← Blog

Jessica Tedja
Cyber Investigation Specialist, APAC

Vesta Matveeva
Head of High-Tech Crime Investigation Department, APAC

The Cybercriminal with Four Faces: Revealing Group-IB's Investigation into ALTDOS, DESORDEN, GHOSTR and 0mid16B

Following the arrest of the cybercriminal behind the aliases ALTDOS, DESORDEN, GHOSTR, and 0mid16B, Group-IB provides a deep dive into his activities, uncovering striking similarities and unmasking the cybercriminal that breached more than 90 instances of data leaks worldwide over the span of four years in operation.

March 20, 2025 · min to read · Cyber Investigations

Cyber Investigation Data Leak Extortion Threat Intelligence

Introduction

"*THIS IS DESORDEN HACKER GROUP. WE HAVE HACKED AND BREACHED INTO YOUR SERVERS.*"

This chilling message heralded a cyberattack that turned an ordinary day into chaos for victimized companies. What started as a routine day then quickly spiraled into panic as they faced a devastating data breach.

The attack was part of a planned campaign motivated by financial gain. The threat actor was notorious for executing high-profile data breaches in Asia and internationally. He targeted internet-facing Windows servers, specifically searching for databases that contained personal information. After compromising these servers, he exfiltrated the victim's data and, in some cases, encrypted it on the compromised servers. His ultimate goal was to extort the victim into paying the ransom, or risk public exposure of their data, which could lead to financial losses and reputational damage for the victim.

To communicate his demands, the threat actor left ransom notes on the victim's servers or sent them via email, detailing which databases had been exfiltrated and how the victim could make the payment. At times, he escalated his tactics by sending threatening emails or notifications via

messaging platforms to the victim's customers. If the victim failed to respond or refused to pay, the threat actor took his extortion efforts further by reporting the breach to data protection regulators to attract legal scrutiny, and by announcing the sale of the compromised data on dark web forums, to further exploit the situation for profit.

Group-IB's Investigations and Threat Intelligence analysts have been tracking the actor since he began his journey in 2020. Over the years, the threat actor changed his aliases three times, and drew significant media attention over the course of his criminal exploits. In this article, we uncover his evolution under the aliases of ALTDOS, DESORDEN, GHOSTR and 0mid16B, examining the patterns that linked his operations, and exposing how he used multi-accounting to remain undetected, until his arrest on 26 February 2025 in a joint operation by the Royal Thai Police, and the Singapore Police Force.

Act 1: The emergence of ALTDOS

The threat actor first emerged publicly on 4 December 2020, under the alias ALTDOS, announcing that he had conducted an attack on a financial institution based in Thailand. Seeking to amplify the impact of the attack, ALTDOS contacted multiple news outlets in Thailand, and DataBreaches.net, a platform that tracks and reports on data breaches, security incidents, and cybersecurity news.

According to an article published by DataBreaches.net on 10 December 2020, ALTDOS contacted the victim company's executives via email on 5 December 2020, demanding a ransom of 170 BTC in return for not publishing the stolen data.The ransom amount was valued at more than US$3 million at the time of the attack. When the victim company did not comply with his demands, ALTDOS retaliated by publicly dumping the compromised data, setting a precedent for future attacks. Later, we discovered that this actor had non-public victims even earlier than December 2020.

As ALTDOS, the threat actor continued to use the same modus operandi for subsequent attacks, primarily targeting companies in ASEAN countries such as Singapore, Thailand, Bangladesh, and Malaysia. However, over time, he adapted and refined his tactics. He began publishing full sets of compromised data on dark web forums like CryptBB and RaidForums, and then transitioned to selling the stolen data as well. The shift to using dark web forums for dumping complete databases may have been intended to send a message to future victims about the potential consequences if they did not comply with his demands. The transition to selling compromised data on dark web forums likely served to maximize his profits and broaden the scope of his criminal activities.

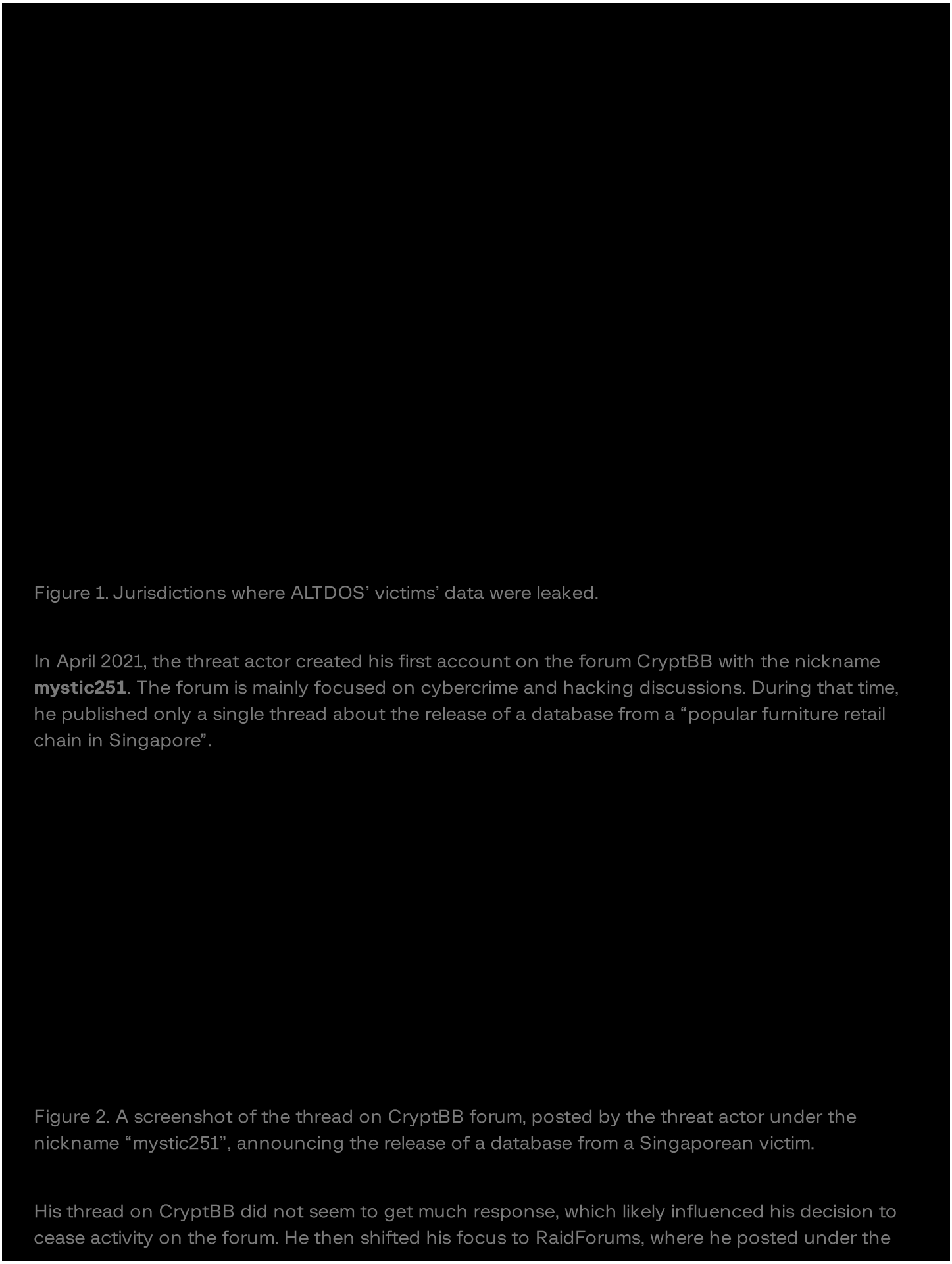

Figure 1. Jurisdictions where ALTDOS' victims' data were leaked.

In April 2021, the threat actor created his first account on the forum CryptBB with the nickname **mystic251**. The forum is mainly focused on cybercrime and hacking discussions. During that time, he published only a single thread about the release of a database from a "popular furniture retail chain in Singapore".

Figure 2. A screenshot of the thread on CryptBB forum, posted by the threat actor under the nickname "mystic251", announcing the release of a database from a Singaporean victim.

His thread on CryptBB did not seem to get much response, which likely influenced his decision to cease activity on the forum. He then shifted his focus to RaidForums, where he posted under the

alias **altdos**. Unlike on CryptBB, his thread attracted considerable attention on RaidForums, receiving numerous replies.

Figure 3. A screenshot of a post under the nickname altdos on RaidForums.

RaidForums was a data breach and marketplace platform popular among cybercriminals. ALTDOS' early attempts on CryptBB suggest he was still learning the best practices of selling breached data, indicating a lack of experience at the time.

Further investigation revealed the threat actor's Tactics, Techniques, and Procedures (TTPs). He targeted victims by utilizing SQL injection tools, such as sqlmap, to conduct reconnaissance on exposed databases, or exploiting vulnerable web servers to gain unauthorized access to sensitive data. He then deployed a beacon from a cracked version of CobaltStrike to maintain control over the compromised servers. During the course of Group-IB's investigations, the threat actor did not engage in significant lateral movement, and instead exfiltrated the data to his rented cloud servers, later using it for blackmail against the victim company.

Then in September 2021, ALTDOS suddenly ceased his operations. The threat actor would resume his activity four days later under a different alias, which we will detail in the next section. Group-IB's hypothesis on this abrupt identity shift is that cybercriminals often treat their online personas like brands, and ALTDOS' frequent tactical shifts and inconsistent methods initially painted him as an inexperienced operator. By adopting a new identity, he may have sought to establish himself as a more professional and formidable figure in the underground cybercrime market.

Act 2: Reinventing as DESORDEN

On 26 September 2021, a threat actor with the name DESORDEN started actively selling breached databases on RaidForums. Group-IB's analysis found striking similarities between DESORDEN and ALTDOS.

Both shared a similar writing style, and their victimology overlapped significantly, with a primary focus on Asian companies. Given these patterns, Group-IB conducted a deeper investigation into DESORDEN's activities, searching for further links to ALTDOS that could confirm they were, in fact, the same individual operating under a new alias.

Based on the comparison, Group-IB observed that both ALTDOS and DESORDEN used capital letters when mentioning the nickname, and provided a video as proof of the attack. The sentence "Here is a video screen recording of the stolen ..." was identically used by both aliases. Additionally, both ALTDOS and DESORDEN provided a link to the file sharing website, with a video recording.

Figure 4. A comparison of one of ALTDOS' posts (top), and DESORDEN's post (bottom) on RaidForums.

There were also similarities in the way the ransom notes were drafted. Both ALTDOS and DESORDEN consistently followed a distinct pattern, with each message beginning with "Today is <date>", using a day-first format followed by the month name and year (e.g., "3rd August 2022"). Immediately after the date, the threat actor introduced himself in a standardized manner, always starting with "This is <threat actor's nickname>". The ransom notes shown below were captured on the hacker's machine, which is likely a Kali Linux, since part of the logo typical for Kali Linux is visible on the background of both screenshots.

Figure 5. A comparison of ALTDOS' ransom note (top), and DESORDEN's ransom note (bottom).

Over time, the threat actor appeared to use capital letters more frequently. As seen on the ransom note above, he wrote the note in all capital letters. DESORDEN also added the word "group" after his nickname. It is a common tactic among individual threat actors to impersonate a group of threat actors, as they believe it adds more weight to their actions. ALTDOS has always referred to himself with the word "we".

Aside from sharing a similar victim profile, writing style, and web services with ALTDOS, DESORDEN also exhibited identical TTPs. These correlations led us to conclude that the same individual behind ALTDOS was highly likely operating under the DESORDEN alias.

DESORDEN was initially active on RaidForums and later migrated to BreachForums after RaidForums was taken down by law enforcement in 2022. Operating under this alias for the longest period, he gained significant notoriety, establishing himself as a formidable figure in the cybercrime ecosystem. This phase marked his most notable evolution, as he refined his tactics, expanded his reach, and solidified his reputation as a high-profile threat actor.

Figure 6. Jurisdictions where DESORDEN's victims' data were leaked.

Over a two-year period, DESORDEN compromised more than 30 victims, significantly escalating his cybercrime activities. During this time, he briefly collaborated with notorious BreachForums figures, including @Bjorka and @cod. However, this partnership lasted only a few months, suggesting that he ultimately preferred to operate alone.

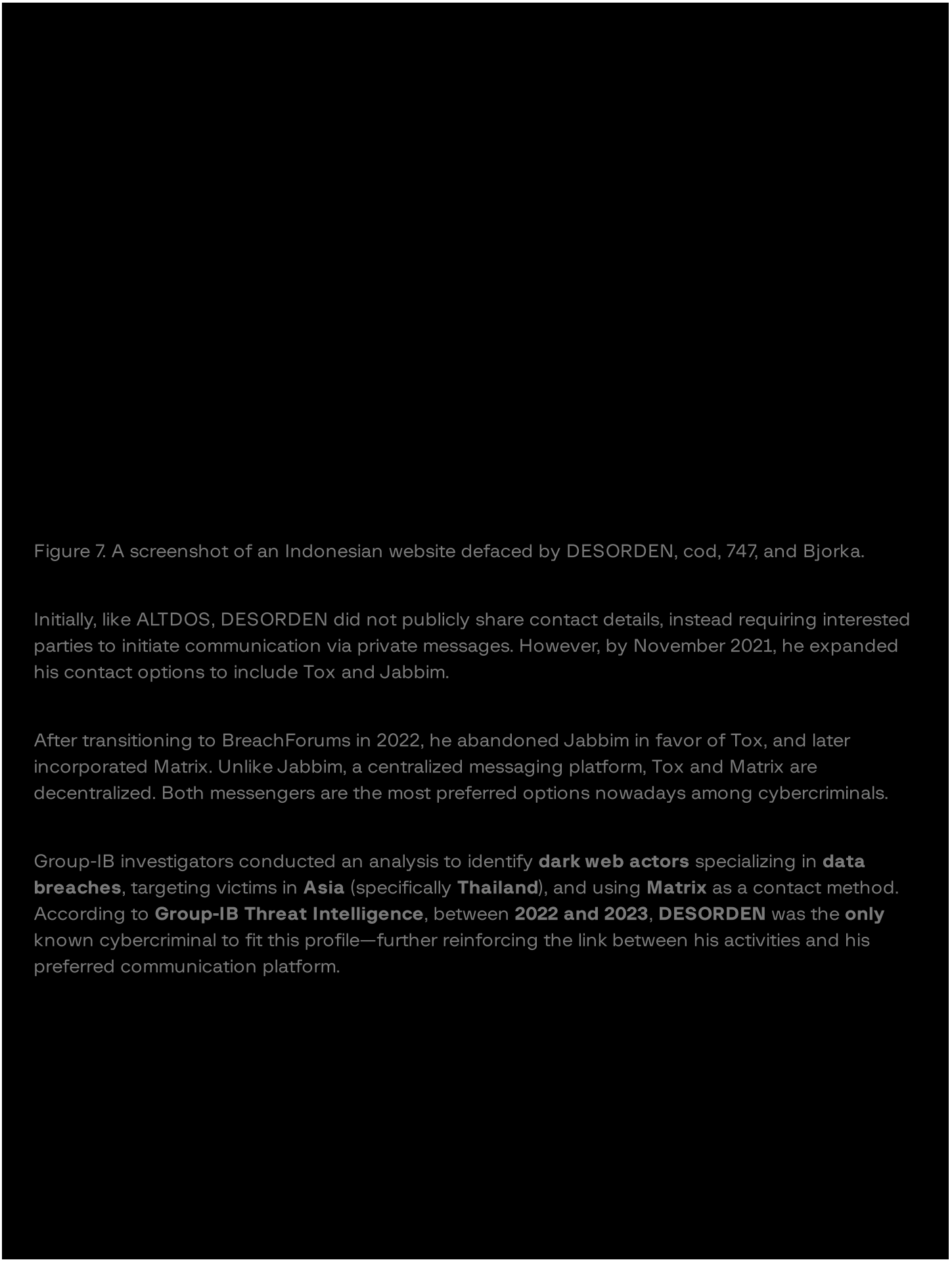

Figure 7. A screenshot of an Indonesian website defaced by DESORDEN, cod, 747, and Bjorka.

Initially, like ALTDOS, DESORDEN did not publicly share contact details, instead requiring interested parties to initiate communication via private messages. However, by November 2021, he expanded his contact options to include Tox and Jabbim.

After transitioning to BreachForums in 2022, he abandoned Jabbim in favor of Tox, and later incorporated Matrix. Unlike Jabbim, a centralized messaging platform, Tox and Matrix are decentralized. Both messengers are the most preferred options nowadays among cybercriminals.

Group-IB investigators conducted an analysis to identify **dark web actors** specializing in **data breaches**, targeting victims in **Asia** (specifically **Thailand**), and using **Matrix** as a contact method. According to **Group-IB Threat Intelligence**, between **2022 and 2023**, **DESORDEN** was the **only** known cybercriminal to fit this profile—further reinforcing the link between his activities and his preferred communication platform.

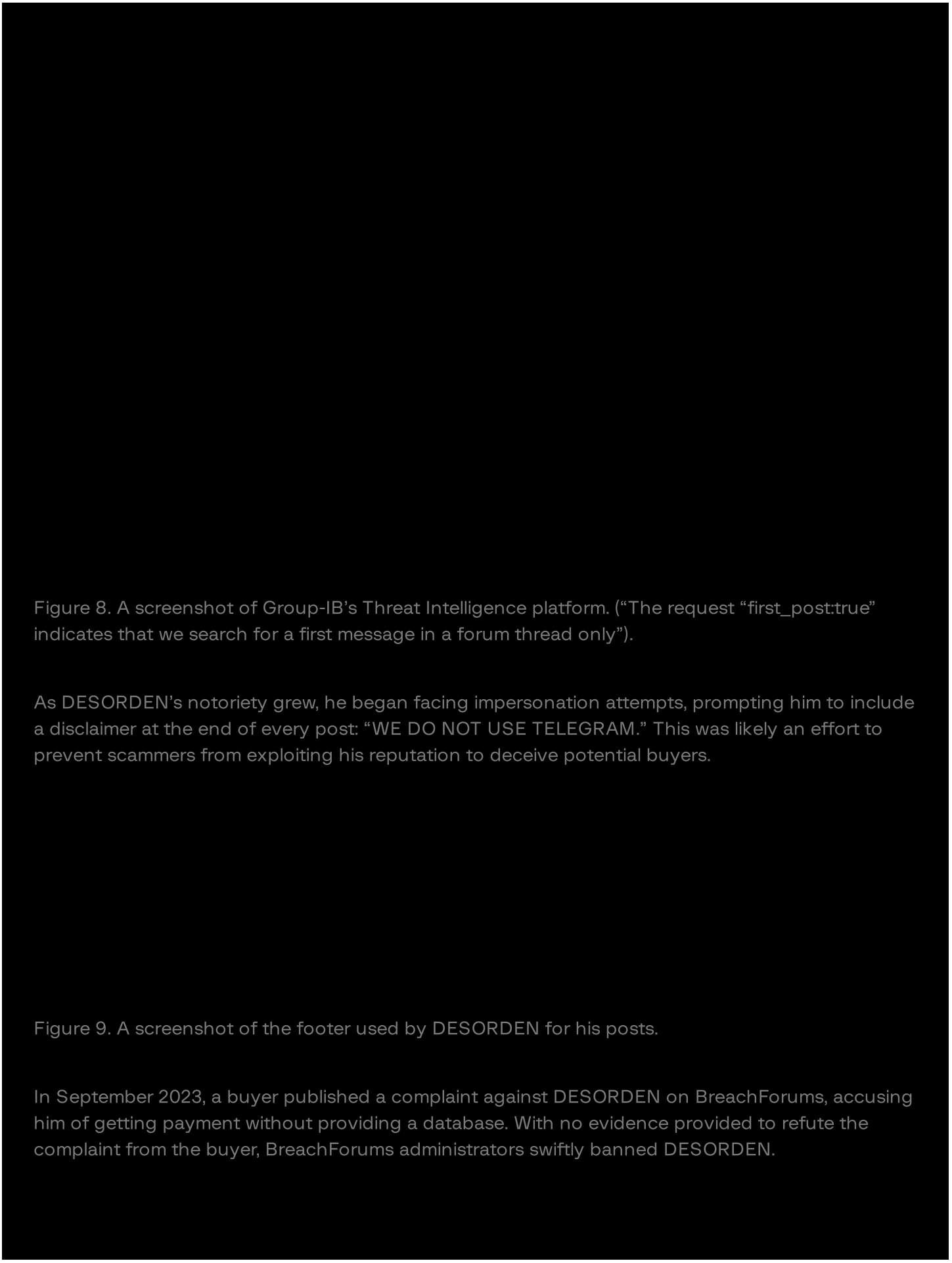

Figure 8. A screenshot of Group-IB's Threat Intelligence platform. ("The request "first_post:true" indicates that we search for a first message in a forum thread only").

As DESORDEN's notoriety grew, he began facing impersonation attempts, prompting him to include a disclaimer at the end of every post: "WE DO NOT USE TELEGRAM." This was likely an effort to prevent scammers from exploiting his reputation to deceive potential buyers.

Figure 9. A screenshot of the footer used by DESORDEN for his posts.

In September 2023, a buyer published a complaint against DESORDEN on BreachForums, accusing him of getting payment without providing a database. With no evidence provided to refute the complaint from the buyer, BreachForums administrators swiftly banned DESORDEN.

Figure 10. A screenshot of a message from DESORDEN to his buyer.

Once again, DESORDEN's activities came to an abrupt halt — but this time, it was not by choice.

In underground marketplaces like BreachForums, reputation is everything. Credibility and trustworthiness are critical for cybercriminals, as buyers are constantly evaluating whom to trust with illicit transactions. With numerous competitors vying for customers, being labeled a scammer can severely damage a hacker's ability to operate.

For DESORDEN, the scam report and subsequent ban meant a severe reputational blow, making it nearly impossible to sell stolen data or engage with other cybercriminals under that alias. As a result, he was forced to reinvent himself once again.

Act 3: Third time's the charm as GHOSTR

Just a week later, in October 2023, a new BreachForums account under the alias GHOSTR emerged, quickly amassing nearly 30 victims, with a primary focus on Asia and Canada. Given the rapid reappearance and operational similarities, we conducted a deeper analysis to determine potential connections between GHOSTR and DESORDEN.

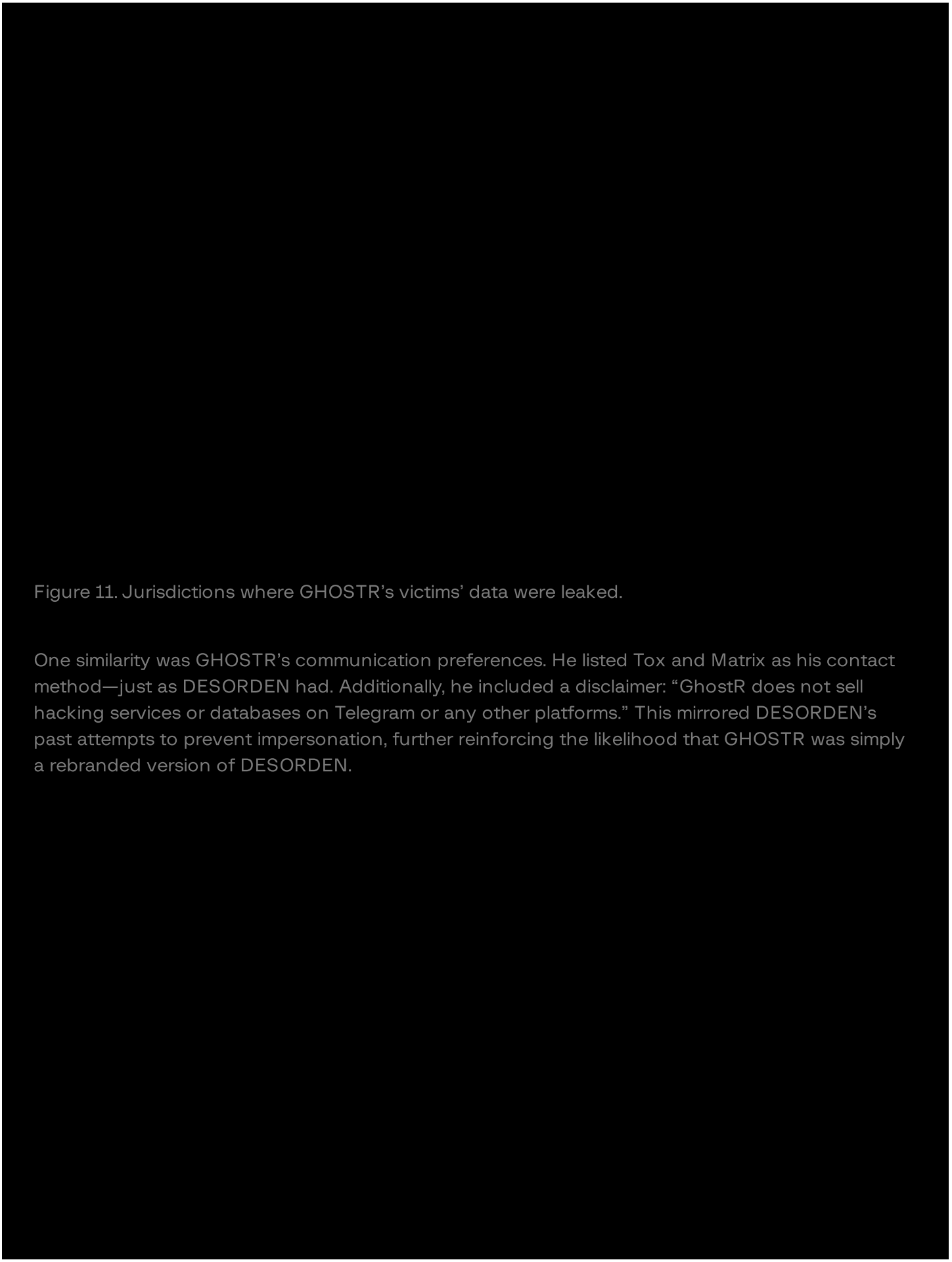

Figure 11. Jurisdictions where GHOSTR's victims' data were leaked.

One similarity was GHOSTR's communication preferences. He listed Tox and Matrix as his contact method—just as DESORDEN had. Additionally, he included a disclaimer: "GhostR does not sell hacking services or databases on Telegram or any other platforms." This mirrored DESORDEN's past attempts to prevent impersonation, further reinforcing the likelihood that GHOSTR was simply a rebranded version of DESORDEN.

Figure 12. A screenshot of GHOSTR's profile on BreachForums.

According to Group-IB Threat Intelligence, between 2023 and 2024, GHOSTR was the only other threat actor, aside from DESORDEN, who used Matrix as a contact method and targeted victims in Thailand for data breaches.

Figure 13. A screenshot of Group-IB's Threat Intelligence platform.

This overlap in both communication channels and victimology further reinforced the connection between the two aliases, suggesting that GHOSTR was simply DESORDEN operating under a new identity.

The avatars used by GHOSTR and DESORDEN also bore notable similarities, further supporting the connection between the two aliases.

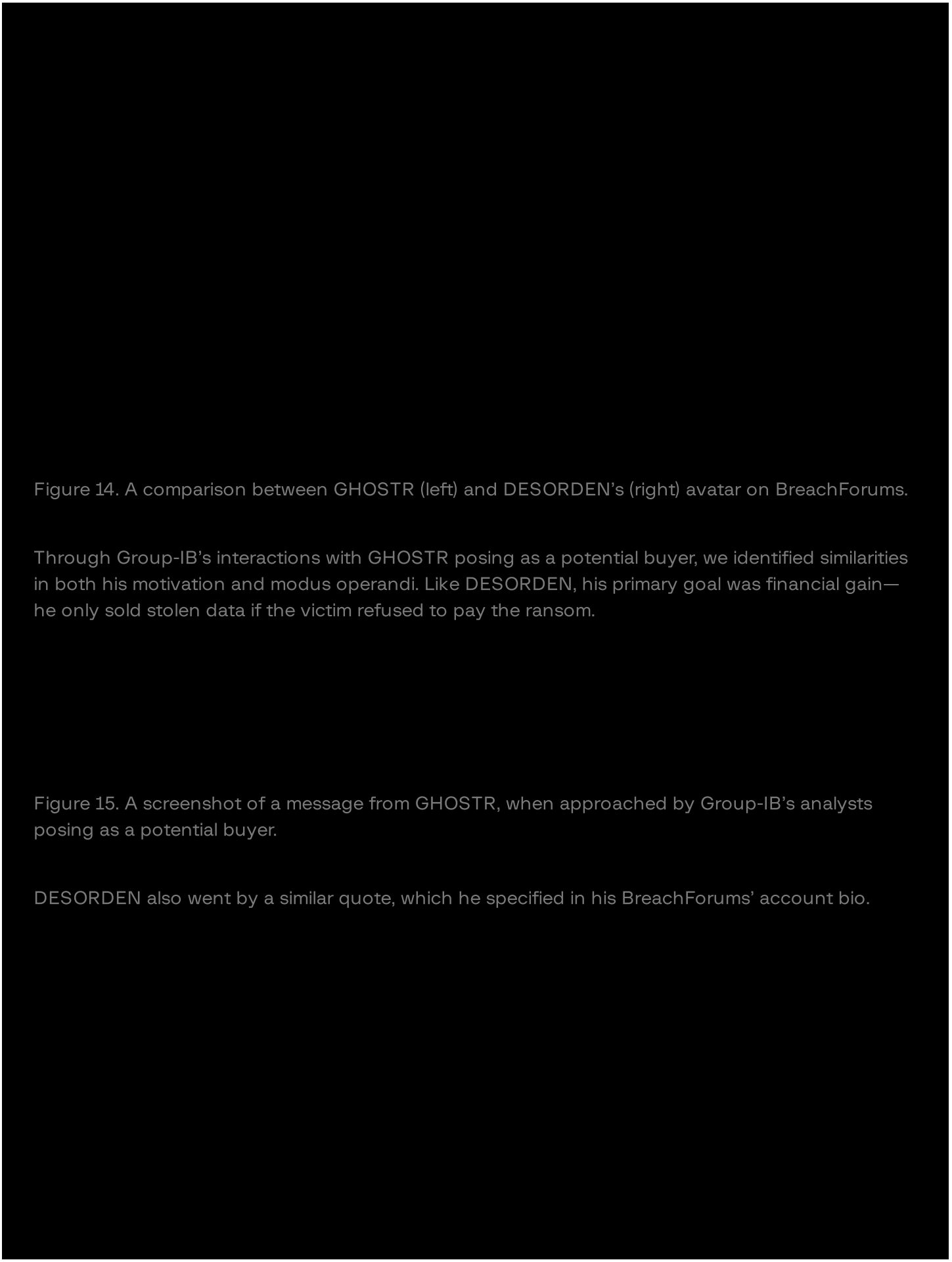

Figure 14. A comparison between GHOSTR (left) and DESORDEN's (right) avatar on BreachForums.

Through Group-IB's interactions with GHOSTR posing as a potential buyer, we identified similarities in both his motivation and modus operandi. Like DESORDEN, his primary goal was financial gain—he only sold stolen data if the victim refused to pay the ransom.

Figure 15. A screenshot of a message from GHOSTR, when approached by Group-IB's analysts posing as a potential buyer.

DESORDEN also went by a similar quote, which he specified in his BreachForums' account bio.

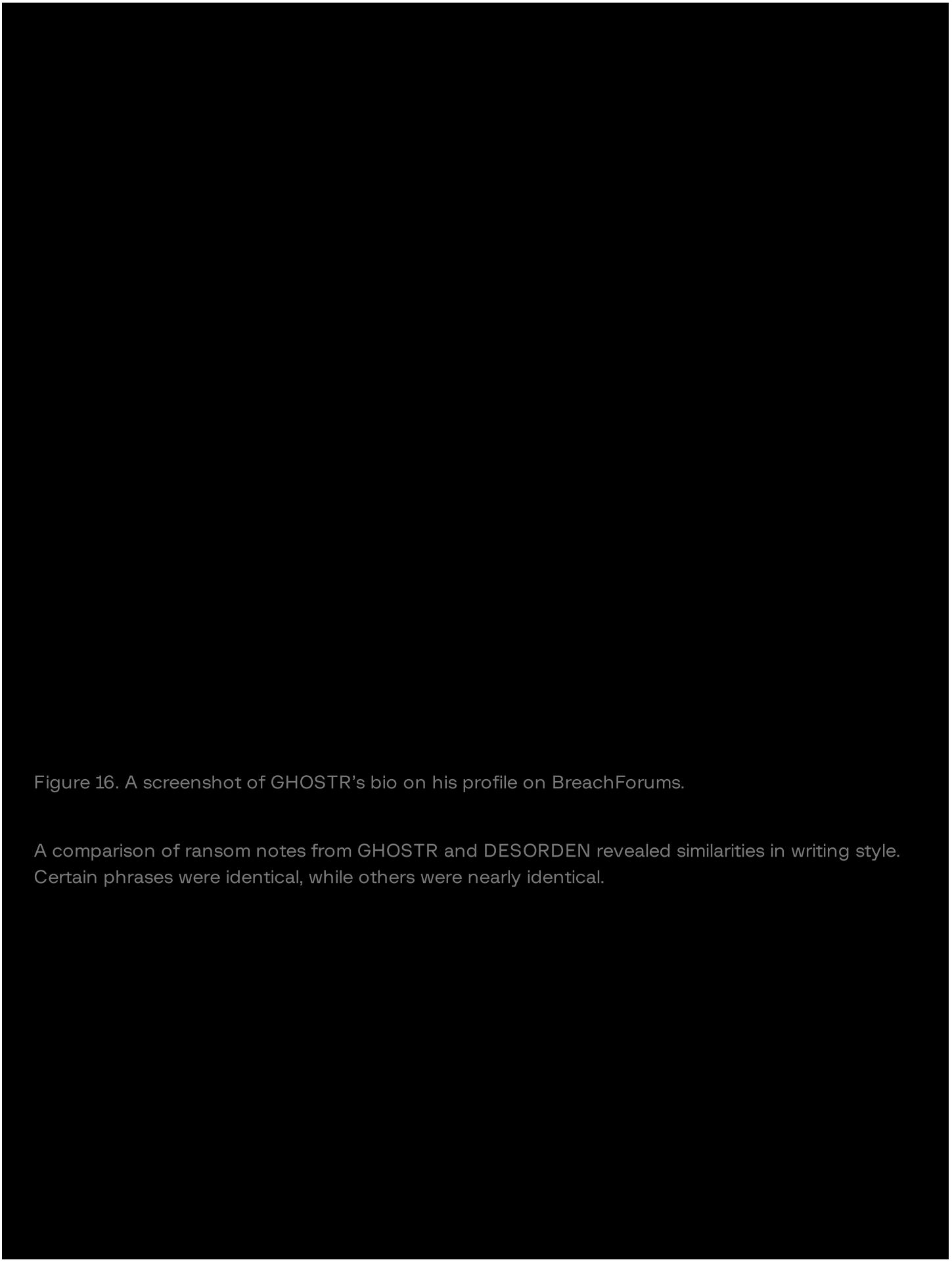

Figure 16. A screenshot of GHOSTR's bio on his profile on BreachForums.

A comparison of ransom notes from GHOSTR and DESORDEN revealed similarities in writing style. Certain phrases were identical, while others were nearly identical.

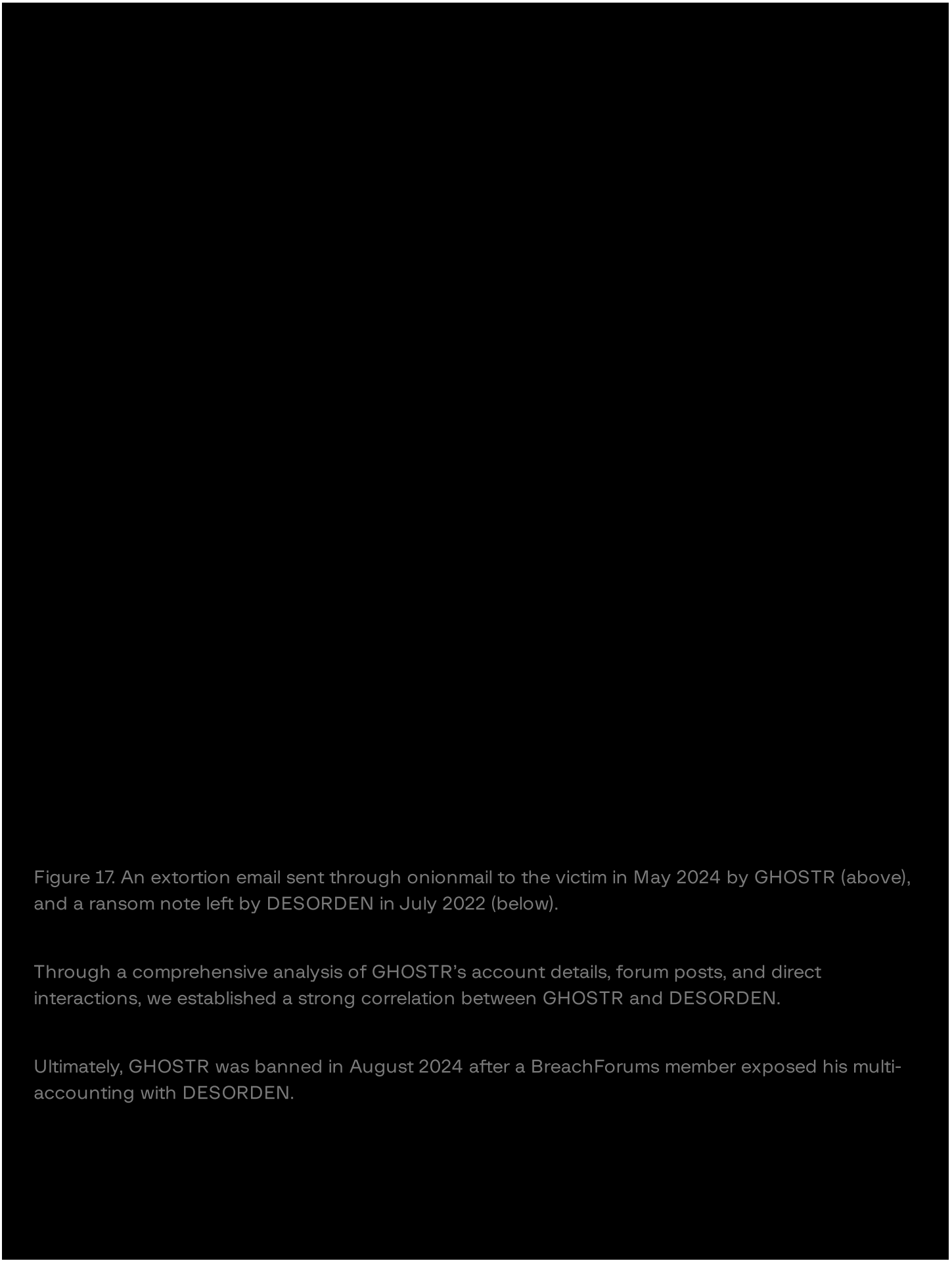

Figure 17. An extortion email sent through onionmail to the victim in May 2024 by GHOSTR (above), and a ransom note left by DESORDEN in July 2022 (below).

Through a comprehensive analysis of GHOSTR's account details, forum posts, and direct interactions, we established a strong correlation between GHOSTR and DESORDEN.

Ultimately, GHOSTR was banned in August 2024 after a BreachForums member exposed his multi-accounting with DESORDEN.

Figure 18. A screenshot of GHOSTR's profile on BreachForums after the ban.

Figure 19. A screenshot of a message sent by one of the moderators of BreachForums, in response to whether GHOSTR was DESORDEN.

Multi-accounting is a serious violation in underground cybercrime markets, as it compromises platform integrity and erodes trust within the community. By creating multiple accounts, individuals can manipulate reputations, evade restrictions, and engage in deceptive practices, ultimately undermining the credibility and reliability of these marketplaces.

GHOSTR's ban for multi-accounting with DESORDEN underscores the severe consequences of such actions. This incident reinforced the importance of transparency in underground forums, where reputation is a critical asset for cybercriminals looking to operate successfully.

Act 4: Masquerading as 0mid16B

Learning from past mistakes, the threat actor resurfaced once again—this time under the alias 0mid16B. Determined to avoid detection, he altered his avatar, tweaked his writing style, and shifted

his strategy, using X (formerly Twitter) to publicly announce his victims instead of relying solely on dark web forums.

Another key shift was in target demographics. Unlike his previous aliases, which primarily focused on Asian companies, 0mid16B expanded his operations globally, with a significant number of victims located outside Asia, including the United States. However, similar to GHOSTR and DESORDEN, the actor kept referring to himself as a “group”.

Figure 20. Jurisdictions where 0mid16B’s victims’ data were leaked.

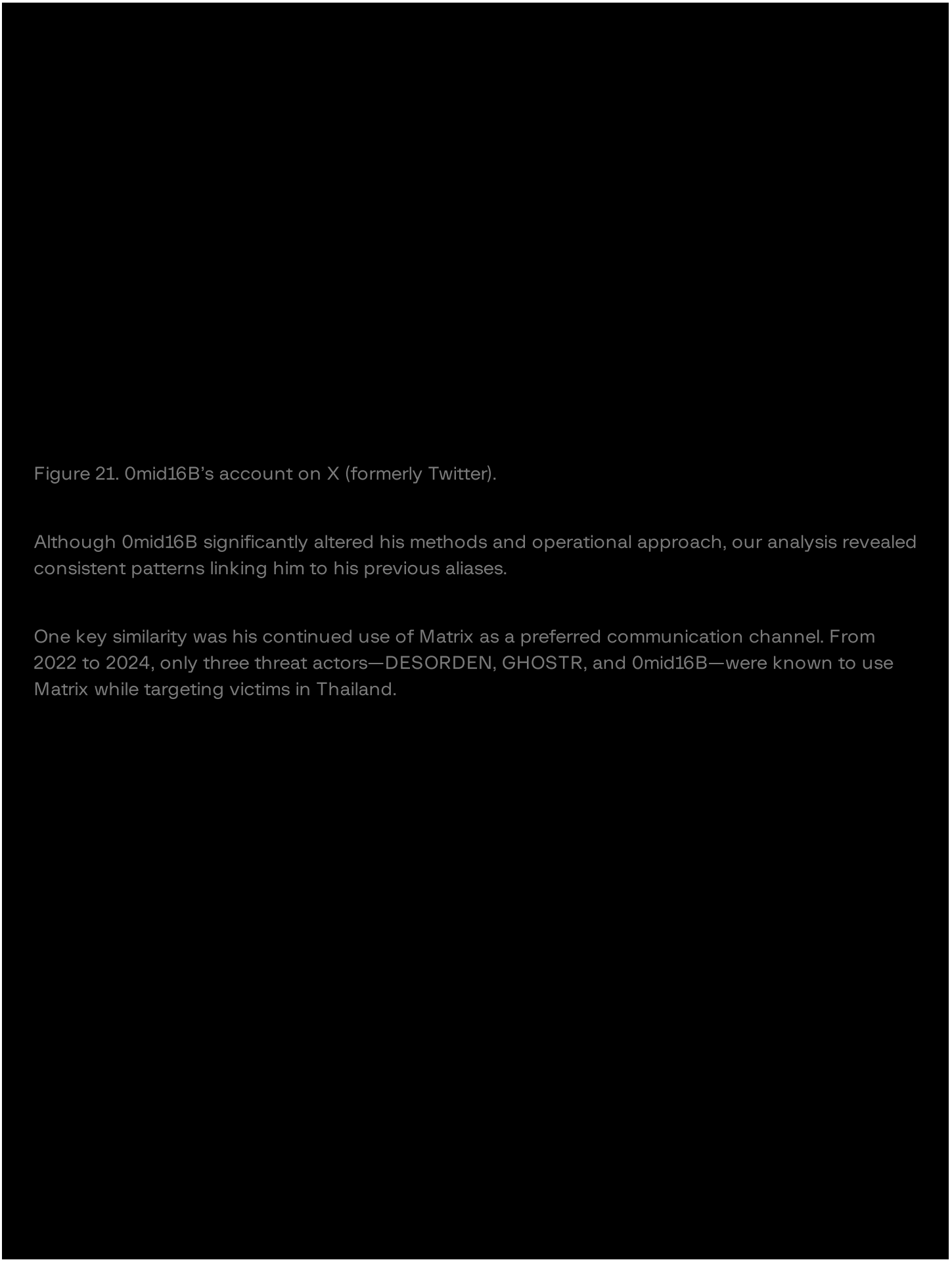

Figure 21. 0mid16B's account on X (formerly Twitter).

Although 0mid16B significantly altered his methods and operational approach, our analysis revealed consistent patterns linking him to his previous aliases.

One key similarity was his continued use of Matrix as a preferred communication channel. From 2022 to 2024, only three threat actors—DESORDEN, GHOSTR, and 0mid16B—were known to use Matrix while targeting victims in Thailand.

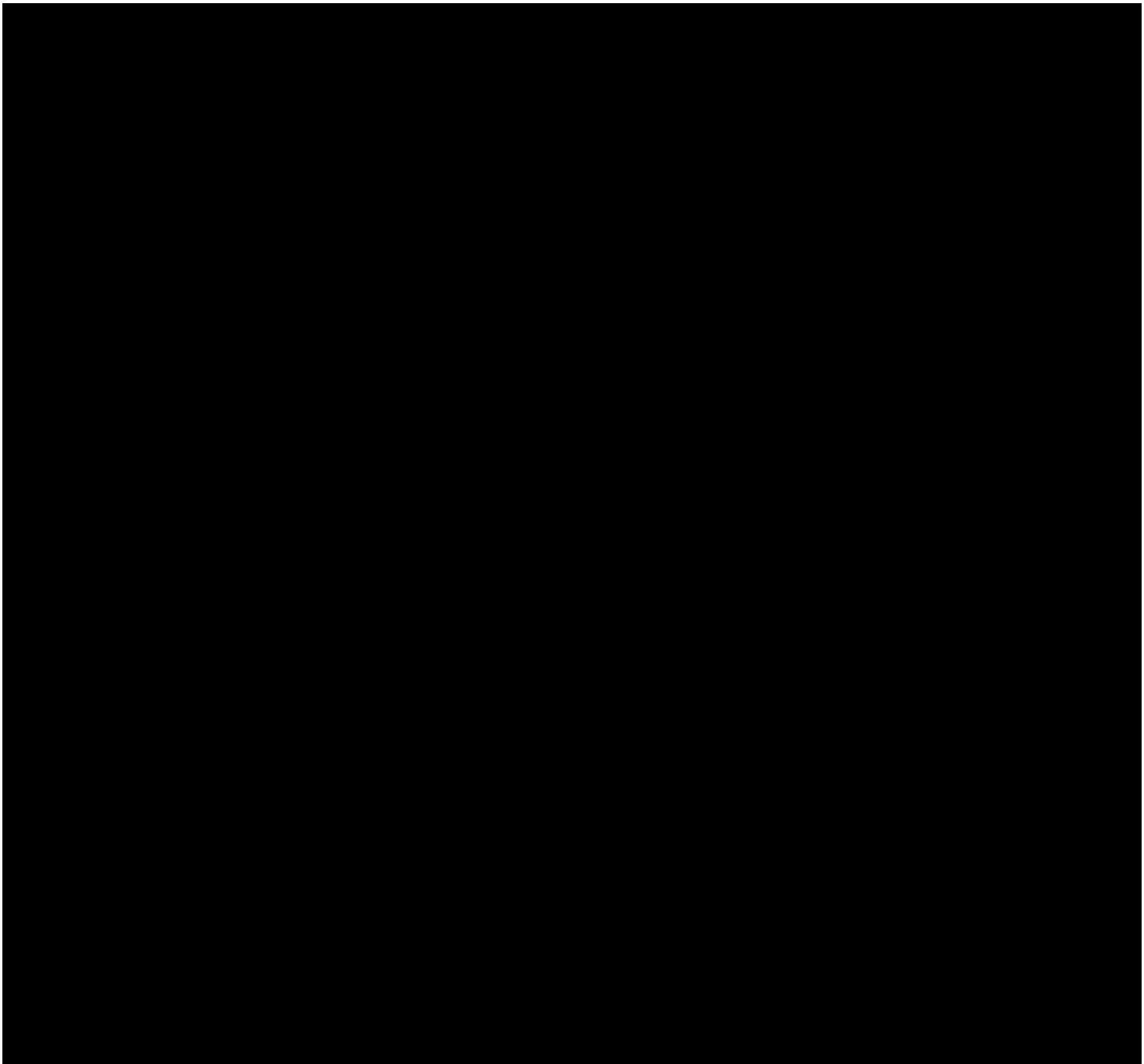

Figure 22. A screenshot of Group-IB's Threat Intelligence platform.

One persistent detail across all four of his aliases was his method of publishing stolen data screenshots. Regardless of his rebranding, he consistently uploaded images directly from the same device, revealing a key operational fingerprint.

Each time, the device interface was similar to Kali Linux, and the stolen data was stored in the same /media folder structure. The drive name remained identical across all aliases—"sf_E_DRIVE"—with one exception: under ALTDOS, the drive was labeled "sf_Storage". Additionally, he always used the victim's name as the folder name, a pattern seen repeatedly in his leaked screenshots.

This setup strongly suggests that he relied on VirtualBox, a popular virtualization tool, to run Kali Linux for his attacks. In VirtualBox, shared folders are typically mounted using the “sf_” prefix, followed by the name assigned to the shared folder or the drive letter of the host system’s shared resource. For instance, if a user configures a shared folder as “E_DRIVE”, it appears in Kali Linux as /media/sf_E_DRIVE.

Given this consistent digital footprint, we can infer that 0mid16B—like his previous aliases—used VirtualBox with Kali Linux to conduct his operations, further cementing the connection between his multiple identities.

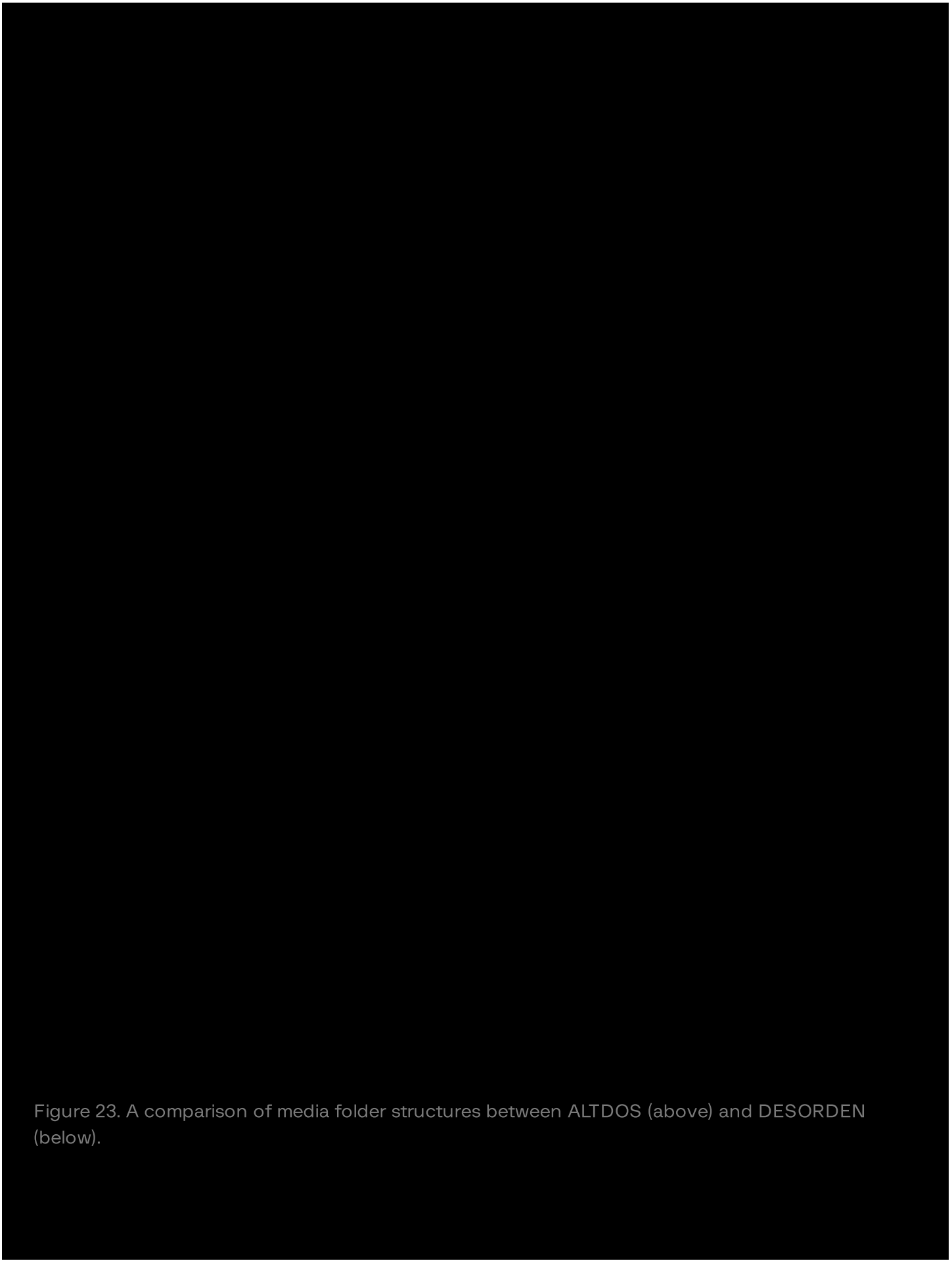

Figure 23. A comparison of media folder structures between ALTDOS (above) and DESORDEN (below).

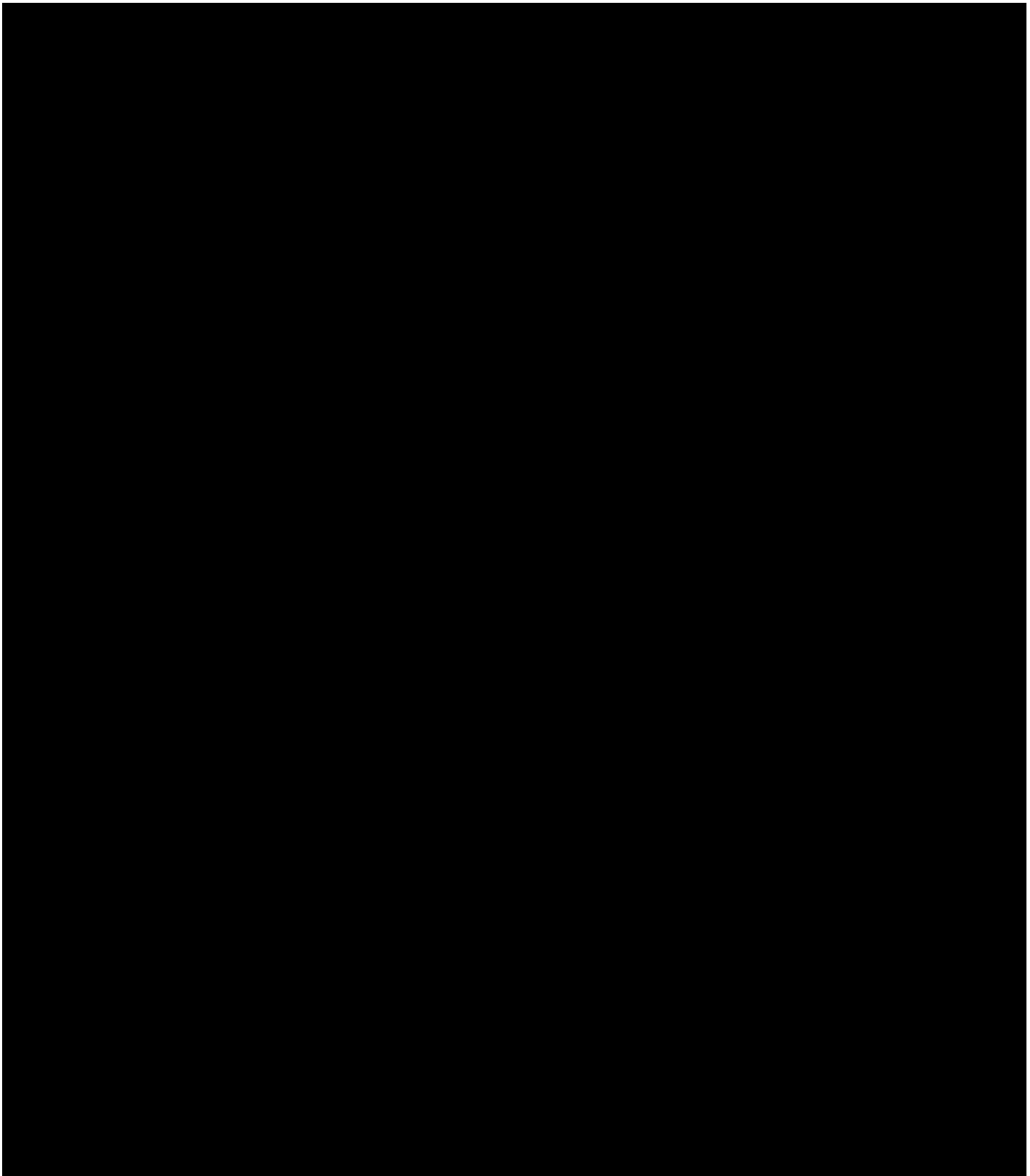

Figure 24. A comparison of media folder structures between GHOSTR (above) and 0mid16B (below).

Under the alias 0mid16B, the threat actor underwent a drastic transformation—a strategic move prompted by the exposure and banning of his previous GHOSTR identity, which had been linked to DESORDEN.

To distance himself from his past aliases, he shifted his approach, incorporating X (formerly Twitter) as a new platform for victim announcements. By adopting these new communication channels, 0mid16B attempted to break past associations, obscure his identity, and regain credibility in the cybercriminal underground.

The Final Act: The Downfall

Since his emergence, this threat actor's approach stood out as unconventional, setting him apart from typical dark web criminals. Unlike many cybercriminals who operate in groups, we believe he worked alone, yet managed to achieve significant success while evading detection for an extended period.

The investigation into his activities was complex and prolonged. Despite repeatedly leaving digital fingerprints across multiple aliases, his meticulous operational security (OPSEC) made it exceptionally difficult to uncover his true identity.

One key indicator of his strict OPSEC practices was an instructional guide published by DESORDEN, outlining security measures that he likely followed to maintain anonymity. The consistency of his tactics, aliases, and cybercriminal methods suggests that his self-imposed security discipline played a major role in his ability to stay undetected for so long.

Figure 25. A post published by DESORDEN about OPSEC practices, monitored by Group-IB's Threat Intelligence platform.

For more than 4 years, the threat actor known as ALTDOS, DESORDEN, GHOSTR, and 0mid16B has been the most prolific yet elusive cybercriminal in the Asia-Pacific. But in the end, it was his digital breadcrumbs that ultimately led to his discovery. Since his emergence, 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 him across his multiple aliases, and contributed to the ongoing investigations by the law enforcement agencies. On 26 February 2025, the threat actor was finally arrested in Thailand by the Royal Thai Police.

Figure 26. A screenshot of 0mid16B's X account after his arrest in Thailand on 26 February, 2025.

During the press conference, the Royal Thai Police also revealed that the cybercriminal confessed that his main target was large private companies and he avoided attacking government agencies because he did not want the public to be affected.

MITRE ATT&CK

Recommendations

As cyber threats continue to evolve, organizations must adopt proactive security measures to defend against data breaches, extortion, and advanced cyberattacks. The case of ALTDOS, DESORDEN, GHOSTR, and 0mid16B highlights the increasing sophistication of threat actors, who continually adapt their methods to exploit vulnerabilities across industries.

To mitigate these risks, businesses must implement robust security strategies that focus on prevention, detection, and rapid response. The following recommendations outline critical cybersecurity measures designed to protect organizations from unauthorized access, data theft, and ransomware attacks.

- Implement a patch management policy to ensure firmware and software are regularly updated with the latest security patches to protect against known vulnerabilities.
- Implement network segregation and enforce strict firewall rules to limit lateral movement within the network.
- Disable unnecessary RDP access, and restrict it to trusted IP addresses only.
- Regularly monitor and audit accounts; remove or disable dormant accounts to prevent unauthorized access.
- Implement multi-factor authentication (MFA) for VPN and other remote access services to add an additional layer of security.
- Implement application control on hosts to prevent installation and execution of unauthorised programs.
- Implement Endpoint Detection and Response (EDR) solution to detect and respond to suspicious activities such as deployment of backdoors or indicators of compromise (IOCs) associated with popular penetration testing frameworks.
- Engage in MTH (Managed Threat Hunting) service, to proactively hunt for unknown threats and sophisticated attacks.

Encrypt sensitive data both at rest and in transit to make it useless even if exfiltrated by an attacker.

Subscribe to an incident response retainer service to ensure access to a team of cybersecurity professionals who can effectively respond to any incidents that may occur within the infrastructure.

Do not hesitate to contact the Group-IB Investigation team in case you suffer a data breach to seek professional assistance in handling the incident as well as further investigation.

Share this article

Found it interesting? Don't hesitate to share it to wow your friends or colleagues