NATO 'actively addressing' alleged cyberattack affecting some websites

therecord.media/nato-siegedsec-unclassified-websites-alleged-cyberattack

NATO flags fly over an operation in Poland in 2017. Image: U.S. Army / Charles Rosemond

Jonathan Greig

October 3rd, 2023

The North Atlantic Treaty Organization (NATO) said it is investigating claims that data was stolen from unclassified websites under the military alliance's control.

A hacking group named SiegedSec — which has been at the center of several recent hacks involving U.S. municipalities over the last year — claimed to have stolen 9 GB of data.

A spokesperson for NATO told Recorded Future News that it is now investigating the claims but said that the alliance has not faced any operational issues.

"NATO is facing persistent cyber threats and takes cyber security seriously. NATO cyber experts are actively addressing incidents affecting some unclassified NATO websites," the spokesperson said.

In posts on Telegram, SiegedSec boasted of accessing several training portals and informational platforms run by NATO. The data was allegedly stolen from:

- Joint Advanced Distributed Learning

- NATO Lessons Learned Portal
- Logistics Network Portal
- Communities of of Interest Cooperation Portal
- NATO Investment Division Portal
- NATO Standardization Office

The group shared a link to the data that was taken, and most of the more than 3,000 documents were taken from the NATO Standardization Office.

NATO did not respond to further questions about when the intrusion may have occurred or whether other information was accessed.

“Additional cyber security measures have been put in place,” the spokesperson said. “There has been no impact on NATO missions, operations and military deployments.”

This is NATO’s second incident involving SiegedSec hackers after an attack in July. The group said it stole information from the organization’s Communities of Interest Cooperation Portal. That batch of data included personal information of people from at least 31 countries, according to news reports at the time.

NATO told Recorded Future News after that incident that the alliance’s cyber experts were looking into the incident. No update was ever published about whether the leaks were legitimate.

SiegedSec attacked several state-run websites this summer, targeting platforms in Nebraska, South Dakota, Texas, Pennsylvania and South Carolina.

A week later, the group claimed to have attacked government systems run by the city of Fort Worth, Texas, but officials later determined that much of that information was already publicly available.

SiegedSec claimed it hacked the governments of Arkansas and Kentucky last year after the state banned abortion following the Supreme Court decision to overturn Roe v. Wade. But state officials also confirmed that the group simply downloaded publicly available record data.

- News
- Government

Tags

- SiegedSec
- NATO
- military

No previous article

No new articles

Jonathan Greig

Jonathan Greig is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.