

Exclusive: Hacktivists Attack Anti-Abortion U.S. States

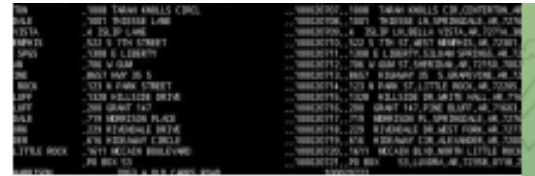
webz.io/dwp/exclusive-hacktivists-attack-anti-abortion-u-s-states/



Last week's controversial ruling of the U.S. Supreme Court, which overturned Roe v. Wade, sent shockwaves through the world and the web. It came as no surprise to us to see that the heated debate around abortion rights moved to the dark web. But one group, took it a step further by launching an attack against "pro-life" states in the U.S.

Using our Cyber API, we were able to detect the first cyber attack since the ruling. A new hacktivist group, **SiegedSec**, targeted states that support the ban on abortions, in a show of support to "pro-choice" groups.

A day after the ruling, on June 25, the group posted internal documents and files they stole from the servers of the states of Kentucky and Arkansas on their Telegram channel:



TIME FOR SOME 1337 H4CKTIVISM!!!
(4 the record, we will still do blackhat stuff ;)

Like many, we are also pro-choice, one shouldn't be denied access to abortion.

As added pressure to the U.S government, we have leaked many internal documents and files retrieved from Kentucky's and Arkansas' government server. These docs have plenty of employee PII and lots more.

These files are about 7-8GB in total.

LEAK:

THE ATTACKS WILL CONTINUE!

Our main targets are any pro-life entities, including government servers of the states with anti-abortion laws.

KEEP PROTESTING, KEEP YOURSELF SAFE, FUCK THE GOVERNMENT

~ SIEGEDSEC OUT ~



57 20:47

The announcement the group made on the attack on their Telegram account

They leaked between 7-8GB of documents, including PIIs of employees of these states.

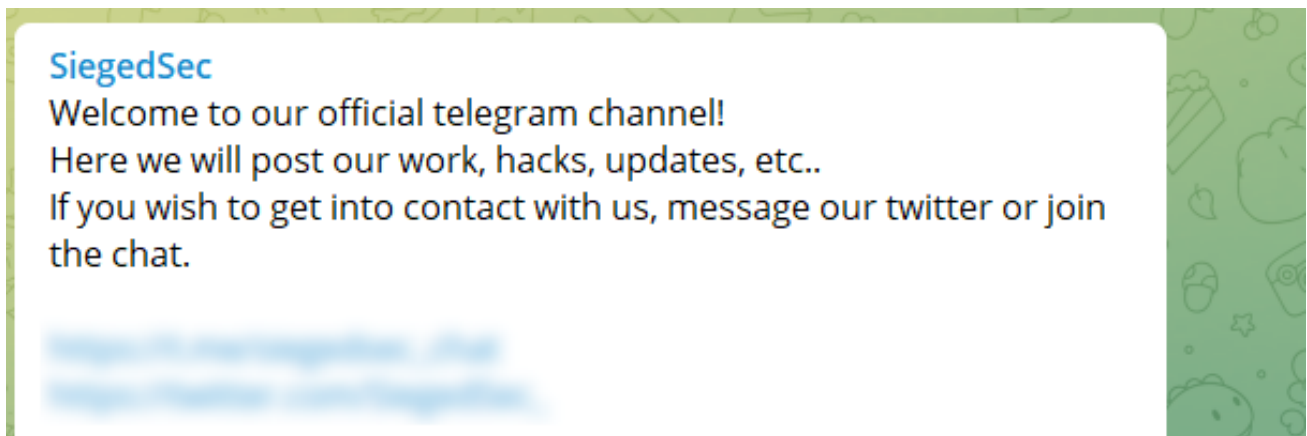


A screenshot of the file host sharing platform the leak was uploaded to **SiegedSec** claimed they will continue to target servers of the states that support a ban on abortion.

Who is SiegedSec?

The group first appeared a few months ago, and has since attacked several different companies from various industries around the world including information technology, insurance, and finance.

They then leaked databases belonging to their victims, which include usernames, emails, hashed/plaintext passwords, PII, sensitive information, and more. We have not seen any proof that they extort their victims for the data they steal.



To show the extent of their attacks, the groups also claimed they had defaced over 100+ domains, but they were stopped by the companies who detected the activity and took action:

- Brush Dental Care 2020 - <https://app.getflywheel.com/org/taylor-gray-kristof/brush-dental-care-2020>
- BrushDentalCare 2020 Ireland - <https://app.getflywheel.com/org/taylor-gray-kristof/brushdentalcare-2020-ireland>
- Cannons Auto Collision - <https://app.getflywheel.com/org/taylor-gray-kristof/cannons-auto-collision>

...of

We started work on defacing over 100+ domains, including those affected by our last hack. The admins quickly caught on though, and removed our defacements, changed passwords, and contacted help to make sure we were out of their accounts and servers.

(HINT: WE WERENT)

Here are screenshots from their contact to their host asking for malware scans and talking about our defacements.

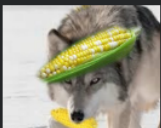
👁 220 6:49

Where is the group active?

Hacking Forums

A user named **YourAnonWolf** posted several leaks on behalf of **SiegedSec**, linking himself to the group. He published on **breached.co**, the new popular hacking forum that attempts to replace Raidforums.

NewsVoir -India's leading News Distributor- hacked, 27GB of databases leaked
 by YourAnonWolf - Wednesday June 1, 2022 at 02:59 AM



YourAnonWolf

June 1, 2022, 02:59 AM (This post was last modified: June 3, 2022, 03:19 PM by YourAnonWolf.)

Another good hit by **SiegedSec** ~
 NewsVoir, India's leading News Distributor, has been hacked, and all databases from the server has been exfiltrated.
 27GB uncompressed / 4GB compressed / 154 DBs
 Contains PII, emails, password hashes, and other regular database stuff.

Leaked by: YourAnonWolf/SiegedSec

A post *YourAnonWolf* published on *breached.co*

We took a closer look at *YourAnonWolf* and were able to find a post he had published before he was publicly linked to *SiegedSec*. A little over a year ago, he posted a leak of a domain that belongs to an Israeli organization on *pastebin*:

www.ittn.org.il database leak – Pastebin.com

[View on Cyber API](#) | [View on Website](#)

YourAnonWolf | [pastebin.com](#) | paste | 2021-02-18

```
www.ittn.org.il database leaked Leaked by @YourAnonWolf Database: ittn_web Table:
system_user [20 entries] +-----+ + + + + + + + + + + + | id | name | email | active | status | tto_pic |
tto_url | password | tto_info | username | name_long | import_way | last_login | +-----+ + + + + + + +
```

Twitter account

The group also created a new account, on Twitter earlier this year, as the last one was suspended:



An image of the new Siegedsec account on Twitter

Hacktivism against abortion ban

This is not the first time a hacktivist group targeted a U.S. state that moved to ban abortions. In October 2021, Anonymous launched a series of attacks as part of their Operation Jane campaign against a Texas law that prohibited abortions.

The famous attack was against Epik, a web hosting company used by large right-wing clients, such as Parler, Gab, 8chan as well as the Republican Party of Texas. In total, over 480GB of data belonging to Epik was stolen and leaked.

As the new Supreme Court ruling sets a new phase in the battle over abortion rights, we may continue to see more hacktivists taking a clear stance by launching new attacks against “pro-life” groups and states.

[Hacking Groups Trending](#)



Avishag Yulevich

Senior Cyber Analyst

Not subscribed to our Dark Web Pulse updates?

By submitting you agree to Webz.io's [Privacy Policy](#) and further marketing communications.