Thai media and content conglomerate Mono Next Public Company hit by ALTDOS hackers (UPDATE1) - DataBreaches.Net

Published: 2021-01-07 · Archived: 2026-04-09 02:04:46 UTC

The same hacking group that hit Country Group Securities (CGSEC) in Thailand has revealed a recent attack on **Mono Next Public Company Limited**, a media and content conglomerate in Thailand.

 About MonoAs described by Thailand's Securities and Exchange Commission, Mono Group divides its businesses into 5 business operations **MONO29** (Digital TV business), **MONOMAX** (Video on Demand business providing movies and series as well as being an international movie distributor under the name **MONO Streaming3**), **MONOCyber** (Online business on website MThai as well as providing strategic planning and Holistic Communications service for product brands), **Master Content Provider**: Content acquisition and marketing for Interactive TV business, and **29Shopping** (Home shopping business).

According to Dun & Bradstreet, Mono Group generated $71.24 million (USD) in 2019.

Threat actors calling themselves ALTDOS claim to have hacked 29shopping.com on January 6, mono29.com on January 3, and mono.co.th on December 25. They also claim to have successfully completed other attacks across Mono's networks since November 2020 that resulted in the exfiltration of hundreds of gigabytes of data.

Attempts to negotiate ransom demands with Mono were reportedly unsuccessful, a spokesperson informed DataBreaches.net, leading to them starting to dump data. The first small dump was customer data from 29shopping.com from 2018 to this month.

ALTDOS had previously informed this site that they do not use ransomware, but they do exfiltrate data and then try to get entities to pay them not to dump the data they acquired.

In addition to the .csv file with 1448 rows, ALTDOS also provided DataBreaches.net with screencaps showing the scope of what else they could access.

 Scrrenshot of folders with size of one folder

Screencaps provided by ALTDOS showed folders containing 167 GB of data, with Mono29 sql was almost 40 GB in size. Redacted by DataBreaches.net, who has not seen any of the contents of those

folders.

In response to a question from this site as to how they gained access, the spokesperson for what was described as a team replied:

> There are many methods which we've used to gain initial access to their networks ranging from sniffing, brute force to code injections.

Their motives, the spokesperson wrote, are purely financial and not political at all:

> There is nothing political about our attacks. It's all about the money. ALTDOS main focus is in ASEAN and we attack many targets ranging from Bangladesh, Philippines, Malaysia to Thailand. Apparently, this is our 2nd Thai attack and Thai companies are hard to negotiate. Perhaps, it is difficult to communicate with the victims due to language barrier?

DataBreaches.net reached out to Mono to request a response to ALTDOS's claims. No reply has been received as yet, but the time difference could contribute to that. This post will be updated if a reply is received.

UPDATE: DataBreaches.net has received a statement from MONO. The English version of their statement begins:

> It is revealed that an attacker (hacker(s)) has claimed to access the company's data causing data breach of employee's personal information and extorted money by threatening to expose the information to the public.
>
> Due to this unusual circumstance, Mono Next Public Company Limited and subsidiaries would like to announce that the company has a security system to protect the personal information database of all employees and clients. The data is kept on a system located in the Company's computer center and cloud server with sufficient protection and security measures according to the rights protection enforcement. Moreover, the system has been regularly monitored.
>
> The attacker (hacker(s)) has accessed some employee's data, such as name, last name, and age, and some online customer's data were leaked. Nevertheless, credit card or financial information and copy of identification card remain safe. As for financial report, the company has already disclosed the information to the public.
>
> Therefore, the extortion is considered a cybercrime that defamed the company for the advantage of the attacker (hacker(s)). The attacker also stated that if the company ignores the extortion, the information will be revealed to the public. Consequently, the attacker (hacker(s)) will become recognized and continue to extort other companies, targeting all public companies in the Stock Exchange of Thailand.

The remainder of the statement is to basically ask news outlets NOT to report on the attack and any data dumps, as it will encourage further attacks and extortion attempts. It is an argument that we have heard many times before, and while there may be merit to the notion of not reinforcing or assisting criminals by reporting on them, this site has always weighed that against the importance of notifying consumers and patients whose data has already been

stolen and may be being misused. MONO's statement does not seem to state whether they are notifying any employees or customers of data theft. DataBreaches.net has sent them a follow-up inquiry on that point.

In exchange for news outlets not reporting, it seems, MONO claims that "when the trial ends" (they seem to be assuming that the attackers will be caught and tried?), " the company will be pleased to inform news agencies to report the news as a case study in terms of preventive management. Because they have already been attacked and data allegedly exfiltrated, it is not intuitively obvious what "preventive management" they would be describing.

MONO's statement also indicates that they are increasing their security.

If MONO responds to the inquiry about whether they are notifying everyone whose data has been stolen, this post will be updated again. In the interim, the attacker's email account seems to have been killed off.
