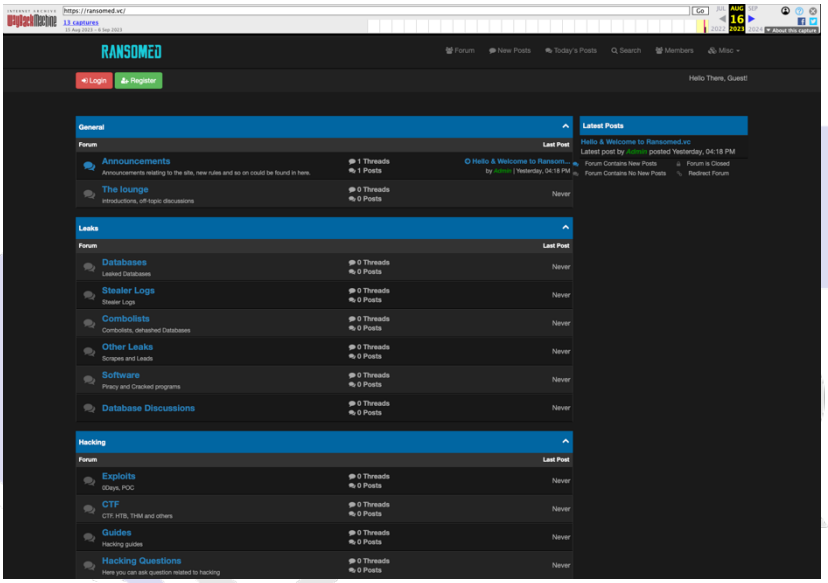
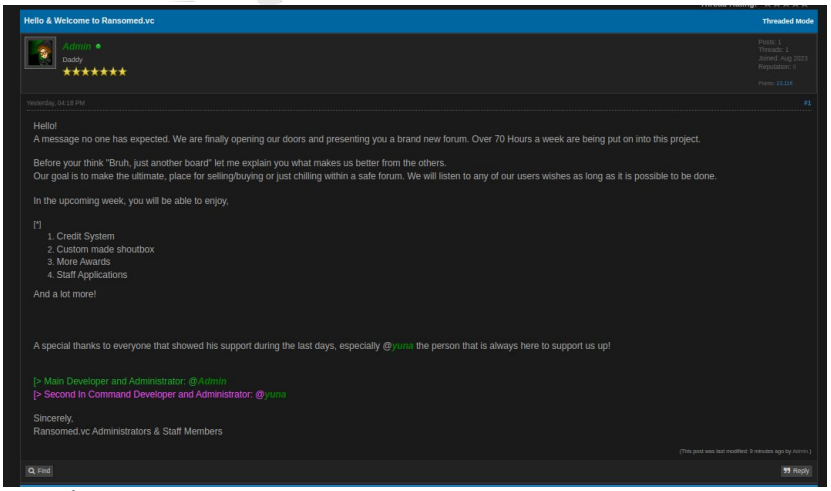
RANSOMED[.]VC – forum, ransomware czy haktywiści?

Wstęp:
Współczesna cyberprzestępczość jest złożoną i dynamicznie rozwijającą się dziedziną, która koncentruje się nie tylko na osiągnięciu zysku, ale także na wpływaniu 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:

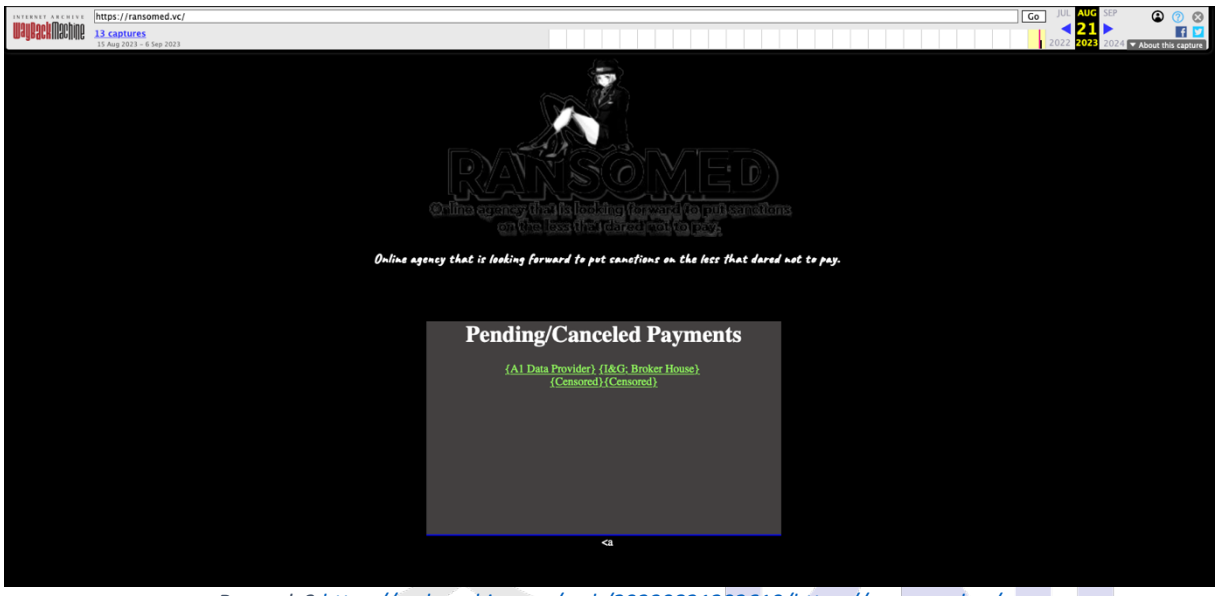


Rysunek 1 https://web.archive.org/web/20230816134436/https://ransomed.vc/



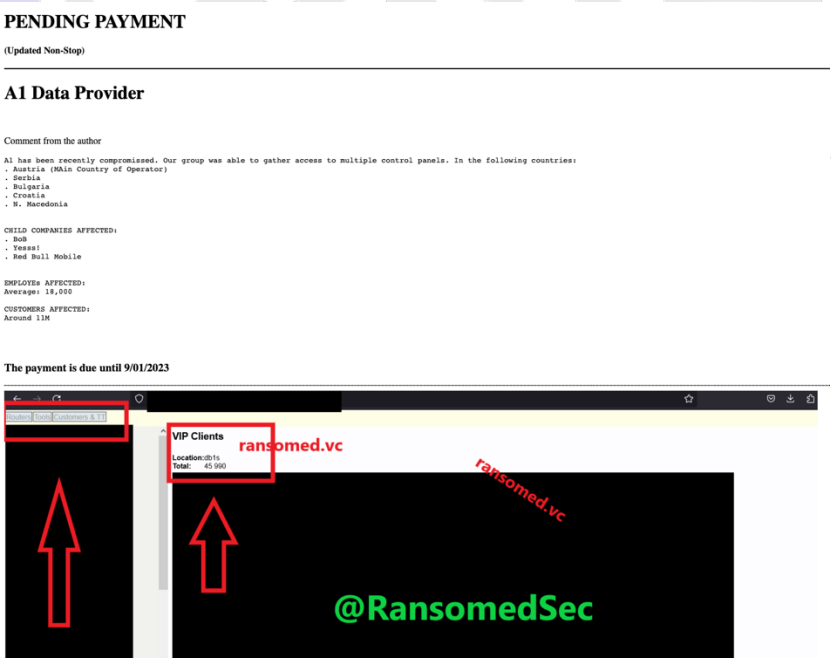
Rysunek 2 Źródło: https://twitter.com/FalconFeedsio/status/1691764241156673677/photo/1

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



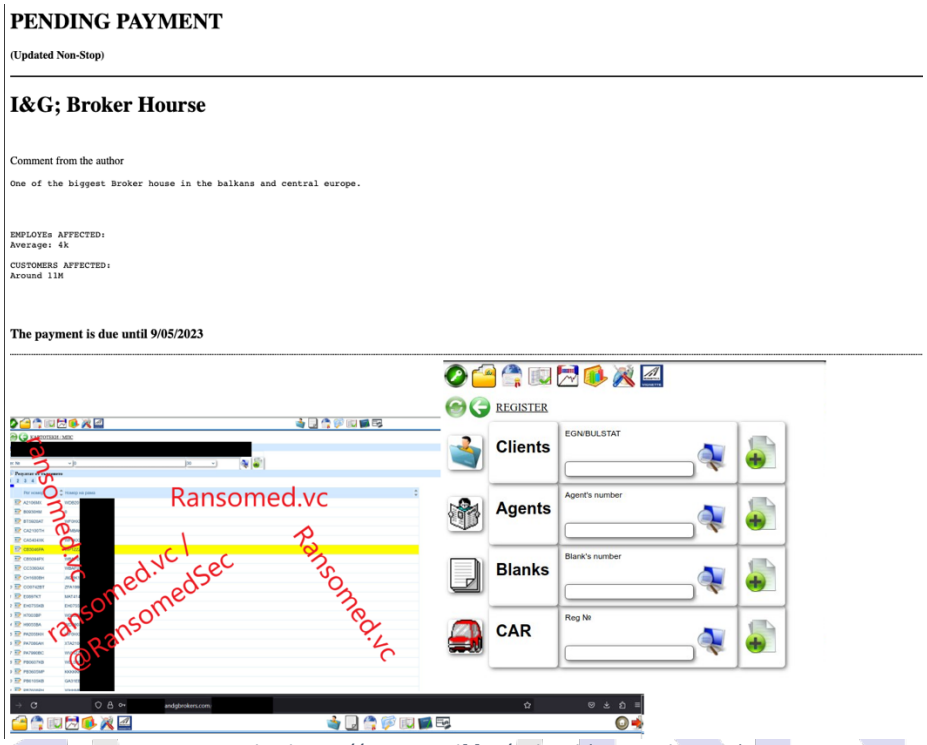
Rysunek 3 https://web.archive.org/web/20230821202610/https://ransomed.vc/

Pierwszymi ofiarami, osób stojących za ransomed[.]vc były firmy:
- A1 Data Provider:



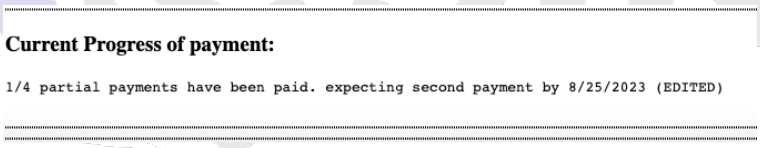
Rysunek 4 https://ransomed[.]vc/a1.html (już nieaktywny)

- I&G; Broker House:



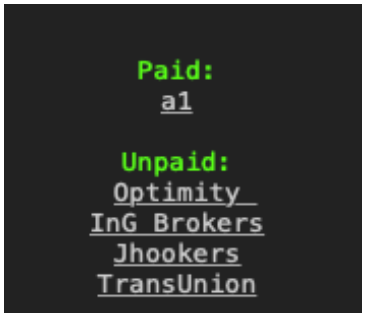
Rysunek 5 https://ransomed[.]vc/ig.html (już nieaktywny)

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

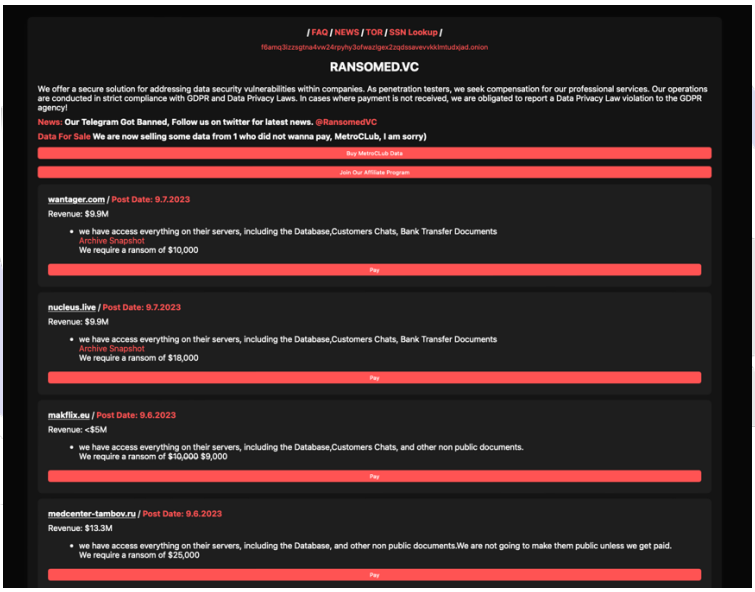
Lub opłaciły je w całości:



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

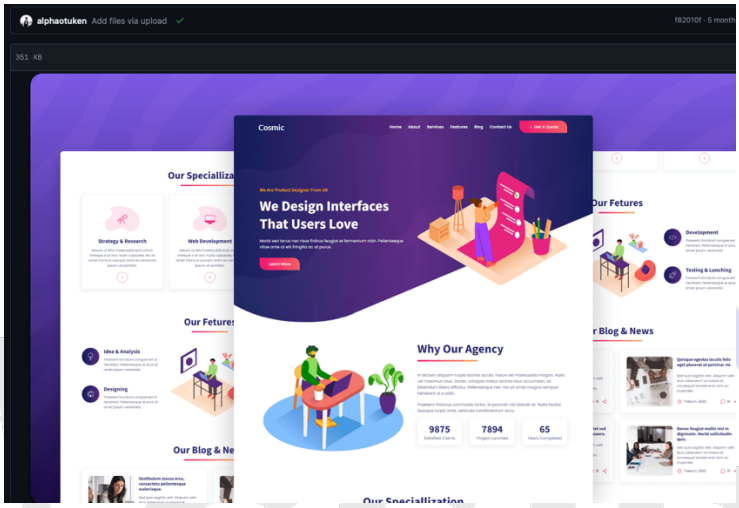
Po krótkiej analizie wyników z fuzz'era, można byłoby stwierdzić, że ransomed[.]vc korzysta z gotowych elementów szablonu pochodzącego z serwisu GitHub (https://github.com/alphaotuken/Cosmic), od zapewne nieświadomego użytkownika @alphaotuken:

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

/**
 * copyright 2023 alphaotuken
 */



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

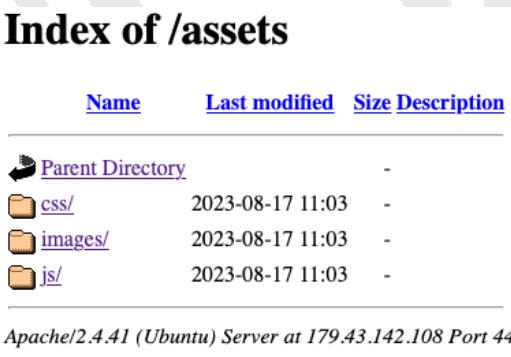
Rysunek 10 Fragment kodu pochodzący z pliku .css ze strony https://ransomed[.]vc

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

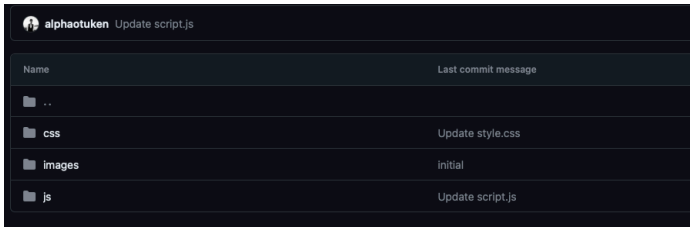


Index of /assets

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 wesji strony ransomed[.]vc

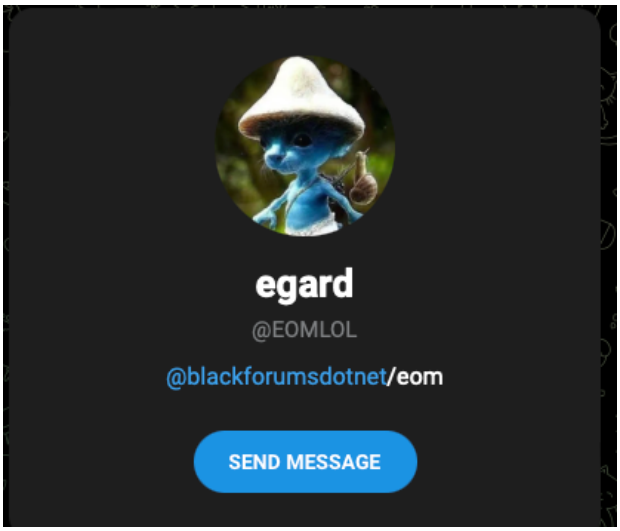
Dla porównania <meta name> w nowej wersji strony: ransomed[.]vc:

<!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, -

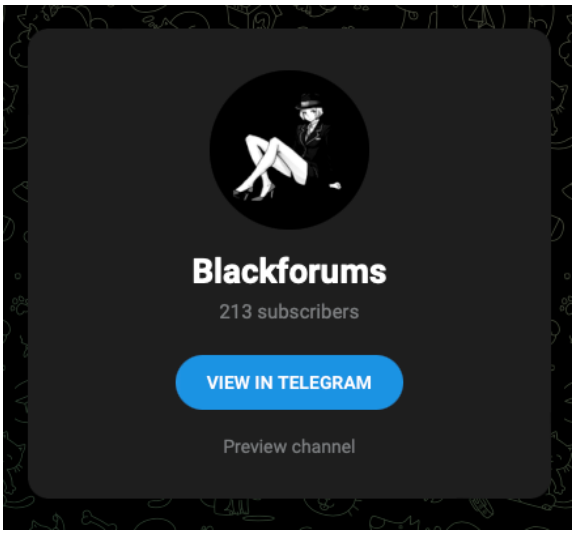
Rysunek 16 Meta name z najnowszej wesji strony ransomed[.]vc (na dzień 06.09.2023)

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

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



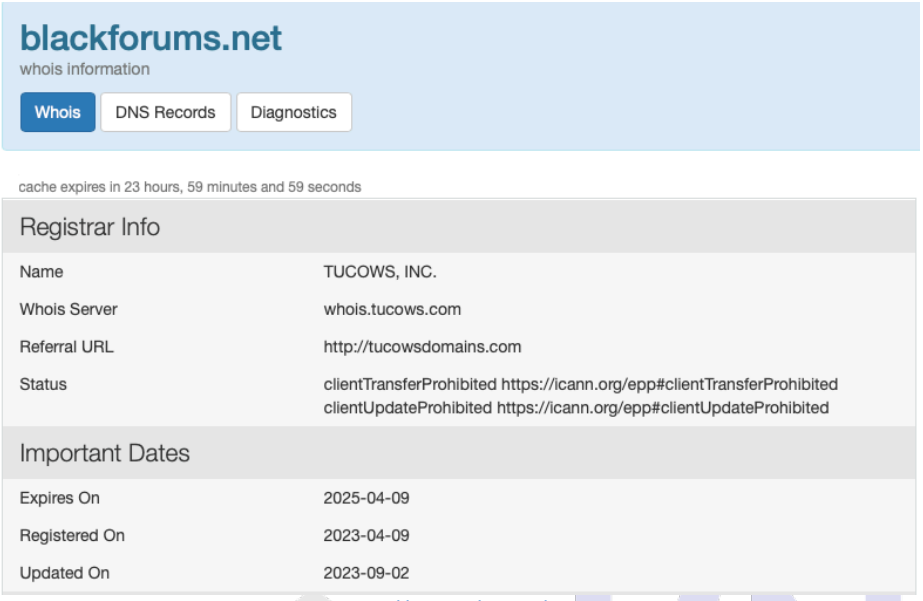
Rysunek 18 Wizytówka kanału @Blackforumsdotnet

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

Rysunek 19 Wiadomość na kanale @Blackforumsdotnet

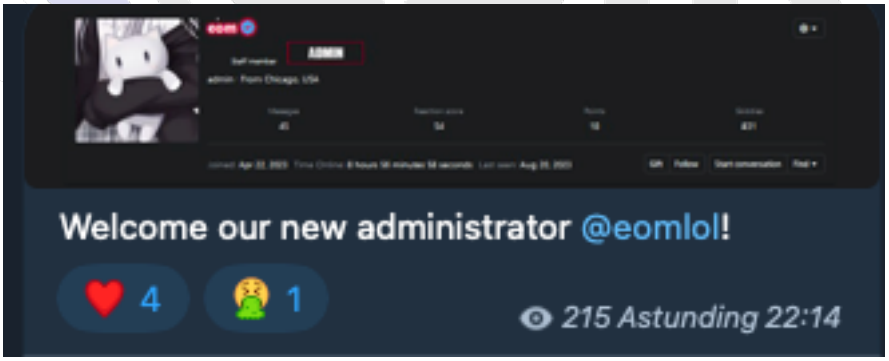
W wiadomości mamy linki do kolejnych kanałów, które przenoszą do chatów społeczności forum hxxps://blackforums[.]net

Who.is dla domeny blackforums[.]net:



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

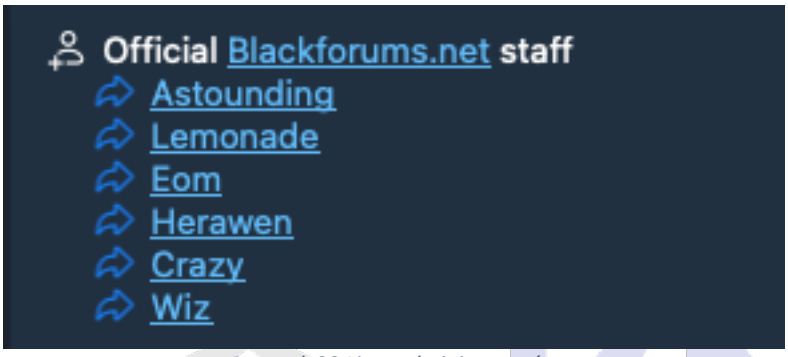
Wracając do kanałów Telegram powiązanych z BlackForums, jeden z nich możemy określić jako „main channel”: hxxps://t[.]me/blackforumsbf, gdzie w dniu 05.09.2023 użytkownik: @EOMLOL został ogłoszony jednym z administratorów forum:



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

Jako zespół administrujący BlackForums wymienieni są użytkownicy tacy jak:

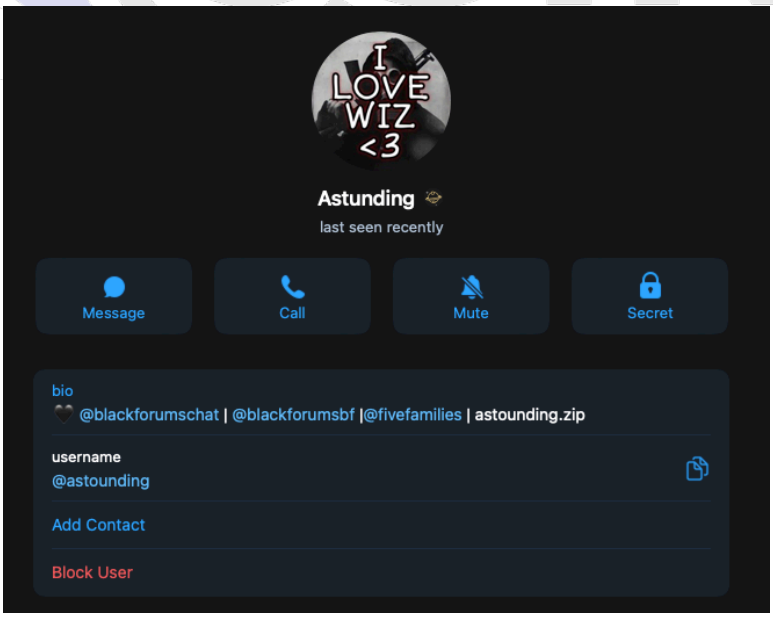
@Astounding
@Lemonade
@Eom
@Herawen
@Crazy
@Wiz



Rysunek 22 Lista administratorów

Przejdźmy do analizy, każdego konta z powyższych:
Nazwa:
@Astounding

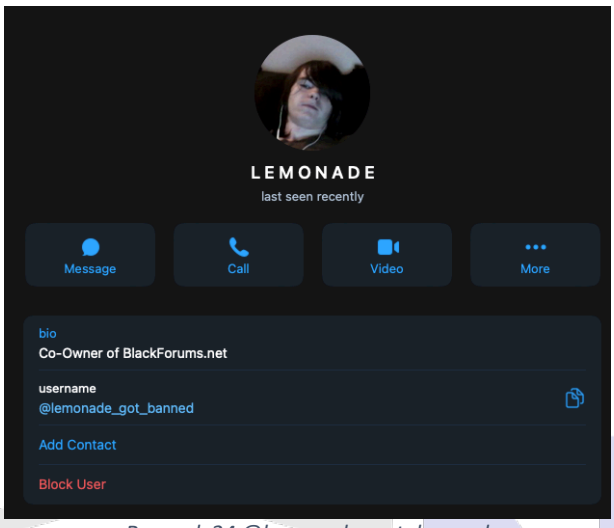
Opis:
🖤 @blackforumschat | @blackforumsbf |@fivefamilies | astounding.zip



Rysunek 23 @Astounding

Nazwa:
@lemonade_got_banned

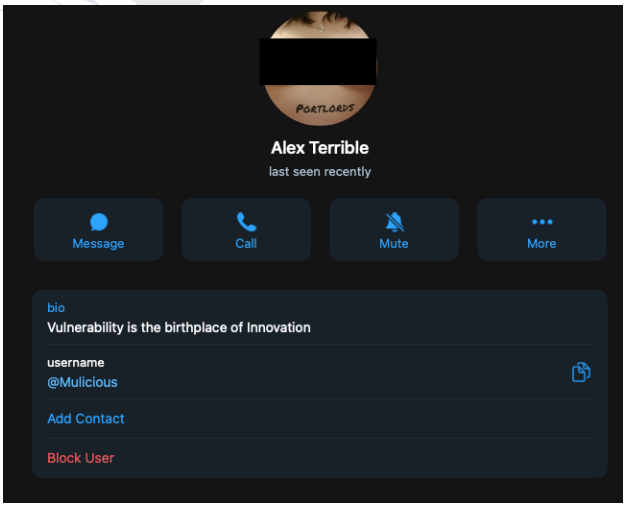
Opis:
Co-Owner of BlackForums.net



Rysunek 24 @lemonade_got_banned

Nazwa:
@Mulicious

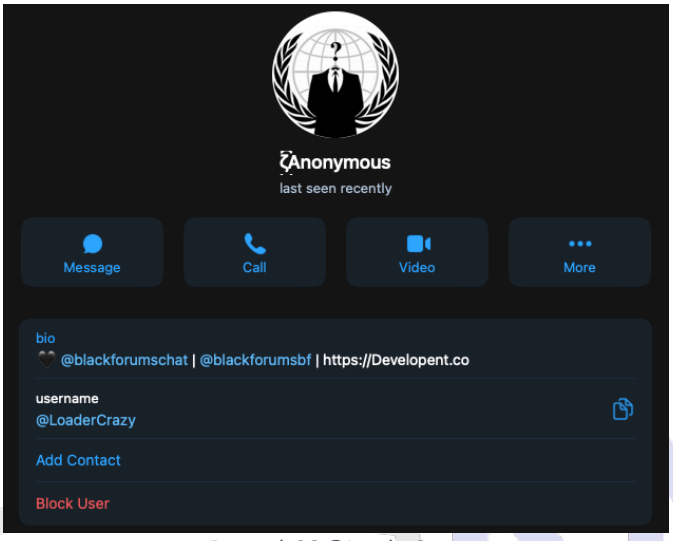
Opis:
Vulnerability is the birthplace of Innovation



Rysunek 25 @Mulicious

Nazwa:
@LoaderCrazy

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



Rysunek 26 @LoaderCrazy

Nazwa:
@ThreatSecurity

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

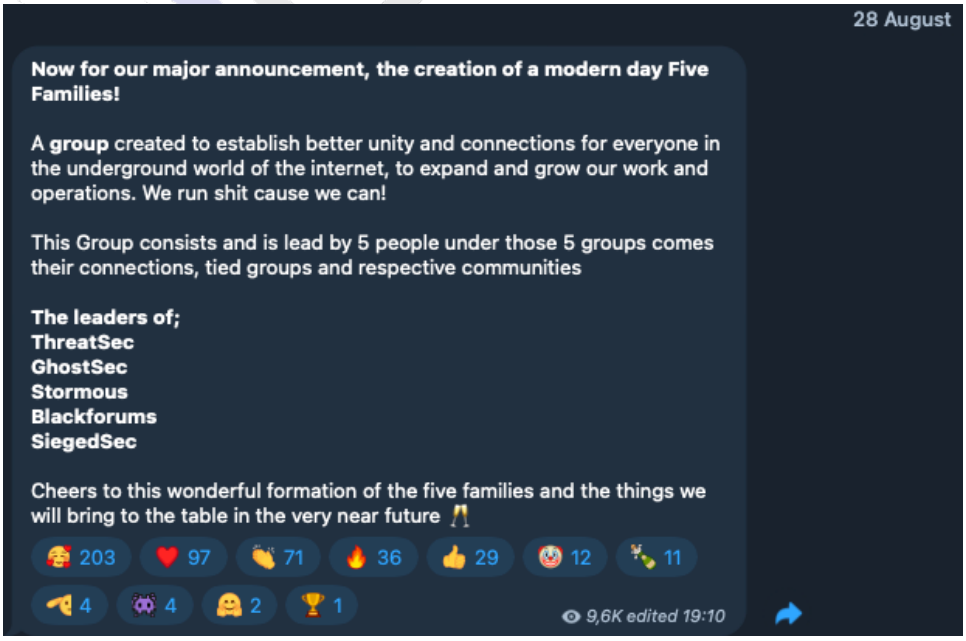
Rysunek 27 @ThreatSecurity

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

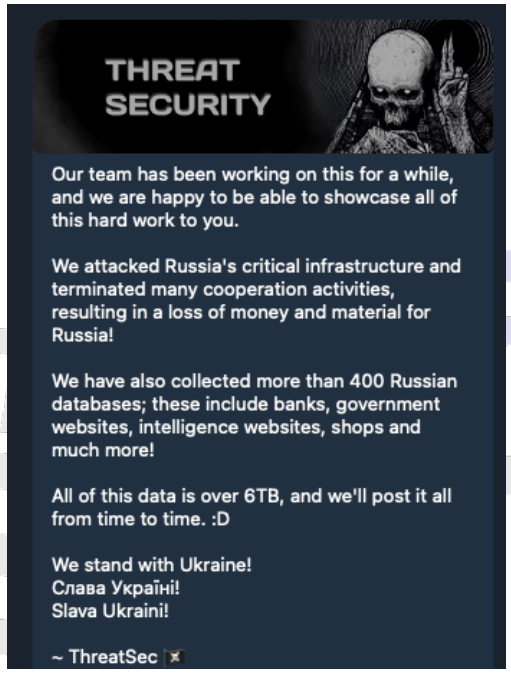
28.08.2023 na kanale @FiveFamilies pojawiła się wiadomość o poniższej treści:



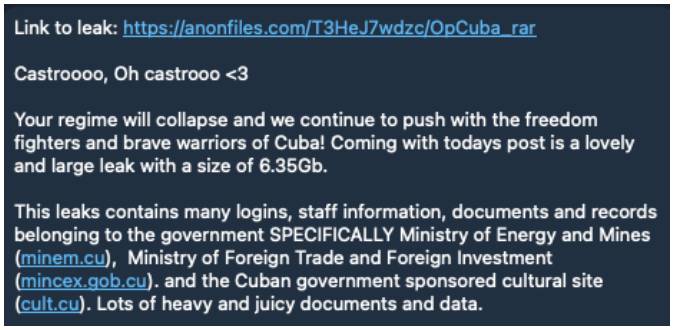
Rysunek 29 hxxps://t[.]me/FiveFamilies/9

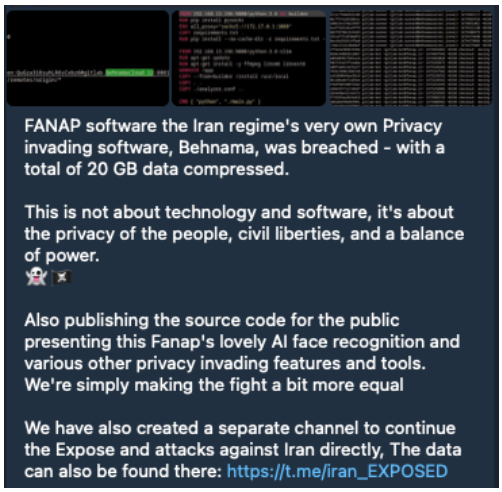
W której to możemy przeczytać, że w skład tytułowej FiveFamilies wchodzą niżej wymienione grupy:

- **ThreatSec** - data powstania: 22.05.2023
Grupa jest odpowiedzialna za m.in. ataki na genesys.com oraz Rosję:

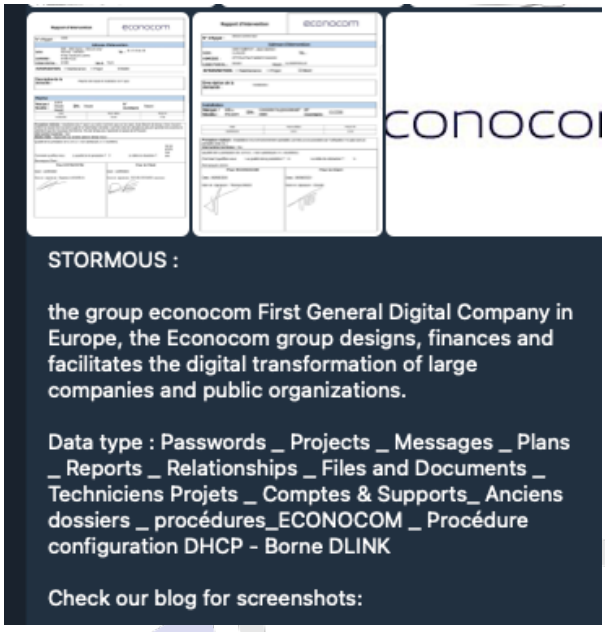


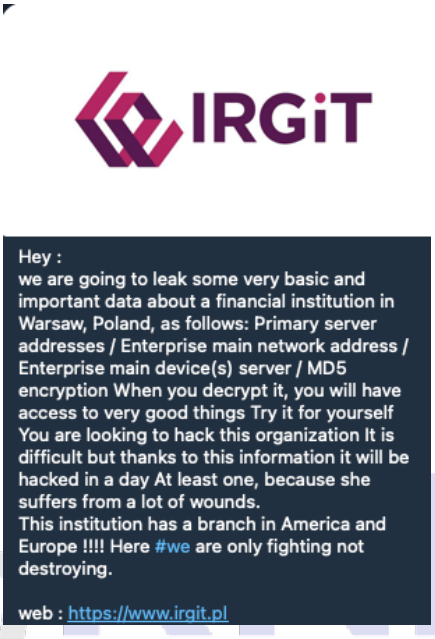
- **GhostSec** – data powstania: 25.10.2020
Grupa jest odpowiedzialna za m.in. ataki na Iran oraz Kubę:



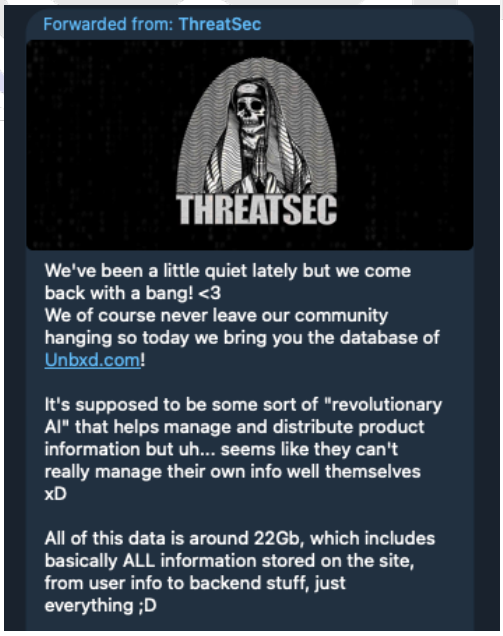


- **Stormous** – data powstania: 30.04.2021
Grupa jest odpowiedzialna za m.in. próbę ataku na polską Izbę Rozliczeniową Giełd Towarowych S.A. (do ataku w rzeczywistości nie doszło, a opublikowane przez nich informacje o wycieku okazały się nieprawdziwe) oraz przedsiębiorstwa z Europy:

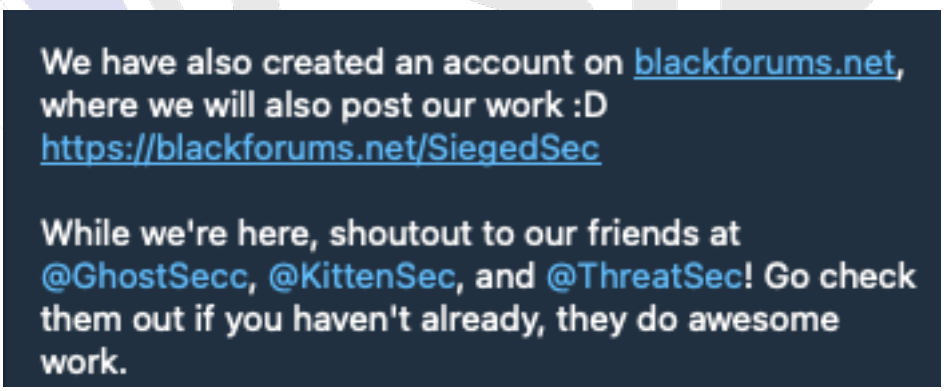




- **Blackforums** – data powstania: 09.04.2023
Do grupy należy utrzymanie forum oraz wykonywanie pracy medialnej np. poprzez wklejanie do jednego kanału, informacji pochodzących od @FiveFamilies:



- SiegedSec – data powstania: 03.04.2022
Grupa jest odpowiedzialna za m.in. publikację danych z NATO COI oraz atakami na przedsiębiorstwa amerykańskie:



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.

1. **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.
2. **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.
3. **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.