ALTDOS claims some of their servers were seized but they did not lose data - DataBreaches.Net

Published: 2021-09-06 · Archived: 2026-04-09 02:13:37 UTC

It would be great if the good guys had backups as good as the threat actors have.

Threat actors who call themselves "ALTDOS" have re-emerged after a brief hiatus that had left this site wondering if something had happened to them following a joint advisory about them.

ALTDOS has attacked a number of ASEAN firms, as DataBreaches.net has documented over a series of posts and reports. Most recently, ALTDOS had started disclosing a breach involving OT Group/OrangeTee in Singapore, and had indicated that they would be dumping data. But they suddenly went silent three days after a joint advisory was issued about them by law enforcement, and they did not respond to any inquiries from this site, which has not been their usual pattern.

In an email to DataBreaches.net yesterday responding to this site's inquiries about the joint advisory and the OrangeTee attack, they wrote:

> The last email we sent to OT Group included many videos of subsequent breaches until 26th August 2021, 2 weeks after OT Group announced the breach publicly. Servers containing some data and the videos were seized shortly after ALTDOS emailed them on 27th August.

A copy of that email was provided to DataBreaches.net. It informed OT Group/OrangeTee that there were videos showing continued access and exfiltration up through August 26, weeks after the firm had publicly acknowledged awareness of the hack. A copy of the videos was uploaded to a file-sharing site for OT Group to download. That file was no longer available when DataBreaches.net tried the link in the email.

The email also threatened, in part, to distribute the videos to regulators and media, along with data from OrangeTee. That approach — of publicly trying to embarrass companies and notifying media to help increase embarrassment or pressure– has been a consistent element across all of the ALTDOS ASEAN attacks that DataBreaches.net is aware of. But their email to OT Group also gave this site an indication of how much extortion ALTDOS demanded of these victims:

> ALTDOS shall give your management one last opportunity to save yourself from this mess once we publish the breach videos and databases. ALTDOS will take a step back on the numbers. Instead of initial asking of 10 BTC, OT Group can choose to pay just 1 BTC and ALTDOS will disappear entirely without leaking any videos or data.

Three days after the joint advisory, and less than one day after that email to OT Group/OrangeTee, some of their servers were seized, ALTDOS claims.

It appears that OT Group did not decide to pay the 1 BTC, as ALTDOS started dumping data. Re-appearing on a popular forum to dump some of it, they noted the seizure as the cause of their delay:

> We took some time to begin the leak due to technical issues arising from the seizure of some of our servers, which caused partial data corruption during sync. ALTDOS has already recovered our databases.

In a statement to DataBreaches.net, the threat actors responded to an inquiry from this site as to who had seized their servers and under what authority:

> ALTDOS does not know specifically which authority seized the servers, only received emails from the server company that our 3 servers were seized by authorities and requested more information from ALTDOS in the event where ALTDOS wants the data backup.

The threat actors wrote that they were not concerned about the seizure:

> ALTDOS has incremental backups performed across different servers, not a concern in case of seizures. Only require extra time to recover the full data which has already been completed.

DataBreaches.net has reached out to CSA Singapore and the PDPC to inquire as to who seized the servers, but no response was immediately forthcoming other than auto-acknowledgements from both agencies. The Singapore Police, who were involved in the joint advisory, do not have any statement on their site that would indicate their involvement in the seizure. It is possible, of course, that the seizure is not related to Singapore authorities but to some other authority related to non-Singapore victims, but the timeframe seems to suggest relationship to the OrangeTee incident.

This post will be updated if or when more information becomes available, but DataBreaches.net's reply email to ALTDOS has bounced back that their email address, which had been working as of several hours ago, no longer exists.
