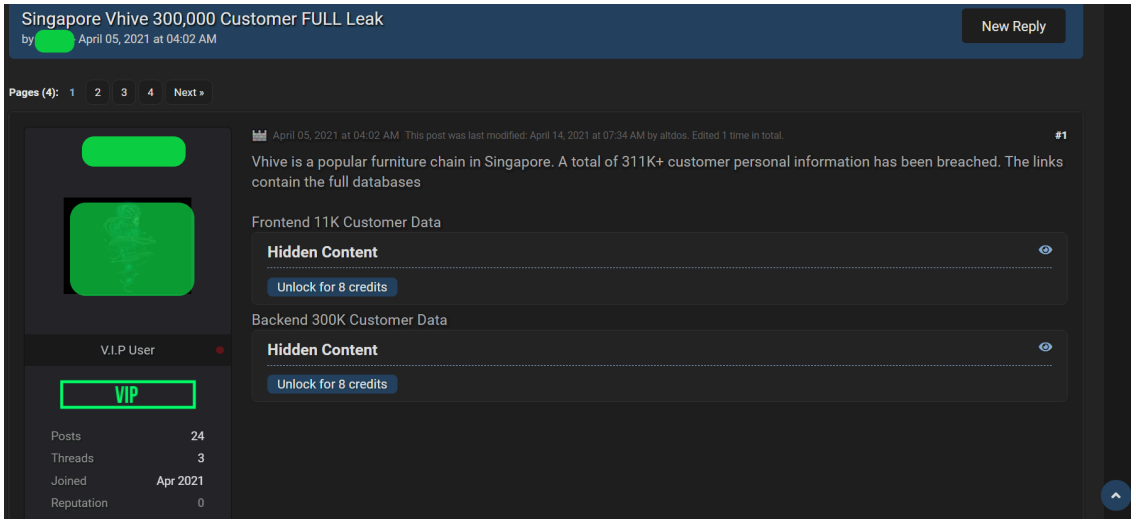
ASEAN companies still targeted by ALTDOS threat actors - DataBreaches.Net

Published: 2021-06-09 · Archived: 2026-04-09 02:10:39 UTC

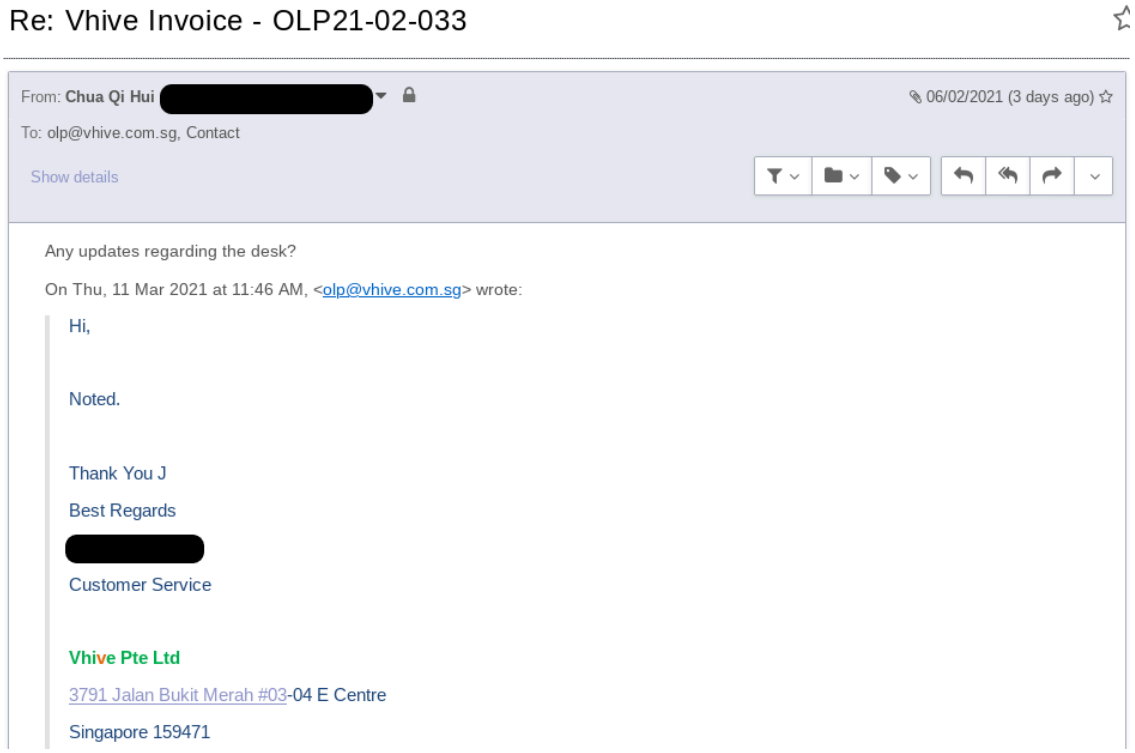
In December of 2020, DataBreaches.net reported on a threat actor (or actors) calling themself "ALTDOS" who had attacked a Thai securities trading firm, **Country Group Securities (CGSEC)** . CGSEC wasn't the only Thai entity they attacked, and within weeks, they had attacked **MonoNext** and **3BB**, subsidiaries of **Jasmine International.** Angered by the entities' response or lack of response to demands, ALTDOS ultimately dumped their data. Less than one month later, this site reported another attack by them, this one involving **Bangladesh Export Import Company Limited** ("BEXIMCO"). And in March, they attacked **Vhive** furniture retailer in Singapore. When the retailer allegedly reneged on an agreement to pay them, ALTDOS escalated, taking control of the firm's email server and sending out emails to customers. They also dumped their customer data.



When Vhive allegedly reneged on promise to pay them, ALTDOS dumped all their customer data on a popular forum. Image: DataBreaches.net.

In all of the above cases, ALTDOS dumped customer or personal information, using a variety of dump sites or leak sites to post data. But that wasn't the end of their activity and attacks.

Somewhat stunningly, perhaps, DataBreaches.net discovered this week that ALTDOS appears to **still** be in control of Vhive's email server. As proof of claims, ALTDOS provided DataBreaches.net with a screen cap of an email from June 2.



Redacted by DataBreaches.net

DataBreaches.net reached out to Vhive to inquire as to how ALTDOS still has access to their email server, but received no response.

In early April, DataBreaches.net had reached out to Singapore's Data Protection Commission to ask if the Vhive incident had been reported to them. A spokesperson for the PDPC responded that they were aware of the incident and were investigating. Under their procedures, the results of their investigation are confidential, but the commission does publish decisions in cases where it has found a contravention of data protection provisions of the PDPA. At the present time, there is no decision for Vhive listed on the commission's site, which may mean that the PDPC concluded its investigation and found no violation, or that the investigation is still open.

Regardless of what the PDPC does or does not do, if ALTDOS still has access to Vhive's email server, that is cause for concern.

But Vhive was not the last attack by ALTDOS. There have been two more Singapore entities attacked by ALTDOS recently (or at least two that we currently know about).

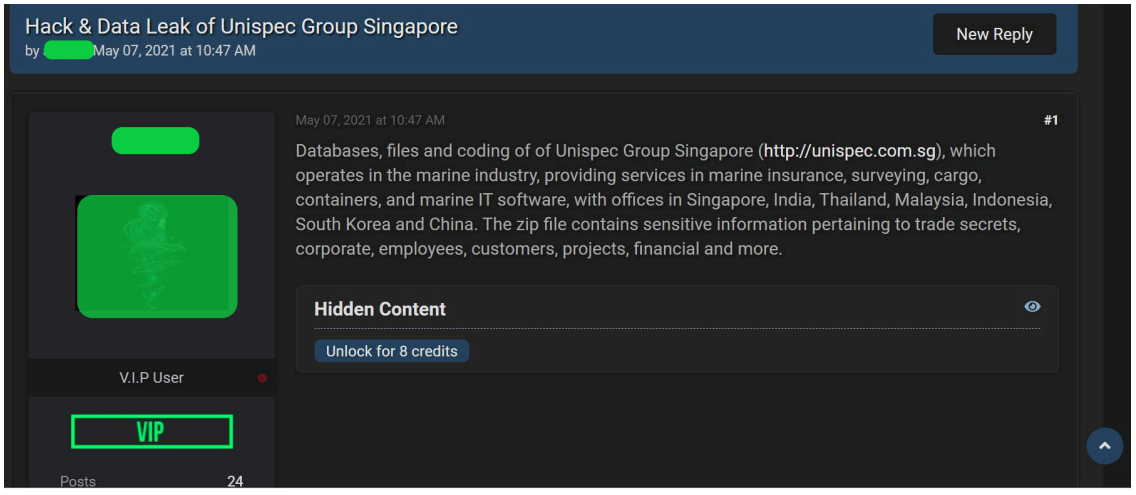
Unispec Group Singapore

ALTDOS claimed to have attacked **Unispec Group Singapore**, which operates in the marine industry, providing services in marine insurance, surveying, cargo, containers, and marine IT software. UniSpec has offices in Singapore, India, Thailand, Malaysia, Indonesia, South Korea and China.

In a statement provided to DataBreaches.net, ALTDOS claimed that they had

> hacked into their intranet servers and stolen all of their coding, files and databases. Data and files include sensitive information pertaining to trade secrets, corporate, employees, customers, projects, financial and more.

ALTDOS uploaded some video proof of claims. They tell this site that when the firm did not reply to their emails, ALTDOS began dumping data on May 7.



ALTDOS leaked UniSpec data on a popular forum where hacked or leaked data may be bought, sold, or shared. Image: DataBreaches.net

Unlike ALTDOS's earlier attacks, the UniSpec data dump was not because the target refused to pay any demands. ALTDOS claims that they never even made any specific monetary demand on UniSpec. When the entity did not respond to their emails, they just went into dump or sale mode.

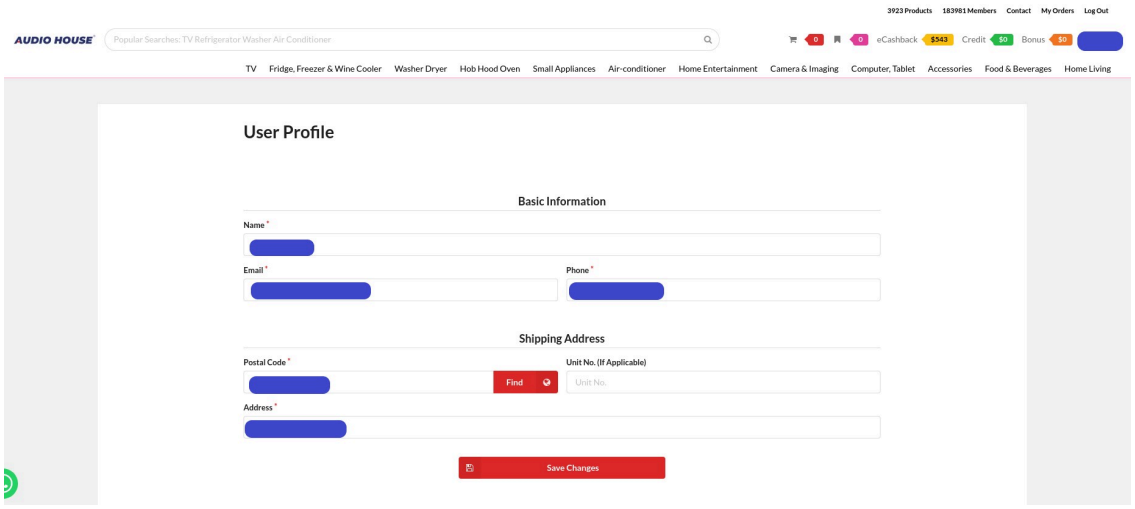
> "Our current style is to write an email asking for a reply from their management without stating any monetary demands from the victim," ALTDOS told DataBreaches.net. "Since Unispec did not reply, ALTDOS did not state any demands. The email account that was used to contact Unispec was already deactivated by protonmail."

While they did not reply directly to ALTDOS, UniSpec reportedly filed takedown requests with gofile.io, file.io, pastebin, and some other sites where the threat actors uploaded files.

DataBreaches.net did reach out to UniSpec to ask how the attack may have impacted them and whether they have notified employees and the PDPC about the attack, but no reply has been received.

AudioHouse

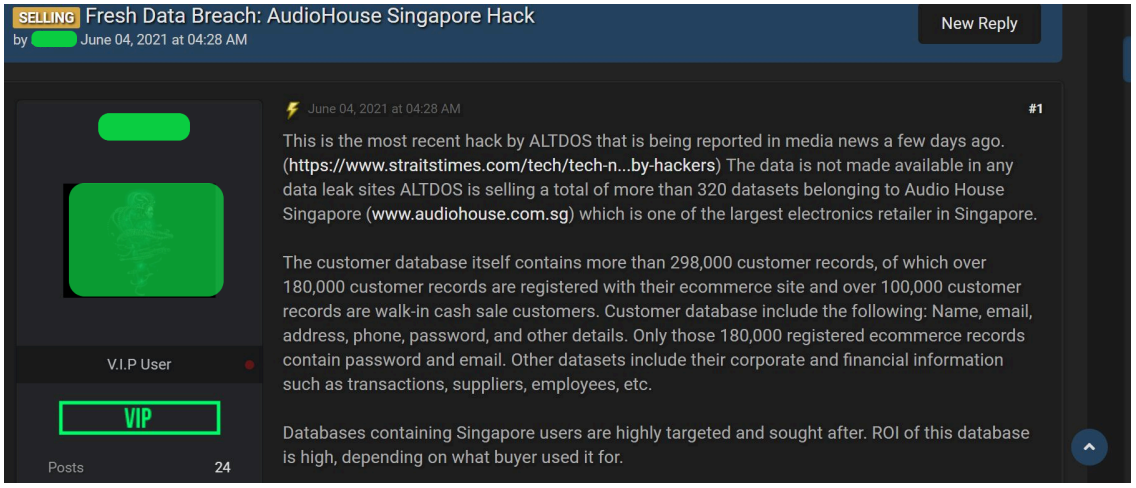
ALTDOS also claims to have hacked and stolen more than 290,000 customers' personal information from **AudioHouse**, one of Singapore's largest electronic retailers. The firm has since reported the attack to the authorities and to their local news media.



This AudioHouse user profile was redacted by DataBreaches.net.

In support of their claims, ALTDOS provided DataBreaches.net with a video recording of what they claim are 320 stolen database and Part 10 of a customer database that they had uploaded.

Because AudioHouse did not respond to their emails but went to the authorities and media, ALTDOS listed their data for sale on June 4.



ALTDOS offered AudioHouse data for sale. Image: DataBreaches.net.

What Are They Doing?

Since DataBreaches.net first became aware of ALTDOS, it has been somewhat of a puzzle. In the past, they have not asked for the kind of exorbitant ransoms other threat actors have demanded, and in some cases, as we see above, they wind up not making any financial demands at all and just leak the data or advertise it as being for sale. That does not seem like a particularly profitable business model, and DataBreaches.net asked them about it. They replied:

> Depending on the type of data, ALTDOS usually dump out partial data and proceed to use middleman to sell the data to other groups.

As they informed this site last year, they have continued to focus on ASEAN companies. But are any paying them? Their attacks do not seem to get much coverage. Are consumers there less concerned or outraged about breaches involving their consumer data, or is there just a concerted public effort not to reward threat actors by reporting on them or paying them?

According to ALTDOS, and DataBreaches.net has no way to confirm this: 70% of the breached companies pay them and then nothing is disclosed publicly about the hacks. For the other 30%, “ALTDOS will either do a full data dump or sell the data to middleman which in both cases, will end up in the hands of other groups capable in extracting more monetary value with use of other methods.”

ALTDOS continues to decline to answer any of this site’s questions as to how it gains a foothold in the victims’ systems, saying only that they use different methods, depending on many factors involving the target.

So how serious a threat are they to ASEAN people? They seem to be a serious enough threat that they already acquired and dumped more than 600,000 Singapore residents’ information. Are their corporate victims sharing information with other entities and law enforcement there? Are entities taking steps to harden their security to prevent their attacks? If they are, it’s not being publicly discussed.
