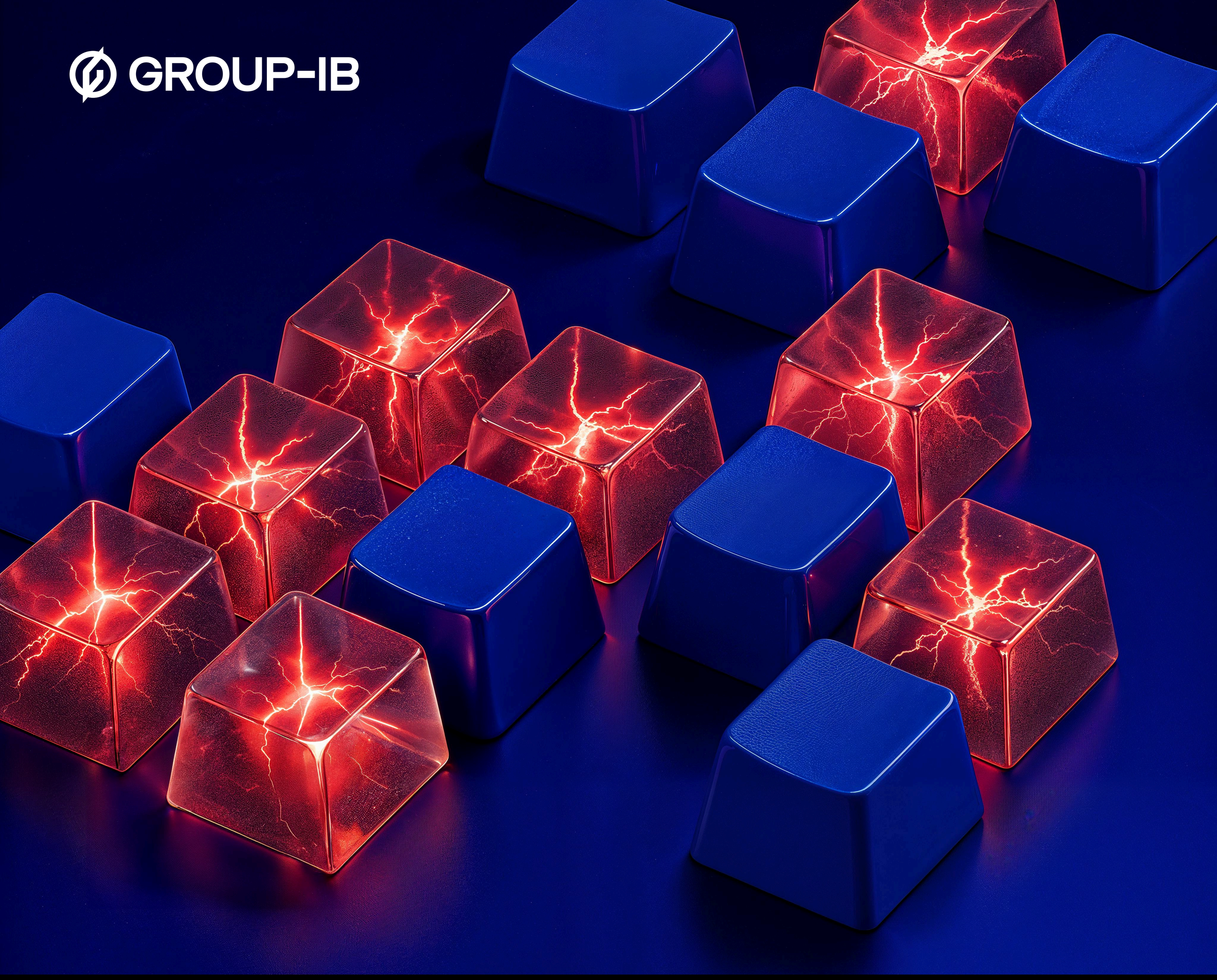
GROUP-IB



Threat Research

Hacktivists at War

The Cambodia–Thailand Cyber Escalation

July–August 2025

GROUP-IB.COM

Table of contents

1. Disclaimer

1. The report was written by Group-IB experts without any third-party funding.

2. The report is for information purposes only and Group-IB is limiting its distribution. Readers are not authorized to use it for commercial purposes or any other purposes not related to training or personal non-commercial use. Group-IB grants readers the right to use the report worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the report itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.

3. The entire report is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use any of its content without the copyright holder's prior written consent.

4. In case of copyright infringement, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the offender as provided by law, including recovery of damages.

2. Acknowledgements

Authors

Sittipat Palawooth, Junior Analyst (APAC)
Khat Atith, Cyber Intelligence Analyst (APAC)

3. Introduction

Since 24 July 2025, a military conflict between Cambodia and Thailand has escalated into a series of cyberattacks. The activity has been driven primarily by hacktivist groups supporting both countries. Despite the ceasefire agreements issued on 28 July and 7 August, the campaigns led by cyber activists have remained active and ongoing.

Hacktivism has emerged as a key component of this cyber conflict, with nationalist groups conducting disruptive operations in protest and retaliation. These actions often correlate with physical events and typically involve website defacements, distributed denial-of-service (DDoS) attacks, occasional data leaks, and disinformation campaigns.

The majority of the detected attacks appear to be opportunistic and unsophisticated, although some hacktivist groups claimed significant data exfiltration and large-scale service disruption. Attribution to state-sponsored groups remains unconfirmed, although accusations have been exchanged between the two governments.

The Group-IB Threat Intelligence team is actively tracking **19 hacktivist groups** involved in the cyber offensive operations targeting Cambodia and Thailand. This report provides an overview of hacktivist activity during the conflict from **24 July to 7 August**, and offers relevant recommendations for organizations seeking to defend against these digital threats.

04 Key Findings

1. Armed conflict between Cambodia and Thailand triggered a spike in large-scale hacktivist activity involving 139 cyber attacks, of which 103 were DDoS attacks. A total of 350 attacks have been observed by Group-IB since May 2025.
2. During the spike, the attack rate of the involved hacktivist groups rose by 241%, compared to the baseline established in June-July.
3. 11 pro-Cambodian and 8 pro-Thai distinct hacktivist groups have been directly involved in offensive operations on both sides. Notably, 14 of the identified threat actors have emerged after May 2025 when the tension between countries began escalating.
4. Cambodian-affiliated groups such as BL4CK CYB3R, NxbbSec, and DarkStormTeam targeted Thai government, education, and healthcare sectors.
5. Thai-affiliated groups including BlackEye-Thai, CyberSafe TH, Thai Is God, conducted retaliatory operations against the Cambodian government, banking, and education sectors.
6. No confirmed impact on critical infrastructure has been reported as of the publishing of this report.

05 Border conflict escalated into cyberspace

The current surge of cyber activity between Cambodia and Thailand is a result of escalating tensions that began in May 2025. On 28 May, a border incident involving military personnel resulted in the death of a Cambodian soldier. Following this event, tensions increased as both sides reinforced their military presence along the border.

The situation escalated further after two landmine explosions on 16 July and 23 July injured several Thai soldiers. Multiple armed clashes began on 24 July along the border.

Shortly after the physical conflict, cyberattacks were observed across both Cambodian and Thai digital landscape. These attacks included website defacements, DDoS attempts, and other disruptive activities targeting government, financial, and other industries in both countries. Despite a ceasefire agreed on 28 July, cyber operations by hacktivist groups from both sides of the conflict continue unabated.

The next section provides an overview of the hacktivist actors involved and presents statistics on the cyberattacks observed during this period.

06

Key hacktivist groups and attack volume

Group-IB Threat Intelligence team has profiled multiple hacktivist clusters active in this cyberconflict - **11 pro-Cambodian** groups and **8 pro-Thailand** actors. **14** of these groups appeared after May 2025 as tensions escalated, employing low-complexity techniques such as DDoS attacks and website defacements. Such attacks are aimed at visibility and disruption rather than sustained access.

Group-IB customers can access our Threat Intelligence portal for more information about the respective threat actors by clicking on their names.

Pro-Cambodia hacktivists:

Hacktivist Groups	First Discovered	Attack Techniques	Main Targeted Industries
BL4CK CYB3R (aka AnonSecKh)	March 2025	DDoS, Leaks	Government and military, Education, Healthcare
DarkStormTeam	August 2023	DDoS, Leaks	Government and military, Education, Food and beverage
NxbbSec	May 2025	DDoS, Defacement, Leaks	Government and military, Education, Healthcare
NxbbSec	May 2025	DDoS, Defacement, Leaks	Government and military, Education, Healthcare
NRSTSEC	June 2025	DDoS, Leaks	Government and military, Education, Energy
H3C4KEDZ	May 2025	Leaks	Government and military, Healthcare, Education
K0LzSec	May 2023	DDoS, Defacement, Leaks	Government and military, Education, Financial services
CyberKingdomKH	August 2025	Leaks	Government and military
UnknowSEC	August 2025	DDoS, Leaks	Government and Military, Education
KXICHIXXSEC	July 2025	DDoS, Defacement, Leaks	Government and military, Education, Manufacturing
NNDSEC	July 2025	Defacement, Leaks	Government and military, Transportation, Food and beverage
404NOTFOUNDCYBER	July 2025	DDoS, Defacement, Leaks	Government and military

Pro-Thai hacktivists:

Hacktivist Groups	First Discovered	Attack Techniques	Main Targeted Industries
RootSec	April 2025	DDoS, Defacement, Leaks	Government and military
Electronic Army Special Forces (Lực Lượng Đặc Biệt Quân Đội Điện Tử)	May 2025	DDoS, Defacement, Leaks	Government and military
BlackEye-Thai	July 2025	DDoS, Leaks	Government and military, Media and Entertainment, Financial services
Keymous	February 2025	DDoS, Leaks	Government and military, Financial services, Media and Entertainment
KH Nightmare	July 2025	DDoS, Defacement, Leaks	Government and military, Financial services
Anonymous SRVN	May 2025	DDoS, Defacement, Leaks	Education, Government and military
CyberSafe TH	June 2025	DDoS	Government and military, Financial services, Transportation
Thai is god	July 2025	DDoS, Defacement, Leaks	Government and military, Financial services

The hacktivist activity targeting Cambodian infrastructure was concentrated mostly on the **government and military** sectors, followed by **financial services** and **education**. In Thailand, **government and military** remained the primary focus, with sustained pressure on education and healthcare websites.

There is no evidence of the involvement of nation-state groups in the conflict between Cambodia and Thailand. Thai officials have alleged that Cambodia received assistance from North Korea-sponsored groups, while Cambodian authorities, in return, have accused pro-Thai groups like **BlackEye-Thai** of broad intrusion attempts against government networks. Still, the involvement of North Korean operators is not supported by verifiable technical indicators in public reporting.

Between 28 May and 7 August 2025, Group-IB detected **350 cyber attacks** linked to the Cambodia-Thailand conflict. Out of this amount, **262 attacks (75%)** targeted Thailand infrastructure, and **88 attacks (25%)** were aimed at Cambodian websites.

The hacktivist activity can be divided into three phases that are aligned with events on the ground:

1. **Border Tension** phase lasted from 28 May till 10 June. This phase accounted for **126 attacks (approximately 6.1 attacks per day)**. It was the first wave of hacktivist operations targeting public-facing infrastructure in both countries.
2. **Low Activity** phase is defined from 11 June to 23 July. The volume of attacks during this period was low - **85 attacks** overall or **2.9 attacks per day**. This phase serves as the baseline for measuring the spike.
3. **Conflict Spike** happened on 24 July when the conflict on the ground erupted. Despite the ceasefire, hacktivist operations remain ongoing as of 7 August. **139 attacks** were detected during these 2 weeks, at a rate of **9.9 attacks per day**.

Based on this evaluation, hacktivist activity originating from Cambodia and Thailand spiked sharply. The daily attack rate rose by **241%** from the low-activity plateau in June-July, and about **62% higher** than the activity during the Border Tension phase in May 2025, as illustrated in the chart below (Figure 1).

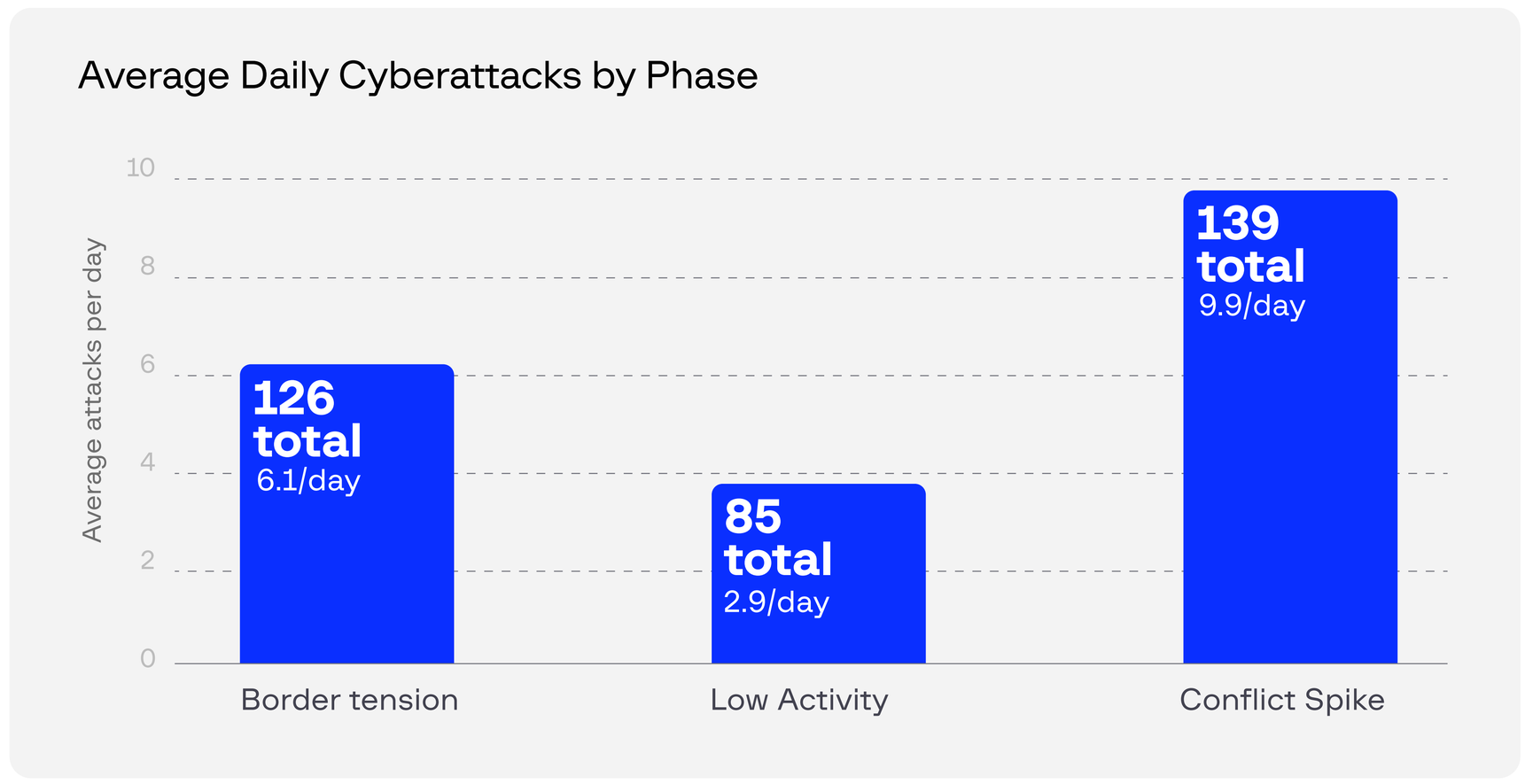


Figure 1. Average daily cyberattacks by phase in the conflict.

DDoS was the preferred technique used by the hacktivists from both sides of the conflict, contributing approximately **31%** (**109**) of all attacks observed throughout the conflict. Other attacks include defacements and data leakages caused by credentials abuse and website exploitation.

07 Notable incidents

In a significant escalation of the cyber hostilities, the hacktivist group **Keymous** claimed responsibility for breaching two critical Cambodian government systems — the Government Planning Portal and the National Vehicle License Plate System. The announcements, made in their Telegram channel, detail both the methods and the scale of the attacks.

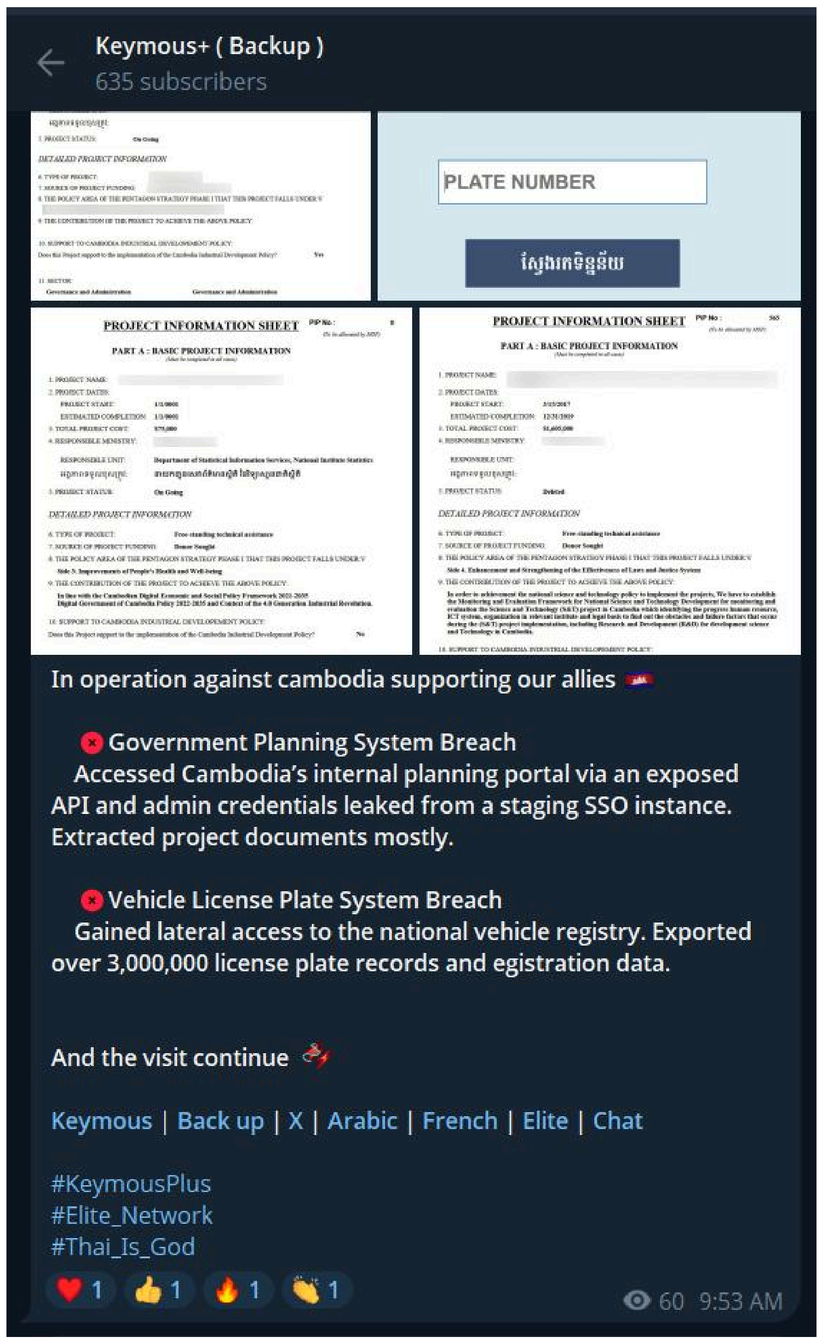
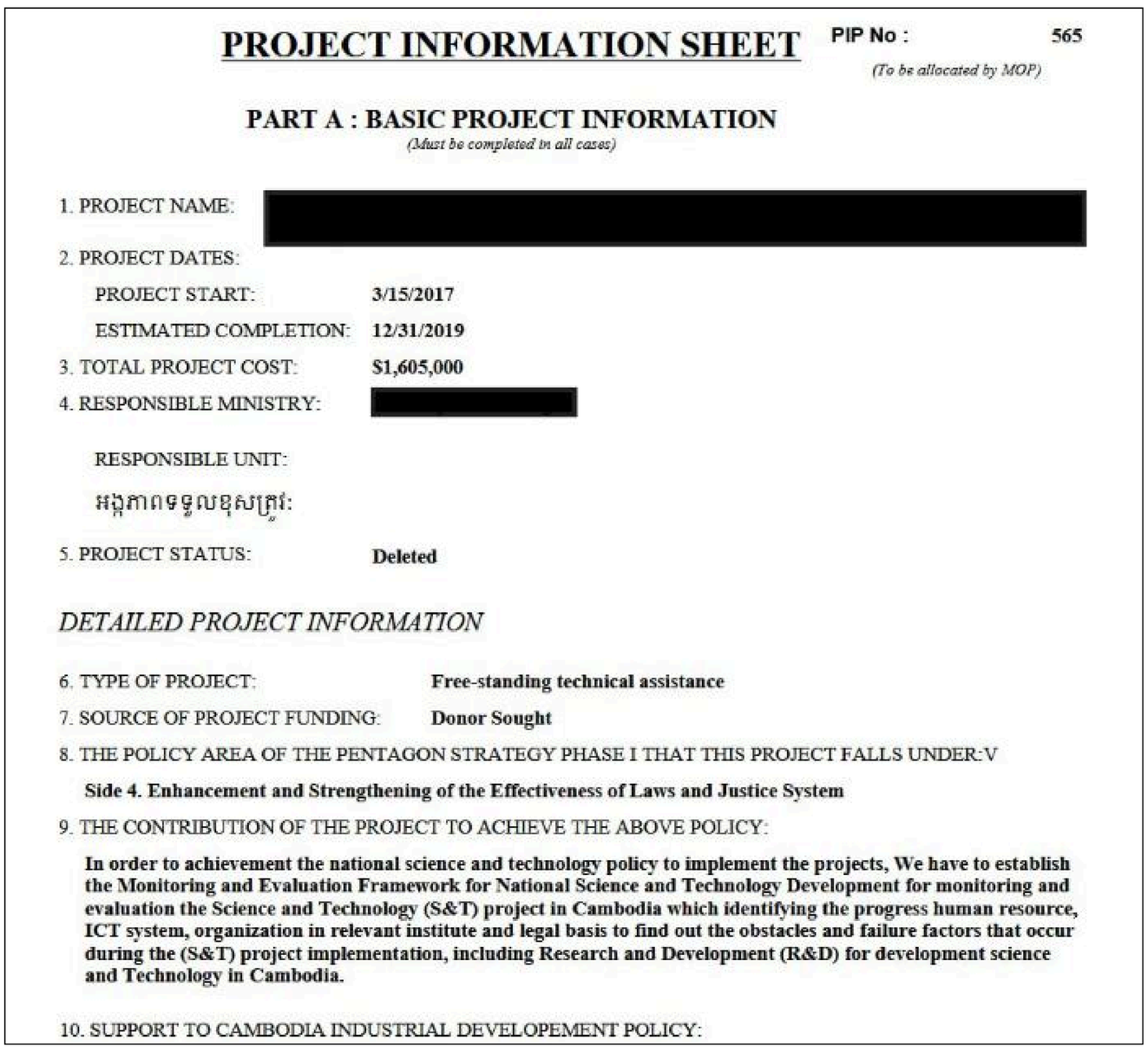


Figure 2. A post about the outcome of the attack published in a Telegram channel associated with Keymous.

According to Keymous, the first intrusion targeted Cambodia's internal government planning portal, accessed via an exposed API and admin credentials leaked from a staging Single Sign-On (SSO) instance. From there, Keymous reportedly extracted a cache of internal project documents.



PROJECT INFORMATION SHEET PIP No : 565

(To be allocated by MOP)

PART A : BASIC PROJECT INFORMATION

(Must be completed in all cases)

1. PROJECT NAME: [redacted]
2. PROJECT DATES:
   - PROJECT START: **3/15/2017**
   - ESTIMATED COMPLETION: **12/31/2019**
3. TOTAL PROJECT COST: **$1,605,000**
4. RESPONSIBLE MINISTRY: [redacted]
   - RESPONSIBLE UNIT:
   - អង្គភាពទទួលខុសត្រូវ:
5. PROJECT STATUS: **Deleted**

DETAILED PROJECT INFORMATION

6. TYPE OF PROJECT: **Free-standing technical assistance**
7. SOURCE OF PROJECT FUNDING: **Donor Sought**
8. THE POLICY AREA OF THE PENTAGON STRATEGY PHASE I THAT THIS PROJECT FALLS UNDER:V

   Side 4. Enhancement and Strengthening of the Effectiveness of Laws and Justice System
9. THE CONTRIBUTION OF THE PROJECT TO ACHIEVE THE ABOVE POLICY:

   In order to achievement the national science and technology policy to implement the projects, We have to establish the Monitoring and Evaluation Framework for National Science and Technology Development for monitoring and evaluation the Science and Technology (S&T) project in Cambodia which identifying the progress human resource, ICT system, organization in relevant institute and legal basis to find out the obstacles and failure factors that occur during the (S&T) project implementation, including Research and Development (R&D) for development science and Technology in Cambodia.
10. SUPPORT TO CAMBODIA INDUSTRIAL DEVELOPEMENT POLICY:

Figure 3. A screenshot sample of the alleged internal document from a planning portal of the Cambodian government that was published by Keymous via their Telegram channel.

In a separate operation, Keymous claimed to have gained lateral access to Cambodia's national vehicle registry, enabling them to export over 3 million license plate records and registration details. Screenshots shared in their Telegram channel, including a sample showing a 1993 Toyota Camry registered in Phnom Penh, were used to validate the breach.

Keymous, known for recent politically motivated DDoS and defacement cyberattacks, appears to be leveraging these breaches as part of a broader campaign aimed at undermining Cambodian institutions and public trust.

Figure 4. A screenshot of the vehicle registration details of a 1993 Toyota Camry registered in Phnom Penh, shared by Keymous via their Telegram channel.

DDoS attacks and website defacements are hacktivists' favorite methods. During such conflicts, it is common to encounter hundreds of messages claiming successful DDoS attempts and website disruptions. Such claims proliferate rapidly, but in most cases they are unverifiable. They are posted in unverified channels making it difficult to confirm whether attacks actually occurred, or were successful. While most hacktivist DDoS claims are unverifiable, this does not necessarily mean the attacks were unsuccessful. In one example,, a Thai news agency, The Nation, reported that a DDoS attack was initiated on their website, which registered 223-million hits within just 24 hours."

Beyond the sporadic DDoS attacks claimed to be carried out by both sides, there has been frequent use of credentials sourced from stealer log clouds and combolists that has been observed. If these publicly available credentials go unmonitored and the affected accounts lack extra layers of protection, they can lead to unauthorized access to user and even higher privilege accounts, potentially resulting in the theft or exposure of sensitive information.

In one such instance found by Group-IB, a new and previously undocumented pro-Cambodian hacktivist group known as **UnknowSEC** claimed to have obtained credit card information of customers of a financial institution in Thailand. The message appeared on their Telegram channel in early August.

Further analysis of the partially masked credit card numbers with visible BINs, and the visual appearance of the interface revealed that the screenshots originated from accounts within a card management application. The associated credentials were identified in publicly available infostealer logs and combolists, with some user device compromise timestamps dating back to 2021.

In a recent and different case, a pro-Cambodian hacktivist collective, **NNDSEC**, claimed to have gained access to a mailbox belonging to an employee of the Thai government.

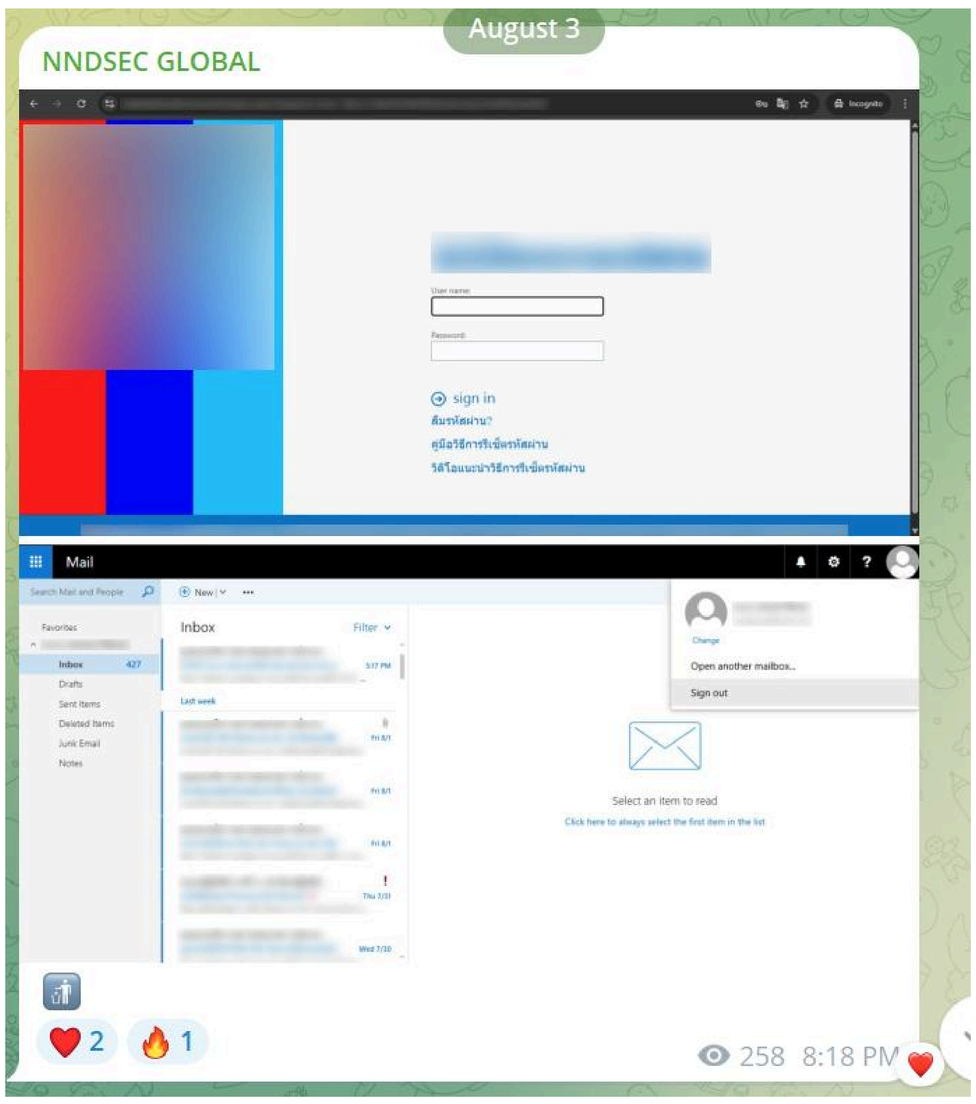


Figure 5. Screenshot of alleged mailbox access.

The credentials for this account, apparently lacking two-factor authentication (2FA), appeared in public stealer logs in October 2024. Another such example appeared in the channel of **NXBB SEC** in mid July 2025, where credentials sourced from combolists were used to gain access to a WordPress admin dashboard of a Thai travel platform. The credentials were first seen in combolists in April 2025.

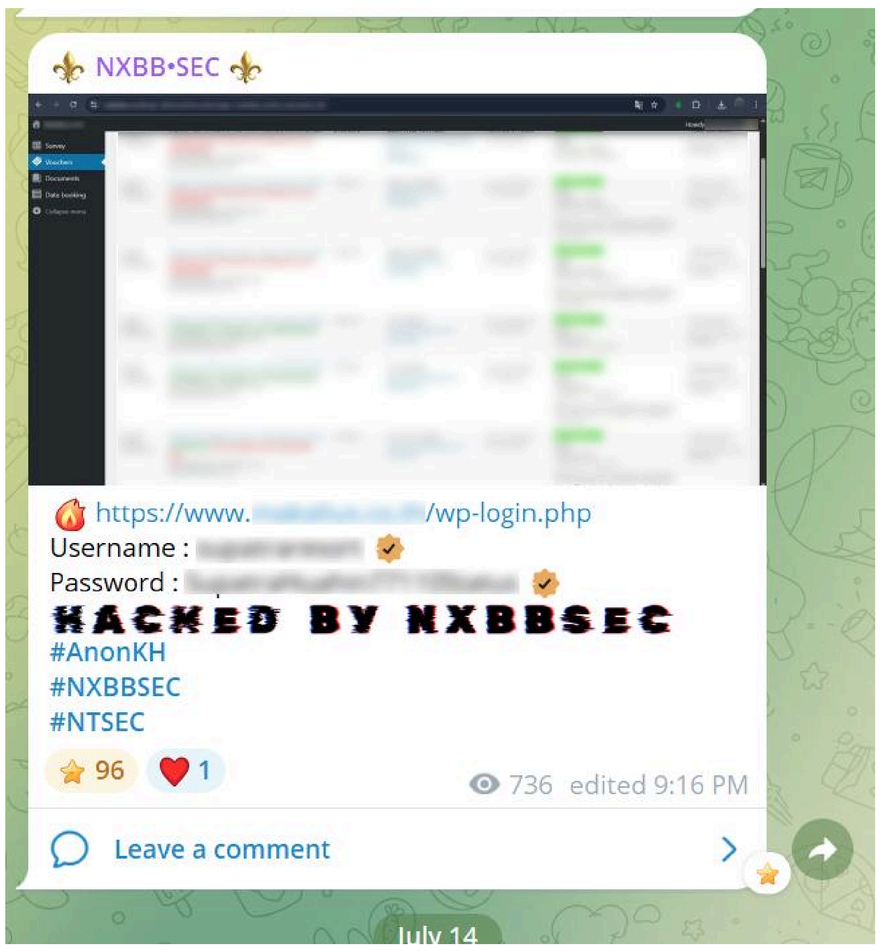


Figure 6. Screenshot of alleged access for a Wordpress dashboard.

However, even simple, publicly sourced credentials can potentially open pathways for more impactful incidents. For instance, on 3 August 2025, a pro-Cambodia hacktivist group, **Cyber KingdomKH**, claimed to have accessed a dashboard of a prominent Thai company involved in airport management.

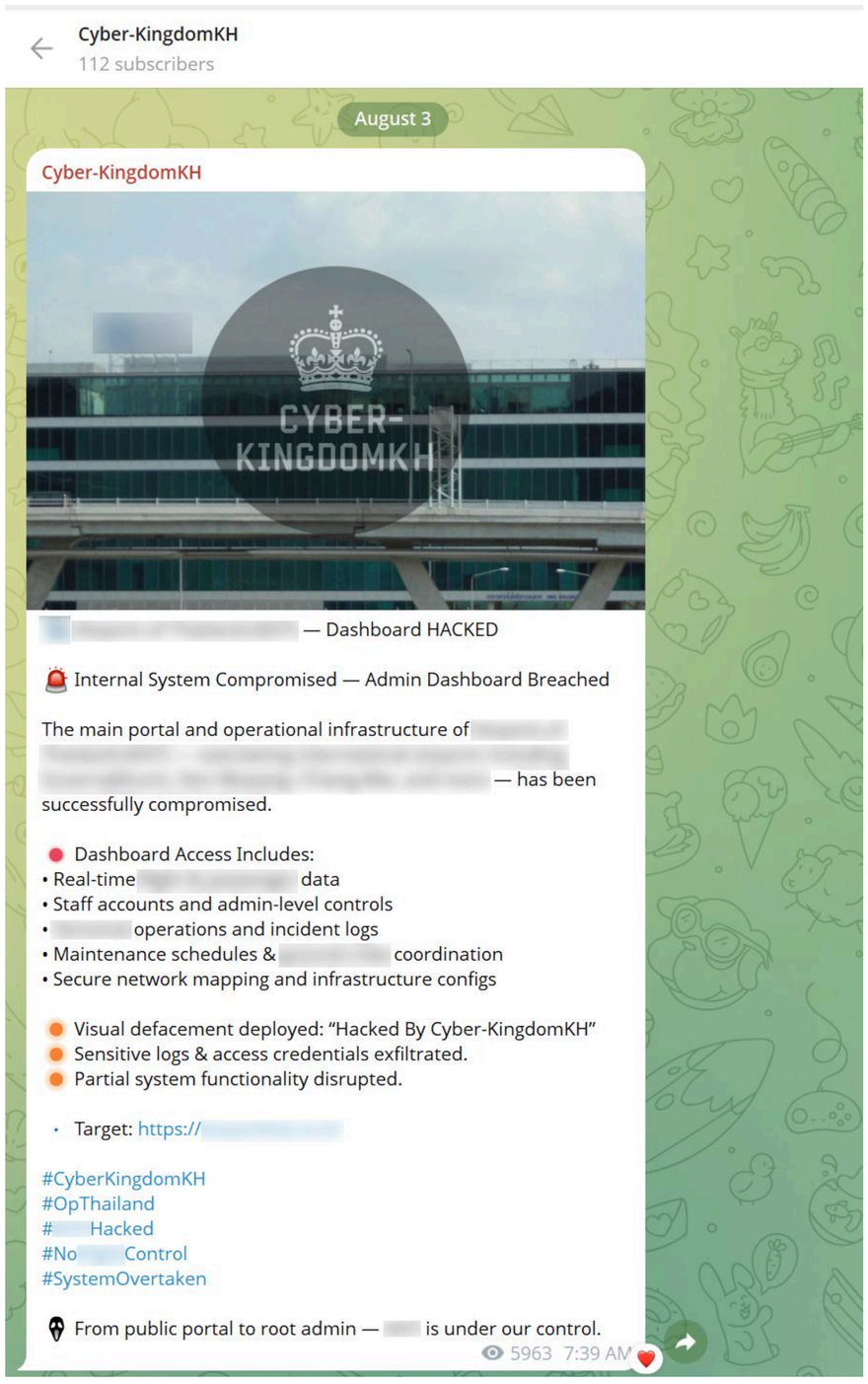


Figure 7. Cyber KingdomKH Claims

The screenshots and files posted in their Telegram channel suggested that the hacktivist could have obtained access to an admin console of the TIBCO Spotfire Server for the management and monitoring of at least two nodes (that are not directly public) visible on the screenshots. The references to Spotfire are seen in the file names, config files. The dump exposed the cluster’s configuration files, logs, network topology, routing details, and more.

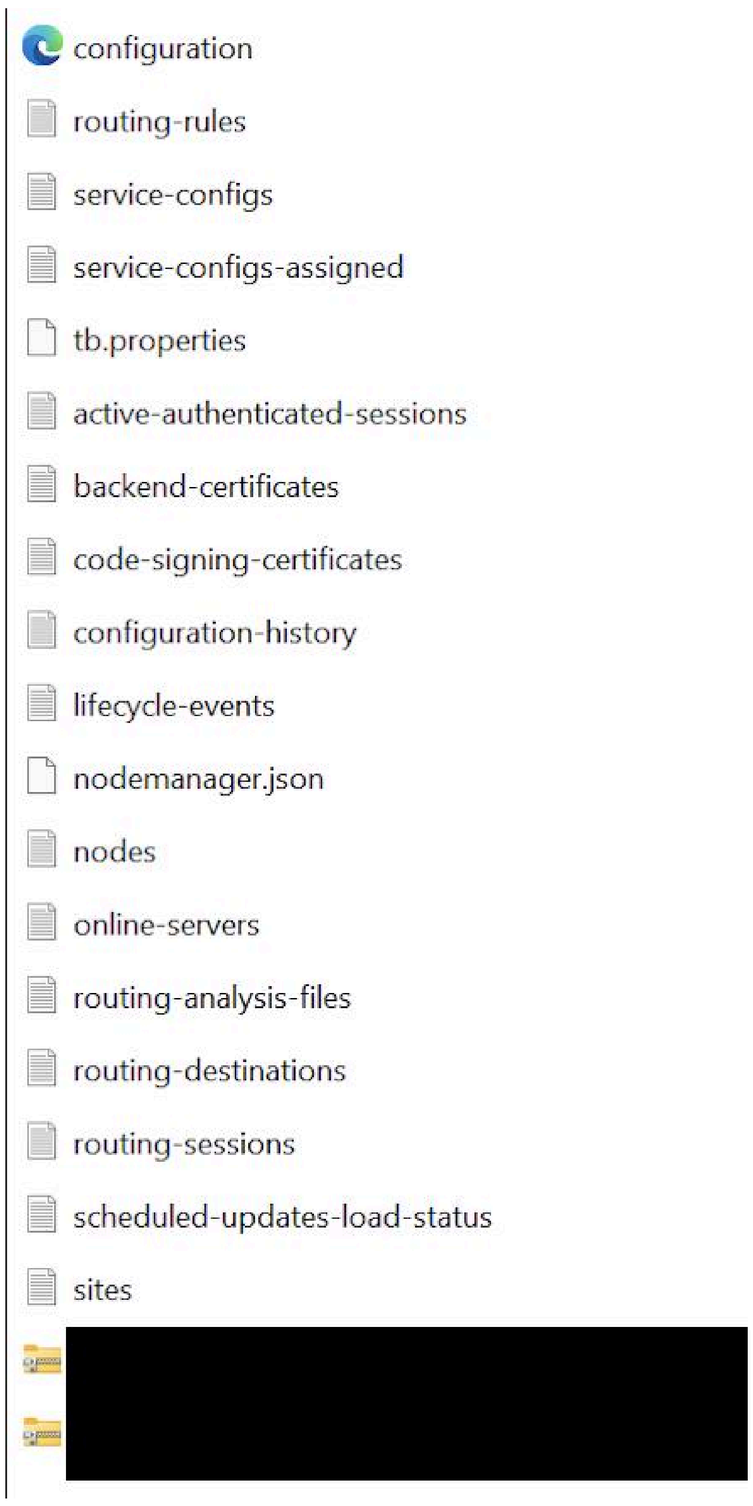


Figure 8. Content of management and monitoring console

Timestamps in the server log file suggests that the hacktivists completed the dump on 3 August, the same day as the post they published on their Telegram channel.

DEBUG 2025-08-03T09:40:06,234+0700 [scheduledupdates@SPOTFIRESYSTEM, #D-176000, #50395579] api.query.QueryManagerService: Entering getDataBlock with id REDACTED

The analysis of the configuration file found in the dump revealed internal hosts, and DC hostnames that are related to the alleged victim mentioned by the hacktivists on the screenshot. The format of the dump and content of the files indicate that the data is most likely not synthetic. The config file and logs mentions admin accounts, and the credentials with the same usernames were seen in public logs and combolists, which could potentially be the initial vector. There are also public references suggesting that the alleged victim had indeed used spotfire for infrastructure management. The potential impact of such alleged unauthorized access, if exploited further, can include the exposure of its user database (based on the screenshot its connected to MySQL server), potential encryption of two what appears to be production servers, and extortion, etc.

08 Exaggerated claims

Exaggerated claims by hacktivists are not uncommon during conflicts because these groups often seek influence and attention beyond their actual impact. By inflating the scale of an attack, they can intimidate the public and attract more subscribers and supporters of their cause, even if the real damage is limited or minimal.

On 26 June 2025, BL4CK CYB3R, one of the pro-Cambodian hacktivist collectives, claimed to have “hacked” a Thai government platform and posted an archive as a proof. The group also listed the same data for sale on a dark web forum. However, their claims were later found to be somewhat exaggerated.

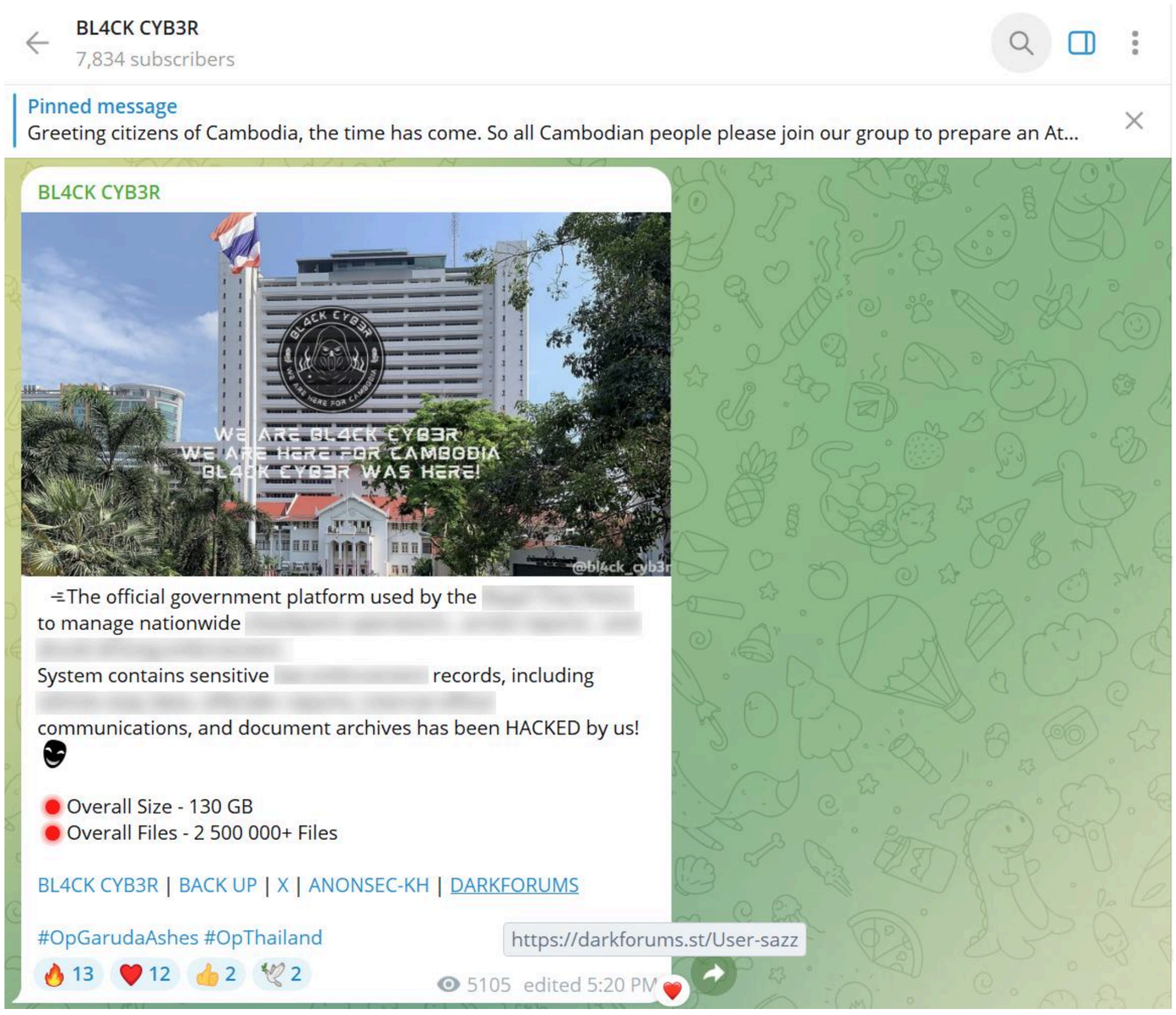


Figure 9. BL4CK CYB3R appropriated claim of the attack on Thai government website.

It was later revealed that the so-called “leak” was a word-for-word copy of a post on a dark web by another completely unrelated threat actor, named “Kazu”. “Kazu” was seen confronting the seller associated with BL4CK CYB3R on the forum thread, accusing them of scamming. Eventually, the ‘seller’ admitted attempting a scam.

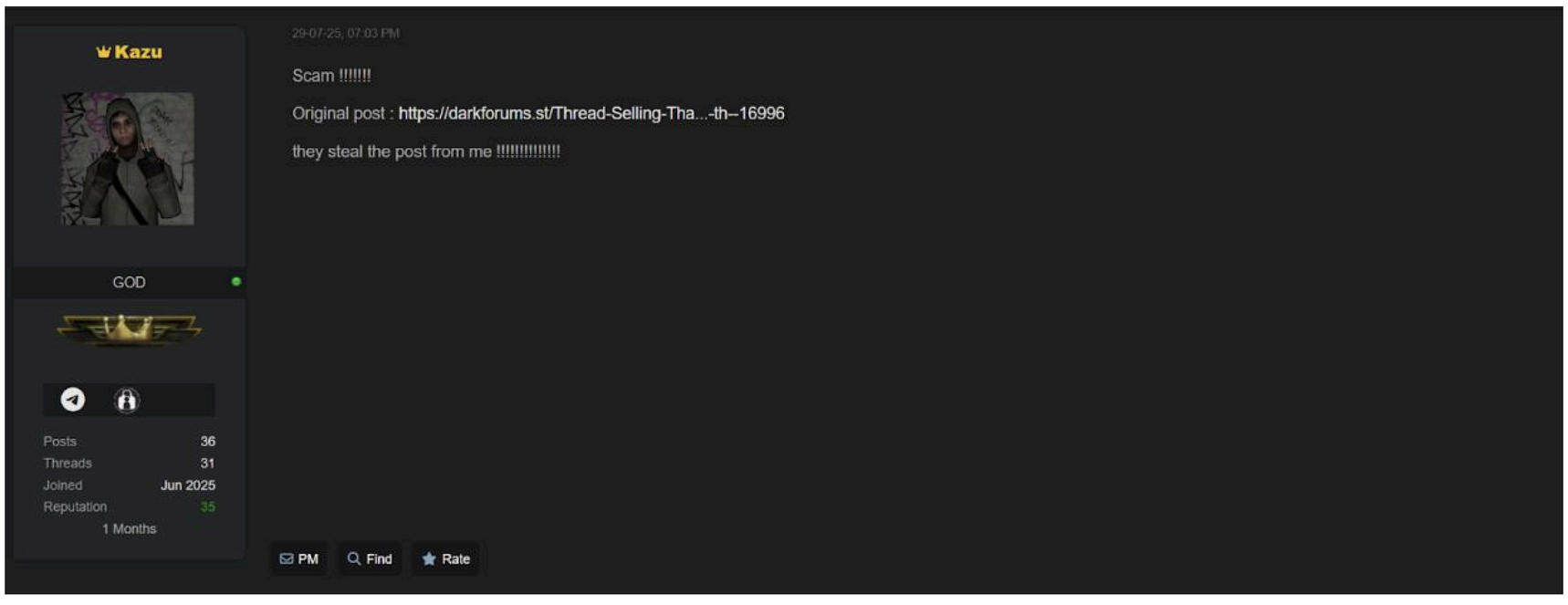


Figure 10. Resentment of the threat actor Kazu who claimed responsibility for the incident.

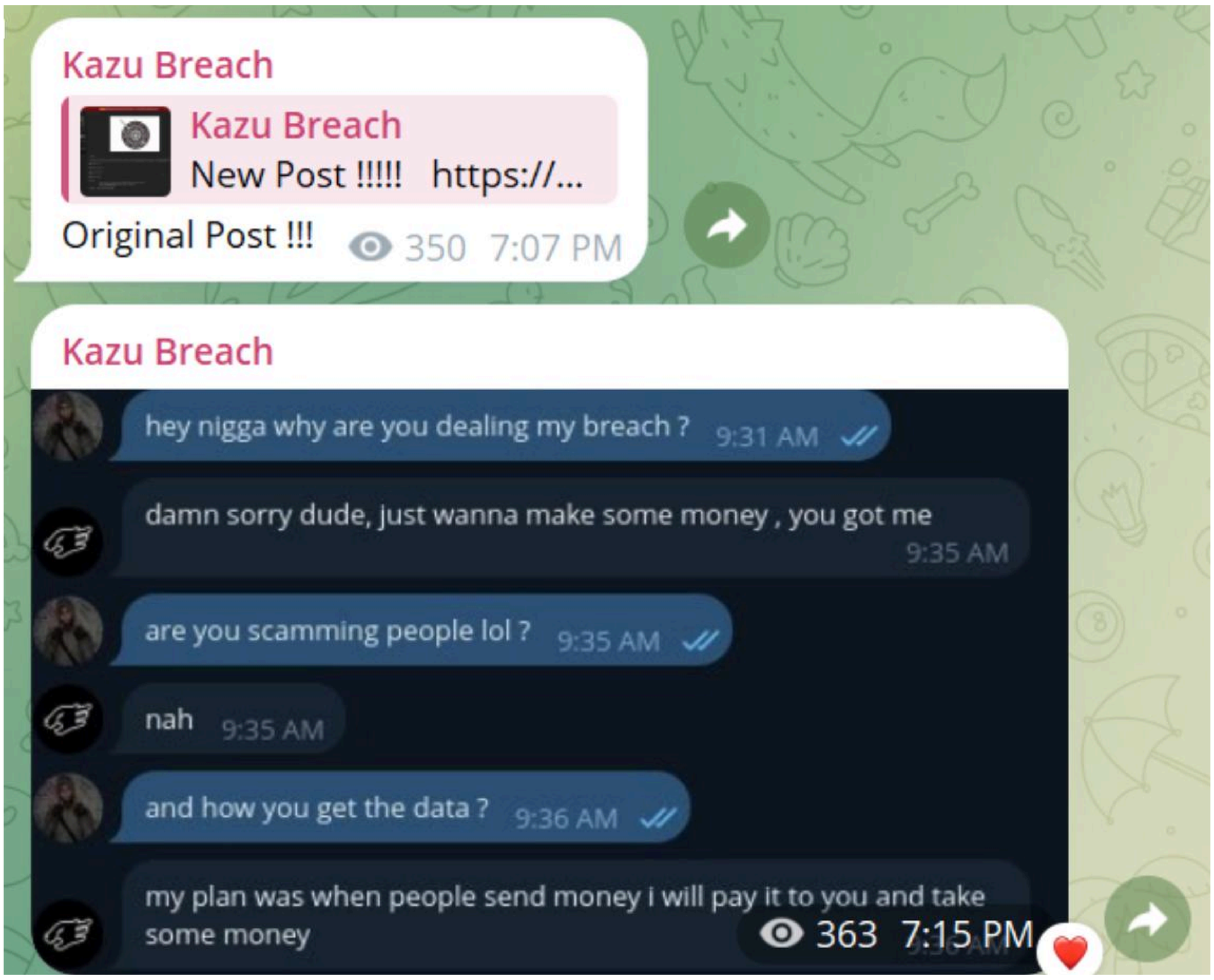


Figure 11. BL4CK CYB3R admitting the false claim in a private message with the actor associated with the attack.

As seen below, the profile picture of the “seller” matches that of the one used by BL4CK CYB3R, which is referenced in their posts on an underground forum.

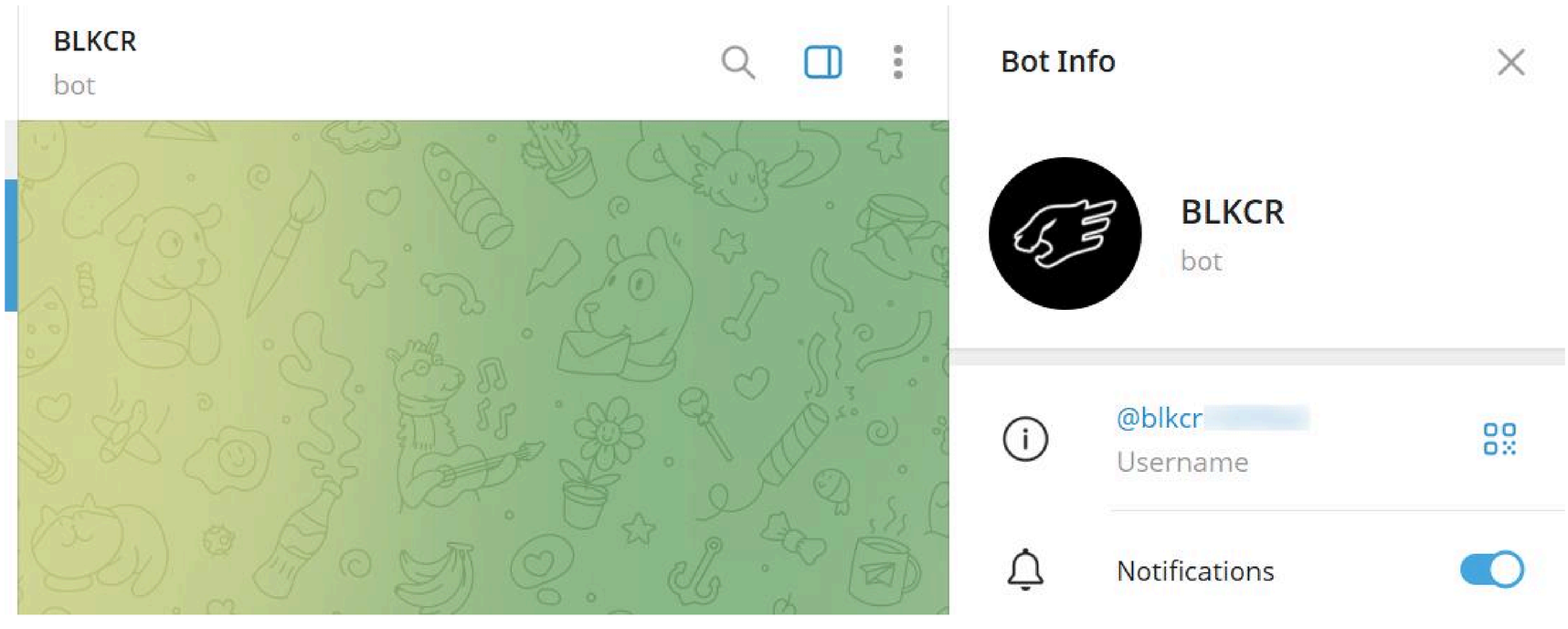


Figure 12. Telegram profile picture matches the avatar of BL4CK CYB3R.

In a different case, a pro-Cambodian hacktivist collective posted a link to a website that displays real-time CCTV feeds across Pattaya, which is intentionally made public allowing anyone to view current road conditions.

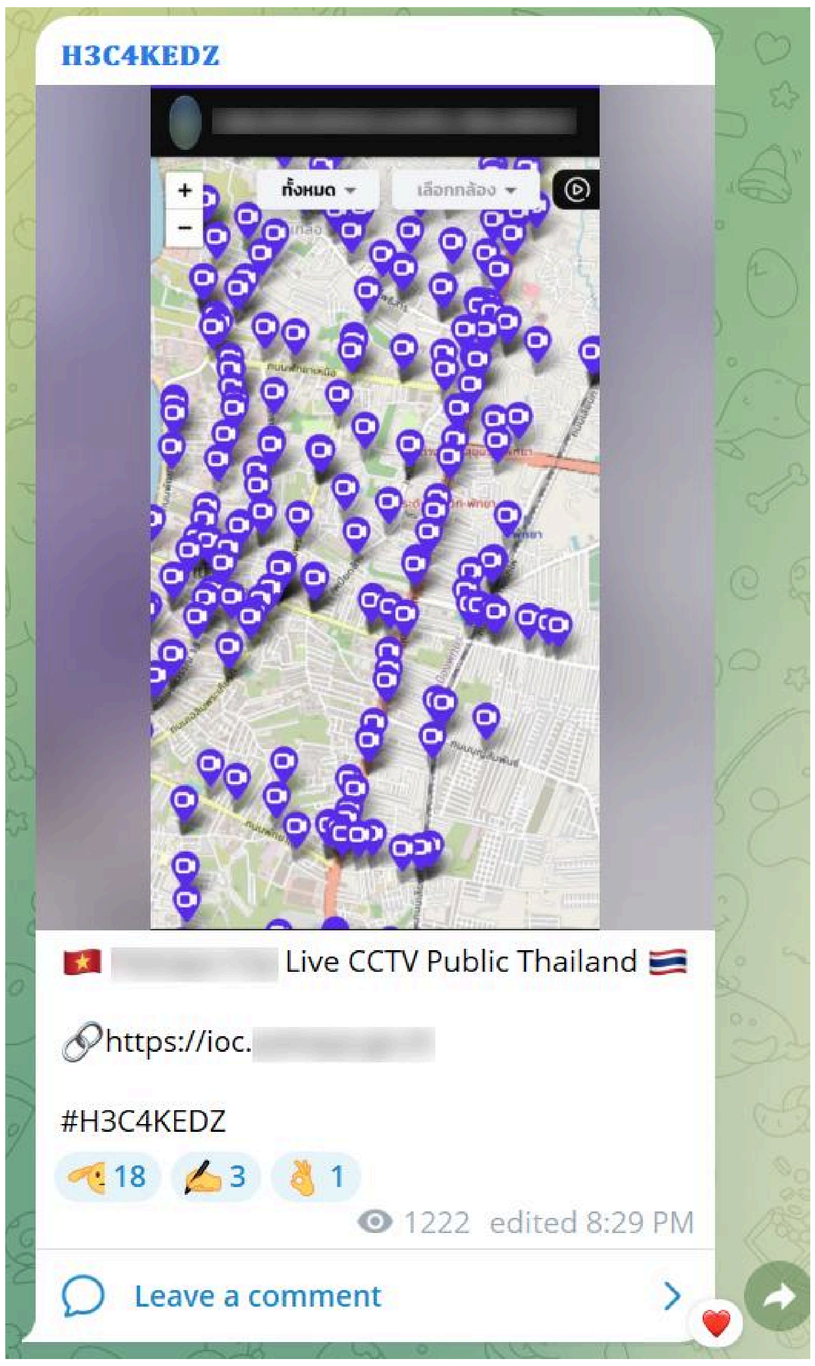


Figure 13. Claim of CCTV access in Pattaya, Thailand, which is a publicly accessible subdomain

As for the exaggerated claim from Thailand's side, **KH Nightmare** recently announced what they described as a massive breach of **71 Cambodian government organizations**. In their Telegram post, the group claimed that the "800GB leak" contained authentic emails from Cambodian officials, spanning from the early 2010s to the 2020s, along with internal documents, attachments, and communications from multiple ministries, and further asserting that this confirmed the data's legitimacy.

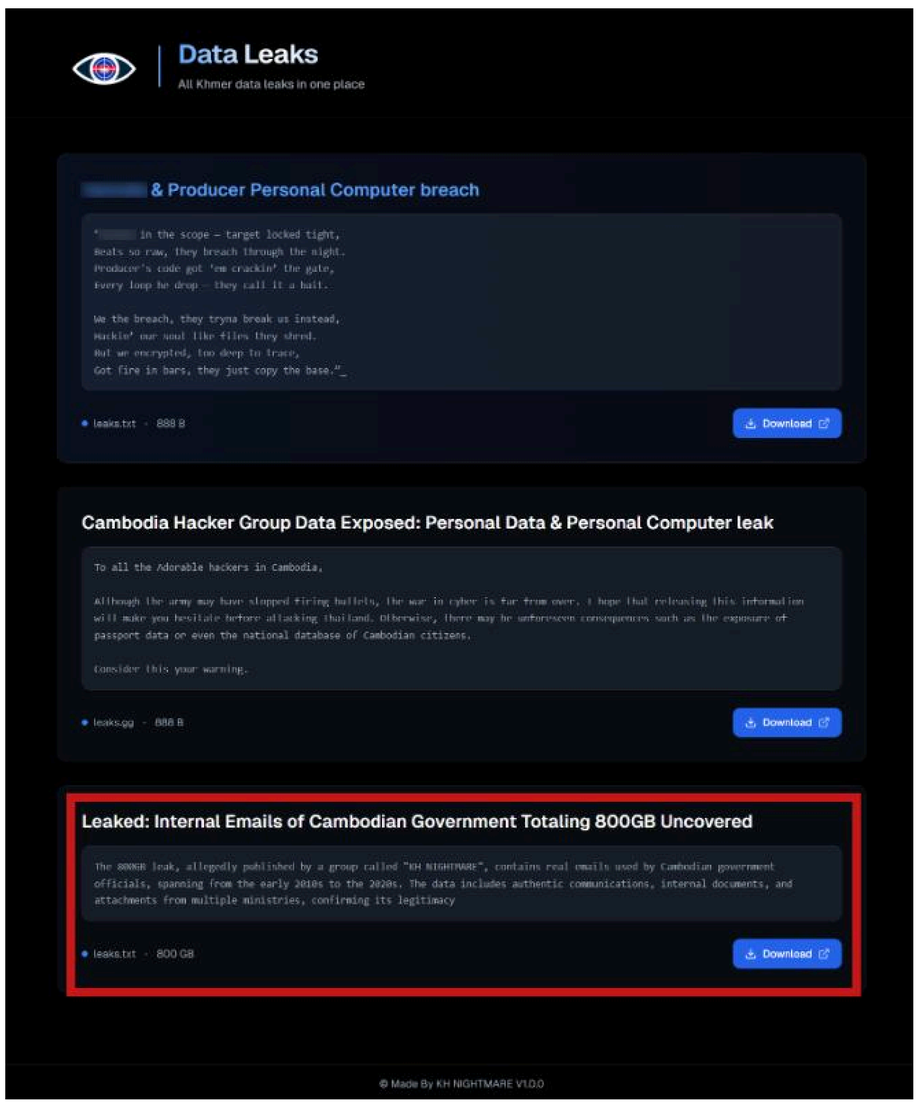


Figure 14. KH Nightmare's claim of 800 GB data breach of Cambodian government websites published on a data leak site (DLS).

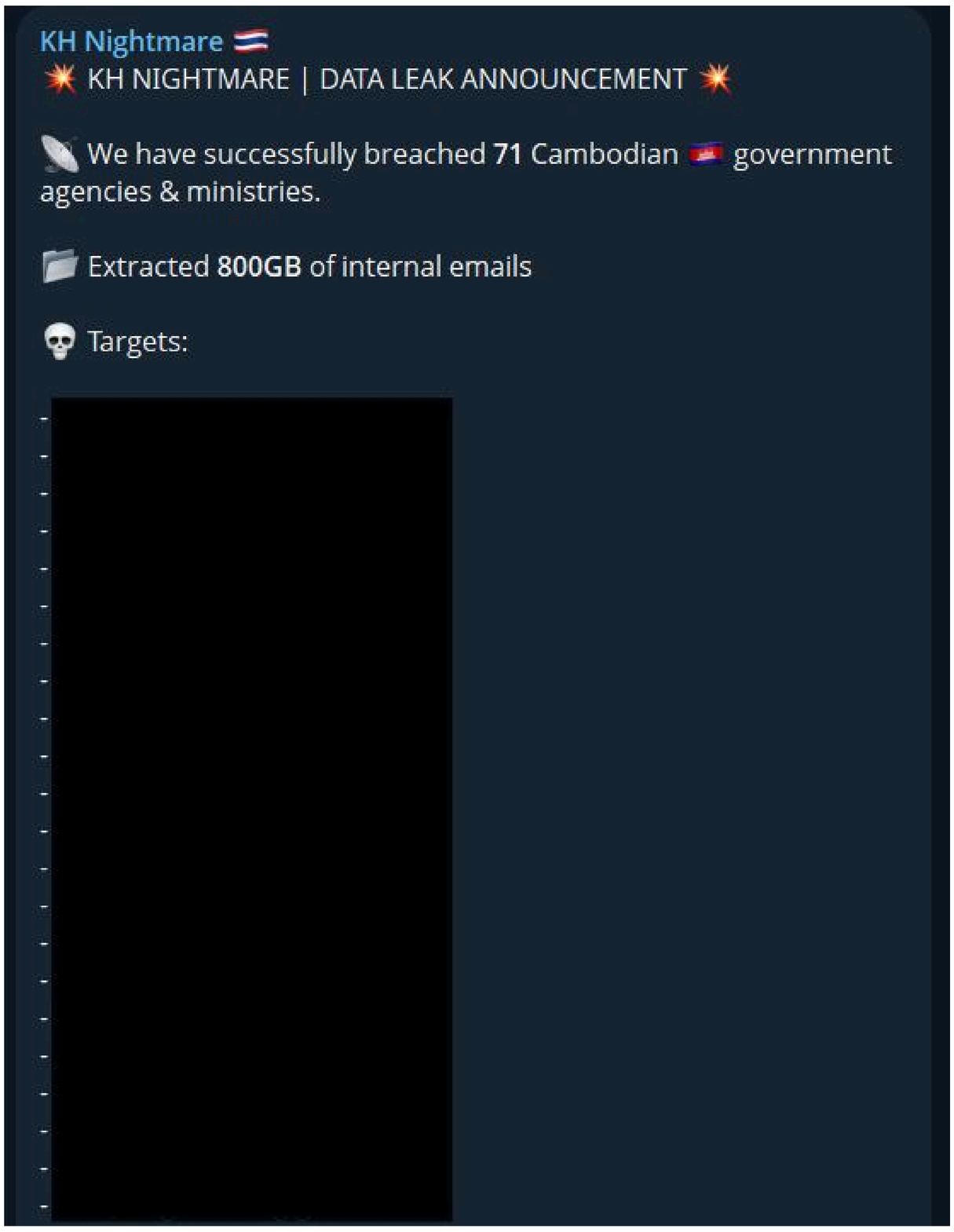


Figure 15. The same claim of the data breach of 71 Cambodian government websites published on Telegram.

However, closer inspection of the leaked files tell a different story. The so-called breach consists primarily of **ULP (URL–Login–Password) lists**, many of which appear to be credentials harvested from exposed systems or unrelated data dumps, rather than fresh exfiltration from live government networks.
While some of the credentials and email addresses may indeed belong to Cambodian government officials, the lack of direct evidence tying this dataset to recent, large-scale intrusions suggests that KH Nightmare's claims were **heavily exaggerated** for impact.

09 Conclusion

The Cambodia–Thailand cyber conflict highlights how political and military tensions can quickly extend into the digital space. Hacktivist groups have played a central role in this activity, conducting operations such as website defacements, DDoS attacks, and data leaks. As outlined in this report, some groups have also made bold, attention-seeking statements intended to amplify their visibility and escalate the conflict – an approach that is typical for hacktivists to amplify their reputation and increase their following.

These activities continue despite the formal ceasefire reached on 28 July 2025, indicating that cyber threats can persist regardless of geopolitical developments between nations. Most of the observed attacks have been opportunistic, often leveraging publicly available tools, compromised credentials circulating in the dark web, and other low-complexity attack methods. State-sponsored involvement at this stage remains unconfirmed.

To reduce exposure to ongoing and future activity, security teams in both countries should implement DDoS mitigation strategies, strengthen web application security, and monitor for leaked credentials in public data sources.

10 Recommendations

In order to address threats caused by the escalation between Cambodia and Thailand, Group-IB advises implementing the following measures:

1. DDoS Attacks

- Use Group-IB's Threat Intelligence to stay updated on hacktivist groups' tactics, techniques and procedures (TTPs), upcoming campaign attacks and IP infrastructure.
- Our tailored threat intelligence provides organizations with context-specific threat landscape and relevant risks, customized reporting, and early warnings—moving beyond generic alerts to improve response time and mitigation efficiency.
- Many threat actors employ automated DDoS tools to execute their attacks. These tools often utilize predefined lists of proxy addresses. These lists are collected, regularly updated, and provided by Threat Intelligence systems. Additionally, some attackers conceal their real IP addresses using standard methods like VPNs, proxies, or TOR. Group-IB's Threat Intelligence also collects this information and can enhance lists of suspicious IP addresses to facilitate the process of blocking incoming malicious traffic.
- Enable anti-DDoS protection and ensure it's active. Diversify providers: use multiple ISPs or cloud providers to ensure redundancy. If one is attacked, you can fall back on others.
- Upstream filtering: Work with ISPs that offer malicious traffic filtering to block malicious traffic before it reaches your network.
- Scale resources: Auto-scale resources to absorb traffic spikes, especially using cloud services that provide auto-scaling.

10

- Rate limiting: Cap the number of requests a user can send in a certain time frame.
- Bot protection: If you are facing an L7 DDoS attack on web apps and the current provider has issues, ensure your organization has bot protection in place.
- Geofencing: Block non-region-related IP access for critical applications in the active face of an attack.
- Use blacklisting and whitelisting.
- Save logs during DDoS attacks: Technical information about the attack can significantly improve your detection and prevention capabilities after an in-depth analysis. Furthermore, it offers valuable insights for further investigation.

2. Defacements

- Regular Backups: Store backups both on-site and off-site to ensure you can quickly restore your website after a defacement.
- Update CMS: Make sure that your Content Management System (CMS) is not accessible from the internet and is regularly updated to the latest version. Update all plugins, themes, and extensions. Outdated plugins can be a common vector for attacks.
- Regularly update web-server backend software to prevent exploitation with common CVEs.
- Web Application Firewall (WAF): Configure a WAF to inspect incoming traffic, block malicious requests and attempts to exploit vulnerabilities.
- Start searching for your publicly facing shadow IT assets to uncover potential vulnerabilities that can be exploited by threat actors. We recommend solutions such as Attack Surface Management.
- Limit shadow IT: Limit your exposure by disabling unnecessary services that are not in use and do not use default URLs for login or admin panels.
- Restrict CMS access: The emergence of underground markets has simplified the attack process for potential intruders, including hacktivists. These illegal marketplaces provide pre-compromised CMS access or web shells, removing the need for attackers to breach these systems themselves. Use Threat Intelligence platforms to obtain information about any unauthorized access that may be up for sale. It can preempt potential threat activities, neutralizing risks before other malicious actors purchase and exploit this access.
- Implement geofencing during the active phase of an attack.

3. Data leaks

- Use Group-IB Threat Intelligence to monitor for compromised corporate credentials of your employees. Make sure your employees' passwords are regularly updated and that they do not reuse old passwords.
- Strengthen your password policy. Make sure your employees' passwords are regularly updated and that they do not reuse old or same passwords. Companies should not only establish strong password policies but also regularly update them to stay ahead of evolving threats and security best practices. Employee training and enforcement of these policies are equally important to ensure compliance and data security

GROUP-IB

Group-IB is a creator of cybersecurity technologies to investigate, prevent and fight digital crime.

1,550+
Successful investigations of high-tech crime cases

500+
Employees

60
Countries

$1 bln+
Saved by our client companies through our technologies

#1*
Incident Response Retainer vendor

*According to Cybersecurity Excellence Awards

11
Unique Digital Crime Resistance Centers

Global partnerships

INTERPOL

EUROPOL

AFRIPOL

Recognized by top industry experts

FORRESTER®

Aité Novarica

kuppingercole ANALYSTS

Gartner®

IDC

FROST & SULLIVAN

Fight against cybercrime

GROUP-IB.COM