Group-IB contributes to joint operation of Royal Thai Police and Singapore Police Force leading to arrest of cybercriminal behind more than 90 data leaks worldwide

Media Center → Press Releases

February 27, 2025 · 4 min to read

Asia-Pacific Cybersecurity Data leaks Royal Thai Police Singapore Police Force

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.

Group-IB's Threat Intelligence and High-Tech Crime Investigation teams located in the Digital Crime Resistance Centers (DCRCs) in Thailand and Singapore have been tracking the cybercriminal since 2020. He first emerged under the alias ALTDOS with victims mostly in Thailand. The main goal of his attacks was to exfiltrate the compromised databases containing personal data and to demand payment for not disclosing it to the public. If the victim refused to pay, he did not announce the leaks on dark web forums. Instead he notified the media or personal data protection regulators, with the aim of inflicting greater reputational and financial damage on his victims.

Later he also asserted pressure on his victims by sending direct customer notifications via email or via instant messengers to force them into submission. In rare occasions, Group-IB has also observed the cybercriminal encrypting the victim's databases.

Relatively quickly he expanded the victim geography beyond Thailand and started to publish data leaks to be sold on popular dark web forums. He was highly regarded on data leak forums as an owner of a large number of unique data leaks, and commanded a higher price for the leaked data.

To attack victims, the cybercriminal leveraged SQL injection tools like sqlmap and exploiting vulnerable Remote Desktop Protocol (RDP) servers to gain unauthorized access to sensitive data. The cybercriminal then installed a beacon of a cracked version of the CobaltStrike to control compromised servers. Based on Group-IB's findings, the cybercriminal did not perform significant lateral movement, and exfiltrated data to their rented cloud servers for further blackmailing of a company.

The investigation of this cybercriminal was hampered by the fact that he changed his nicknames and approach to work several times. Group-IB discovered that from 2020 until February 2025 he

operated under several aliases including ALTDOS, DESORDEN, GHOSTR and 0mid16B. Group-IB's dark web monitoring technologies analysed and correlated the similar styles of writing, format of posts, and preferences in data sharing websites, messengers and target regions. The connections were further confirmed by the timeline of accounts activity and correlations in posted databases.

Group-IB's investigation team analyzed every instance of alias changes. At times, he created a new digital persona to avoid correlation with previous attacks. In 2023, he was banned for scamming, and later, in 2024, for multi-accounting.

He gained further notoriety under the nickname DESORDEN, primarily targeting companies in Asia-Pacific countries. His main targets included industries such as healthcare, retail, property investment, finance, e-commerce, logistics, technology, hospitality, insurance, and recruitment. In the later stages of DESORDEN—and more intensively under the aliases GHOSTR and 0mid16B—he expanded his attacks to companies in the United Kingdom, the Middle East, Canada, and the United States.

The Royal Thai Police raiding the cybercriminal's premises. Courtesy of the Royal Thai Police.

During the operation, the Royal Thai Police seized several laptops and electronic devices, as well as a large number of luxury goods that was purchased with the cybercriminal with proceeds from the sale of the data leaks.

Electronic devices and luxury goods seized during the operation. Courtesy of the Royal Thai Police.

Dmitry Volkov
CEO, Group-IB

"This case highlights the evolution of cybercriminal tactics, not just through technical exploits, but through coercion, intimidation, and reputational threats. We are proud to have assisted the Royal Thai Police and the

Singapore Police Force, and we are grateful for their efforts in bringing the cybercriminal to justice. Working together, we have prevented him from causing further breaches, and protected the personal data of millions. This operation reaffirms our commitment to continue our fight against cybercrime alongside global and local law enforcement agencies, and ensuring a safer digital world for all."

According to Group-IB's High-Tech Crime Trends Report 2025, Thailand was among the top 10 jurisdictions globally with 18 instances of data leaks in 2024. Globally, there were 1,107 instances of new data leaks in 2024, which compromised more than 6.4 billion user data strings worldwide, including email and passwords, as well as phone numbers published on the dark web.

About Group-IB

Founded in 2003 and headquartered in Singapore, Group-IB is a leading creator of cybersecurity technologies to investigate, prevent, and fight digital crime. Combating cybercrime is in the company's DNA, shaping its technological capabilities to defend businesses, citizens, and support law enforcement operations.

Group-IB's Digital Crime Resistance Centers (DCRCs) are located in the Middle East, Europe, Central Asia, and Asia-Pacific to help critically analyze and promptly mitigate regional and country-specific threats. These mission-critical units help Group-IB strengthen its contribution to global cybercrime prevention and continually expand its threat-hunting capabilities.

Group-IB's decentralized and autonomous operational structure helps it offer tailored, comprehensive support services with a high level of expertise. We map and mitigate adversaries' tactics in each region, delivering customized cybersecurity solutions tailored to risk profiles and requirements of various industries, including retail, healthcare, gambling, financial services, manufacturing, crypto, and more.

The company's global security leaders work in synergy with some of the industry's most advanced technologies to offer detection and response capabilities that eliminate cyber disruptions agilely.

Group-IB's Unified Risk Platform (URP) underpins its conviction to build a secure and trusted cyber environment by utilizing intelligence-driven technology and agile expertise that completely detects and defends against all nuances of digital crime. The platform proactively protects organizations' critical infrastructure from sophisticated attacks while continuously analyzing potentially dangerous behavior all over their network.

The comprehensive suite includes the world's most trusted Threat Intelligence, The most complete Fraud Protection, AI-powered Digital Risk Protection, Multi-layered protection with Managed Extended Detection and Response (XDR), All-infrastructure Business Email Protection, and External Attack Surface Management.

Furthermore, Group-IB's full-cycle incident response and investigation capabilities have consistently elevated industry standards. This includes the 77,000+ hours of cybersecurity incident response completed by our sector-leading DFIR Laboratory, more than 1,400 successful investigations completed by the High-Tech Crime Investigations Department, and round-the-clock efforts of CERT-GIB.

Time and again, its solutions and services have been revered by leading advisory and analyst agencies such as Aite Novarica, Gartner®, Forrester, Frost & Sullivan, KuppingerCole Analysts AG, and more.

Being an active partner in global investigations, Group-IB collaborates with international law enforcement organizations such as INTERPOL, EUROPOL and AFRIPOL to create a safer cyberspace. Group-IB is also a member of the Europol European Cybercrime Centre's (EC3) Advisory Group on Internet Security, which was created to foster closer cooperation between Europol and its leading non-law enforcement partners.

Read next

March 19, 2026

Group-IB Partners with Copy Cat Group to Strengthen Intelligence-Led Cybersecurity Across East Africa

March 13, 2026

Group-IB Supports INTERPOL's Operation Synergia III, Contributing Intelligence to Global Cybercrime Takedown

March 12, 2026

Group-IB Expands into the Americas with Launch of Digital Crime Resistance Center in Chile

March 3, 2026

Group-IB and Nebrija University Strengthen Cybersecurity Education Through MOU and Threat Intelligence Integration

February 26, 2026

Group-IB Partners with Savex Technologies to Advance Predictive Threat Intelligence and Cyber Fraud Protection Across India and SAARC

February 16, 2026

National Polytechnic University of Armenia and Group-IB sign strategic partnership to strengthen cybersecurity education and research in Armenia

Go to all Press Releases →

Contact

APAC: +65 3159 3798

EU & NA: +31 20 226 90 90

MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends