

# Dark Web Profile: SiegedSec

Published: 2023-10-18 · Archived: 2026-04-05 13:56:07 UTC

*[Update] July 11, 2024: “SiegedSec Disbands”*

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.

*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:

*Fig. 1. Telegram chat channel of SiegedSec*

The last thing that caught our eye was the group’s [Twitter](#) account, which was continuously suspended:

*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.

*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.

*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.

*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.

*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.

*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.

*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.

*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

*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.

*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.

*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.

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

*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 hackers**. The similarities between SiegedSec and other notorious hacking groups are noteworthy, in conclusion, their progression should be closely monitored.

## SiegedSec Disbands

In a recent event, the notorious hacking group SiegedSec announced its disbandment. The announcement was made through a Telegram post, where the group cited reasons such as mental health, the stress of mass publicity, and the desire to avoid legal scrutiny as driving factors behind their decision.

SiegedSec's latest Telegram post

## 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
<b>Reconnaissance</b>	
Active Scanning	<a href="#">T1595</a>
<b>Initial Access</b>	
Exploit Public-Facing Application	<a href="#">T1190</a>
Drive-by Compromise	<a href="#">T1189</a>
<b>Collection</b>	
Archive Collected Data: Archive via Utility	<a href="#">T1560.001</a>
<b>Exfiltration</b>	
Exfiltration Over Web Service	<a href="#">T1567</a>

---

Source: <https://socradar.io/threat-actor-profile-siegedsec/>