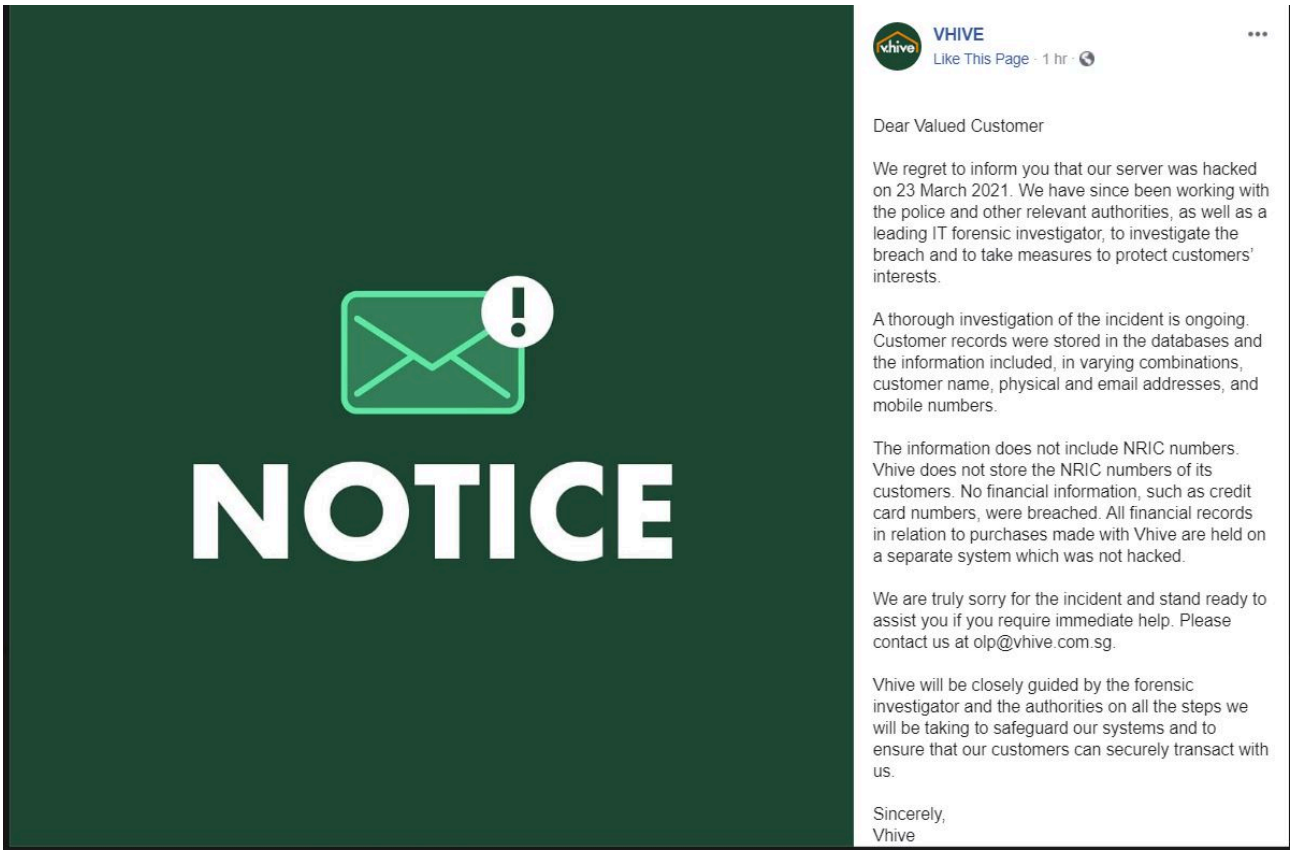
Sg: Vhive alerts consumers to cyberattack - DataBreaches.Net

Published: 2021-03-29 · Archived: 2026-04-11 02:08:40 UTC

Vhive, a popular retail furniture chain in Singapore, has posted a notice on their web site and Facebook page announcing a cyberattack that occurred on March 23.

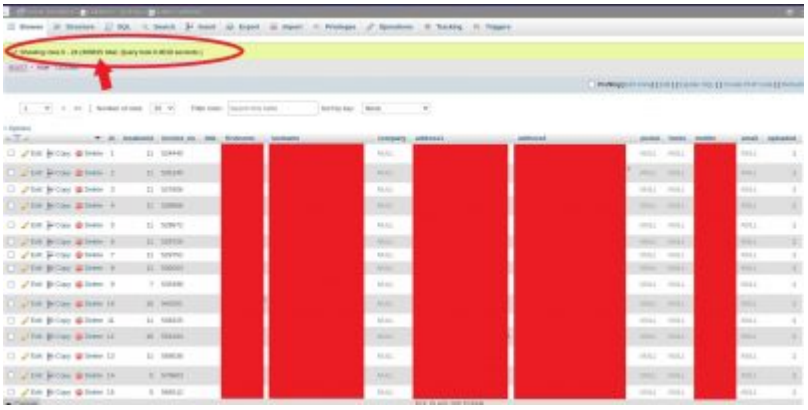


Based on information provided to DataBreaches.net by the threat actors, this appear to have been a double extortion attack by ALTDOS threat actors that involves more than 300,000 customer records as well as other types of documents including transactions records and payment records. According to Vhive, the attack did not involve NRIC numbers (national registration identity card numbers required for every Singapore resident over age 15). Nor did it reportedly involve any financial information or credit card data.

The initial attack of vhive.com.sg allegedly occurred on March 21, with the private network server breached on March 22. A timeline claimed by the threat actors indicates that Vhive was able to recover its site and files using backups on March 23, but allegedly "failed to resolve major vulnerabilities, allowing ALTDOS to continue our attacks." Those attacks allegedly continued on March 25, when ALTDOS downloaded source coding and files, and "encrypted all files on its server with a ransomware attack."

As proof of compromise, ALTDOS provided a number of mp4's showing them scrolling through directories and folders. They also provided some screencaps, including the one below which has been redacted by

DataBreaches.net. It shows that there were more than 300,000 records in the “systemv” “customer” table. DataBreaches.net has redacted the customers’ names, addresses, and mobile phone numbers.



The threat actors do not indicate what kind of ransomware was involved, but in a past attack, they had informed this site that they generally avoid ransomware and had simply used AES 256 encryption.

According to the attackers, there was some negotiation with Vhive management on March 26, and when they asked for more time, ALTDOS gave the firm a 48-hour deadline. On March 28, Vhive announced the breach on its web site and terminated negotiations with ALTDOS, who predictably responded by announcing that they will start dumping data within a few days.

DataBreaches.net reached out to Vhive to ask for more details about the ransomware aspect and to inquire whether they wished to make any additional statement about the attack. This post will be updated if or when a response is received.

Source: https://www.databreaches.net/sg-vhive-alerts-consumers-to-cyberattack/