Thai entities continue to fall prey to cyberattacks and leaks

databreaches.net/thai-entities-continue-to-fall-prey-to-cyberattacks-and-leaks/

Dissent July 31, 2022

For over one year, DataBreaches.net has highlighted some breaches of ASEAN victims by groups such as ALTDOS and DESORDEN. In addition to those two groups, there are also numerous other leaks and breaches, as DataBreaches noted in our recent post about leaks and breaches in Indonesia.

But even while DataBreaches was researching and preparing the post on Indonesia, DESORDEN threat actors continued to announce new victims in Thailand and further headaches for earlier Thai victims who had not paid their demands.

And then it appeared things might get even worse.

Four Breaches of Thai Entities DESORDEN Announced This Week

The first was **Frasers Property Thailand Public Company Limited**. DESORDEN provided DataBreaches with samples of the data and a video suggesting the scope of the breach. They also posted the breach on a popular hacking-related forum with a free sample. Their listing claims the breach involved "312,834 personal data information of their customers, along with their HR, financial and corporate data."

DataBreaches has not spotted any media coverage or notice on Fraser's website. A request sent to Fraser for a copy of any notification or press release, and a question about who has been notified did not receive an immediate reply.

The second DESORDEN victim was **Union Auction Public Company Limited.** As with Fraser, DESORDEN made a public claim on a hacking-related forum, offered free sample data, and made the rest available for purchase. In this case, they claimed to have acquired 30,000+ personal data information of their victim's members. Finding no notice on Union Auction's website nor media coverage, DataBreaches sent an email inquiry requesting a copy of any notification and asking who had been notified of this breach at this point. The email bounced back, undelivered, and an attempt to use their site contact form failed.

The third DESORDEN victim is also a publicly listed firm: **Srikrung Broker Co., Ltd.**, an insurance broker company. Srkikrung issued a statement acknowledging the breach. DESORDEN claims it stole more than 369 GB of data with approximately 3.28 million customer records and 462,980 agent records in its public listing on a hacking forum.

Then just today, DESORDEN sent an update to DataBreaches, indicating that three days after breaching Srikrung Broker, they breached another business under that company: **724.co.th**, an insurance marketplace. This latest breach, they claim, involved 1.75 TB of scanned ID copies and loan documents and has also been posted to a hacking forum. An attempt by DataBreaches to connect to 724's website this morning timed out.

DESORDEN listings on a hacking forum. Some listings are explicitly for sale. Others provide a sample and invite people to contact them on TOX for purchase inquiries. With one exception, all of the entries color-coded red by DataBreaches.net are Thai entities.

Other Listings Related to Data of Thai Entities

DESORDEN isn't the only source of leaks or breaches affecting Thai entities, of course, with ALTDOS having previously been a significant threat actor in the region. DataBreaches also found other listings by other vendors or threat actors over the past few months on a popular forum where people can sell or acquire data:

- An April listing offering data from **Pruksa Clinic** claimed to have 48,303,229 records.
- Another listing offered 5.9 million citizens' data with their full name, date of birth, mobile telephone number, and complete address.
- A listing for "huge data of thailand citizen" claimed to have data from a Thai university with email, address, phone, full name, and other files.
- A listing with data purportedly from the Royal Thai Police, knowledge management of police partrol platform (KMPPP). Using leaked credentials, someone was reportedly able to scrape data containing the information of 6793 cyber villages across Thailand.
- A listing about the Thai **Ministry of Public Health** with a Covid database.
- Some data allegedly leaked from the **Thailand Institute Of Nuclear Technology**.

NOTE: DataBreaches has not attempted to validate any of the claims in the postings described above, and not all of them are even still available. They are presented here merely to demonstrate an interest in the underground for data from Thailand, and people are more than willing to profit by meeting that need.

And Then Things Seemed to Be About to Get Worse

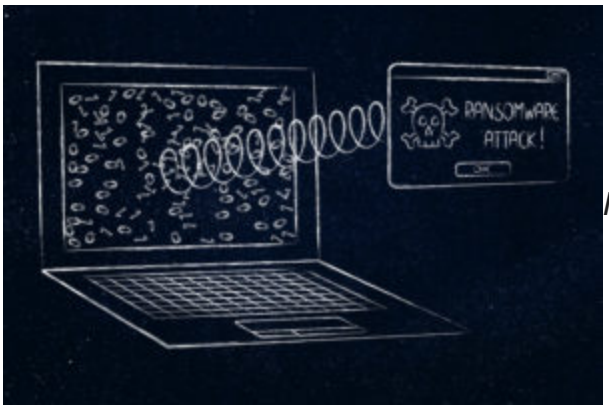


Image: Dreamstime

In the past few days, DESORDEN started making ransomware builds freely available to members of a hacking-related forum. Because DataBreaches was unaware of any incidents in which DESORDEN had used ransomware in its attacks on entities, DataBreaches asked them whether they had used it and whether their offer of free ransomware builds by others to forum members signaled that they would also be using ransomware more often in their activities. DataBreaches also asked DESORDEN if they had considered that by making these builds freely available to all, some young and inexperienced people might try to use them to attack hospitals or critical infrastructure.

DESORDEN responded that they do not use ransomware in most of their attacks — not even during the Acer India attack. But even when they deploy ransomware, they write, they would not use the types offered on the forum or any type or version already hashed by VirusTotal because those are impossible to deploy on systems that have even basic antivirus protection.

As to the two specific ransomware builds they offered freely on a forum, they note that CHAOS Ransomware Builder is a wiper, although it is advertised as ransomware, and it doesn't work with any properly installed AV system. The other offering, Yashma Ransomware Builder, is an upgraded one that has not been detected often in the wild. And here's where their answer became particularly interesting:

> We have already submitted it to VirusTotal 12 days ago before we post it for free. In one way, we are helping others to prevent attacks by Yashima ransomware. You can see the data submission here: https://www.virustotal.com/gui/file/f9a5a72ead096594c5d59abe706e3716f6000c3b4ebd7690f2eb114a37d1a7db/detection/f-f9a5a72ead096594c5d59abe706e3716f6000c3b4ebd7690f2eb114a37d1a7db-1652338917
>
> The Yashma was provided to us by a credible source for reverse engineering purposes. We have already submitted to VirusTotal which will be uploaded to majority AV detection. So it is almost impossible for young wannabes to deploy it on basic AV protected systems, as basic as Windows Defender. Also, ransomware is not easily deployed as seen in movies or online news. Deploying it require skills in underlying systems.

So that was a bit of a surprise: DESORDEN offered a free build of others' ransomware but first uploaded it to virustotal.com so that it will be detected by more systems and be less likely to succeed if entities use basic security hygiene like updated antivirus protection.

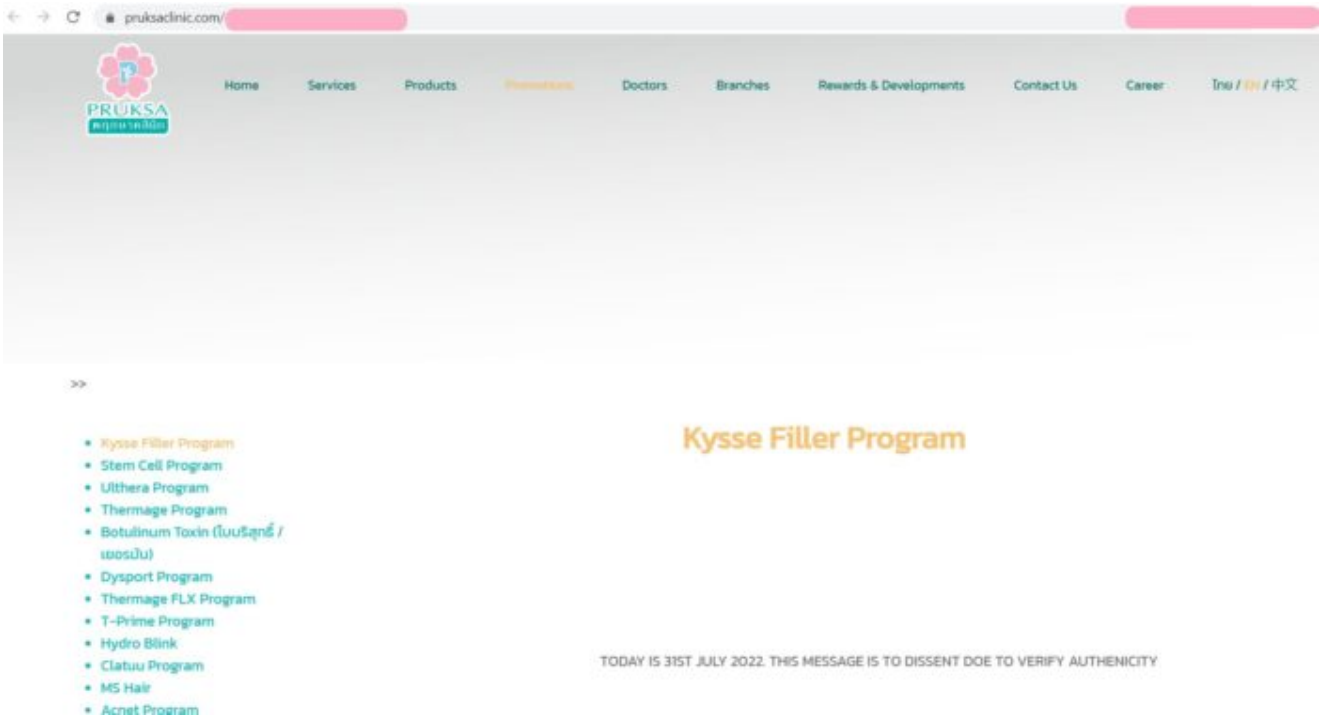
DataBreaches will continue to try to cover ASEAN breaches, and hopes that the country's regulator will publish some guidance to entities there if they have not done so already.

UPDATE: Hours after posting this, I heard from DESORDEN, who wrote that they were suspicious of the Pruksa Clinic listing mentioned in the post because, "A leak involving 48 million would be big, considering Thailand population of only 70 million. Also, a clinic of this size is impossible to have such many customer records. So we went on to investigate on the target."

That translated into they hacked in to the clinic, looked around, and reported that the clinic only had a few thousand patients.

> To prove, we are in their system. We put a message for you on one of their page:

And indeed they had. When I checked the url they provided, it took me to a page on Pruksa Clinic, and here is what I saw:



So now we know to be suspicious of that listing claiming 48 million. But as DESORDEN subsequently explained, their motive wasn't totally altruistic:

> We were only concerned when we saw 48 million records in Thailand being leaked via a private company. As far as we know, Mistine hack is the largest heist in terms of 20 million customers and 10 million sales representatives from a private company in Thailand. And obviously we aim to continue holding the records, as long as we could. =)

Whatever their motive, this is a useful reminder not to just believe whatever is posted in forums for sale or tokens.

Related Posts:

- 'I think Indonesia's cybersecurity is run by 14-year…
- DESORDEN leaks more data from Indonesia; "Indo data…
- Recent cyberattacks put Thai citizens' privacy and…
- A massive database of 8 billion Thai internet records leaks
- Customer data from hundreds of Indonesian and…