



**| Flash |**

# SiegedSec Hacktivist Group Creates New Data Leak Site

F-2023-12-13b

Classification: TLP:GREEN

Criticality: High

Intelligence Requirements: Deep Dark Web & Criminal Underground,  
Threat Actor Targeting

**December 13, 2023**

## Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM (EST) on December 13, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

# | Flash | SiegedSec Hacktivist Group Creates New Data Leak Site

## › Key Findings

- SiegedSec, a hacktivist group established prior to the Russian invasion of Ukraine, established a new leak site in December 2023.
- The group has posted sensitive information on the leak site, including a database of alleged NATO documentation.
- SiegedSec has conducted attacks against numerous sectors and nations, with a recent focus on government organizations, and will likely continue to leak sensitive data via the new leak site.

## | Details

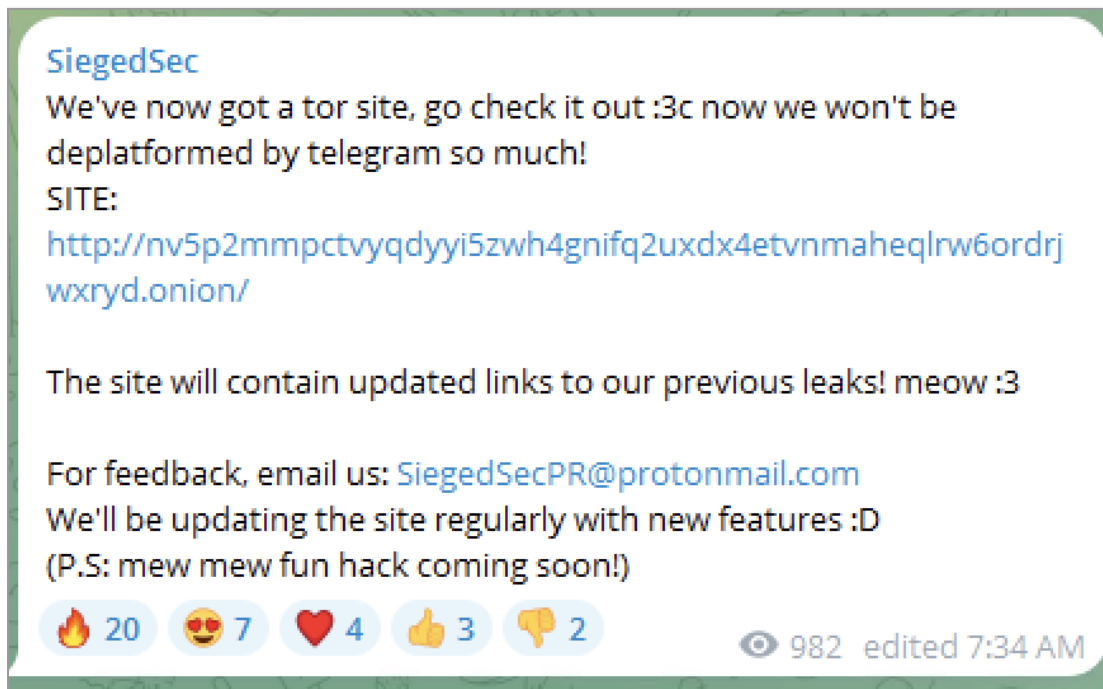
SiegedSec is a cyber hacktivist group that emerged days before Russia's invasion of Ukraine. The group is led by a well-known hacktivist who goes by the handle "YourAnonWolf."<sup>1</sup> The group continues to leak sensitive data from targeted organizations, and there are no indications SiegedSec has employed or plans to employ ransomware to extort its victims. The group appears to be motivated by both the enjoyment of the

---

<sup>1</sup> [hXXps://malpedia.caad.fkie.fraunhofer\[.\]de/actor/siegedsec](https://malpedia.caad.fkie.fraunhofer.de/actor/siegedsec)

experience and the potential clout acquired by openly ridiculing entities with what SiegedSec judges are inadequate cybersecurity protections.<sup>2</sup>

On December 11, 2023, SiegedSec reportedly created a new .onion data leak site to share information about victims' data leaks due to its frequent Telegram bans. The group posted a database containing purported NATO documents on the site.



### **SiegedSec Data Leak Site Announcement**

*Source: ZeroFox Intelligence*

## **| Analyst Commentary**

Although SiegedSec initially targeted a variety of sectors, its scope appears to have narrowed to government and government-adjacent organizations in recent months. The group focuses on NATO countries, including the United States—especially after the Russia-Ukraine war broke out. SiegedSec has recently conducted a number of U.S. attacks:

---

<sup>2</sup>

[hXXps://www.dallasnews\[.\]com/news/2023/06/26/what-we-know-about-the-cyberattack-on-the-city-of-fort-worth/](https://www.dallasnews.com/news/2023/06/26/what-we-know-about-the-cyberattack-on-the-city-of-fort-worth/)

- In June, the group claimed responsibility for the defacement and breaches of various U.S. state government websites in order to protest the states' restrictions or bans on access to gender-affirming care for minors.<sup>3</sup>
- In July, SiegedSec claimed to have stolen and leaked data from NATO's Communities of Interest (COI) Cooperation Portal.<sup>4</sup>
- On September 30, SiegedSec claimed to have stolen roughly 3,000 NATO documents totaling more than 9 GB of data. As a proof of compromise, the organization provided a series of screenshots indicating access to hacked systems.<sup>5</sup>
- The group also claimed responsibility for an attack on the Idaho National Laboratory (INL) on November 20 and the subsequent leak of personally identifiable information for hundreds of thousands of users, employees, and citizens.<sup>6</sup>

## | Recommendations

- Implement the principle of least privilege and role-based access policies.
- Implement network segmentation to separate resources.
- Implement strong password policies and phishing-resistant multi-factor authentication (MFA).
- Ensure critical, proprietary, or sensitive data is continuously backed up to secure, off-site, or cloud servers.
- Develop a dynamic and comprehensive incident response plan.
- Conduct cybersecurity and awareness training for internal users.
- Continuously monitor for unusual activity on devices and activity related to insider threats.
- Utilize the ZeroFox Platform to perform searches on relevant indicators of compromise (IOCs) and monitor for further developments.

---

<sup>3</sup> [hXXps://www.govtech.com/security/hacks-of-govt-websites-reportedly-protest-anti-trans-legislation](https://www.govtech.com/security/hacks-of-govt-websites-reportedly-protest-anti-trans-legislation)

<sup>4</sup>

[hXXps://www.bleepingcomputer.com/news/security/nato-investigates-alleged-data-theft-by-siegedsec-hackers/](https://www.bleepingcomputer.com/news/security/nato-investigates-alleged-data-theft-by-siegedsec-hackers/)

<sup>5</sup> [hXXps://securityaffairs.com/152007/hacking/nato-investigating-new-siegedsec-attack.html](https://securityaffairs.com/152007/hacking/nato-investigating-new-siegedsec-attack.html)

<sup>6</sup> [hXXps://securityaffairs.com/154598/hackivism/siegedsec-hacked-idaho-national-laboratory.html](https://securityaffairs.com/154598/hackivism/siegedsec-hacked-idaho-national-laboratory.html)

## | Appendix A: Traffic Light Protocol for Information Dissemination

|                         | Red                                                                                                                                                                                                    | Amber                                                                                                                                                                                                                                                                                                                        |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:RED</b> when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused. | <b>Sources may use</b><br><b>TLP:AMBER</b> when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.                                                                                                           |
| HOW MAY IT BE SHARED?   | <b>Recipients may NOT share</b><br><b>TLP:RED</b> with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.                                     | <b>Recipients may ONLY share</b><br><b>TLP:AMBER</b> information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.<br><b>Note that</b><br><b>TLP:AMBER+STRICT</b> restricts sharing to the organization only. |
|                         | Green                                                                                                                                                                                                  | Clear                                                                                                                                                                                                                                                                                                                        |
| WHEN SHOULD IT BE USED? | <b>Sources may use</b><br><b>TLP:GREEN</b> when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.              | <b>Sources may use</b><br><b>TLP:CLEAR</b> when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.                                                                                                                                                      |
| HOW MAY IT BE SHARED?   | <b>Recipients may share</b><br><b>TLP:GREEN</b> information with peers and partner organizations within their sector or community but not via publicly accessible channels.                            | <b>Recipients may share</b><br><b>TLP:CLEAR</b> information without restriction, subject to copyright controls.                                                                                                                                                                                                              |

## | Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

| Almost No Chance | Very Unlikely | Unlikely | Roughly Even Chance | Likely | Very Likely | Almost Certain |
|------------------|---------------|----------|---------------------|--------|-------------|----------------|
| 1-5%             | 5-20%         | 20-45%   | 45-55%              | 55-80% | 80-95%      | 95-99%         |