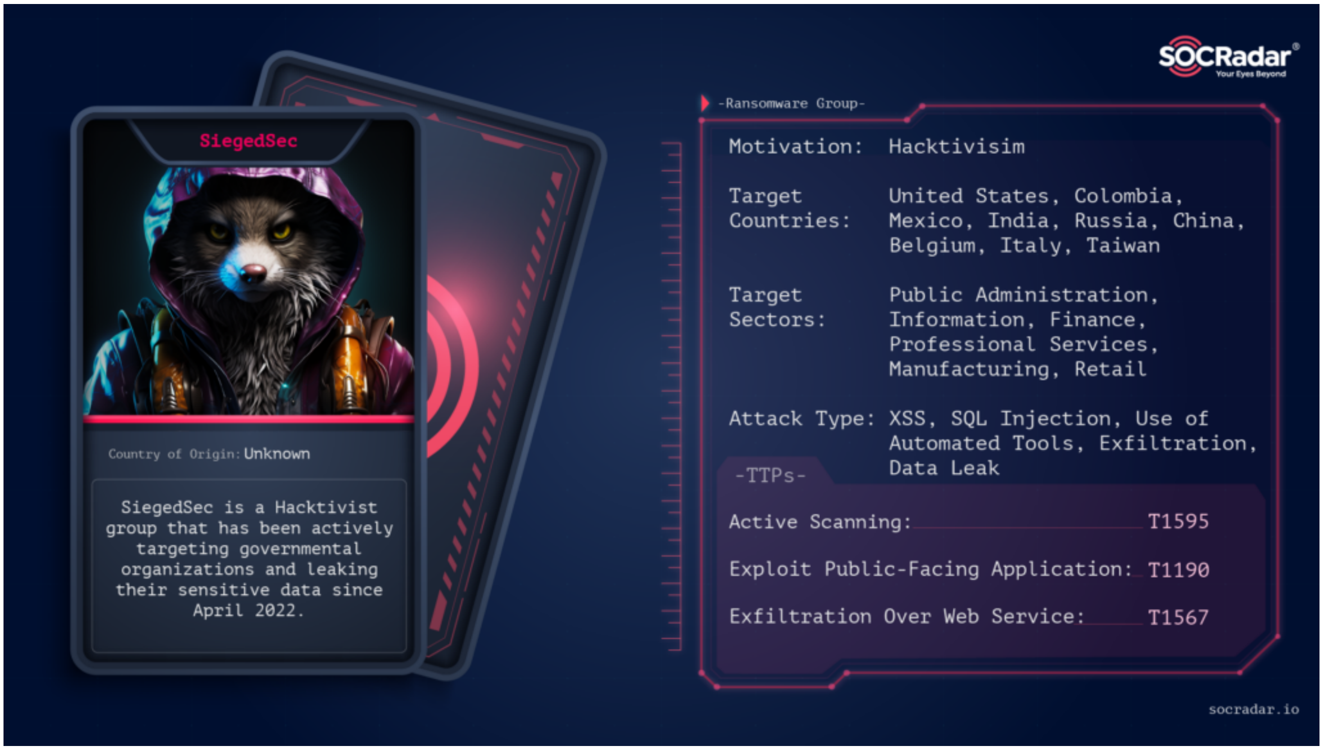
Threat Actor Profile: SiegedSec

socradar.io/threat-actor-profile-siegedsec/

October 18, 2023

In the ever-changing digital landscape, new cyber adversaries continuously emerge. One of the latest entrants in this arena is SiegedSec, an emergent cyber threat group that gained momentum during Russia's invasion of Ukraine. Positioning themselves as masters of data leaks, they have expanded their reach, targeting many sectors across the globe. This article seeks to demystify SiegedSec, offering insights into their attack methodologies, instruments, victims, and most recent activities, while also offering advice on how businesses can fortify their defenses against such cyber onslaughts.



Country of Origin: Unknown

SiegedSec is a Hacktivist group that has been actively targeting governmental organizations and leaking their sensitive data since April 2022.

-Ransomware Group-

Motivation: Hacktivisim

Target Countries: United States, Colombia, Mexico, India, Russia, China, Belgium, Italy, Taiwan

Target Sectors: Public Administration, Information, Finance, Professional Services, Manufacturing, Retail

Attack Type: XSS, SQL Injection, Use of Automated Tools, Exfiltration, Data Leak

-TTPs-

Active Scanning: T1595

Exploit Public-Facing Application: T1190

Exfiltration Over Web Service: T1567

SiegedSec Threat Actor Profile card

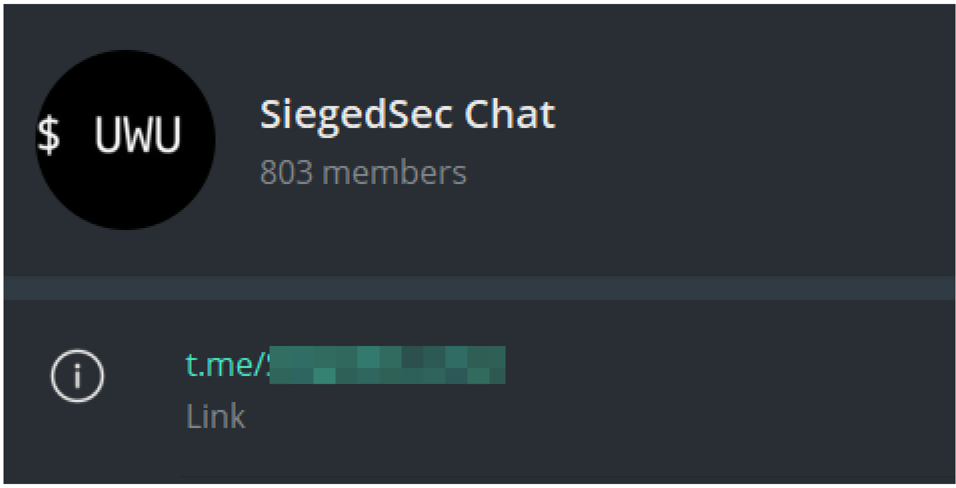
Who is SiegedSec?

SiegedSec is a hacktivist group that appeared coincidentally days before Russia's invasion of Ukraine. Under the leadership of a hacktivist known as **"YourAnonWolf"**, the group has swiftly advanced in its potency, announcing an increasing volume of victims after they appeared.

> The group self-identifies itself as "gay furry hackers" and is known for its comical slogans and vulgar language. They have connections with other hacker groups like GhostSec and have members probably ranging in age from 18 to 26.

The group created its Telegram channel on April 3, 2022, which can be taken as the date of the first appearance of the group.

The group also has a chat channel where, apart from attacks, a lot of casual conversation and sexual jokes are made:



SiegedSec Chat

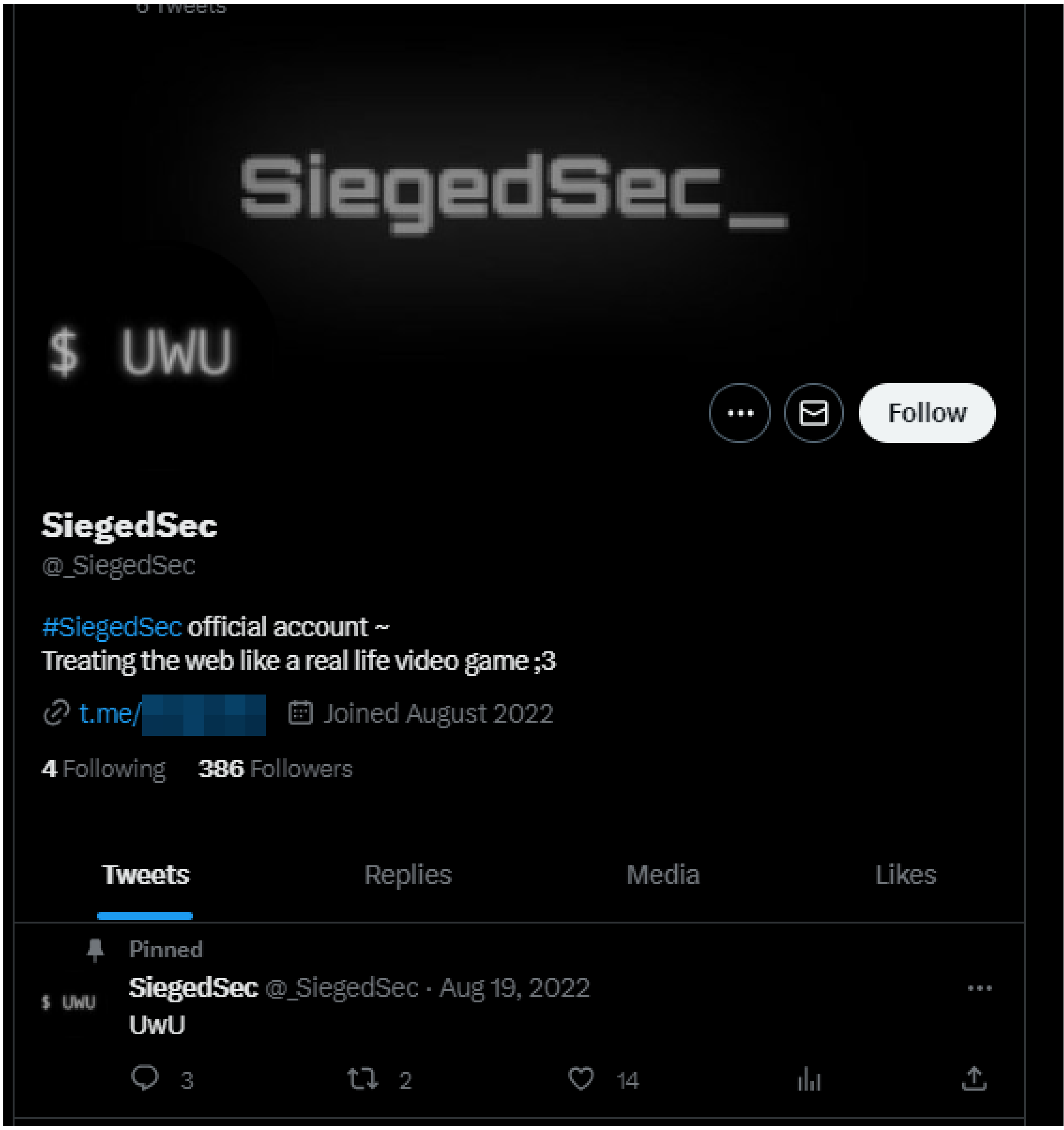
803 members

t.me/[redacted]

Link

Fig. 1. Telegram chat channel of SiegedSec

The last thing that caught our eye was the group’s Twitter account, which was continuously suspended:



SiegedSec
@_SiegedSec

#SiegedSec official account ~
Treating the web like a real life video game ;3

t.me/[redacted] Joined August 2022

4 Following 386 Followers

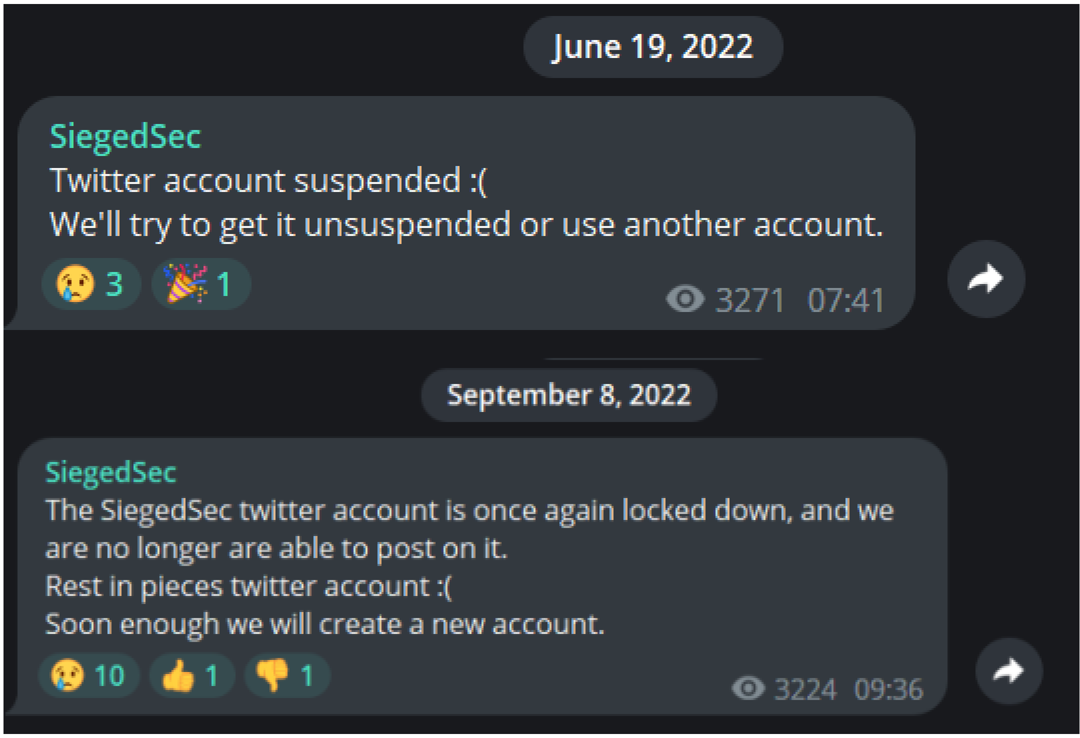
Pinned
SiegedSec @_SiegedSec · Aug 19, 2022
UwU

3 2 14

Fig. 2.

Twitter page of SiegedSec

We see that the Twitter page of SiegedSec has been inactive for a long time; we think this is due to the fact that they are frequently suspended.



June 19, 2022

SiegedSec
Twitter account suspended :(
We'll try to get it unsuspended or use another account.

😢 3 🎉 1 3271 07:41

September 8, 2022

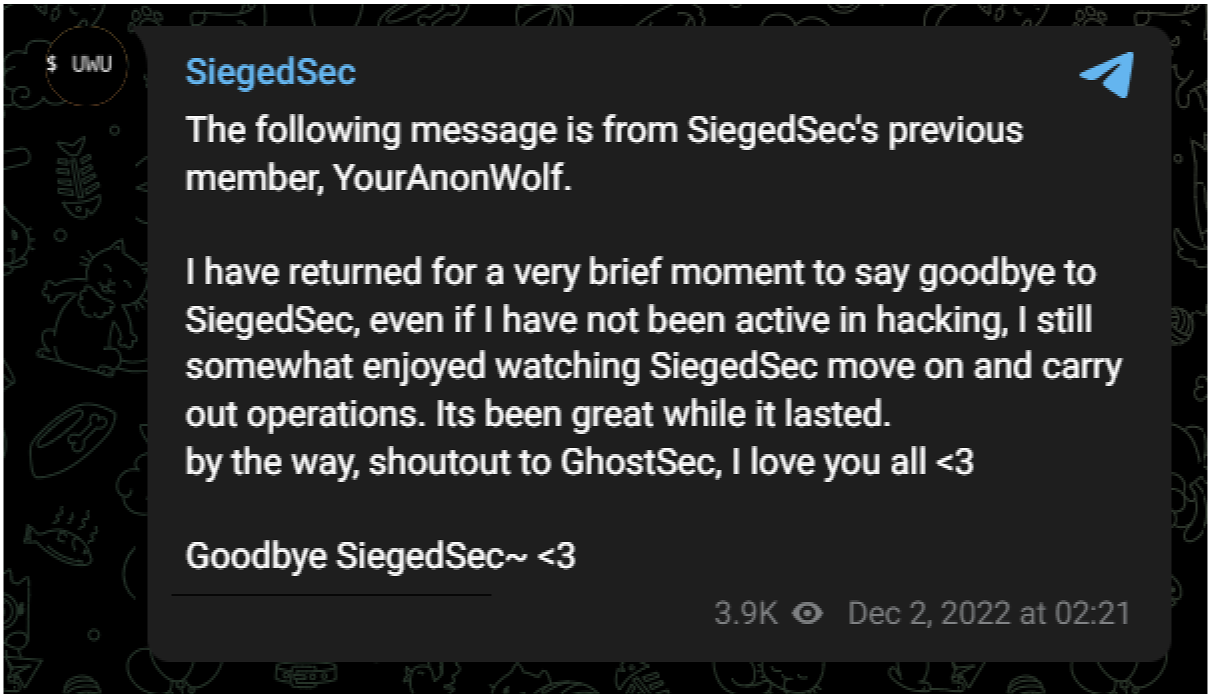
SiegedSec
The SiegedSec twitter account is once again locked down, and we are no longer are able to post on it.
Rest in pieces twitter account :(
Soon enough we will create a new account.

😢 10 👍 1 👎 1 3224 09:36

Fig. 3. Some of SiegedSec's Telegram posts complaining about their Twitter accounts being suspended

The founder/administrator of the group is "YourAnonWolf". When we look at the chat channel, we see that the user is currently managing the group under the nickname **vio**.

We have seen posts about vio leaving the group at various times, but we don't know which user was running the group when vio left.



SiegedSec
The following message is from SiegedSec's previous member, YourAnonWolf.

I have returned for a very brief moment to say goodbye to SiegedSec, even if I have not been active in hacking, I still somewhat enjoyed watching SiegedSec move on and carry out operations. Its been great while it lasted.
by the way, shoutout to GhostSec, I love you all <3

Goodbye SiegedSec~ <3

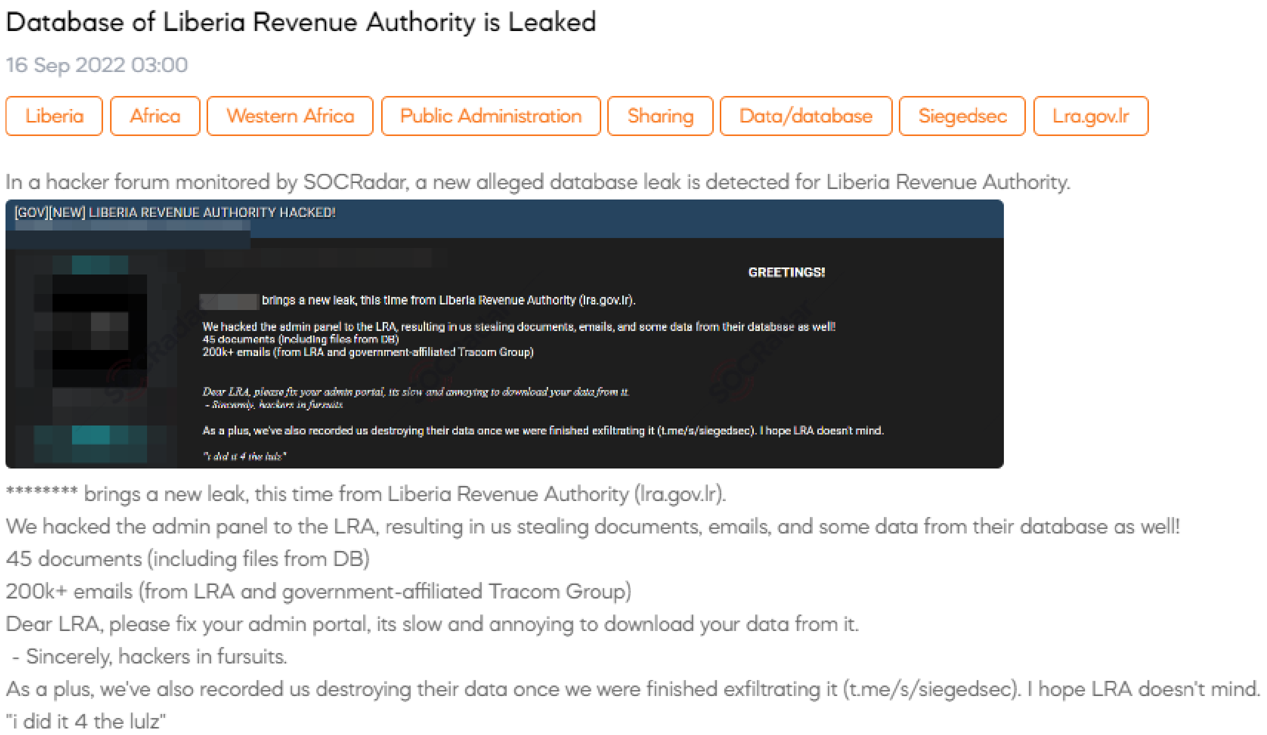
3.9K Dec 2, 2022 at 02:21

Fig. 4. One of vio's messages leaving SiegedSec

How does SiegedSec attack?

SiegedSec's attacks include:

- Defacement and compromise of websites,
- Leaking sensitive information,
- Gaining unauthorized access to databases and emails.



Database of Liberia Revenue Authority is Leaked

16 Sep 2022 03:00

Liberia | Africa | Western Africa | Public Administration | Sharing | Data/database | Siegedsec | Lra.gov.lr

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for Liberia Revenue Authority.

[GOV][NEW] LIBERIA REVENUE AUTHORITY HACKED!

GREETINGS!

[redacted] brings a new leak, this time from Liberia Revenue Authority (lra.gov.lr).

We hacked the admin panel to the LRA, resulting in us stealing documents, emails, and some data from their database as well!
45 documents (including files from DB)
200k+ emails (from LRA and government-affiliated Tracom Group)

Dear LRA, please fix your admin portal, its slow and annoying to download your data from it.
- Sincerely, hackers in fursuits.

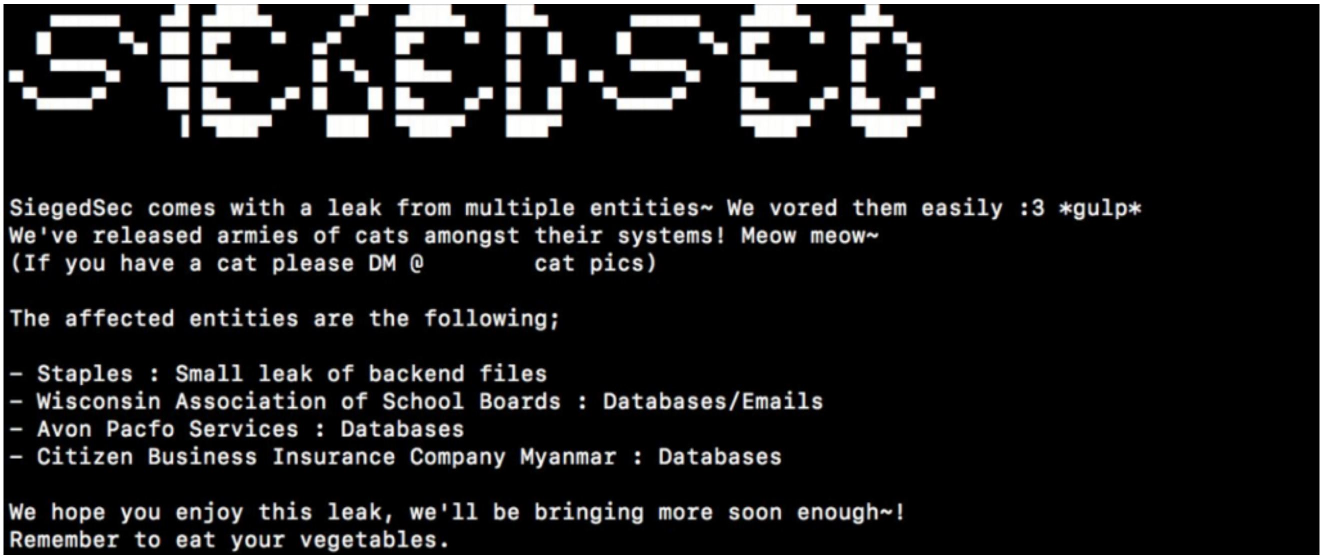
As a plus, we've also recorded us destroying their data once we were finished exfiltrating it (t.me/s/siegedsec). I hope LRA doesn't mind.

"i did it 4 the lulz"

******** brings a new leak, this time from Liberia Revenue Authority (lra.gov.lr).
We hacked the admin panel to the LRA, resulting in us stealing documents, emails, and some data from their database as well!
45 documents (including files from DB)
200k+ emails (from LRA and government-affiliated Tracom Group)
Dear LRA, please fix your admin portal, its slow and annoying to download your data from it.
 - Sincerely, hackers in fursuits.
As a plus, we've also recorded us destroying their data once we were finished exfiltrating it (t.me/s/siegedsec). I hope LRA doesn't mind.
"i did it 4 the lulz"

Fig. 5. A database leak post made by a member of the group on BreachForum (Source:SOCRadar)

Their attacks often include juvenile and crude language and graphics. Based on some of the group's posts, the group says that the attacks are for fun.



```
SiegedSec comes with a leak from multiple entities~ We vored them easily :3 *gulp*
We've released armies of cats amongst their systems! Meow meow~
(If you have a cat please DM @        cat pics)

The affected entities are the following;

- Staples : Small leak of backend files
- Wisconsin Association of School Boards : Databases/Emails
- Avon Pacfo Services : Databases
- Citizen Business Insurance Company Myanmar : Databases

We hope you enjoy this leak, we'll be bringing more soon enough~!
Remember to eat your vegetables.
```

Fig. 6. An example of an attack announcement made by the group

SiegedSec's attacks are primarily carried out using basic **SQL injection and Cross-Site Scripting (XSS)** attacks. The group's technical prowess has been compared to **Lulzsec**, a high-profiled cyber threat group from the early 2010s.

What are the targets of SiegedSec?

Sectors

They have targeted companies across diverse industry sectors, including healthcare, IT, insurance, legal, and finance.

Including current events, such as NATO, it is observed that it mostly attacks the sector called "Public Administration", in other words, government organizations.

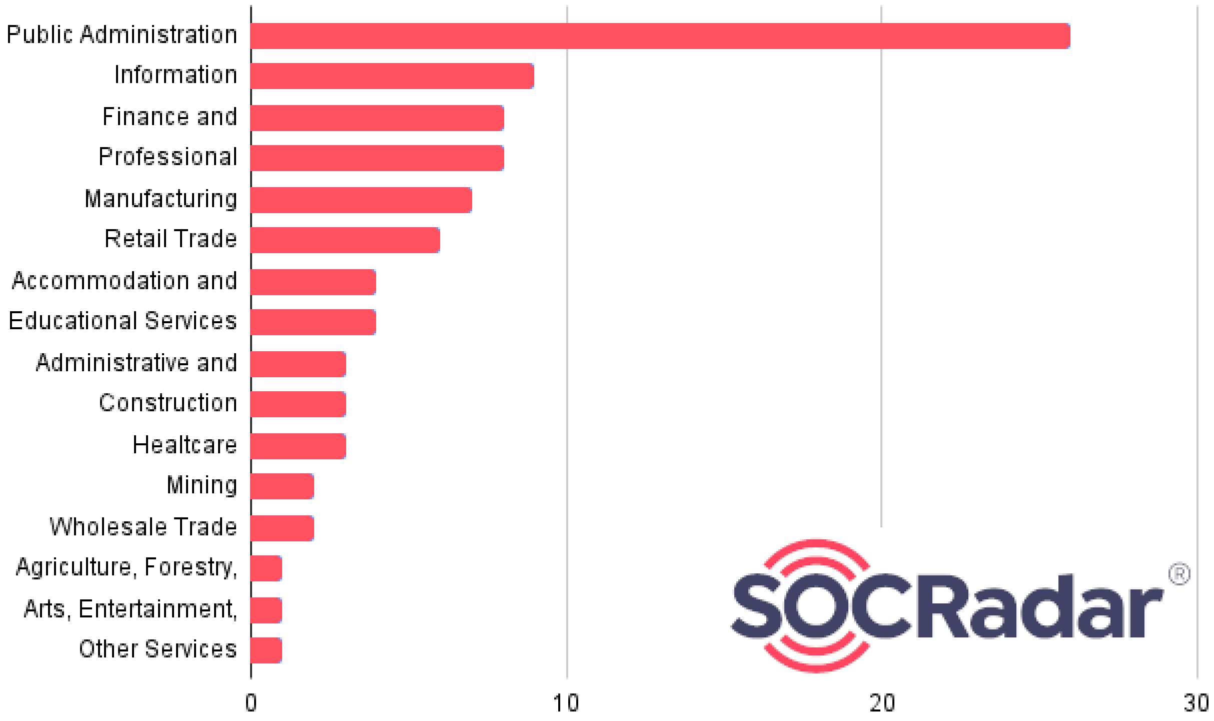


Fig. 7. Distribution of industries in which companies are affected by SiegedSec (Source: SOCRadar)

Countries

SiegedSec has successfully targeted companies across various industries and locations, including **India**, **Indonesia**, **South Africa**, **USA**, **Philippines**, **Mexico**, and others. They have leaked data from at least 30 different companies since their start in February 2022, showing no preference for industries or locations.

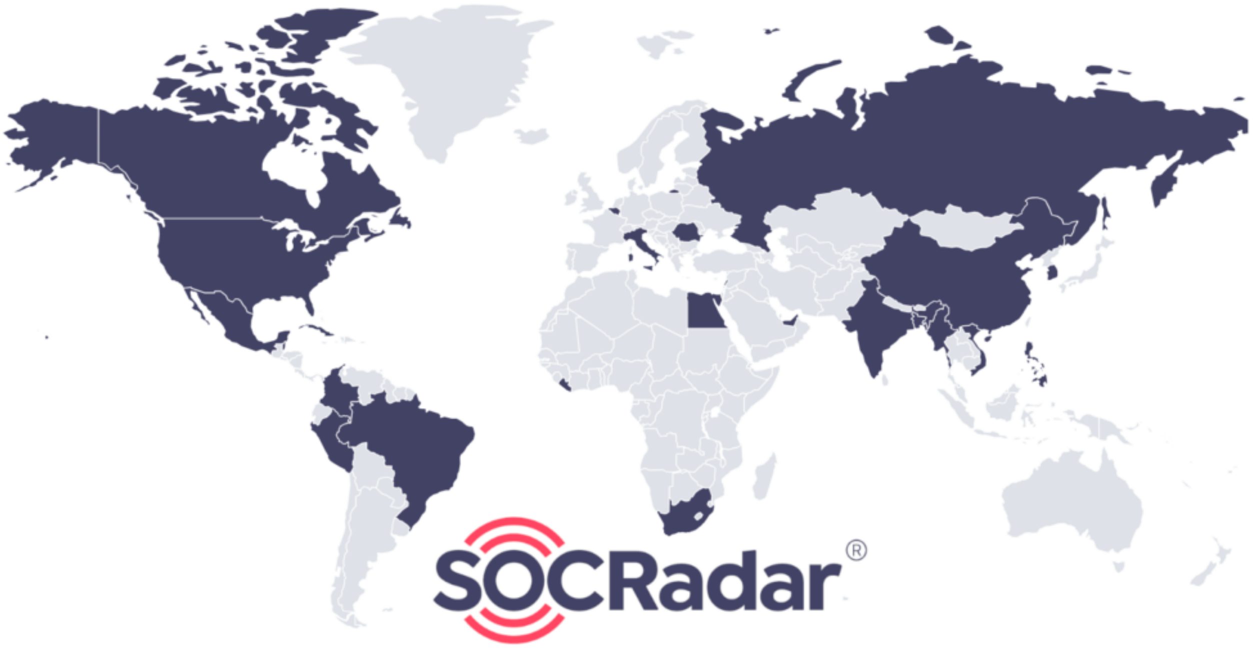


Fig. 8. Countries Affected by SiegedSec (Source: SOCRadar)

Checking the countries where the organizations they attacked are located, it is seen that the majority (about **32%**) is the organizations located in the **United States**.

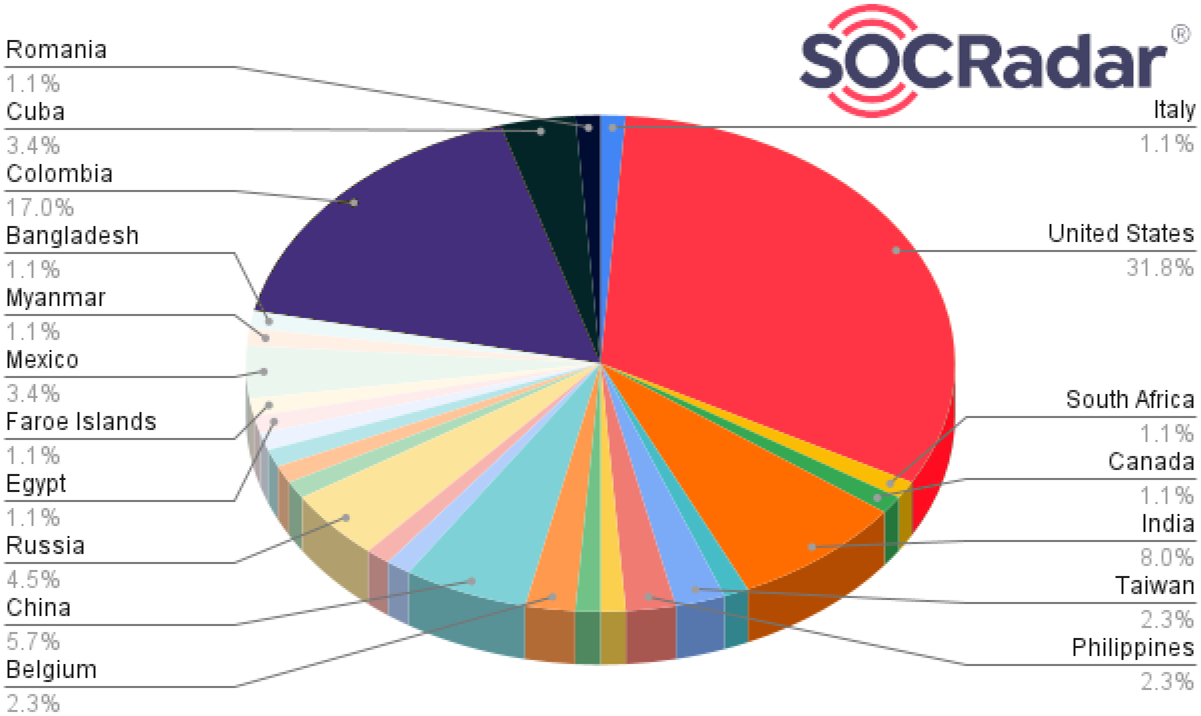
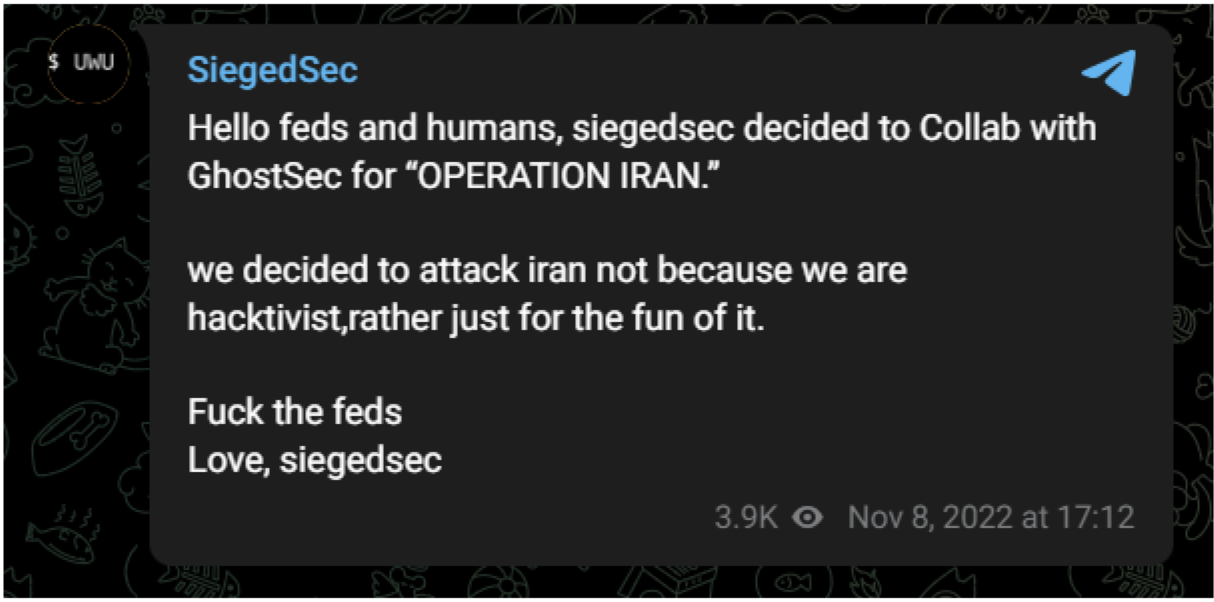


Fig. 9. Affected country distribution from SiegedSec (Source: SOCRadar)

Is there any relation between SiegedSec and other groups?

Looking at some of the group’s posts, it seems that they have a friendly relationship with **GhostSec**, another hacktivist group.



SiegedSec

Hello feds and humans, siegedsec decided to Collab with GhostSec for "OPERATION IRAN."

we decided to attack iran not because we are hacktivist,rather just for the fun of it.

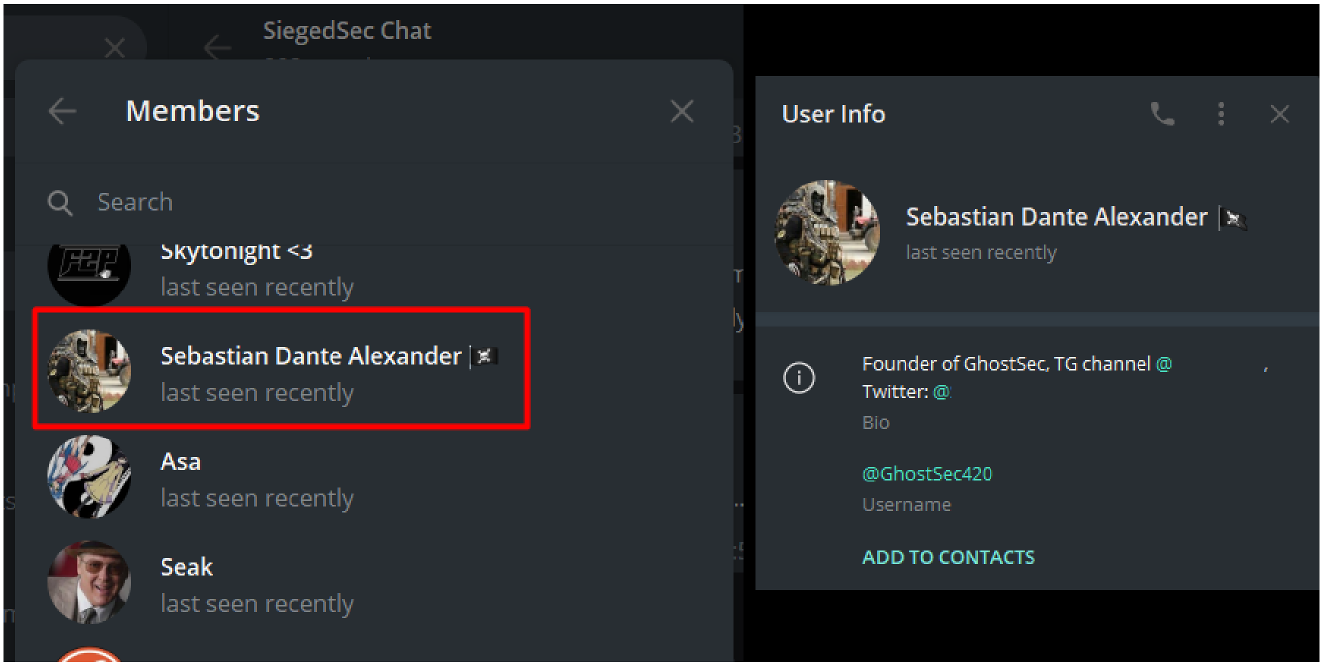
Fuck the feds
Love, siegedsec

3.9K Nov 8, 2022 at 17:12

Fig. 10.

SiegedSec's announcement that they will assist GhostSec's "Operation Iran" activity

At the same time, in SiegedSec's chat group, we see that there is a user who manages the GhostSec's Telegram channel and in the profile information of SiegedSec's administrator vio, we see that vio is a GhostSec member.



SiegedSec Chat

Members

Search

Skytonight <3
last seen recently

Sebastian Dante Alexander |
last seen recently

Asa
last seen recently

Seak
last seen recently

User Info

Sebastian Dante Alexander |
last seen recently

Founder of GhostSec, TG channel @
Twitter: @
Bio

@GhostSec420
Username

ADD TO CONTACTS

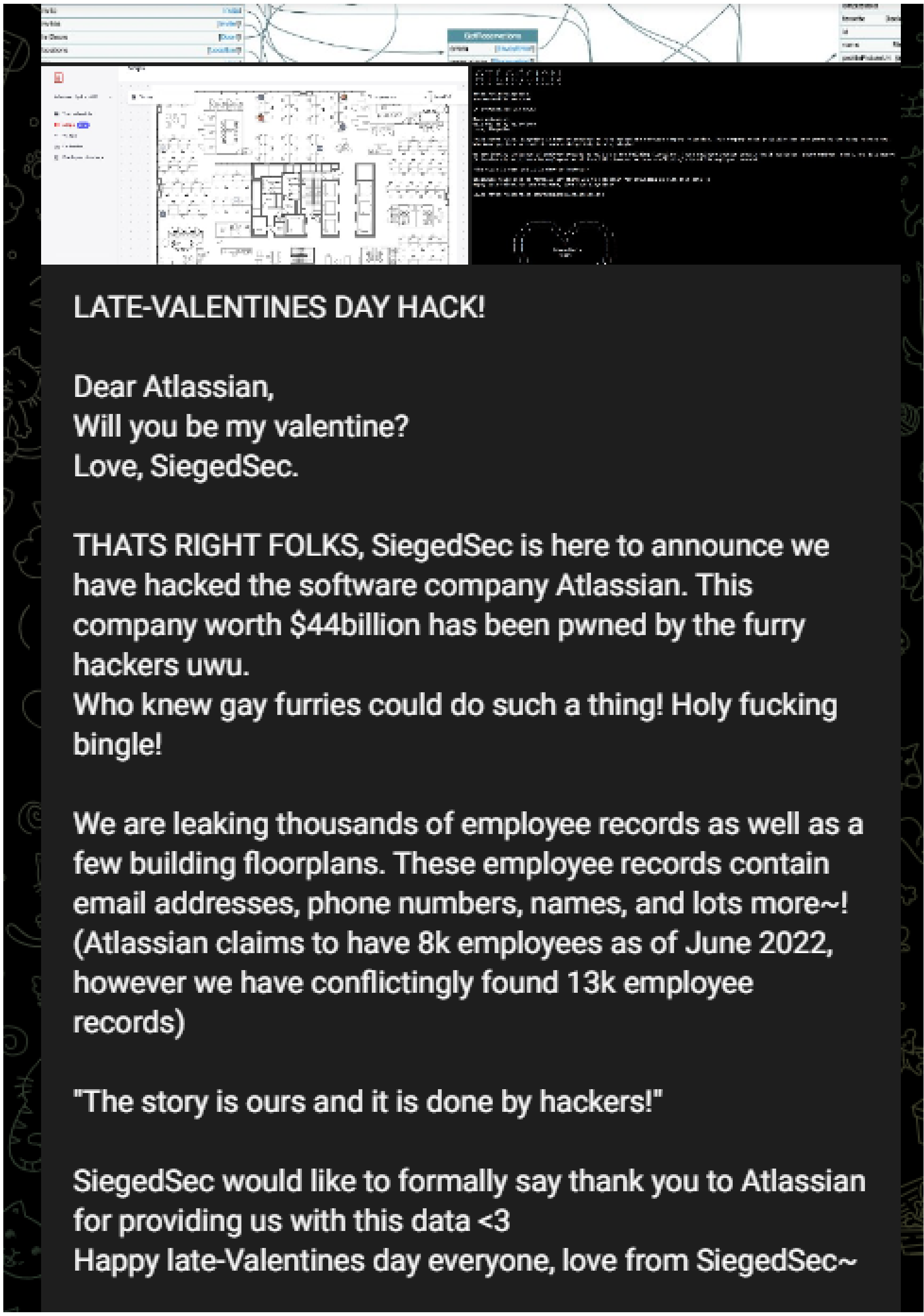
Fig. 11. GhostSec420, a member of the SiegedSec Chat group and Founder of GhostSec

What are the latest activities of SiegedSec?

In recent months, SiegedSec has claimed to have defaced **over 100** domains and leaked significant volumes of stolen data from compromised networks.

Atlassian

On February 15, 2023, one day after Valentine's Day, SiegedSec shared a post with a Valentine's Day reference and Atlassian data with employee information.



LATE-VALENTINES DAY HACK!

Dear Atlassian,
Will you be my valentine?
Love, SiegedSec.

THATS RIGHT FOLKS, SiegedSec is here to announce we have hacked the software company Atlassian. This company worth $44billion has been pwned by the furry hackers uwu.
Who knew gay furries could do such a thing! Holy fucking bingle!

We are leaking thousands of employee records as well as a few building floorplans. These employee records contain email addresses, phone numbers, names, and lots more~! (Atlassian claims to have 8k employees as of June 2022, however we have conflictingly found 13k employee records)

"The story is ours and it is done by hackers!"

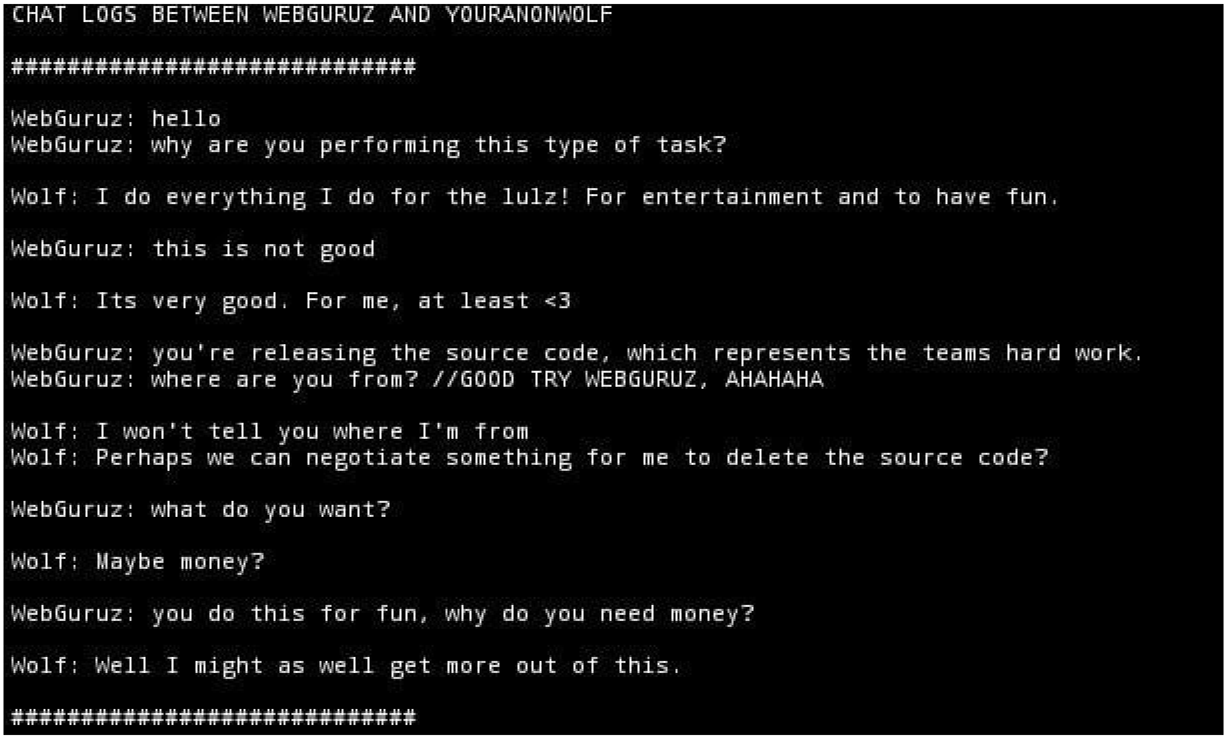
SiegedSec would like to formally say thank you to Atlassian for providing us with this data <3
Happy late-Valentines day everyone, love from SiegedSec~

Fig. 12. SiegedSec's Telegram post about Atlassian

NewsVoir

In late May, they targeted an India-based online news distribution outlet, NewsVoir, leaking extensive documents and data.

They have also hinted at a possible interest in financial compensation for their campaigns. Communication between them and WebGuruz Technologies shows that the possibility of SiegedSec turning to a data extortion team, such as Karakurt, is increasing

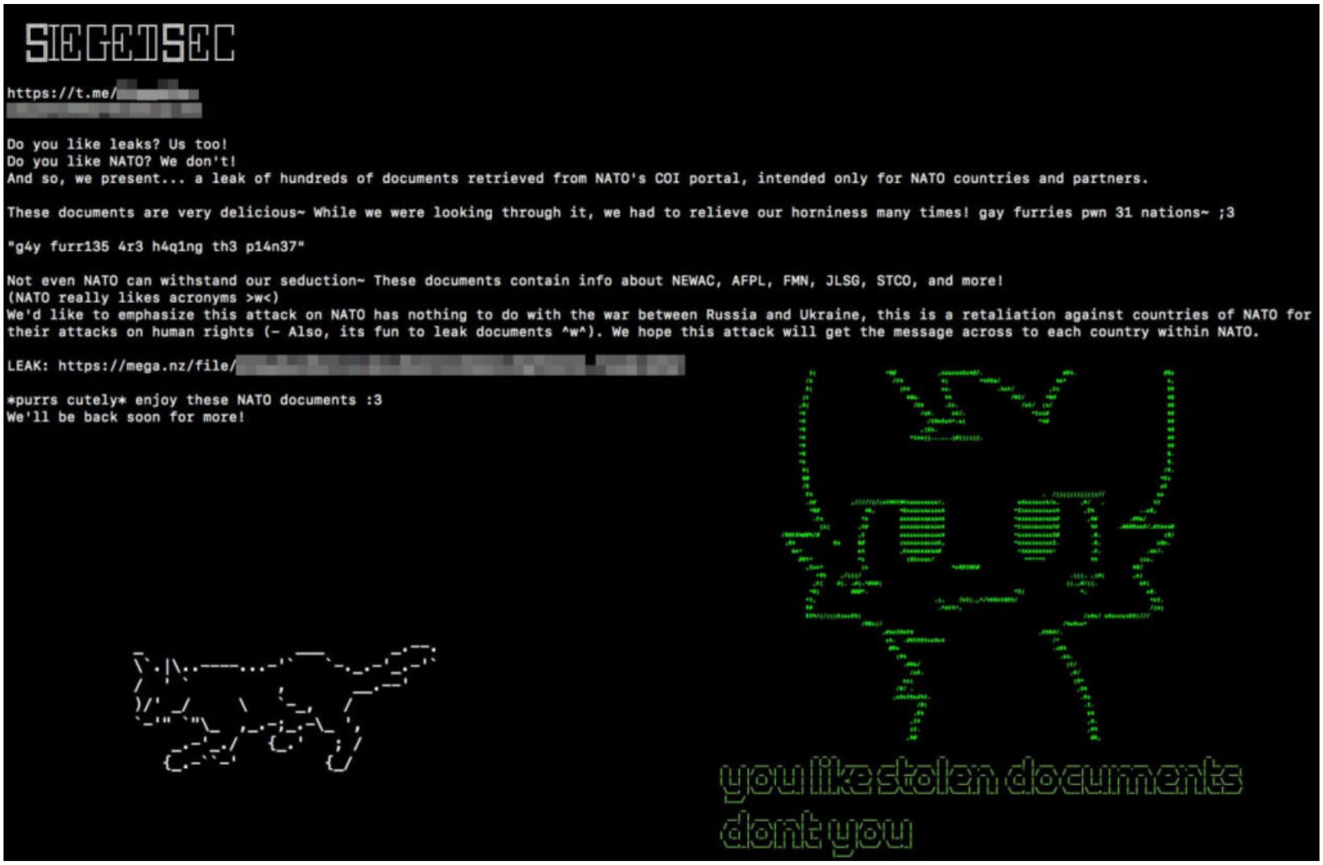


```
CHAT LOGS BETWEEN WEBGURUZ AND YOURANONWOLF

#############################

WebGuruz: hello
WebGuruz: why are you performing this type of task?

Wolf: I do everything I do for the lulz! For entertainment and to have fun.

WebGuruz: this is not good

Wolf: Its very good. For me, at least <3

WebGuruz: you're releasing the source code, which represents the teams hard work.
WebGuruz: where are you from? //GOOD TRY WEBGURUZ, AHAHAHA

Wolf: I won't tell you where I'm from
Wolf: Perhaps we can negotiate something for me to delete the source code?

WebGuruz: what do you want?

Wolf: Maybe money?

WebGuruz: you do this for fun, why do you need money?

Wolf: Well I might as well get more out of this.

#############################
```

Fig. 13. Chat between SiegedSec's admin vio and WebGuruz Technologies LTD

Communities of Interest (COI)

NATO is actively investigating a claim by the hacking group SiegedSec regarding an alleged data theft from the Communities of Interest (COI) Cooperation Portal, an unclassified platform for NATO members. SiegedSec posted what they claim to be hundreds of documents stolen from the portal on Telegram, including **845 MB** of files and **8,000** rows of sensitive user information. The leak, if confirmed, could impact 31 NATO member nations.



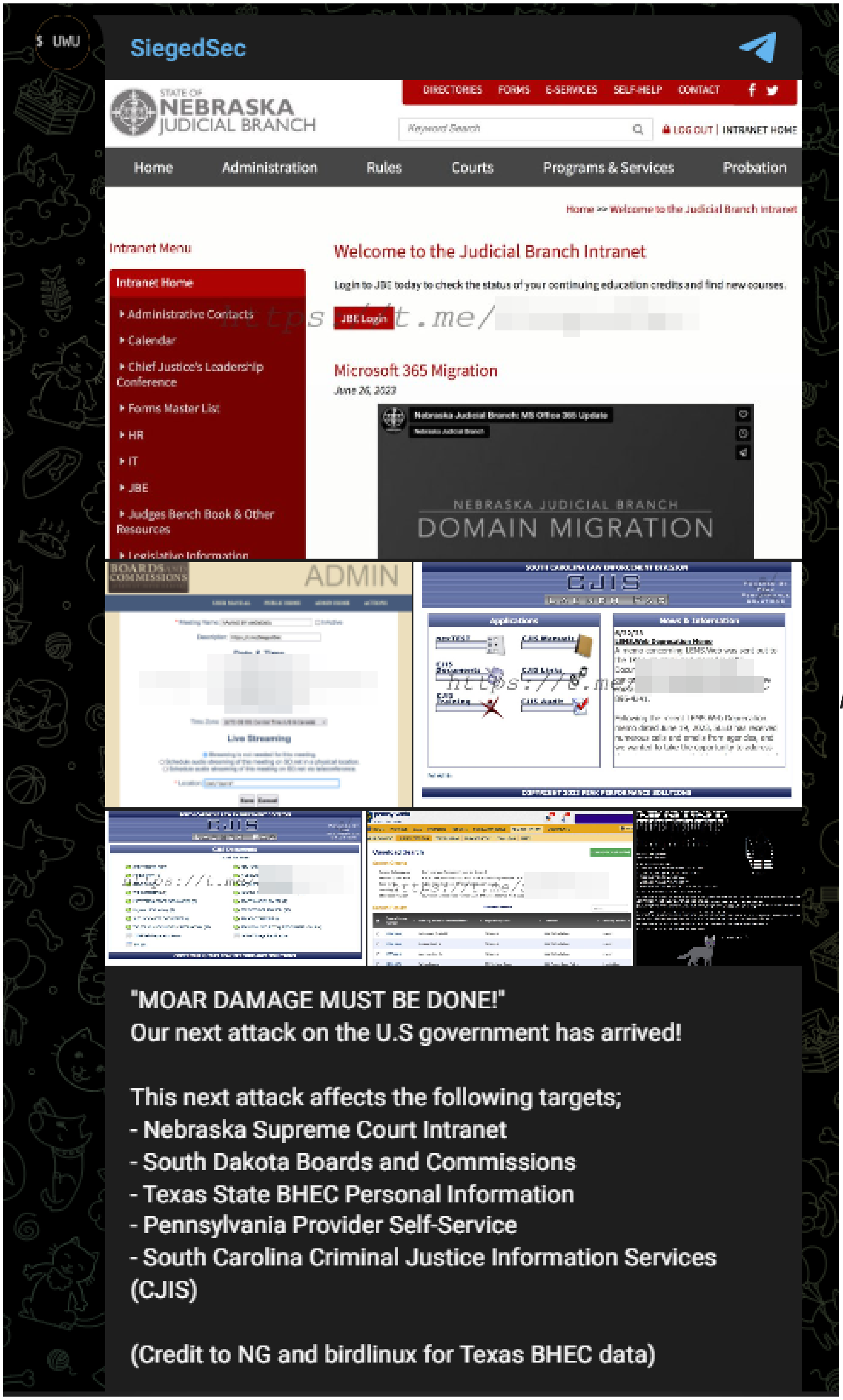
SIEGEDSEC

```
https://t.me/[redacted]

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.

These documents are very delicious~ While we were looking through it, we had to relieve our horniness many times! gay furries pwn 31 nations~ ;3

"g4y furr135 4r3 h4q1ng th3 p14n37"

Not even NATO can withstand our seduction~ These documents contain info about NEWAC, AFPL, FMN, JLSG, STCO, and more!
(NATO really likes acronyms >w<)
We'd like to emphasize this attack on NATO has nothing to do with the war between Russia and Ukraine, this is a retaliation against countries of NATO for
their attacks on human rights (- Also, its fun to leak documents ^w^). We hope this attack will get the message across to each country within NATO.

LEAK: https://mega.nz/file/[redacted]

*purrs cutely* enjoy these NATO documents :3
We'll be back soon for more!
```

Fig. 14. Communities of Interest data leak post of SiegedSec

US Government Websites

In late of June, SiegedSec claimed cyberattacks on five state-run websites, including those related to Nebraska’s Supreme Court, South Dakota’s Boards and Commissions, Texas’s Behavioral Health Executive Council, Pennsylvania’s Provider Self-Service, and South Carolina’s Criminal Justice Information Services (CJIS). Photos of the defaced websites and allegedly stolen data were shared by the group.



Welcome to the Judicial Branch Intranet

Login to JBE today to check the status of your continuing education credits and find new courses.

https://t.me/[redacted]

Microsoft 365 Migration

June 26, 2023

https://t.me/[redacted]

https://t.me/[redacted]

https://t.me/[redacted]

"MOAR DAMAGE MUST BE DONE!"
Our next attack on the U.S government has arrived!

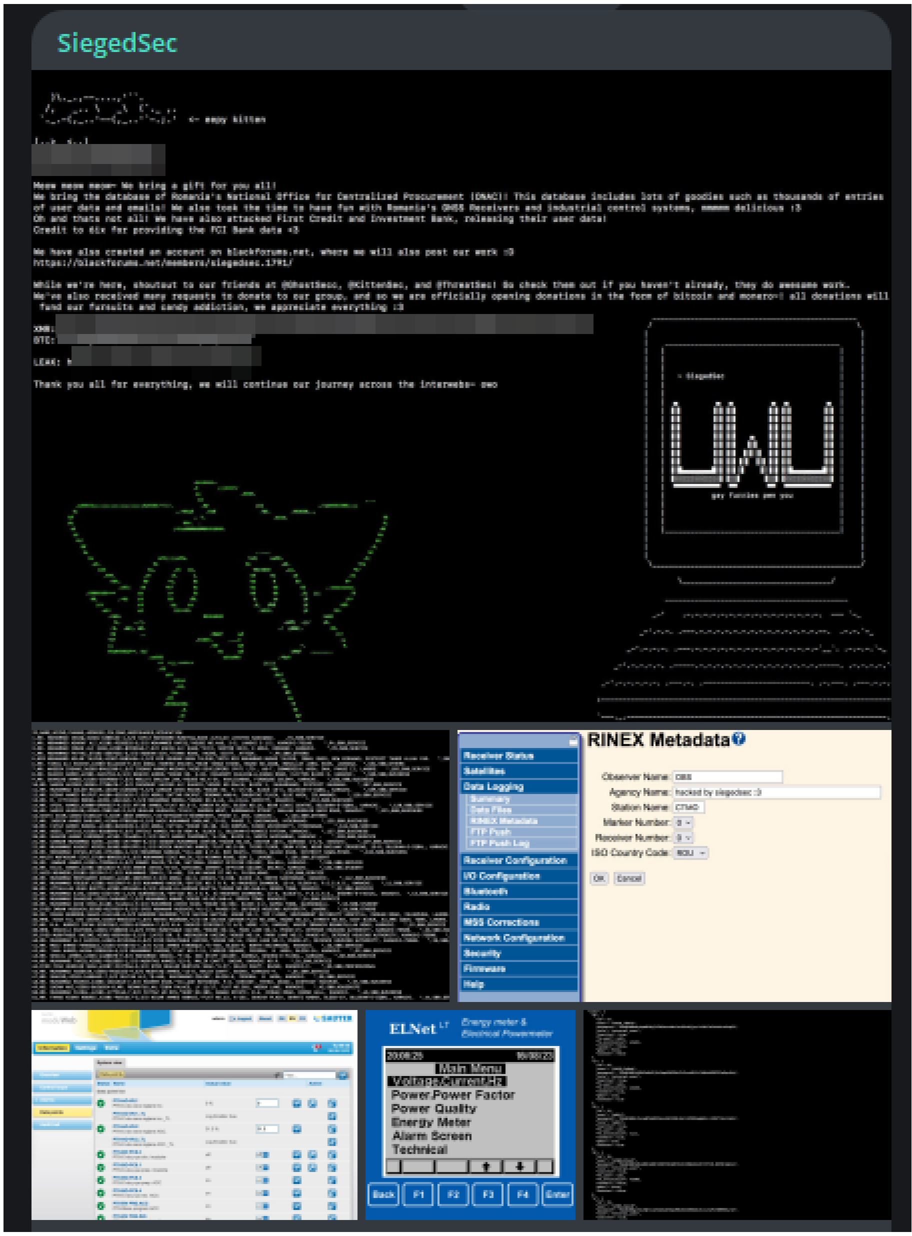
This next attack affects the following targets;
- Nebraska Supreme Court Intranet
- South Dakota Boards and Commissions
- Texas State BHEC Personal Information
- Pennsylvania Provider Self-Service
- South Carolina Criminal Justice Information Services (CJIS)

(Credit to NG and birdlinux for Texas BHEC data)

Fig. 15. SiegedSec's Telegram post about breached US Government websites

Breaches of ONAC, First Credit and Investment Bank

On August 18, SiegedSec claimed responsibility for breaches against Romania's National Office for Centralized Procurement (ONAC) and First Credit and Investment Bank, mentioning an associate of another threat actor, **6ix**, contributing to the latter attack.



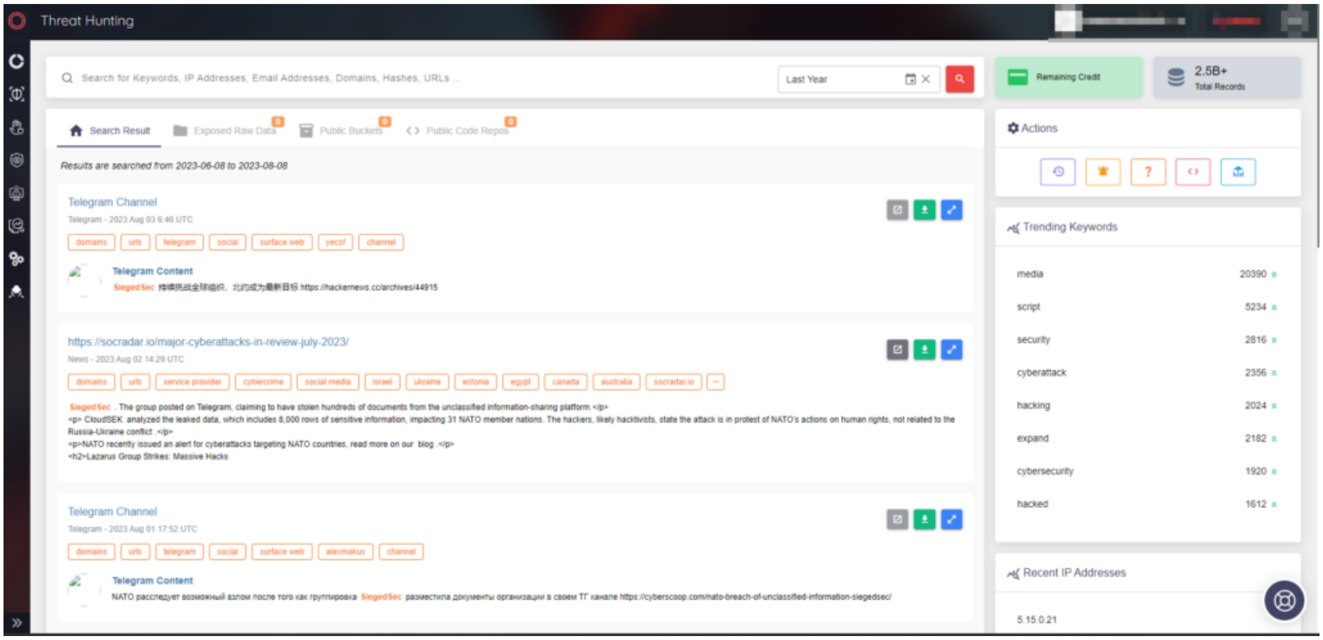
SiegedSec

```
<- eepy kitten

[redacted]

Meow meow meow~ We bring a gift for you all!
We bring the database of Romania's National Office for Centralized Procurement (ONAC)! This database includes lots of goodies such as thousands of entries
of user data and emails! We also took the time to have fun with Romania's GNSS Receivers and industrial control systems, mmmmm delicious :3
Oh and thats not all! We have also attacked First Credit and Investment Bank, releasing their user data!
Credit to 6ix for providing the FCI Bank data <3

We have also created an account on blackforums.net, where we will also post our work :D
https://blackforums.net/members/siegedsec.1791/

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.
We've also received many requests to donate to our group, and so we are officially opening donations in the form of bitcoin and monero~! all donations will
 fund our fursuits and candy addiction, we appreciate everything :3

XMR: [redacted]
BTC: [redacted]

LEAK: [redacted]

Thank you all for everything, we will continue our journey across the interwebs~ owo
```

RINEX Metadata

Observer Name: OBS
Agency Name: hacked by siegedsec :3
Station Name: CTMO
Marker Number: 0
Receiver Number: 0
ISO Country Code: ROU

Fig. 16. ONAC, First Credit and Investment Bank post of SiegedSec



[redacted]

Results are searched from 2023-06-08 to 2023-08-08

Telegram Channel
Telegram - 2023 Aug 03 6:46 UTC
domains | urls | telegram | social | surface web | yecsf | channel
Telegram Content
SiegedSec 持续挑战全球组织。北约成为最新目标 https://hackernews.cc/archives/44915

https://socradar.io/major-cyberattacks-in-review-july-2023/
News - 2023 Aug 02 14:29 UTC
domains | urls | service provider | cybercrime | social media | israel | ukraine | estonia | egypt | canada | australia | socradar.io | ...
SiegedSec . The group posted on Telegram, claiming to have stolen hundreds of documents from the unclassified information-sharing platform.</p>
<p> CloudSEK analyzed the leaked data, which includes 8,000 rows of sensitive information, impacting 31 NATO member nations. The hackers, likely hacktivists, state the attack is in protest of NATO's actions on human rights, not related to the Russia-Ukraine conflict .</p>
<p>NATO recently issued an alert for cyberattacks targeting NATO countries, read more on our blog .</p>
<h2>Lazarus Group Strikes: Massive Hacks

Telegram Channel
Telegram - 2023 Aug 01 17:52 UTC
domains | urls | telegram | social | surface web | alexmakus | channel
Telegram Content
NATO расследует возможный взлом после того как группировка SiegedSec разместила документы организации в своем ТГ канале https://cyberscoop.com/nato-breach-of-unclassified-information-siegedsec/

media	20390
script	5234
security	2816
cyberattack	2356
hacking	2024
expand	2182
cybersecurity	1920
hacked	1612

5.15.0.21

Fig. 17. All resources related to the group or its mentions can be found in the Threat Hunting module of SOCRadar XTI (Source: SOCRadar)

Conclusion

SiegedSec is a rising threat in the cyber landscape, with the potential to evolve into a high-consequential cyber threat. Their activities, though currently small-scale, indicate the involvement of **advanced cyber hacktivists**. The similarities between SiegedSec and other notorious hacking groups are noteworthy, in conclusion, their progression should be closely monitored.

Security recommendations against SiegedSec

As far as we know, the group performs **SQL injection, XSS attacks** and in some research we found information that they use **automated tools for scanning**. In this case, it is vital to seriously check and monitor the ports and assets open to the outside.

Including these, we can list the security measures as follows:

- **Regularly update security measures:** Ensure that all systems are up-to-date with the latest security patches to prevent vulnerabilities that SiegedSec might exploit.
- **Monitor for Unusual Activities:** Keep an eye on network activities and look for any signs of unauthorized access or suspicious behavior.
- **Educate Employees:** Train staff to recognize phishing attempts and other malicious activities that could lead to a breach.
- **Implement Strong Authentication:** Utilize multi-factor authentication to add an extra layer of security.
- **Collaborate with Cybersecurity Experts:** Engage with cybersecurity professionals to assess and strengthen the organization's security posture.

- **Penetration Testing Emphasis:** It is crucial to emphasize the importance of regular penetration testing. By identifying vulnerabilities in your system through penetration tests (also known as pentests), you can patch them before they are exploited.
- **Rate Limiting:** If the SiegedSec group is utilizing automation for their attacks, it is advisable to set up rate limits. Implementing rate limits will help prevent volumetric requests, effectively thwarting automated brute-force or DDoS-type attacks.

By understanding SiegedSec's methods and targets, organizations can take proactive measures to protect themselves against this emerging threat.

MITRE ATT&CK TTPs of SiegedSec

Technique	ID
Reconnaissance	
Active Scanning	T1595
Initial Access	
Exploit Public-Facing Application	T1190
Drive-by Compromise	T1189
Collection	
Archive Collected Data: Archive via Utility	T1560.001
Exfiltration	
Exfiltration Over Web Service	T1567