Recent cyberattacks put Thai citizens' privacy and data security at greater risk

databreaches.net/recent-cyberattacks-put-thai-citizens-privacy-and-data-security-at-greater-risk/

Dissent July 22, 2022

Image: Source

In December of 2021, Thailand's National Cyber Security Agency launched after being delayed by the COVID-19 pandemic. In February, it announced that it intended to roll out 40 subordinate regulations of the Cybersecurity Act this year to strengthen the country's systems. It sounds like an ambitious — but badly needed — update.

For the past few years, DataBreaches has been reporting on breaches in Thailand, but it has not always been clear to what extent the breached entities have fully disclosed their breaches to individuals whose personal or sensitive information may have been caught up in a breach.

In its analysis of global breach notification laws, DLA Piper summarized the current breach notification obligations in Thailand this way:

> In the event of a data breach, Data Controllers must report the breach to the Regulator without undue delay, and in any event, if feasible, within 72 hours of becoming aware of it. Data Controllers also have an obligation to notify the data subjects of the breach and the remedial measures if the breach is likely to result in high risks to the rights and freedoms of individuals.

Of course, not all incidents result in high risk even if they sound dreadful. In August of 2021, Bob Diachenko discovered the records of 106 million travelers to Thailand were exposed due to a misconfiguration. The exposed database contained each visitor's full name, sex, passport number, residency status, visa type, Thai arrival card number, and date of arrival in

Thailand. The National Cybersecurity Agency confirmed the leak, but said it had found no evidence of any data up for sale and no evidence that the exposed data had been accessed by any unauthorized parties.

That was the third leak in as many months. In June, a local blogger had reported that the Bangkok immigration site was leaking passport number, nationality, date of birth, email, telephone number, and visa expiration date. And a Covid vaccination site set up for vaccine registration, Thailandintervac.com, was found to be leaking names, passport numbers and locations, and there were reports that people could edit other people's information.

But in addition to leaks, there were actual cyberattacks. In August 2021, Bangkok Airways revealed it had been the victim of a cyberattack that accessed passengers' names, nationalities, genders, phone numbers, emails, addresses, contact information, passport information, historical travel information, partial credit card information and special meal information. That attack appeared to be the work of LockBit.

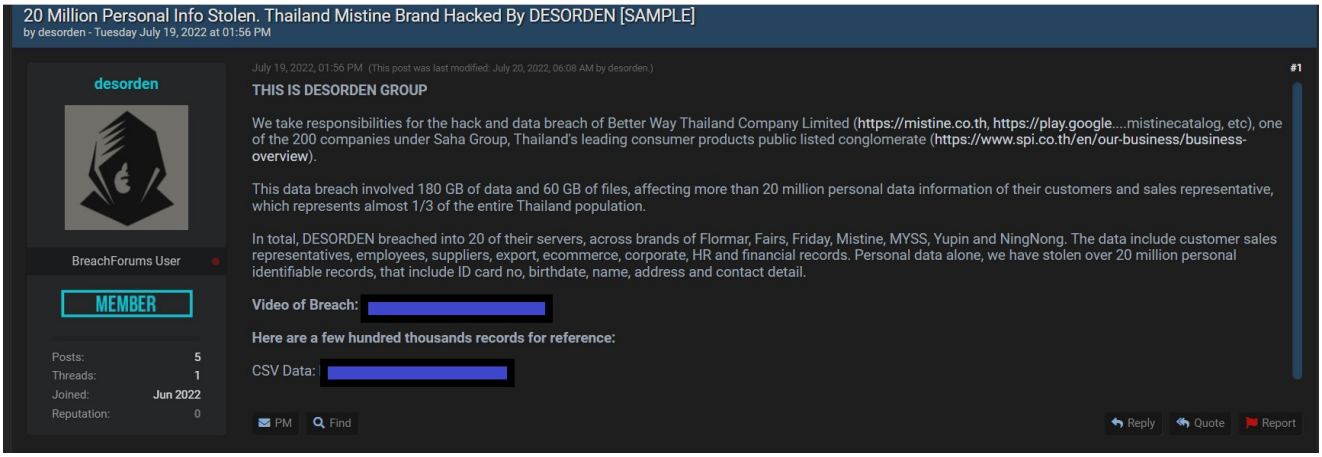
Yet other incidents have also put Thai people at increased risk, especially when groups like ALTDOS and DESORDEN start giving away data freely on popular hacking forums.

In August 2021, Catalin Cimpanu compiled government advisories and incident reports by DataBreaches on threat actors called ALTDOS, describing the group as wreaking havoc across Southeast Asia, including Thai entities. But it wasn't just ALTDOS wreaking havoc. In October 2021, DESORDEN hit Centara Hotel Group and Central Restaurant Group. In that case, the entities did issue public statements about the breach, but whether they ever sent individually mailed notifications to guests or any employees affected is not known to DataBreaches.

In the past week, DataBreaches became aware of two more breaches that put Thai people at increased risk. The first was a breach of **Mistine Better Way Thailand** by DESORDEN. As reported previously on this site, DESORDEN claimed to have acquired 180 GB of data and 60 GB of files, including about 20 million records with information on customers and representatives.

In reporting on the Mistine incident, DataBreaches provided a screenshot from one of the databases DESORDEN shared with this site. That database included employees' first and last names, their password, and their display name. Other fields in that database, not viewable in the screencap, included the employees' addresses and mobile telephone numbers.

DESORDEN subsequently posted data from the breach as a free sample on a popular hacking forum.



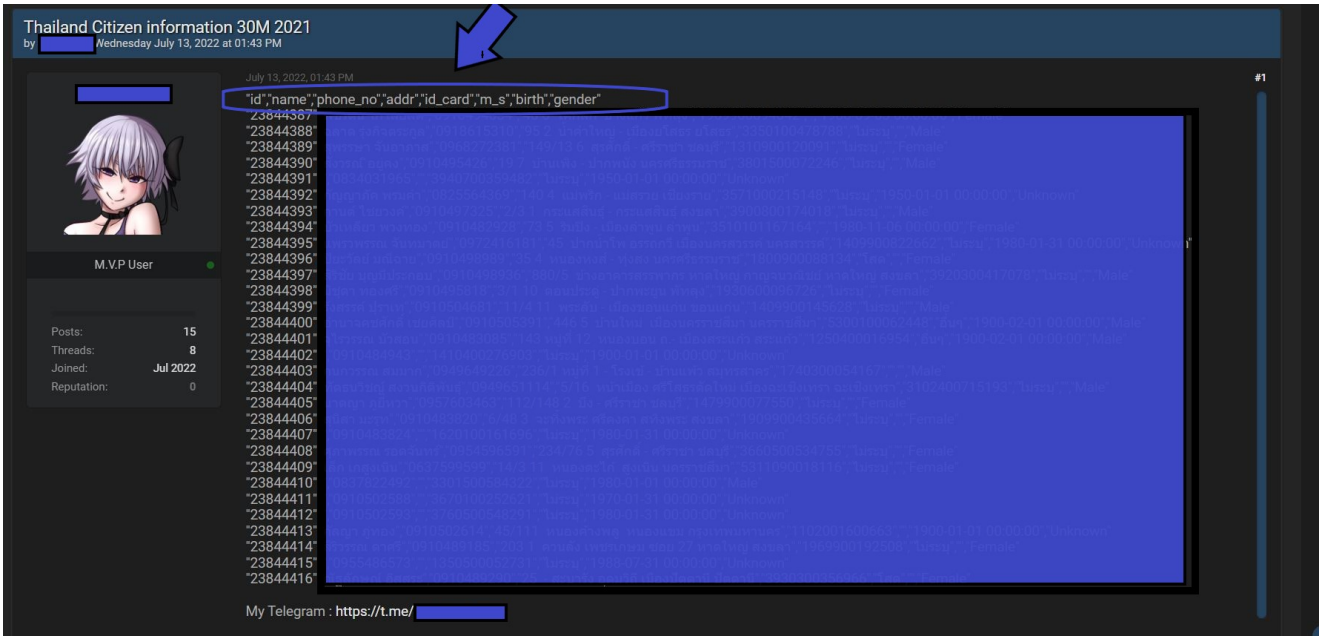
DESORDEN gave away data allegedly from MISTINE on a popular hacking forum. Whether they will sell or give away more data is as yet unclear. Image redacted by DataBreaches.net.

To date, Mistine has not responded to multiple inquiries by DataBreaches asking them to confirm or comment on the breach. There is no notice on their web site and no notice on their Twitter account. DataBreaches can find no press releases or media coverage from Thailand about the claimed hack.

Has MISTINE reported the breach to the regulator, as would appear to be required? DataBreaches does not now.

But the DESORDEN breach and leak is not the only concern for Thai citizens this week. Another individual also provided a free sample of data, but these data are from what is described as a database of 30 million Thai people. The data fields include:

“id”,”name”,”phone_no”,”addr”,”id_card”,”m_s”,”birth”, and “gender:”



Another listing by a different party on a popular hacking forum. In this case, the individual has indicated that the data are for sale. Image redacted by DataBreaches.net.

DataBreaches is attempting to get more details about this second breach, but notes that both this database and the DESORDEN data have mobile phone numbers, which suggests that the two databases might contain a number of overlapping individuals for whom more complete dossiers could now be compiled.

Since DataBreaches does not yet know the source of the second data leak, this site does not know whether that entity is already aware of any leak or breach or if they have notified any regulator or notified any consumers.

DataBreaches has sent inquiries to both THAI-CERT and Thailand's NCSA to seek information about the government's awareness of these latest breaches and to inquire what the government is doing. No replies have been received as yet.