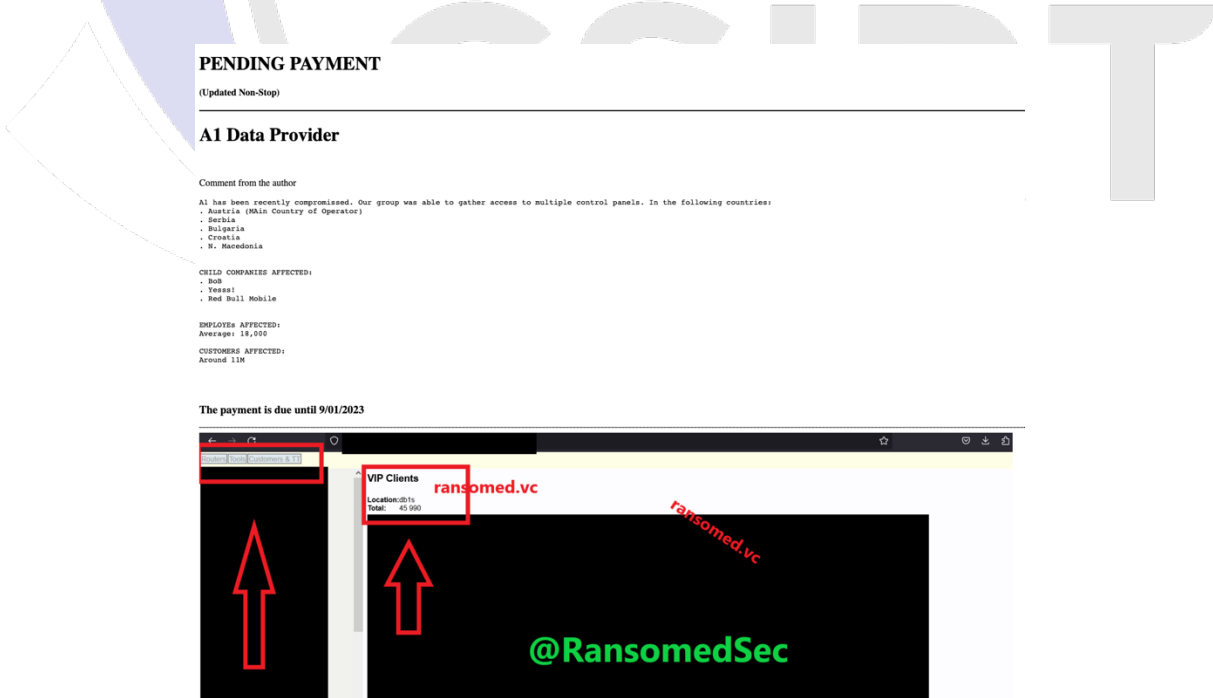
W ciągu zaledwie tygodnia (21.08.2023) strona ta przekształciła się w tzw. "Victim List" - listę firm, które padły ofiarą ataków ransomware.



Rysunek 3 [https://web.archive.org/web/20230821202610/https://ransomed\[.\]vc/](https://web.archive.org/web/20230821202610/https://ransomed[.]vc/)

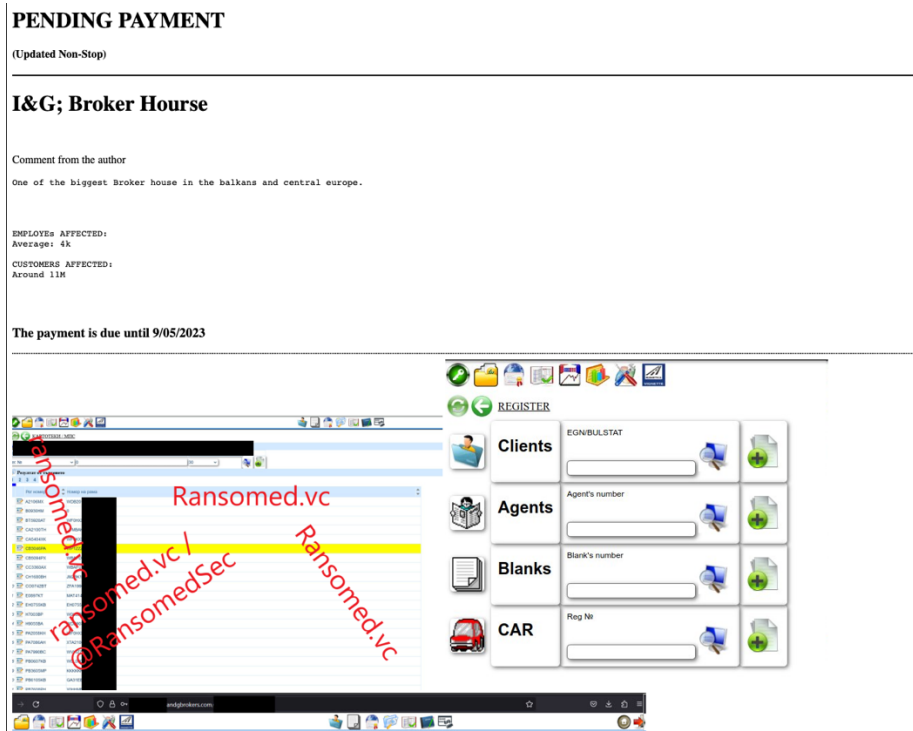
Pierwszymi ofiarami, osób stojących za ransommed[.]vc były firmy:

- A1 Data Provider:



Rysunek 4 [https://ransomed\[.\]vc/a1.html](https://ransomed[.]vc/a1.html) (już nieaktywny)

- I&G; Broker House:



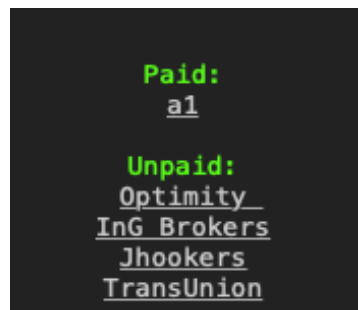
Rysunek 5 [https://ransomed\[.\]vc/ig.html](https://ransomed[.]vc/ig.html) (już nieaktywny)

W ciągu kilku kolejnych dni, lista ofiar powiększała się, a grupa ransomware, twierdziła, że firmy częściowo już opłacają okupy za odszyfrowanie danych:



Rysunek 6 Status płatności okupu przez firmę A1

Lub opłaciły je w całości:

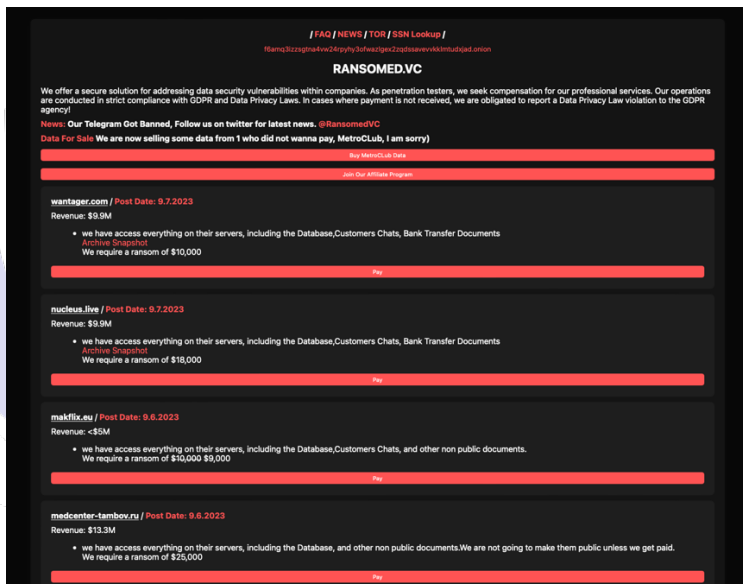


Rysunek 7 Status płatności okupu przez firmę A1

Czas w jakim ransomed[.]vc z forum przekształciło się w victim list, sugerował, że można byłoby doszukiwać się niedociągnięć ze strony atakujących. W dniu 24.08.2023 został wykonany fuzz'ing witryny ransomed[.]vc.



Rysunek 8 Wygląd strony ransomed[.]vc w dniu 24.08.2023



Rysunek 9 Wygląd strony ransomed[.]vc w dniu 06.09.2023

Po krótkiej analizie wyników z fuzz'era, można byłoby stwierdzić, że ransomed[.]vc korzysta z gotowych elementów szablonu pochodzącego z serwisu GitHub (<https://github.com/alphaotuken/Cosmic>), od zapewne nieświadomego użytkownika @alphaotuken:

```

/*-----*\
#style.css
\*-----*/

/**
 * copyright 2023 alphaotuken
 */

/*-----*\
#CUSTOM PROPERTY
\*-----*/

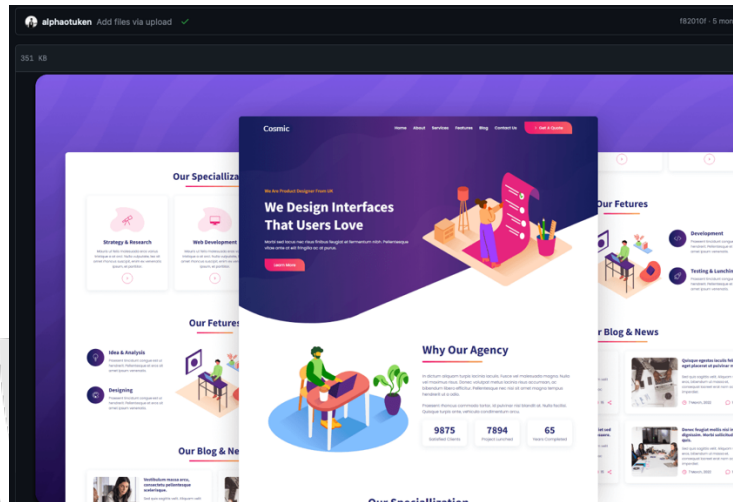
```

Rysunek 10 Fragment kodu pochodzący z pliku .css ze strony [https://ransomed\[.\]vc](https://ransomed[.]vc)

Pliki, które udało mi się pozyskać z serwera ransomed[.]vc jak np. grafiki oraz katalogi z szablonu strony są identyczne:



Rysunek 11 Grafika pochodząca z katalogów ransomed[.]vc



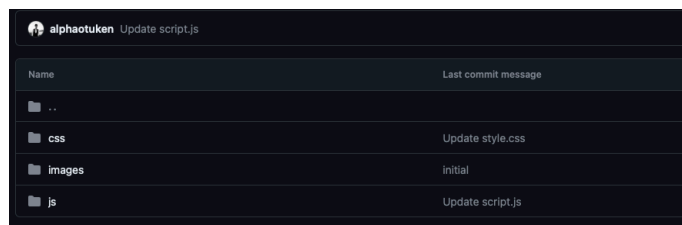
Rysunek 12 Grafika pochodząca z szablonu użytkownika alphaotuken

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

Rysunek 13 Katalog /assets/ z ransomed[.]vc



Rysunek 14 Katalog /assets/ z szablonu użytkownika alphaotuken

Interesujące rezultaty przyniosło także badanie danych metatagów strony za pomocą narzędzia Censys Search.

Wyniki, które przykuły moją uwagę znajdowały się w polu <meta name>:

```
<!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
```

Rysunek 15 Meta name ze starej wersji strony ransomed[.]vc

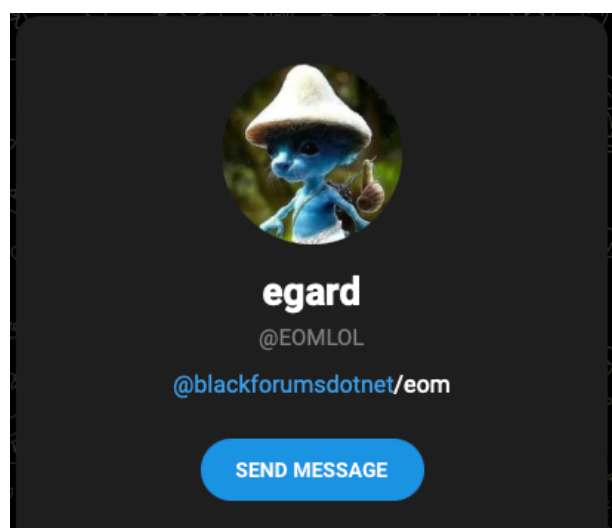
Dla porównania <meta name> w nowej wersji strony: ransomed[.]vc:

```
<!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, -
```

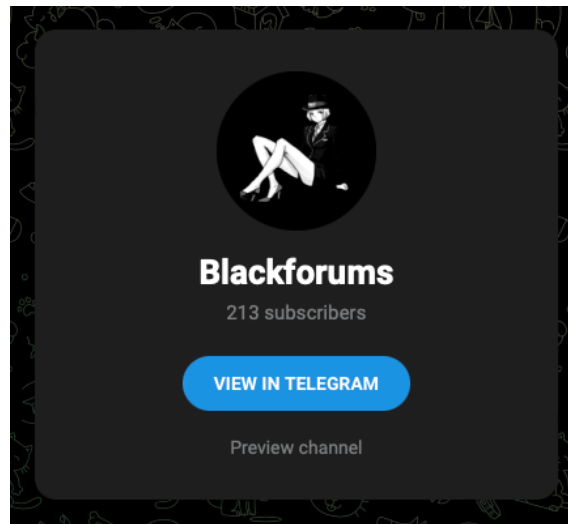
Rysunek 16 Meta name z najnowszej wersji strony ransomed[.]vc (na dzień 06.09.2023)

W pierwotnej wersji strony ransomed[.]vc w sekcji <meta> możemy odnaleźć link do komunikatora telegram: [t\[.\]me/EOMLOL](https://t.me/EOMLOL)

Po wklejeniu powyższego adresu do paska przeglądarki, wyświetli nam się wizytówka Telegram użytkownika: egard (@EOMLOL), który w opisie swojego profilu podlinkowuje do kanału: @blackforumsdotnet.

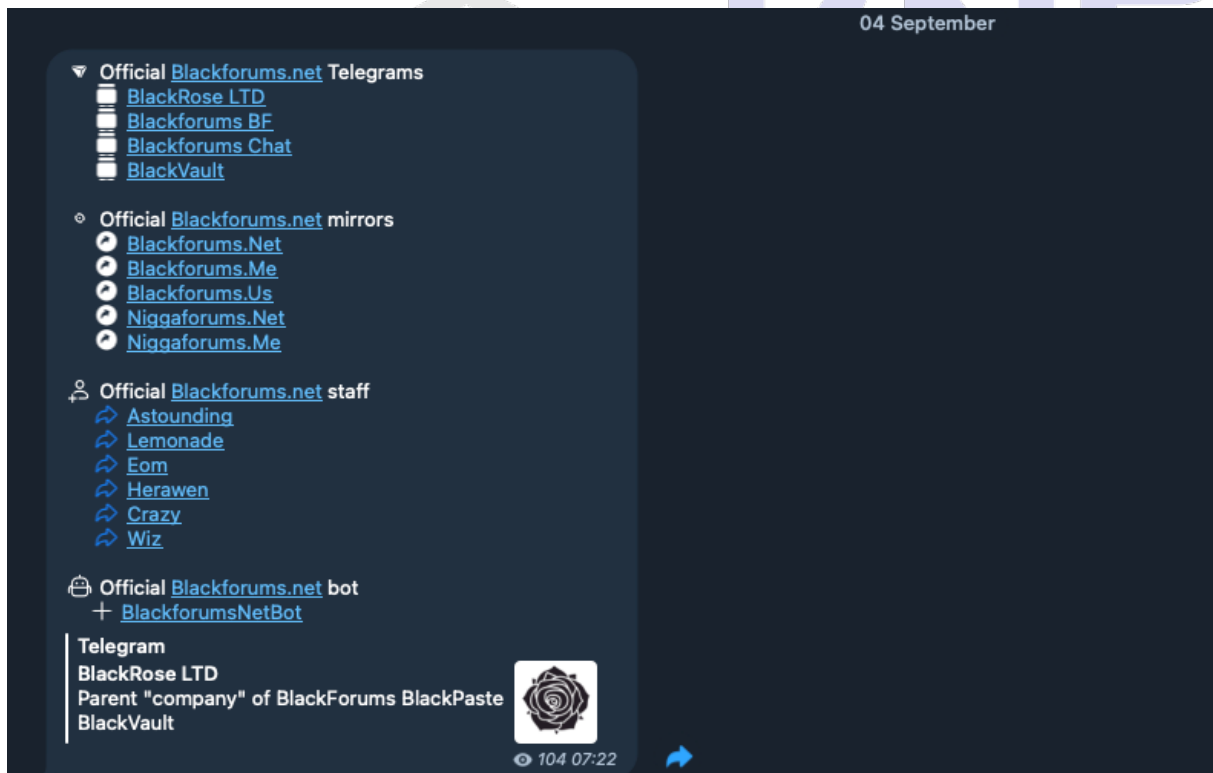


Rysunek 17 [https://t\[.\]me/EOMLOL](https://t.me/EOMLOL)



Rysunek 18 Wizytówka kanału @Blackforumsdotnet

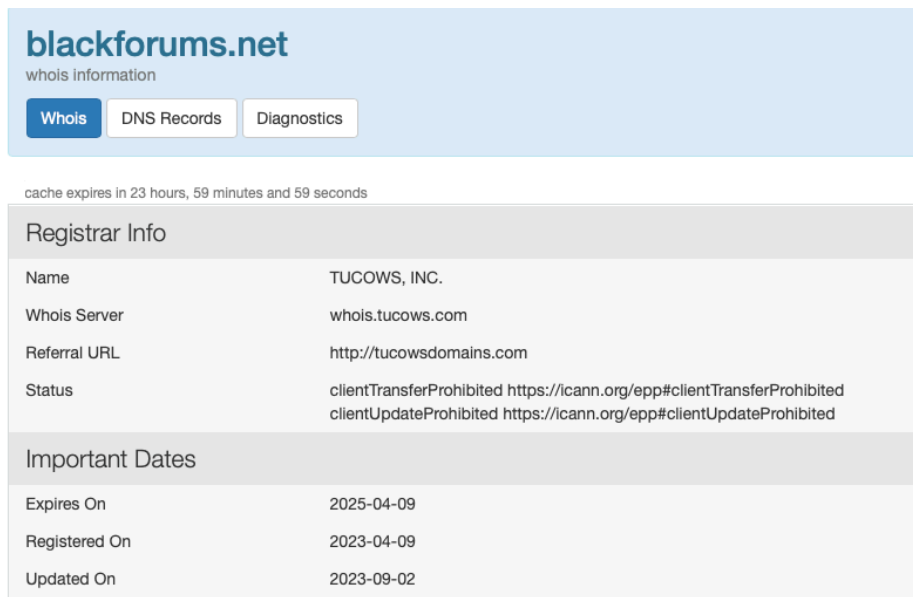
Kanał **@Blackforumsdotnet** został utworzony w dniu 20.07.2023, natomiast pierwsza widoczna wiadomość jest z 04.09.2023:



Rysunek 19 Wiadomość na kanale @Blackforumsdotnet

W wiadomości mamy linki do kolejnych kanałów, które przenoszą do chatów społeczności forum [https://blackforums\[.\]net](https://blackforums[.]net)

Who.is dla domeny blackforums[.]net:



blackforums.net
whois information

Whois DNS Records Diagnostics

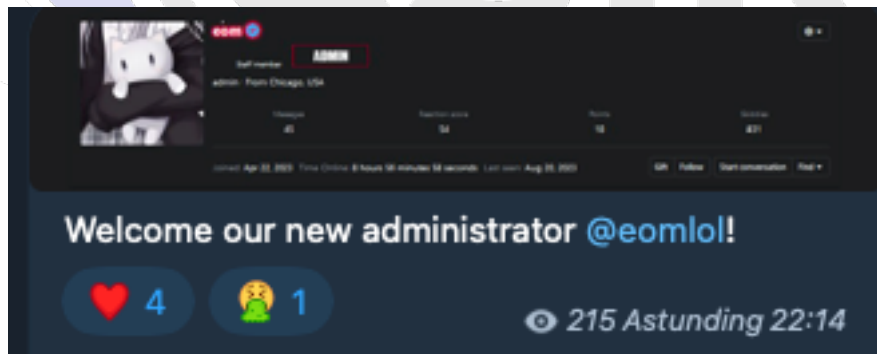
cache expires in 23 hours, 59 minutes and 59 seconds

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

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

Wracając do kanałów Telegram powiązanych z BlackForums, jeden z nich możemy określić jako „main channel”: `hxps://t[.]me/blackforumsbf`, gdzie w dniu 05.09.2023 użytkownik: @EOMLOL został ogłoszony jednym z administratorów forum:



Rysunek 21 `hxps://t[.]me/blackforumsbf/499`

Jako zespół administrujący BlackForums wymienieni są użytkownicy tacy jak:

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



Rysunek 22 Lista administratorów

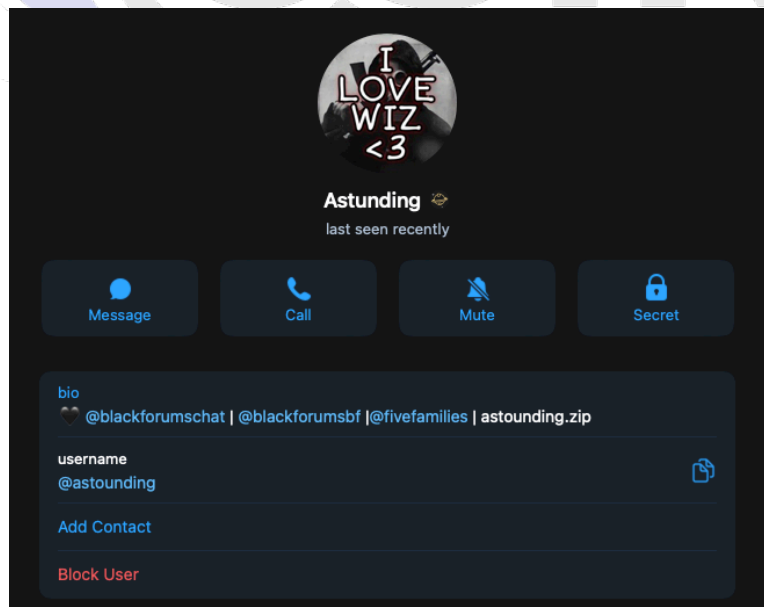
Przejdźmy do analizy, każdego konta z powyższych:

Nazwa:

@Astounding

Opis:

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



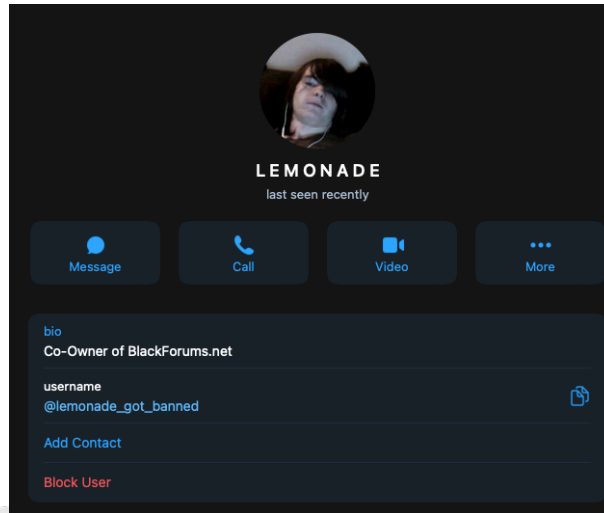
Rysunek 23 @Astounding

Nazwa:

@lemonade_got_banned

Opis:

Co-Owner of BlackForums.net



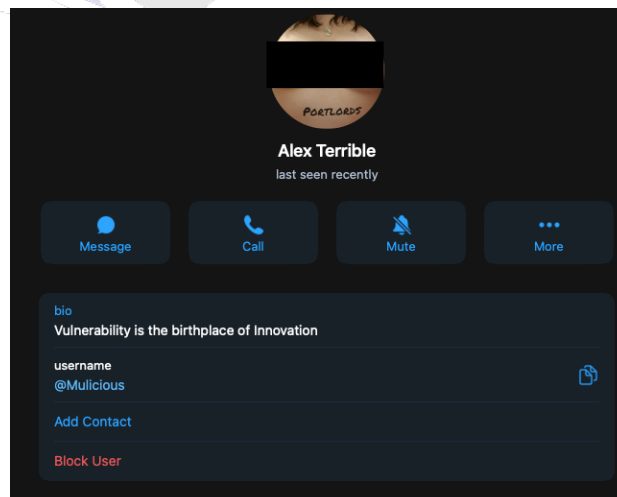
Rysunek 24 @lemonade_got_banned

Nazwa:

@Mulicious

Opis:

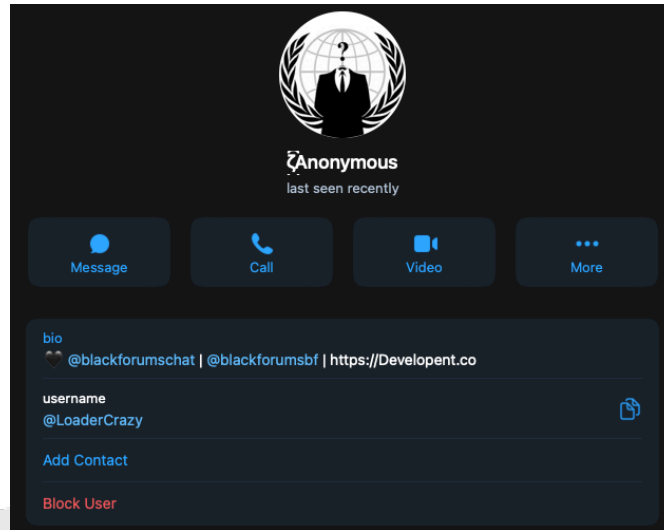
Vulnerability is the birthplace of Innovation



Rysunek 25 @Mulicious

Nazwa:
@LoaderCrazy

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



Rysunek 26 @LoaderCrazy

Nazwa:
@ThreatSecurity

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



Rysunek 27 @ThreatSecurity

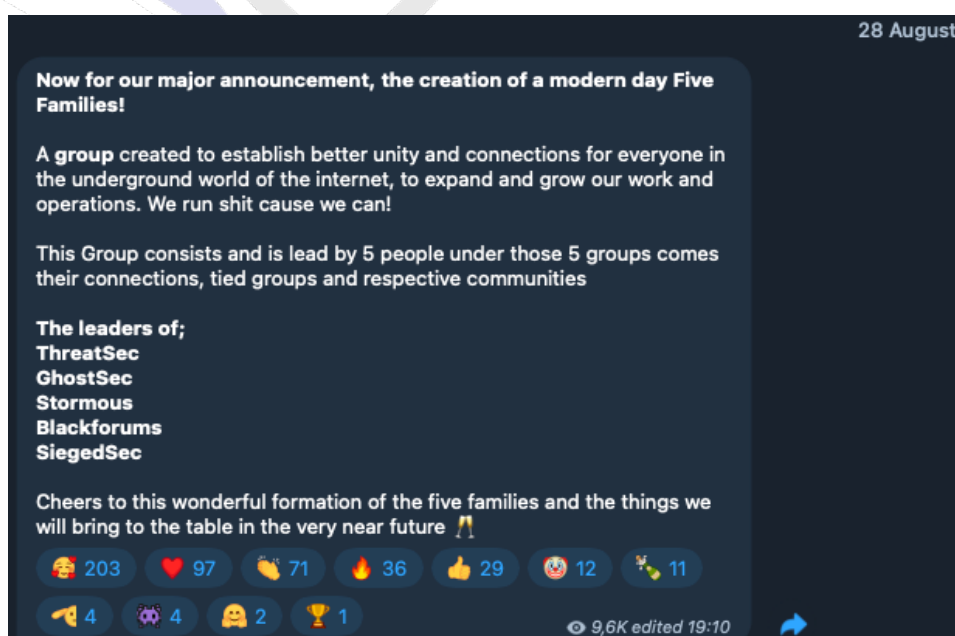
Dwa konta (@ThreatSecurity, @Astounding) z zespołu BlackForums w opisie kont ma podlinkowany kanał o nazwie: **@FiveFamilies**.

FiveFamilies to koalicja składająca się z pięciu grup cyberprzestępczych, z których każda specjalizuje się w określonym obszarze działalności. Wspólnie, ich działania obejmują szeroki wachlarz działań, od ataków na różne kraje po publikację poufnych danych.



Rysunek 28 [hxxps://t\[.\]me/FiveFamilies](https://t.me/FiveFamilies)

28.08.2023 na kanale @FiveFamilies pojawiła się wiadomość o poniższej treści:

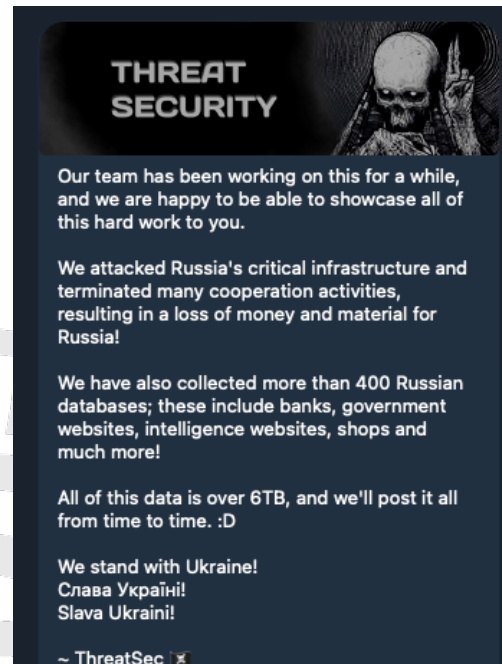
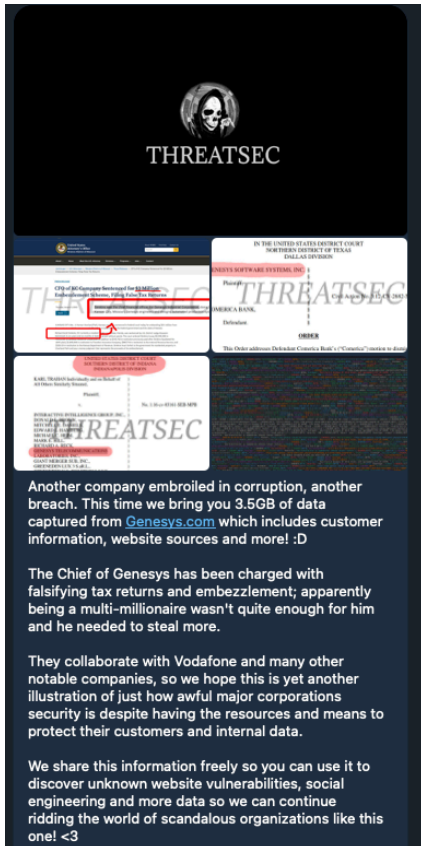


Rysunek 29 [hxxps://t\[.\]me/FiveFamilies/9](https://t.me/FiveFamilies/9)

W której to możemy przeczytać, że w skład tytułowej FiveFamilies wchodzi niżej wymienione grupy:

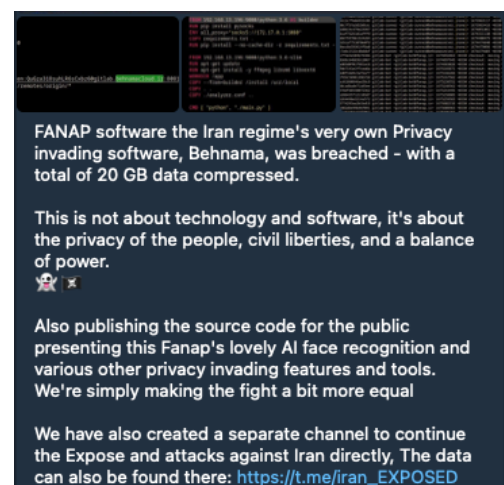
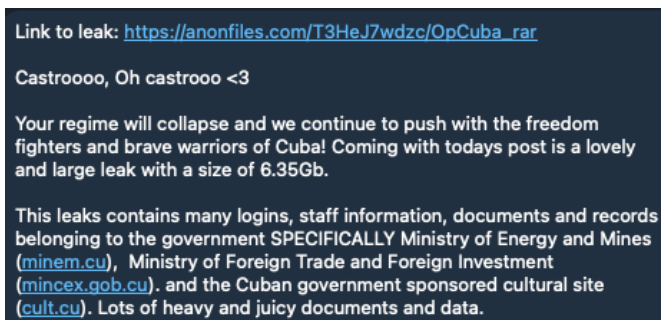
- **ThreatSec** - data powstania: 22.05.2023

Grupa jest odpowiedzialna za m.in. ataki na genesys.com oraz Rosję:






- **GhostSec** – data powstania: 25.10.2020

Grupa jest odpowiedzialna za m.in. ataki na Iran oraz Kubę:



- **Stormous** – data powstania: 30.04.2021

Grupa jest odpowiedzialna za m.in. próbę ataku na polską Izbę Rozliczeniową Giełd Towarowych S.A. (do ataku w rzeczywistości nie doszło, a opublikowane przez nich informacje o wycieku okazały się nieprawdziwe) oraz przedsiębiorstwa z Europy:



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** – data powstania: 09.04.2023

Do grupy należy utrzymanie forum oraz wykonywanie pracy medialnej np. poprzez wklejanie do jednego kanału, informacji pochodzących od @FiveFamilies:

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** – data powstania: 03.04.2022

Grupa jest odpowiedzialna za m.in. publikację danych z NATO COI oraz atakami na przedsiębiorstwa amerykańskie:



Do you like leaks? Us too!
Do you like NATO? We don't!
And so, we present... a leak of hundreds of documents retrieved from NATO's COI portal, intended only for NATO countries and partners.



SiegedSec has a delicious hack to show off!
Recently we have targeted Compas Cable, a cable company based in North Carolina, U.S.

We have gained access to their call management server as well as access to their GPS Satellite ^w^ Although this leak is small, we've enjoyed carrying out this hack. We have shut down their GPS Satellite - After wiping their files, exfiltrating some call logs, and disconnecting their receiver-!

purrs meow :3

LEAK: <https://anonfiles.com/lffBpcj5zd/>

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.

Oś czasu ilustrująca powstawanie grup:



Główne Wnioski:

Ransomed[.]vc, na pierwszy rzut oka mogło wydawać się standardowym forum skierowanym do cyberprzestępców. Jednak po dokładniejszej analizie i badaniu wskazówek skrywanych w różnych miejscach w sieci, stało się jasne, że jest to tylko szczyt góry lodowej w rozbudowanej sieci zorganizowanej działalności w cyberprzestrzeni.

- Ewolucja Działalności:** Dynamiczna zmiana charakteru strony ransomed[.]vc z forum na "Victim List" w krótkim czasie podkreśla elastyczność i adaptacyjność cyberprzestępczych grup działających w sieci.
- Połączenia między różnymi grupami:** Odkrycie związków między różnymi użytkownikami oraz kanałami na platformie Telegram, w tym BlackForums i @FiveFamilies, pokazuje, jak skomplikowane i wielowarstwowe mogą być powiązania między cyberprzestępczymi organizacjami.
- Wykorzystanie gotowych zasobów:** Korzystanie z gotowych szablonów, takich jak ten z serwisu GitHub, wskazuje, że grupy te skupiają się na efektywności, często kosztem profesjonalizmu.

Rekomendacje:

1. **Nieustanny Monitoring:** Organizacje i jednostki muszą nieustannie monitorować i analizować działalność cyberprzestępczą. To nie tylko pozwoli na wczesne wykrycie potencjalnych zagrożeń, ale także da lepsze zrozumienie sposobów działania i motywacji przestępców.
2. **Szkolenia dla pracowników:** Zrozumienie, że cyberprzestępczość jest złożoną i dynamicznie rozwijającą się dziedziną jest kluczem. Organizacje powinny inwestować w regularne szkolenia z zakresu cyberbezpieczeństwa dla swoich pracowników.
3. **Współpraca międzyorganizacyjna:** W obliczu tak złożonych zagrożeń, współpraca między różnymi jednostkami, państwami i organizacjami prywatnymi staje się niezbędna. Dzielenie się informacjami o zagrożeniach, taktyce przestępców i najlepszych praktykach może być kluczem do skutecznego zwalczania cyberprzestępczości.

W rezultacie, ta analiza ransomed[.]vc podkreśla fakt, że cyberprzestępczość stała się bardziej złożona, wymyślna i skoordynowana. Działania podejmowane przez organizacje i jednostki muszą być równie dynamiczne i wszechstronne, aby skutecznie przeciwdziałać tym zagrożeniom w cyfrowym świecie.

