Singapore corporations making progress in preventing cyberattacks - DataBreaches.Net

Published: 2022-09-13 · Archived: 2026-04-09 02:02:15 UTC

It was a back-handed compliment of sorts: experienced hackers telling DataBreaches that it had gotten noticeably harder for them to successfully attack big corporations in Singapore.

“The most difficult country to attack now, are Singapore companies,” they told DataBreaches in a chat.

“A lot has changed since 3 years ago. It is hard to even pinpoint a Singapore server with vulnerabilities these days. Just a few years ago, everything was still pretty much unsecured. Now, hackers ae lucky to even find a Singapore server with vulnerabilities…. we can’t pick up things for months.”

Given how active DESORDEN Group has been in ASEAN countries, for them to make that comment about Singapore is really interesting.

That does not mean that they have been totally unsuccessful, however. They still managed to recently attack a major multi-national shipping and logistics firm headquartered in Singapore — the **Ben Line Agencies** — although it was their first Singapore hit in about a year. DataBreaches sent email inquiries to Ben Line Agencies’ Singapore office and country manager about the attack, but received no replies, even though DESORDEN indicated that it was evident Ben Line was aware of the breach.

DESORDEN noted that the difficulties they experience in successfully hitting a Singapore target as quickly as they used to be able to do might be due to the fact that they are always looking for bigger companies.

“Either way,” their spokesperson told DataBreaches, “it is too time consuming to look at Singapore now.” And *that* is a bit of good news for big businesses in Singapore.

While DESORDEN may find its pool of big targets in Singapore being more difficult to attack, the current media frenzy over Indonesian hacks and data leaks has created new business opportunities for them, it seems. DESORDEN says they have been receiving a number of inquiries from people seeking to hire the hackers-for-hire group to hack Indonesian companies, and they have recently taken on more people to help.

Has Singapore Improved Its Cybersecurity Significantly?

Curious about why large Singapore organizations had become more challenging for DESORDEN to successfully attack, DataBreaches tried to find any data that might shed some light on the topic. While Singapore’s Personal Data Protection Commission (PDPC) authority publishes enforcement actions, undertakings, and guidance papers it issues, DataBreaches could not find any direct reports on how many data security breaches or leaks the regulator had received for 2020, 2021, and 2022 to date.

To try to obtain more information, DataBreaches sent inquiries to both the PDPC and Singapore’s Cyber Security Agency (CSA). The former has not replied as yet, but the latter pointed me to a report on the cybersecurity

landscape in 2021. According to that paper, 137 cases of ransomware were reported to SingCERT in 2021, which represented a 54% increase from 89 cases in 2020. Figures have not been released for 2022.

The report also noted that multiple entities had been hit between March and August 2021 by ALTDOS, a situation that led CSA, the PDPC, and the Singapore Police to issue a joint advisory on ALTDOS. Shortly thereafter, three of ALTDOS's servers were seized, although no government publicly claimed responsibility for the seizure. Of note, ALTDOS subsequently announced one more hack — of a Malaysian firm — and then disappeared as ALTDOS.

Did the advisory or any other measures Singapore took last year have a positive impact on business's cybersecurity measures? A CSA spokesperson responded to DataBreaches' inquiry that "it is good to hear that they are finding it increasingly difficult to attack big companies in Singapore. This means that our local companies are getting more aware of the importance of cybersecurity and the need to practise good cyber hygiene."

Last year, PDPC took enforcement action with monetary penalties against two of ALTDOS's victim companies: Audio House and vHive. And in addition to the regulatory actions, the vHive e-commerce site was down for months following the attack. Were those incidents "wake up" calls for Singapore businesses, or were there some other variables that were more influential? DataBreaches does not know at this point, but it would be great to figure out what made a difference and bottle it for other countries.
