Threat Group Cards: A Threat Actor Encyclopedia

Other threat group: ALTDOS, Desorden

Names	ALTDOS *(self given)* Desorden *(self given)* GHOSTR *(elf given)* 0mid16B *(self given)*	
Country	Singapore	
Motivation	Financial gain	
First seen	2020	
Description	(Group-IB) Group-IB, a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime, announced today that it has contributed to a joint operation of the Royal Thai Police and the Singapore Police Force which led to the arrest of an individual responsible for more than 90 instances of data leaks worldwide, including 65 across the Asia-Pacific region. It resulted in over 13TB of personal data which has been sold on the dark web. In some countries the government agencies were also attacked, compromising sensitive information on a large scale. Operating under aliases ALTDOS, DESORDEN, GHOSTR and 0mid16B, the arrested individual was one of the most active cybercriminals in the Asia-Pacific since 2021, targeting companies and businesses in Thailand, Singapore, Malaysia, Indonesia, India and many more.	
Observed	Countries: Australia, Austria, Cambodia, Canada, France, India, Indonesia, Bangladesh, Malaysia, New Zealand, Pakistan, Philippines, Singapore, Taiwan, Thailand, UK, USA.	
Tools used	Cobalt Strike.	
Operations performed	Dec 2020	“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. <https://www.databreaches.net/thai-securities-trading-firm-goes-offline-after-cyberattack/>

Jan 2021	The same hacking group that hit Country Group Securities (CGSEC) in Thailand has revealed a recent attack on Mono Next Public Company Limited, a media and content conglomerate in Thailand. <https://www.databreaches.net/thai-media-and-content-conglomerate-mono-next-public-company-hit-by-altdos-hackers/>
Jan 2021	Hackers claim to have attacked major Bangladeshi conglomerate <https://www.databreaches.net/hackers-claim-to-have-attacked-major-bangladeshi-conglomerate/>
Mar 2021	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. <https://www.databreaches.net/sg-vhive-alerts-consumers-to-cyberattack/> <https://www.databreaches.net/sg-vhive-attackers-escalate-take-control-of-furniture-retailers-email-server/>
May 2021	Audio House customer data possibly stolen by hackers <https://www.straitstimes.com/tech/tech-news/audio-house-customer-data-possibly-stolen-by-hackers>
Jun 2021	ALTDOS claimed to have attacked Unispec Group Singapore, which operates in the marine industry, providing services in marine insurance, surveying, cargo, containers, and marine IT software. UniSpec has offices in Singapore, India, Thailand, Malaysia, Indonesia, South Korea and China. <https://www.databreaches.net/asean-companies-still-targeted-by-altdos-threat-actors/>
Aug 2021	Singapore-based OrangeTee appears to have suffered a massive hack and data exfiltration by ALTDOS threat actors. <https://www.databreaches.net/singapore-real-estate-firm-breached-by-altdos/>
Sep 2021	ALTDOS claims to have hacked one of Malaysia’s biggest conglomerates <https://www.databreaches.net/altdos-claims-to-have-hacked-one-of-malaysias-biggest-conglomerates/>
Sep 2021	Desorden Group claims to have stolen 200 GB of data from ABX Express <https://www.databreaches.net/desorden-group-claims-to-have-stolen-200-gb-of-data-from-abx-express/>

Oct 2021	Another Malaysia carrier allegedly hacked and data exfiltrated — Skynet <https://www.databreaches.net/another-malaysia-carrier-allegedly-hacked-and-data-exfiltrated-skynet/>
Oct 2021	Acer confirms second security breach this year <https://therecord.media/acer-confirms-second-security-breach-this-year/>
Oct 2021	Acer under fire: Now hackers claim to have hit Acer Taiwan, too <https://www.databreaches.net/acer-under-fire-now-hackers-claim-to-have-hit-acer-taiwan-too/>
Oct 2021	Central Restaurants Group in Thailand hit by Desorden <https://www.databreaches.net/central-restaurants-group-in-thailand-hit-by-desorden/>
Oct 2021	Desorden Group expands attack on Central Group after deal to pay them allegedly fell through <https://www.databreaches.net/desorden-group-expands-attack-on-central-group-after-deal-to-pay-them-allegedly-fell-through/>
Jul 2022	Desorden is back, declares an attack on MISTINE Better Way Thailand Company <https://www.databreaches.net/desorden-is-back-declares-an-attack-on-mistine-better-way-thailand-company/>
Jul 2022	Thai entities continue to fall prey to cyberattacks and leaks <https://www.databreaches.net/thai-entities-continue-to-fall-prey-to-cyberattacks-and-leaks/>
Aug 2022	Major Indonesia tollroad operator hacked by DESORDEN <https://www.databreaches.net/major-indonesia-tollroad-operator-hacked-by-desorden/>
Sep 2022	TH: Major Cineplex and Major Development PCL hit by DESORDEN <https://www.databreaches.net/th-major-cineplex-and-major-development-pcl-hit-by-desorden/>
Sep 2022	Customer data from hundreds of Indonesian and Malaysian restaurants hacked by DESORDEN <https://www.databreaches.net/customer-data-from-hundreds-of-indonesian-and-malaysian-restaurants-hacked-by-desorden/>

Sep 2022	DESORDEN leaks more data from Indonesia; “Indo data is officially worthless” <https://www.databreaches.net/desorden-leaks-more-data-from-indonesia-indo-data-is-officially-worthless/>
Sep 2022	Malaysian Telecom RedOne hit by DESORDEN <https://www.databreaches.net/malaysian-telecom-redone-hit-by-desorden/>
Oct 2022	Thailand’s THE ICON GROUP hacked by DESORDEN <https://www.databreaches.net/thailands-the-icon-group-hacked-by-desorden/>
Oct 2022	Revenge telecom hacking by DESORDEN Group; third attack threatened <https://www.databreaches.net/revenge-telecom-hacking-by-desorden-group-third-attack-threatened/>
Oct 2022	Johnson Fitness and Wellness hit by DESORDEN Group <https://www.databreaches.net/johnson-fitness-and-wellness-hit-by-desorden-group/>
Jul 2023	Major Malaysian water utilities company hit by hackers; Ranhill offline; hackers claim databases and backups deleted <https://www.databreaches.net/major-malaysian-water-utilities-company-hit-by-hackers-ranhill-offline-hackers-claim-databases-and-backups-deleted/>
Mar 2024	Hackers are threatening to leak World-Check, a huge sanctions and financial crimes watchlist <https://techcrunch.com/2024/04/18/world-check-database-leaked-sanctions-financial-crimes-watchlist/>
May 2024	Cooler Master confirms customer info stolen in data breach <https://www.bleepingcomputer.com/news/security/cooler-master-confirms-customer-info-stolen-in-data-breach/>
May 2024	Thailand’s Hatari Electric Faces Major Data Breach: GHOSTR Claims Possession of 617.3 GB of Sensitive Information <https://news.cloudsek.com/2024/05/thailands-hatari-electric-faces-major-data-breach-ghostr-claims-possession-of-617-3-gb-of-sensitive-information/>

	Jun 2024	Singapore-Based Absolute Telecom Allegedly Hit by Cyberattack: Over 34GB of Data Compromised <https://thecyberexpress.com/alleged-absolute-telecom-data-breach/>
	Jun 2024	Victorian Freight Specialists suffers alleged 800+GB data breach <https://www.cyberdaily.au/security/10667-victorian-freight-specialists-suffers-alleged-800-gigabyte-data-breach>
	Jul 2024	Air India Investigating Data Breach Claims Stemming from Arabian Travel Agency Hack <https://thecyberexpress.com/arabian-travel-agency-data-breach-exposed-info/>
	Jul 2024	Third-party breach resulted in Singapore Moneylenders Credit Bureau being leaked by GhostR <https://databreaches.net/2024/07/24/third-party-breach-resulted-in-singapore-moneylenders-credit-bureau-being-leaked-by-ghostr/>
	Nov 2024	Thai loyalty membership card data of 5 million customers put up for sale on hacking forum <https://databreaches.net/2024/11/20/thai-loyalty-membership-card-data-of-5-million-customers-put-up-for-sale-on-hacking-forum/>
	Dec 2024	Today’s insider threat: Ardyss edition <https://databreaches.net/2024/12/24/todays-insider-threat-ardyss-edition/>
	Dec 2024	Hacked on Christmas, DEphoto starts notifying customers, only to be attacked again <https://databreaches.net/2025/01/01/hacked-on-christmas-dephoto-starts-notifying-customers-only-to-be-attacked-again/>
	Jan 2025	Exclusive: Apex Custom Software hacked, threat actors threaten to leak the software <https://databreaches.net/2025/01/30/exclusive-apex-custom-software-hacked-threat-actors-threaten-to-leak-the-software/>
Counter operations	Sep 2021	ALTDOS claims some of their servers were seized but they did not lose data <https://www.databreaches.net/altdos-claims-some-of-their-servers-were-seized-but-they-did-not-lose-data/>

	Feb 2025	Hacker responsible for international data breaches arrested in joint Singapore-Thailand operation <https://www.channelnewsasia.com/singapore/spf-royal-thai-police-global-hacker-arrested-altdos-desorden-ghostr-0mid16b-4963661>
Information	<https://www.csa.gov.sg/singcert/-/media/Singcert/PDFs/Joint-Advisory-on-ALTDOS.pdf> <https://cloudsek.com/threatintelligence/threat-group-desorden-actively-targeting-asian-conglomerates/> <https://www.group-ib.com/media-center/press-releases/joint-operation-with-royal-thai-police-and-singapore-police-force/> <https://www.group-ib.com/blog/the-cybercriminal-with-four-faces-revealing-group-ib-s-investigation-into-altdos-desorden-ghostr-and-0mid16b/>	

Last change to this card: 21 April 2025

Download this actor card in PDF or JSON format
