

# Dark Web Threat Actor Spotlight: SiegedSec

---

 [darkowl.com/blog-content/darkowl-threat-actor-spotlight-siegedsec-and-leaked-data/](https://darkowl.com/blog-content/darkowl-threat-actor-spotlight-siegedsec-and-leaked-data/)

June 15, 2022

## Dark Web Cyber Group Spotlight: SiegedSec

---

### The new criminal gang specializes in leaked data and digital defacement

---

June 27, 2022

Read the latest on SiegedSec's activity relating to the Roe v. Wade overturn in our developing blog, "[Darknet Economy Surges Around Abortion Rights.](#)"

---

June 15, 2022

*DarkOwl analysts regularly follow "darknet threat actors" that openly discuss cyberattacks and disseminate stolen critical corporate and personal data. Such analysis helps DarkOwl's collection team direct crawlers and technical resources to potentially actionable and high-value content for the [Vision platform](#) and its clients.*

### SiegedSec: A New Cyber Threat Actor Group

---

Since Russia's invasion of Ukraine and the subsequent, [first-ever global cyberwar](#), several new offensive cyber cells have surfaced. Many of the groups have a strictly hacktivist mission – knocking commercial and government organizations across Russia offline – while other groups piggyback on the collective energy of widespread offensive cyber operations to successfully fulfill more sinister cybercriminal or purely selfish objectives for personal gain.

One new cyber cell, appearing coincidentally days before the invasion, has named its operation under the *SiegedSec* and adopted variations of the tagline, "sieging their victim's security." The group, led by a renowned hacktivist using the moniker *YourAnonWolf*, has quickly progressed in lethality by increasing the group's volume of victims announced in recent months.

### Defaced and Leaked Data

---

Quick takeaways:

- Since their formation in late February 2022, DarkOwl analysts have observed *SiegedSec* provide proof of the defacement and/or compromise of at least 11 websites with rather juvenile and crude language and graphics included in the defacements.


- In April, the group claimed they had successfully defaced over 100+ domains offering proof of a hosting chat dialogue indicating the account passwords had been changed and the defacements corrected, but the group hinted they still had access to the domains.
- DarkOwl analysts also discovered several thousand compromised LinkedIn profiles with references to *SiegedSec*.

There is evidence that the group has gained access to sensitive information and leaked emails or leaked databases from at least **30 different companies** since their start in February. However, hardly any of the companies announced have released public noticed of cybersecurity incidents since many are smaller businesses or located in non-English speaking parts of the world. The group shows no preference for the industries nor locations of its victims. They have successfully targeted companies across numerous diverse industry sectors around the globe including healthcare, information technology, insurance, legal, and finance. We've witnessed victims announced from India, Pakistan, Indonesia, South Africa, USA, Philippines, Costa Rica, Mexico, and others.

In early April, the group's spokesperson, *YourAnonWolf*, appeared on the popular discussion forum, Breached Forums leaking databases, documents, emails containing 17 different organizations' data including usernames, email addresses, and hashed passwords.

**17 databases leaked & released at once**  
by YourAnonWolf - Monday April 4, 2022 at 11:22 AM

**YourAnonWolf**



New User

MEMBER

Posts: 10  
Threads: 6  
Joined: Mar 2022  
Reputation: 0

April 4, 2022, 11:22 AM (This post was last modified: April 4, 2022, 11:26 AM by YourAnonWolf) #1

Hello!  
I present many databases, documents, emails, and more from many different entities.

Affected corps/companies/organizations:

- Rulmeca Corp
- Crane Building Company Inc.
- MaxPro Films
- McKinley Building Corporation
- NHC Emergency Services
- ACAP (NewityMarket)
- Alpine Resort
- ATS Coop (Meridian Coop)
- Brush Dental Care
- Cameron Management
- The Law Group
- The Loan Source
- Tribute Construction
- ValSource
- VEL CashPlease
- West Mark Corporation
- ZipQuest

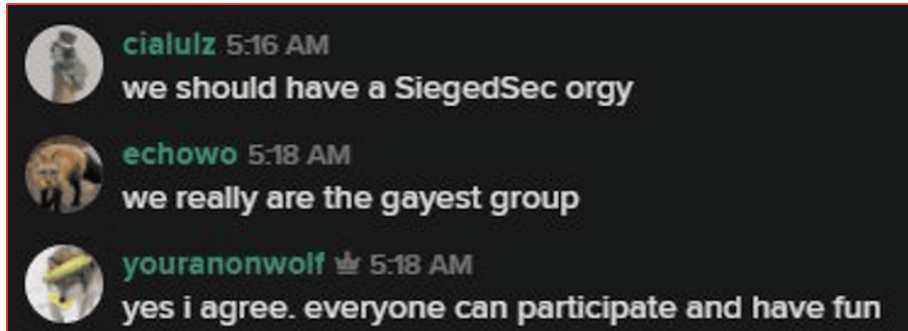
Databases combined: 1,666,427 lines  
Databases contain emails, usernames, email addresses, hashed passwords, PII, and more.  
7 PDF documents retrieved from ACAP assets  
2 ZIP files retrieved from ACAP assets  
Leaked by: SiegedSec/YourAnonWolf

The extent of damage caused by cyberattacks conducted by *SiegedSec* is unknown and many of them have not been mentioned by public news media sources. However, the leaked data shared on their Telegram channel and on deep web forums like Breached could easily be employed by other threat actors to gain access to companies, individuals, and networks by leveraging the private corporate and personal information posted.

## Intentions, Motivations, and Shenanigans

---

As we mentioned earlier, the defacements observed by the group appear to include vulgar language with references to “d\*cks and c\*mdogs.” The group’s Telegram channel and social media accounts include posts from the members that self-identify as “gay furies” with downright comical slogans like “TEH LULZ CONTINUES!”, “uwu gay furies pwn you”, and “HACK THE PLANET.” Their avatar includes the letters “\$ UWU” – imitating a Linux terminal prompt; the “uwu” letters denotes “overwhelmed with cuteness” and is common in the online furry subculture, which anthropomorphize animals with human personalities.



The group has leaked a significant volume of stolen data from compromised networks, but there is no indication the group uses ransomware nor has attempted to sell the stolen data. According to the themes of their social media posts, and the “furry-centric” brand they’ve embodied, the group appears to be motivated by the sheer fun of the experience, the potential clout gained by publicly mocking organizations with insufficient information security controls.

In late May, the group announced they had successfully targeted an India-based online news distribution outlet, called NewsVair. Shortly after the attack they leaked an archive containing 27GB of documents exfiltrated from the organization’s servers, and another archive of hundreds of gigabytes in size consisting of source code and API data on the servers. Last week, the group claimed on their Telegram channel the media outlet’s website provider, WebGuruz contacted them directly and the group leaked a screenshot reportedly from their chat directly with a WebGuruz representative. In the chat transcript, “Wolf” (*YourAnonWolf*) intimates their efforts are not all simply fun, games, and ‘lulz’, but they are possibly interested in financial compensation for their campaigns.

```
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.
```

```
#####
```

## SiegedSec Members & Connections with Other “Hacker” Groups

---

SiegedSec’s Telegram group has limited membership and activity. We discovered a Keybase “team account” that claims the group has 7 active members.

*YourAnonWolf* – a self-declared “corn god and furry” – is the most prominent and vocal member of the group with the longest darknet history of its public members. Another possible member of SiegedSec is *cialulz* who describes themselves as a “15-year-old, Security Researcher & Privacy Advocate. Just an anthropomorphic frog with a thing for computers” and openly uses the #*SiegedSec* hashtag in their social media profiles. *Cialulz* is also named as affiliated with other cyber cells in historical deep web documents in Vision, including the “OSAMA SEC MEMBERS LIST” from 2021 and mentioned in official rosters for GoonSquad (a.k.a. #*WeAreTheGoons*) which apparently was quite active carrying out campaigns in 2017. (Source: *DarkOwl Vision*)

Another moniker mentioned in coordination with *SiegedSec* is “*Sryakarad*”, often shortened to “*Sry*” in darknet chatter. *Sryakarad* was mentioned specifically as a key contributor to *SiegedSec* when the group leaked data from another online media firm they compromised in Pakistan, *e-paper.pakistan*.

In addition to *YourAnonWolf*, *cialuluz*, and *Sry*, other *SiegedSec* members possibly include *echowo* (*EchoNull7*), *mkht1*, *Trav* (*trav0x90*), and *webvuln* (*r00tsauce*), although there are preliminary indications that some of these aliases might be alternative accounts for

*YourAnonWolf* or *cialulz*.

The group also appears to have close associations with *GhostSec*, a prominent hacking group with an extensive darknet history who has become increasingly popular for their attacks against Russia in the cyberwar. Social media accounts affiliated with *SiegedSec* and its members often re-share announcements of attacks conducted by *GhostSec*. *DarkOwl* also noted overlap in the membership of the groups' Telegram channels.

On Breached Forums, *YourAnonWolf* publicly declared that they are a member of both *GhostSec* and *SiegedSec*. *YourAnonWolf* has been historically active conducting campaigns with Anonymous and *GhostSec* targeting unjust governments and countries known for human rights abuses. They also claim to have been previously affiliated with other groups including: *HackersGhost25*, *AxoSec* and *BreachSec*. The status of these other cyber cells is unclear.

A document shared on Pastebin in early June confirmed the aliases of the possible members identified above, but also criticizes the technical prowess of the group, claiming most of their attacks are basic SQL injection and cross-site scripting (XSS) attacks. The paste compared *SiegedSec* to *Lulzsec*, a high-profiled cyber threat group in the early 2010s who similarly initially claimed to have conducted their attacks simply for the "lulz" or laughs, and often mocked their victims for the security flaws they uncovered. The Lulzsec group was comprised of four-young British hackers who infamously successfully targeted the CIA, PBS, Westboro Baptist Church, and Sony gaining significant digital notoriety and infamy.

The group's members, ranging in age between 18 and 26 years old, were all sentenced in 2013 between 20 and 32 months for violation of the UK's computer misuse act in conjunction with the cyber campaigns they conducted. Some of its members were banned from the Internet for upwards of two years and spent time in the Young Offender's Institute to be reformed.

An anonymous response to the paste was uploaded to Pastebin a few days later addressing each of the statements directly, especially those which minimized the skills of the group's members. In response to criticism for using automated scanners, the author stated automated tools have a purpose and not only "skids" use them, even though the original post did not publicly call *SiegedSec* "skids." The response paste was signed –*Unknown* (Source: *DarkOwl Vision*)

Crawled on 2022-06-03 06:51:38 AM

It's 2022, what else do we see?  
Lulzsec but more talented version?  
A cyber crime organization or a group of five outsiders?

-----  
2022, Sry and Youranonwolf gave a birth to SiegedSec.  
They call themselves "gayest group".  
They have four members it includes, sry, youranonwolf, Echowo, cialulz and [mkht1](#).  
Let's get into what they do, they mostly perform sql injection, xss and rce.  
We have found out that, Sry is using Windows 11 as host and Kali linux as a vm.  
What? Lmfao?  
Sry is mostly using automated scanners like ZAP, SQLMAP, ETC.  
Some might call his lame for Sry but, i guess it does help?  
Doing things manually is pretty much better. Sry habits make him sketchy.  
-- RADSOL/tangnerds

-----  
2022, With the information above and couple of simple dorking, it gave me tons of interesting information.  
Mostly critical information of members and how the team is working.  
-- TmWhoislp

-----  
2022, They really hate DDOS attacks and botnets?  
Lmfao  
-- classless

-----  
2022, I love this! They are doing quite a lot of interesting things.  
Keep it up!  
-- mole

-----  
"Fuck the feds" -- SiegedSec  
"Knowledge is power" -- TeamP0isoN  
"Security is a joke" -- LulzSec  
-- THE END --  
#Team CC2  
#2022  
SiegedSec, TeaMp0isoN, lulzsec, youranonwolf, sry, echoowo, experts, 1337 hax0r, real hackers, talented hackers, larp, anonymous.

## Final Thought From Our Analysts

---

Although they are presently a fairly small-scale operation flying under the radar with little to no reporting by the greater global information security community, the data discovered during our analysis and contained in the leaks from their victims indicate that there are advanced cyber hackers involved in the group's operations.

The similarities between *Lulzsec*, LAPSUS\$, and the new group, *SiegedSec* are noteworthy – as *SiegedSec*'s leader, *YourAnonWolf* uses similar popular hacking culture phrases that *LulzSec*'s member, *Topiary* used. History, regardless of real life or virtual events, tends to repeat itself.

DarkOwl assesses that *SiegedSec* has the potential to evolve into a high-consequential cyber threat, especially if the group starts demanding extortion payments in conjunction with their attacks.

**Curious about something you read? Interested in learning more? Contact us to find out how darknet data can shine a light on leaked data.**