Thai securities trading firm goes offline after cyberattack - DataBreaches.Net

Published: 2020-12-10 · Archived: 2026-04-11 02:08:47 UTC

It seems that yet another group of threat actors are trying the double-extortion method, replete with trying to get media coverage.

“ALTDOS,” as they call themselves, contacted a number of news outlets in Thailand and online news sites to announce that they had attacked **CGSEC** on December 4.

“A large Thailand SET public listed company dealing with securities trading has been hacked with its sensitive financial + customer database stolen and files encrypted last Friday (4th December 2020),” the hackers wrote, adding, “CGS deals with securities and financial trading services, however their servers are poorly protected.”

Allegedly, as a result of the firm’s lack of acknowledgement of their emails and demands, the attackers decided to dump some data. As proof of their claims, the attackers posted on popular file-sharing sites some of the data they claim to have exfiltrated.

ALTDOS dumped some data as proof of claims. Screenshot by DataBreaches.net.

Looking at the fields for the different tables, there appears to be a lot of unencrypted personal and financial information of customers and employees.

The web site of Country Group Securities, the victim company, was online last night when DataBreaches.net reached out to them for comment on the claimed attack, but does not appear to be online this morning. On their LinkedIn page, the firm describes themselves as:

> Through the provision of comprehensive research information, reliable sound advice, and exemplary client service, Country Group Securities is emerging as a prominent figure in the Thai equity market. The institutional equity team, comprising of a diverse and experienced group of professionals, is dedicated to providing its clientele with excellent service and expertise. With a focus on the client, the institutional equity team is segregated into two divisions; domestic and international, affording each client individual service and concentrated expert advice.

In communications with DataBreaches.net, a spokesperson for the hacker(s) says that their group’s targets are mainly in the finance or gambling industry. When asked what type of ransomware they were favoring, they

responded:

> During the event of ransomware attacks, there are many cases in which data or files are rendered corrupted even after decryption. Hence, we do not favor the usage of ransomware and we usually do not employ ransomware techniques on targets. Our methodology is to break into systems, steal the data and backup copies of their databases locally with AES-256 encryption.

Commenting specifically on this victim, they wrote:

> It did surprised us that a listed securities trading company actually left their data unencrypted and their systems did not detect our access from a list of suspicious black-listed IP addresses. We did prepared systems for heavy decryption jobs but apparently there wasn't a need for it….. There are many red flags about how this company protects its servers and its sensitive data. For example, the login credentials of its employee workstations are left unencrypted in one of the databases. A ransomware based group would have infected all of their workstations.

The attackers inform DataBreaches.net that on December 5, the attackers emailed the directors of CSG and demanded 170 BTC from the firm (more than $3 million USD at today's rates).

> We received no replies or negotiations till date and CGS has blocked our emails from their mail servers. Obviously, we did expected a negotiation from their management, given the magnitude of the hack – especially the fact that all of their financial records and client's sensitive information are already stolen. However, CGS management thinks they could cover up the hack and keep things under wrap by ignoring our emails. The fact is we are still able to break into the systems after 6th December 2020.

As noted above, since last night, the firm has reportedly taken their servers offline. If a response is received from them, this will be updated.
