Advisories are published, but are enough entities reading them and taking precautions? - DataBreaches.Net

Published: 2021-08-25 · Archived: 2026-04-09 02:06:09 UTC

Three advisories have been released this week about threat actor groups. One involves ALTDOS, one involves HIVE, and one involves the "OnePercent Group," whose name may not sound familiar to many.

ALTDOS (Joint Advisory)

It appears that ALTDOS is getting some serious attention from Singapore's CSA and other agencies in Singapore. These threat actors who target ASEAN entities have not gotten much coverage here in the U.S. other than DataBreaches.net's coverage, and they don't seem to have gotten a great deal of coverage anywhere — perhaps due to cultural differences in disclosing and reporting on breaches. This week, Singapore authorities issued a joint advisory that is the result of a collaborative effort between the Cyber Security Agency of Singapore (CSA), the Personal Data Protection Commission (PDPC) and the Singapore Police Force (SPF).

Interestingly (to me, anyway), the advisory says that ALTDOS uses ransomware, but that the ransomware variant is currently unknown. In the past, when DataBreaches.net had asked ALTDOS what type of ransomware they used, they had answered me:

> 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.

If I hear from them again, I will ask them if that's still the case. Or perhaps it was never the case, but a lot of the claims they have made to this site did check out.

The advisory provides some detection and prevention strategies, but are most ASEAN entities reading this advisory or taking it to heart?

HIVE (Alert Number MC-000150-MW)

The FBI has issued a Flash Alert about HIVE ransomware. The alert contains indicators of compromise for a group that first appeared in June of this year as "Hive." Unlike some other groups, they do not seem to seek media coverage, have not published any "press releases," and do not have any email or other contact information on their onion leak site.

ONEPERCENT GROUP (Alert Number CU-000149-MW)

> The FBI has learned of a cyber-criminal group who self identifies as the “OnePercent Group” and who have used Cobalt Strike to perpetuate ransomware attacks against US companies since November 2020. OnePercent Group actors compromise victims through a phishing email in which an attachment is opened by the user. The attachment’s macros infect the system with the IcedID banking trojan. IcedID downloads additional software to include Cobalt Strike. Cobalt Strike moves laterally in the network, primarily with PowerShell remoting.

As of the time of the alert, the onionsite was offline and has remained offline.
