Threat Group ‘Desorden’ Actively Targeting Asian Conglomerates | Threat Intelligence | CloudSEK

Archived: 2026-04-05 13:07:27 UTC

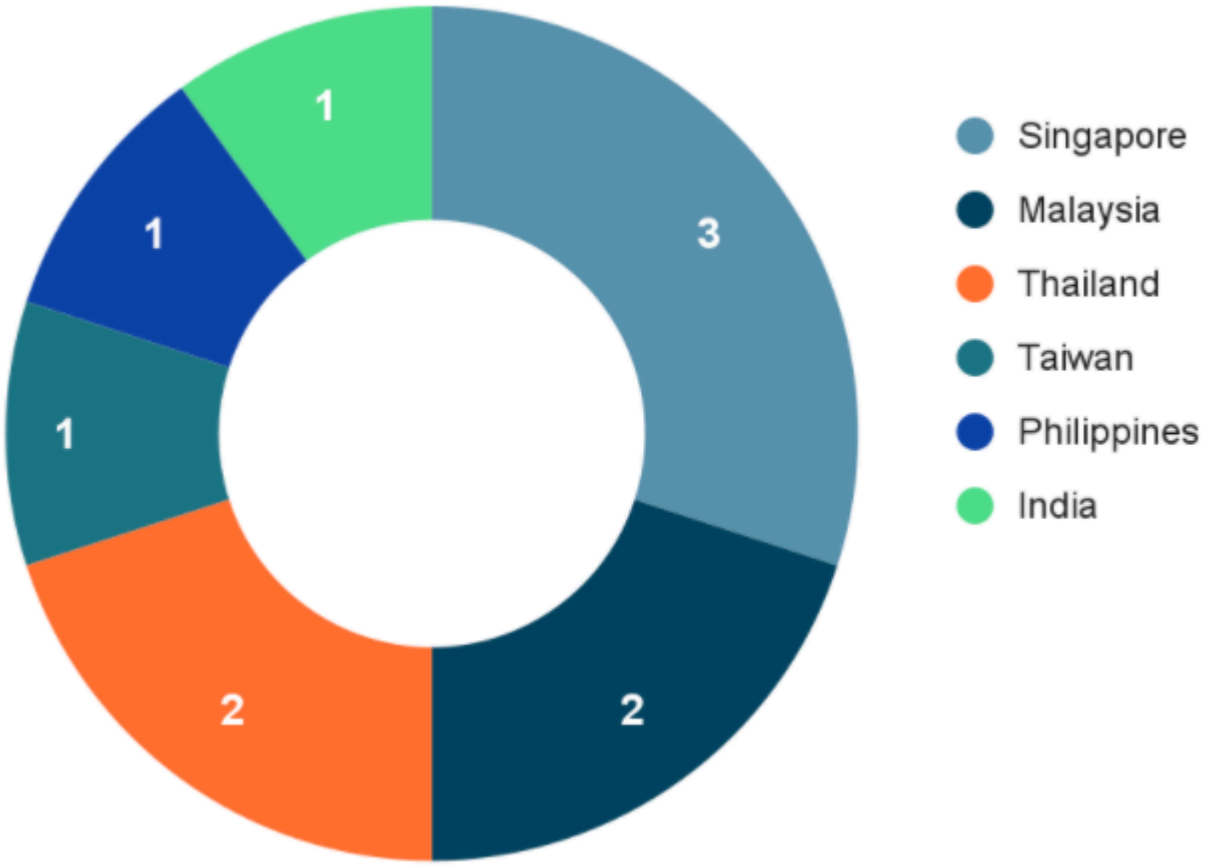
A confidential source has shared previously unknown details about the newly emerging threat actor group Desorden.

TLP: GREEN

About Desorden

- In September 2021, a financially motivated threat actor group dubbed ‘Desorden’ started breaching Asian companies and sharing the breached data on a popular English language cybercrime forum.
- The group's first post on the forum was published on 30 September 2021. The post advertised the database of the Malaysian subsidiary of a global logistics company based in Hong Kong. The post included sample data, as proof of the group’s claims and credibility.
- Since the first post, the group has consistently advertised the data of various Asian companies. As of January 2022 i.e. 4 months, since the group became active, they have shared the data of 10 companies.

[caption id="attachment_19021" align="aligncenter" width="618"]



Desorden victim profile[/caption]

Desorden Modus Operandi

A confidential source, directly in contact with the Desorden group, has shared information about the groups motives and their preferred Tactics, Techniques, and Procedures (TTPs).

Motives and Collaborations

- Currently, the group has no interest in breaching former USSR or European countries.
- The group carefully plans and selects their victims, which are primarily conglomerates in Asia that have high revenues.
- They claim to be a ‘for-hire’ hacking group and do not identify as a ransomware group, despite operating like one.
- The group is looking to recruit hackers who can exploit an organization's vulnerabilities and build new scripts.
- Desorden is engaged in deals with various ransomware groups that don’t focus on Asia. In what seems like an agreement to divide and conquer, Desorden sells vulnerabilities and accesses, to companies in Europe and North America, to ransomware groups that focus on those regions.

Tactics, Techniques, and Procedures (TTPs)

- The group initiates an attack by first performing reconnaissance of the infrastructure and technologies used by the target organization.
- Based on the recon, they develop custom Advanced Package Tool (APT) scripts to infiltrate the organization. The group also uses Python, PowerShell, and C#, based on their requirements.
- The group doesn't crypto-lock a victim's data, like ransomware groups do. Instead, they exfiltrate sensitive information from the victim, and threaten to publicize the data if the company does not heed to their ransom demands.
- The group purportedly works discreetly with the victims to collect the ransom.
    - If a victim pays the demanded ransom, they do not advertise the breach or the company's data.
    - If a victim is initially unresponsive, they publicize the breach, without releasing their data, in an attempt to pressure the victim into paying the ransom.
    - However, if a company refuses to pay the ransom even after these attempts, they dump or sell their data on cybercrime forums.

Desorden's Victim Profile

Since September 2021, Desorden has shared or advertised the databases of 10 high-revenue organizations operating or headquartered in Asia.

Country	No. of Victims	Victim Profile		
Singapore	3	• **Recruitment Firm** • **Department Store** • **Cinema Chain**	: : :	PII and login credentials PII, NRIC details, login credentials Not Available
Malaysia	2	• **Logistics Company** • **Carrier Service**	: :	200 GB customer and partner data Customer database
Thailand	2	• **Hotel Chain** • **Restaurant Group**	: :	400 GB of PII, financial and corporate data 80 GB of PII, financial and transaction data
Taiwan	1	• **Electronics Corp**	:	Employee info, list of vulnerable servers

Philippines	1	• **Supermarket Chain**	**:**	300 GB database
India	1	• **Electronics Corp**	**:**	60 GB of customer and corporate data

---

Source: https://cloudsek.com/threatintelligence/threat-group-desorden-actively-targeting-asian-conglomerates/