Published on July 16, 2025.

DKZ
TEAM D4RKN3TTZ

TEAM1722

A Kurdish Hacktivist Group of the Rise and Fall

Table of Contents

Reported by Team D4rkn3ttz

Published on July 16, 2025.

DKZ
TEAM D4RKN3TTZ

1. Executive Summary

- The hacktivist group Team 1722 was first identified in the second half of 2023 and is believed to be based among the Kurdish population in Iraq.
- In mid-2024, the group appeared to collaborate with other Kurdish hacktivist entities under the BCID (Kurdish Hacker Coalition), including Cyber Rebel Team, Cyb3r Drag0nz, and Byte Blitz.
- Although the group claimed a full personnel change at the end of 2024, evidence suggests that original members—particularly DeadCoder1722—continued their activities, casting doubt on the claim.
- Team 1722 publicly supports a pro-Palestinian stance, but its attack motives and messaging often lack consistency and show signs of performative or self-promotional behavior.
- On June 15, 2024, shortly after escalations in the Iran–Israel conflict, the group announced a suspension of operations and deleted most of its Telegram channels and messages.
- Their attacks were primarily focused on Middle Eastern and Asian targets, including Turkey, Iran, Israel, and India.
- Attacks against South Korea were concentrated during May and June 2024, involving website defacements and minor data leaks.
- Team 1722 primarily employed SQL injection and DDoS (Distributed Denial-of-Service) techniques, and their overall technical proficiency is assessed to be relatively low.

2. History of Team 1722

Figure 2.0.1. This is the official image used by Team 1722 in its Telegram channel profile. The same image has been observed in website defacement incidents attributed to the group.

Figure 2.0.2. In November 2024, Team 1722 declared a change in membership, stating that the internal structure included at least four members. (Source: Hacker News)

Figure 2.0.3. In late May 2024, coordinated activity among the four affiliated groups was observed and reported by the Telegram channel Hacker News.

a. Rise of Team 1722

Team 1722 is a Kurdish hacktivist group with anti-Iran, anti-Israel, and pro-Palestinian ideological leanings, whose members are believed to be primarily Kurdish residents in Iraq. The group has launched cyber attacks in response to geopolitical conflicts and wars, initially focusing on Middle Eastern targets excluding South Korea.

The group was first identified in late 2023, and by mid-2024, it was observed operating under the BCID (Kurdish Hacker Coalition) alongside Cyber Rebel Team, Cyb3r Drag0nz, and Byte Blitz. Team 1722 has openly identified itself as an Iraq-based Kurdish organization.

In late 2024, the group claimed that all previous members had left and that the team had been completely restructured with new personnel. However, this statement is questionable, as DeadCoder1722, widely recognized as the group's leader, was found to remain active even after the claimed restructuring. While the team initially operated with only 3–4 members following the shift, evidence suggests it later expanded to a size of 40 to 80 individuals.

Team 1722's operations have gone beyond purely political or religiously motivated cyberattacks, at times portraying themselves as cyber vigilantes. For example, the group claimed to have assisted a female victim of online exploitation by helping delete leaked private content resulting from a scam. However, no concrete evidence has been presented to verify this claim. Furthermore, during a recent internal conflict, a central figure alleged that the group had in fact deceived or manipulated women, casting further doubt on the authenticity of their previous assertions.

b. Fall of Team 1722

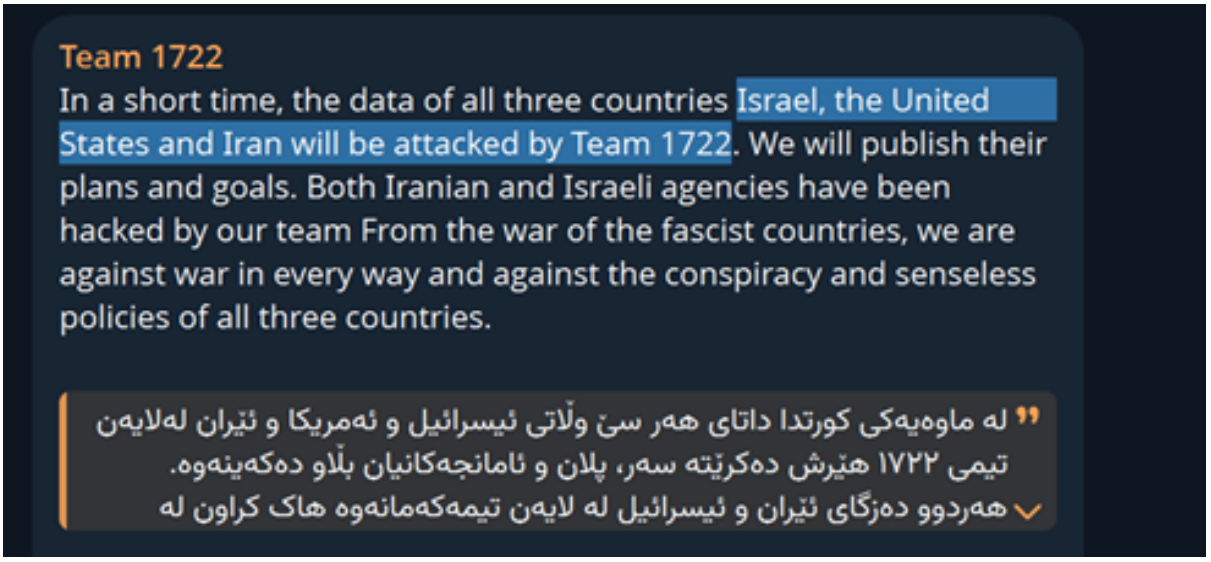

Figure 2.1.1. This image shows Team 1722 publicly declaring its intent to launch cyberattacks against Israel, the United States, and Iran following the escalation of the Iran–Israel conflict.

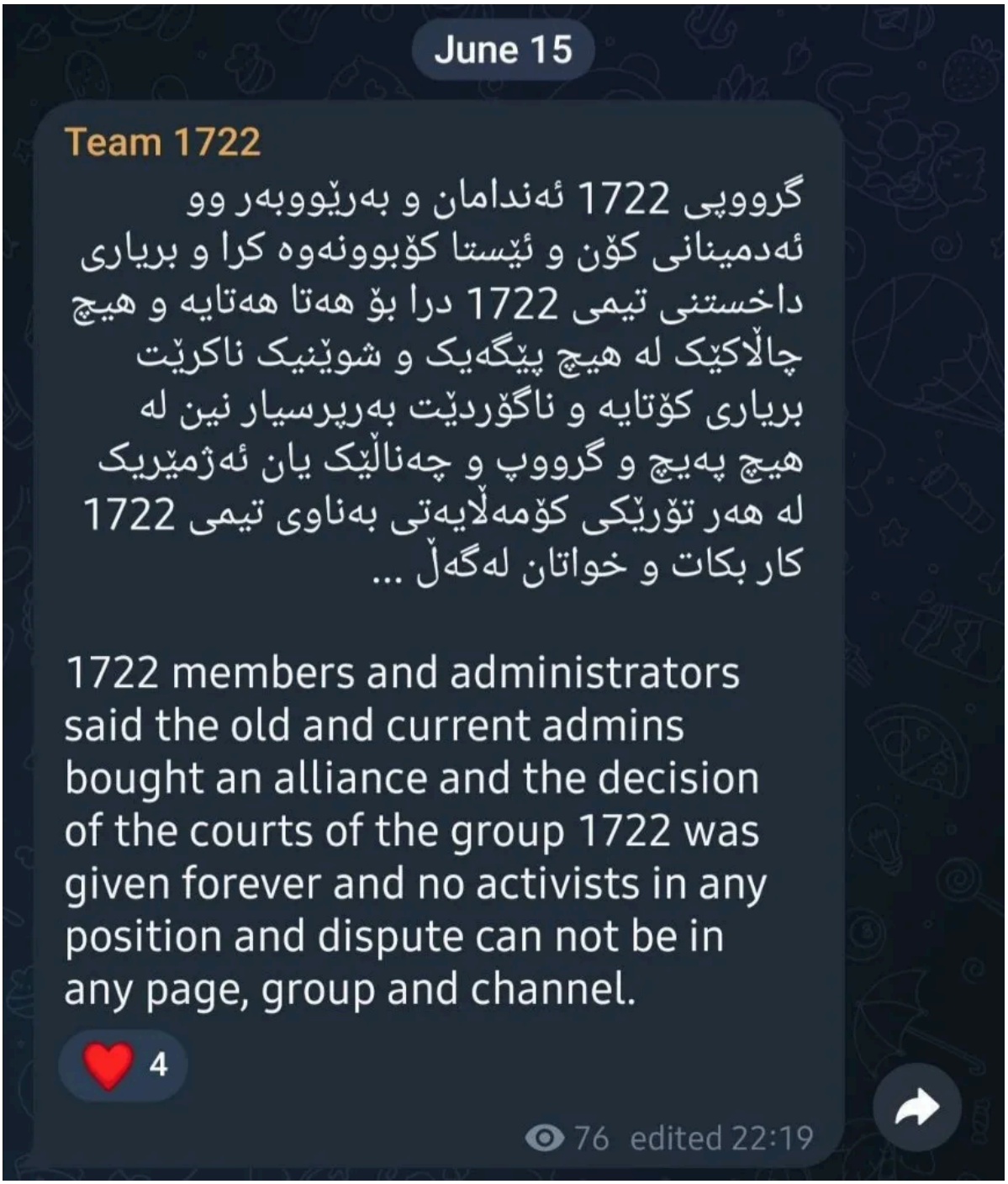

Figure 2.1.2. ***After engaging in anti-Iran operations during the heightened tensions between Iran and Israel, Team 1722 announced the suspension of its activities on June 15, shortly after the conflict intensified.***

Published on July 16, 2025.

In June 2025, as the armed conflict between Iran and Israel escalated into missile exchanges, Team 1722 responded by publicly declaring a wave of cyber operations with an anti-Iran stance. However, just a few days later, on June 12, the group announced a complete suspension of activities following internal discussions. Most of the group's primary Telegram channels were deleted, and nearly all message history was wiped out, except for two minor backup channels.

Subsequently, a new Telegram channel bearing the same name was created. The individual managing this channel began posting insider disclosures, accusing Team 1722 of engaging in unethical behavior. He claimed that the group's so-called cyber vigilante operations were in fact a front for financial extortion. However, control of the channel was soon taken over by another former member, who in turn accused the whistleblower of engaging in similar misconduct. This led to a mutual conflict, with both parties publicly discrediting each other.

Reported by Team D4rkn3ttz

3. Attack Timeline by Team 1722

a. Motivation

Figure 3.1.1. *Team 1722 released a video declaring cyber war against South Korea.*

Figure 3.1.2. *Message delivered through a website defacement attack by the group, "While Palestinian children are without bread and water, are you busy with corruption money?"*

Published on July 16, 2025.

When Team 1722 first launched cyberattacks against South Korea, the group claimed it sought to prove that "no system is perfect." This message may have referred to computer systems, societal systems, or both.

However, in a later website defacement message, the group accused South Korea of generating profit through unethical means and included political statements in support of Palestine.

Subsequently, the group released a cyber declaration of war video targeting South Korea, in which it issued three specific demands.

- First, stop exporting low-quality products.
- Second, do not modify products' authentication codes.
- Third, unconditionally support Palestine.

While these demands and messages clearly demonstrate the group's pro-Palestinian stance, the overall motives and logic behind their attacks lack consistency. Initially framed as a critique of technical or societal vulnerabilities, the group's narrative later shifted to political messaging, vague accusations, and commercial criticisms, suggesting that its operations were largely performative in nature.

Reported by Team D4rkn3ttz

b. Timeline

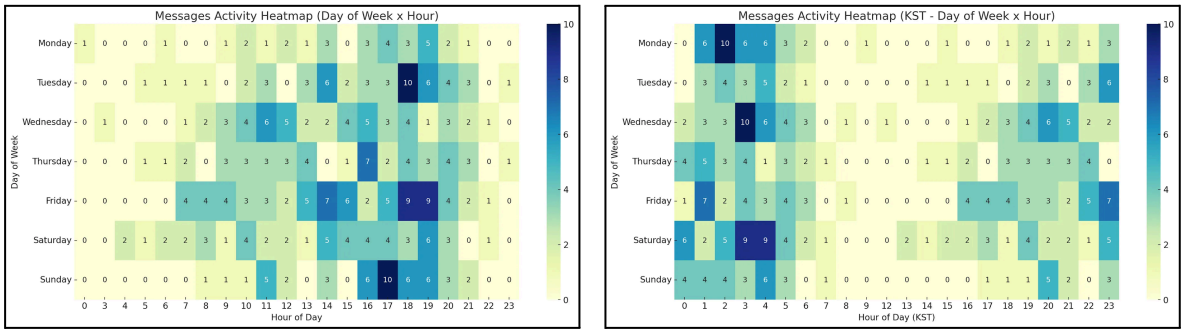

Figure 3.2.1. The chart on the left shows the distribution of Team 1722's activity by Coordinated Universal Time (UTC), while the chart on the right reflects the same distribution adjusted to Korea Standard Time (KST).

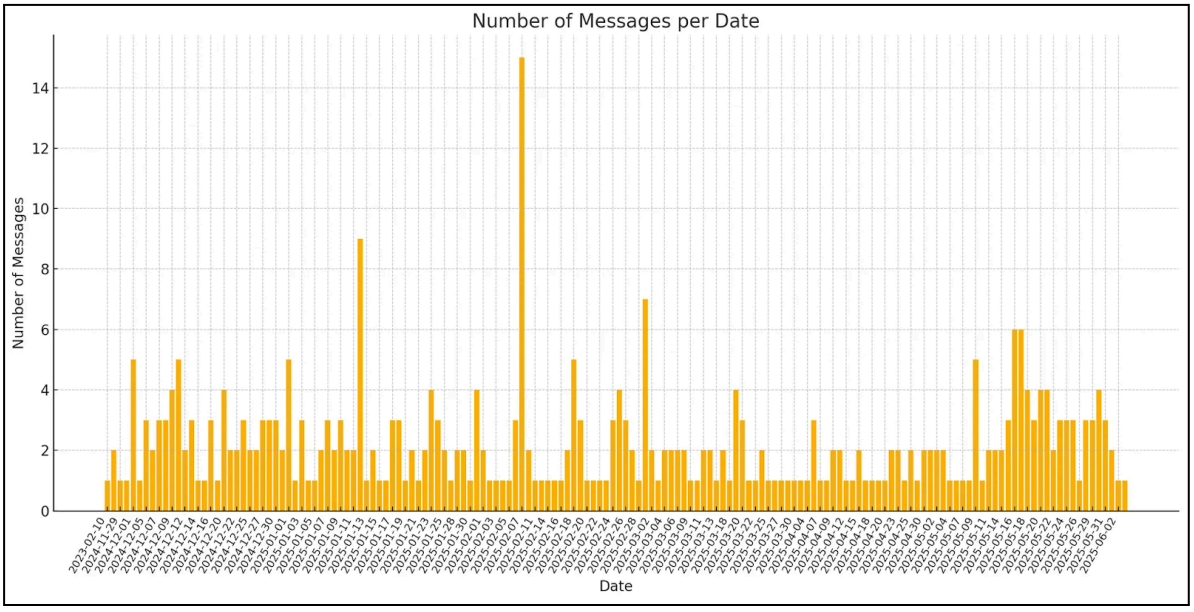

Figure 3.2.2. Team 1722 has been tracked since 2023, and a sudden spike in message volume was observed around February 2025.

However, this was not due to a specific event, but rather the bulk upload of messages related to their self-proclaimed cyber vigilante operations. The graph demonstrates that the group has been active continuously since its emergence, carrying out attacks at a relatively consistent pace.

Most messages posted on Team 1722's Telegram channel include claims of responsibility or details related to their cyber operations. An analysis of the posting timestamps reveals that, in Korea Standard Time (KST), the

group is most active during late-night to early-morning hours—typically between midnight and early morning.

When converted to Coordinated Universal Time (UTC), this corresponds to activity between 14:00 and 19:00, and in Iraq local time (GMT+3), between 17:00 and 22:00. This distribution strongly suggests that Team 1722 is operated by individuals physically residing in Iraq, and that their cyber activities primarily occur during evening hours.

Such a pattern is consistent with that of part-time hacktivist groups, who tend to carry out operations after work hours, using their personal time in the evening and night to engage in cyber activities.

c. Targeted victims

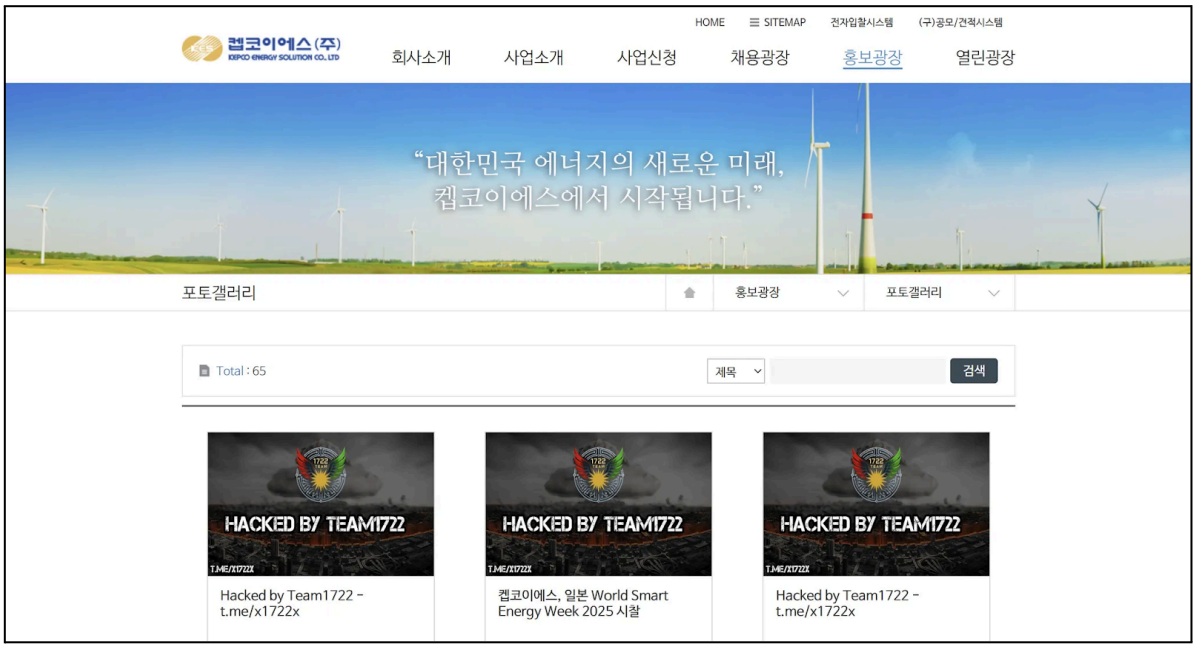

Figure 3.3.1. The group primarily engages in website defacement attacks. A confirmed case involved the defacement of the official website of KEPCO ES (Korea Electric Power Corporation Energy Solution).

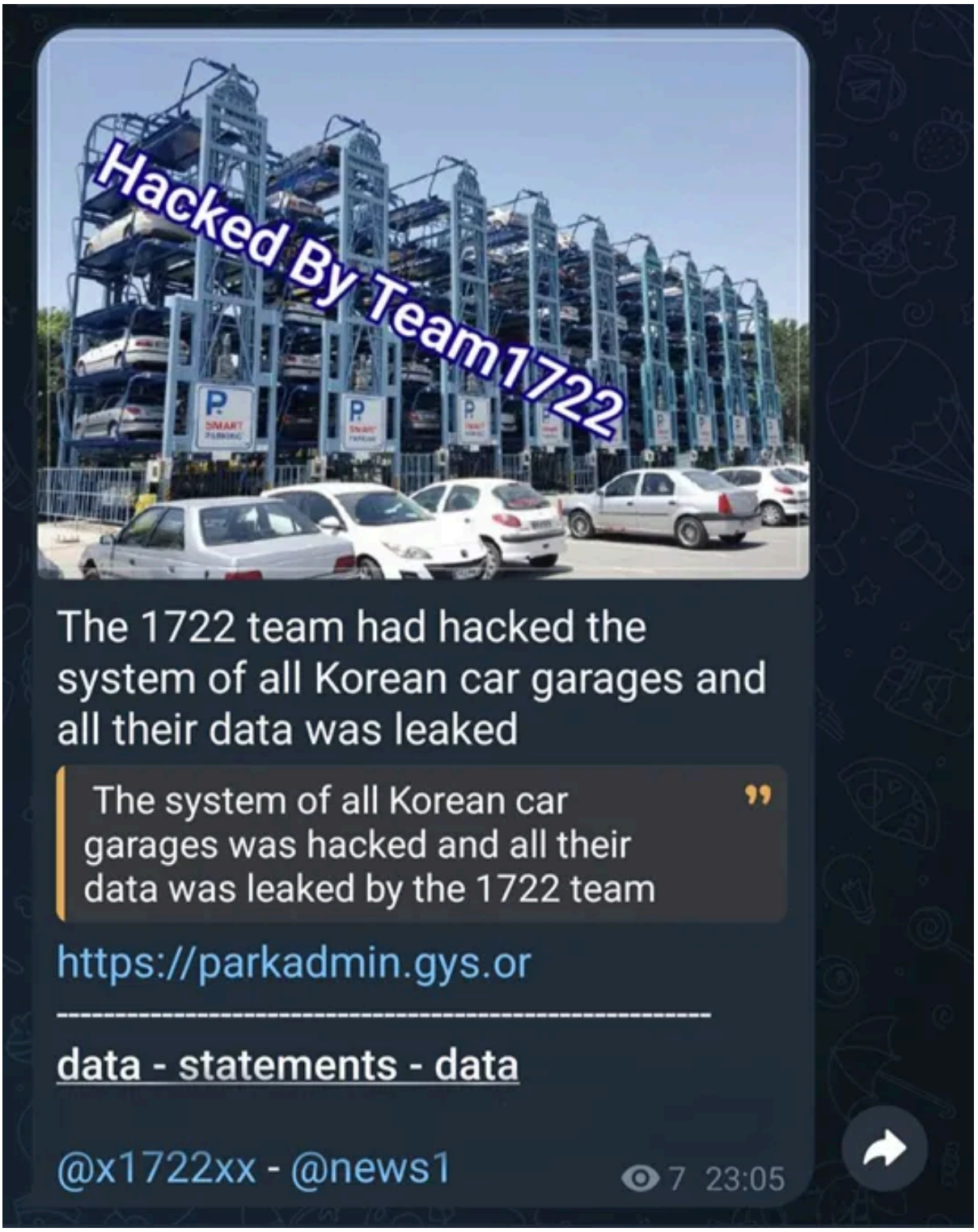

Figure 3.3.2. *The parking management system of Goyang Management Corporation in South Korea was compromised, resulting in the leak of certain user information and vehicle access records.*

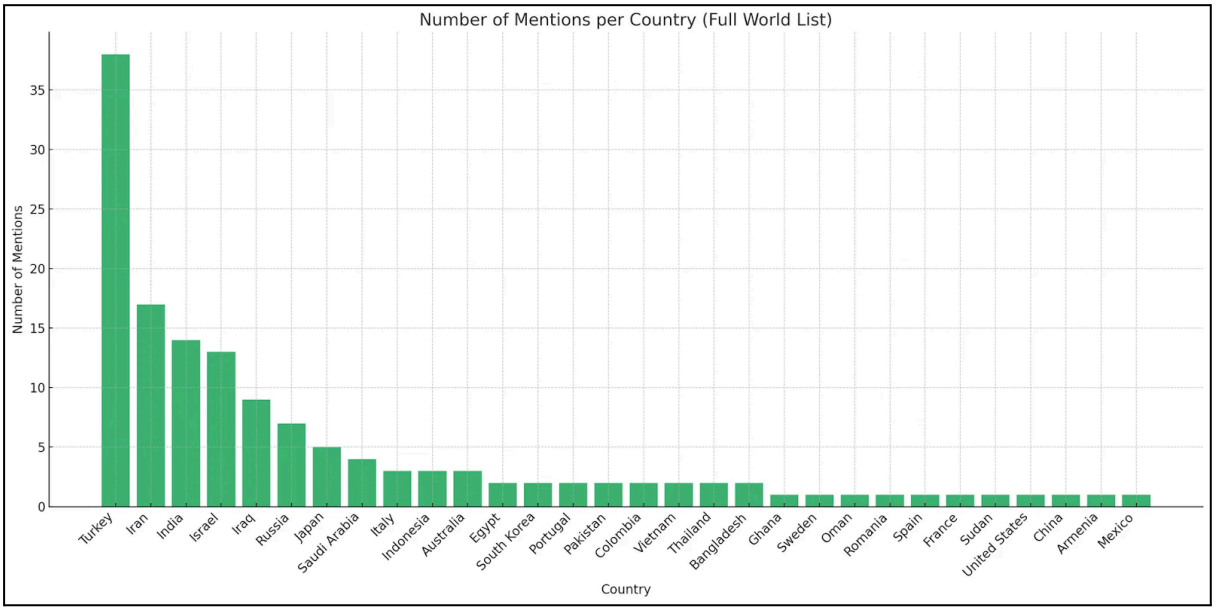

Figure 3.3.3. Number of mentions by country in Team 1722's attack announcement channel. The group appears to direct hostile statements and cyberattacks primarily toward Turkey, Iran, India, and Israel.

An analysis of country name mentions within Team 1722's Telegram channel used for attack announcements provides insight into the group's target distribution. According to the statistics, Team 1722 focused its operations primarily on countries bordering Iran, with Turkey, Iran, India, and Israel being the most frequently referenced. This pattern suggests the group may have targeted these nations due to political grievances or religious hostilities.

Mentions of Korea were relatively low in the dataset. However, this appears to be due to the group's consistent use of the term "Korea" instead of the formal "South Korea", which was the reference term used for data extraction. As a result, the actual volume of attacks against South Korea is underrepresented in the statistical analysis.

In reality, South Korea was the primary focus of the group's attacks between mid-May and mid-June 2025. During this period, Team 1722 released a cyber declaration of war video targeting Korea, followed by a series of website defacement attacks and data leaks.

The group's target selection shows no clear consistency or strategic rationale. In some cases, the attackers misrepresented the nature of their victims, suggesting a lack of understanding of the targeted industry. This

indicates that Team 1722 likely selects targets opportunistically, focusing on websites that appear vulnerable, rather than pursuing specific political or economic objectives.

The group's attacks have largely been limited to visual defacements of websites, and the leaked data typically includes public content or non-sensitive information. This reflects a low level of technical sophistication, as Team 1722 tends to rely on basic, low-complexity attack techniques.

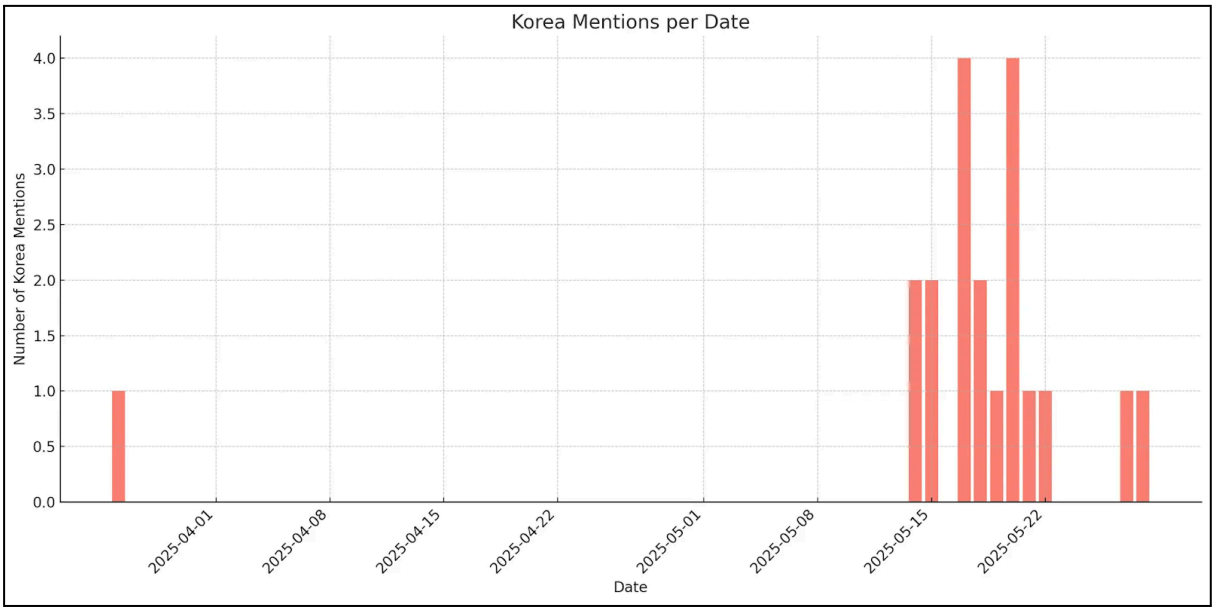

Figure 3.3.4. Cyberattacks targeting South Korea were primarily concentrated between mid-May and late May, with two additional incidents occurring in June. (Mentions related to Korea in April were linked to a foreign website involved in the import and sale of Korean automobiles.)

Published on July 16, 2025.

DKZ
TEAM D4RKN3TTZ

Table 1. *The timeline of the attacked victims*

Date	Domain	Industry / Sector
2025-05-14	globalscout.co.kr	Recruitment
2025-05-14	wheel.co.kr	Mobility Aid Manufacturing
2025-05-15	kepcoes.co.kr	Power Infrastructure
2025-05-15	netprogram.co.kr	English Education
2025-05-16	koldbook.co.kr	Antique Book Restoration
2025-05-16	novotec.co.kr	Life Sciences
2025-05-16	sukmun.co.kr	Sports Park
2025-05-16	kapes.co.kr	Power Infrastructure
2025-05-18	elearnnet.kr, sms.elearnnet.kr	Online Education
2025-05-18	mypartners.co.kr	Shared Office
2025-05-19	salaryday.co.kr	Payroll Solutions

Reported by Team D4rkn3ttz

Published on July 16, 2025.

DKZ
TEAM D4RKN3TTZ

Date	Domain	Industry / Sector
2025-05-19	irontrain.co.kr	English Education
2025-05-20	floweru.co.kr	Floral Retail
2025-05-20	christiandaily.co.kr	Religious News
2025-05-21	parkadmin.gys.or.kr	Urban Management Authority
2025-05-22	hypersoft.co.kr	Software
2025-05-26	blog.wadiz.kr	Crowdfunding
2025-05-28	seungjinsa.firstmall.kr	Silver Jewelry Retail
2025-06-09	adpumpkin.co.kr	Retail
2025-06-12	rookie.co.kr	Sports Newspaper

Reported by Team D4rkn3ttz

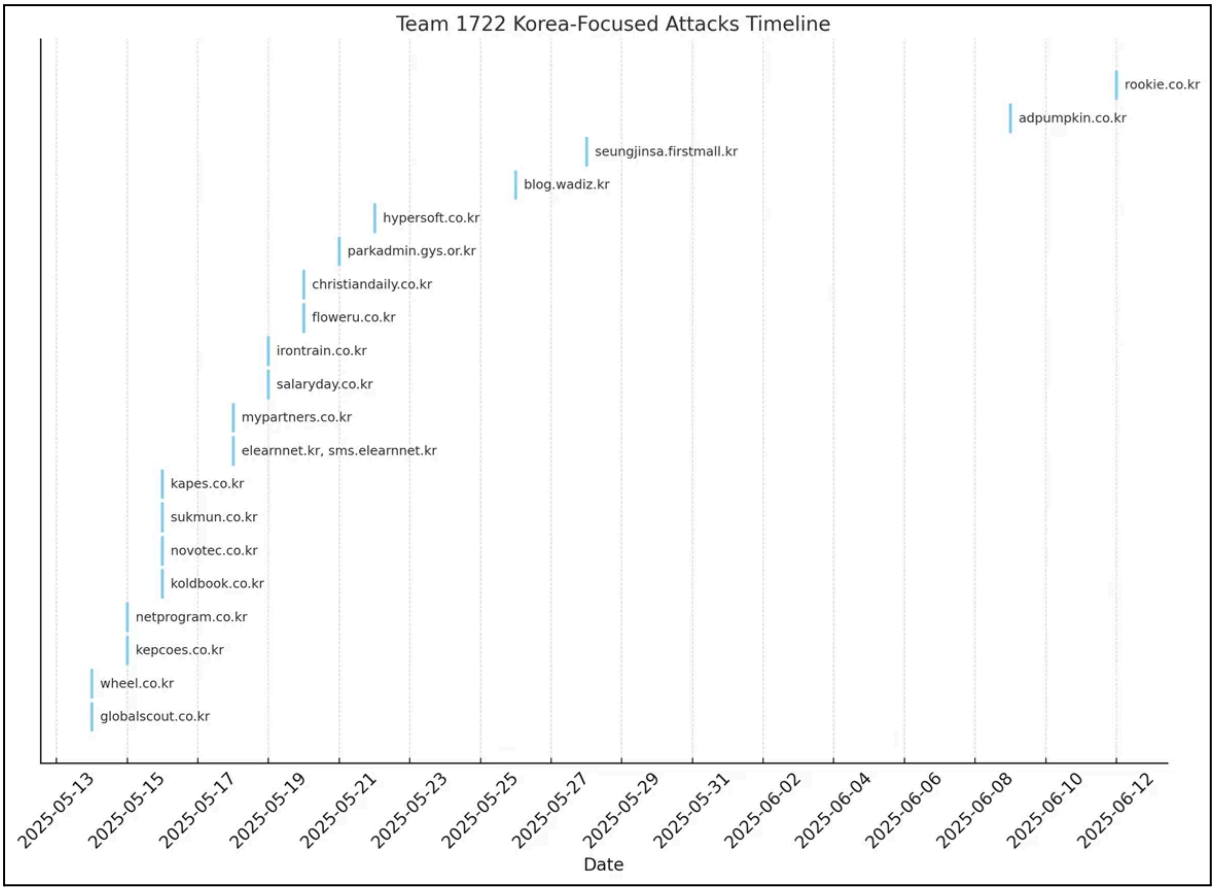

Figure 3.3.5. *South Korean victim organizations are summarized in the form of a timeline.*

Published on July 16, 2025.

4. Tracking Members on Telegram

a. Self-revealed identities

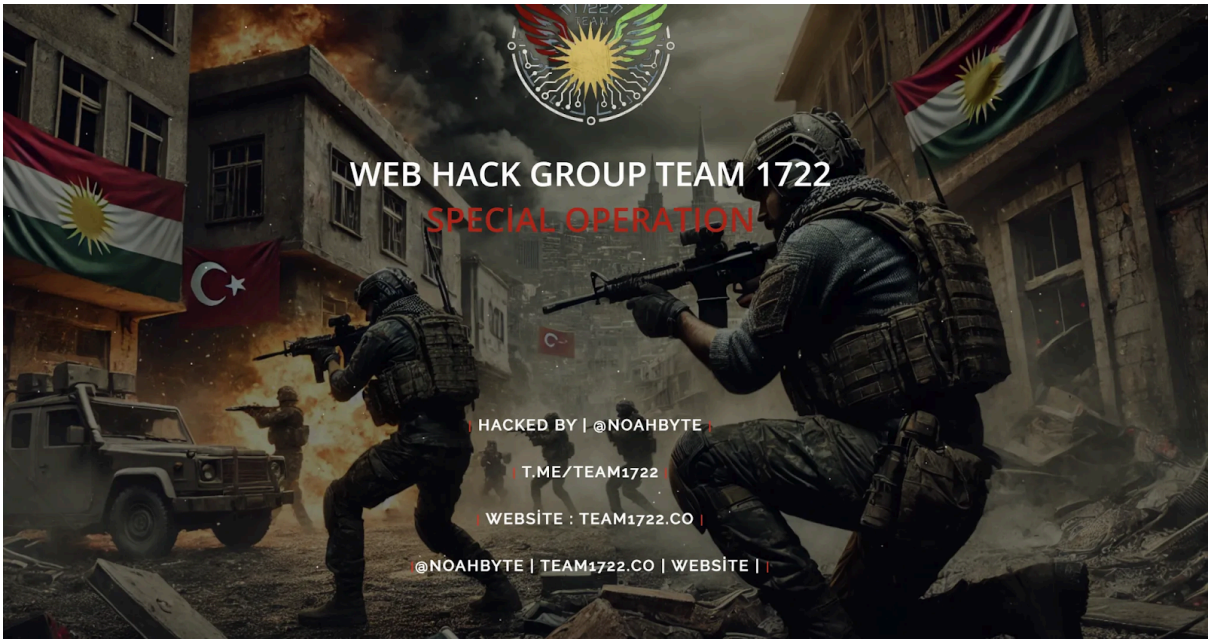

Figure 4.1.1. A website previously defaced by Team 1722 remains unrestored to this day. The alias "NOAHBYTE" is visible on the defacement page. Similar identifiers such as DeadCoder1722, @Black_hat1722, and Exp1o5ive (from ByteBlitz) have also been observed in comparable defacement cases.

Team 1722 has exhibited a highly performative and attention-seeking behavior, often leaving visible traces on defaced websites or voluntarily exposing member accounts within their Telegram channels. In particular, when defaced websites remained unrestored, it became possible to identify the Telegram usernames of specific group members.

Additionally, conversations within the group's Telegram channels often revealed member identities either through self-disclosure or by being tagged by others.

The following is a list of key member accounts identified prior to the group's claimed restructuring. Despite being labeled as former members, some are believed to remain active, thus making their identification still relevant.

Published on July 16, 2025.

- @DeadCoder1722 (DeadCoder)
- @LuciferCoder1722 (Lucifer, LuciferCoder)
- @Bold_Coder1722 (BoldCoder, BoldCoder1722)
- @Robotcode1722 (RobotCoder)
- @NoahByte

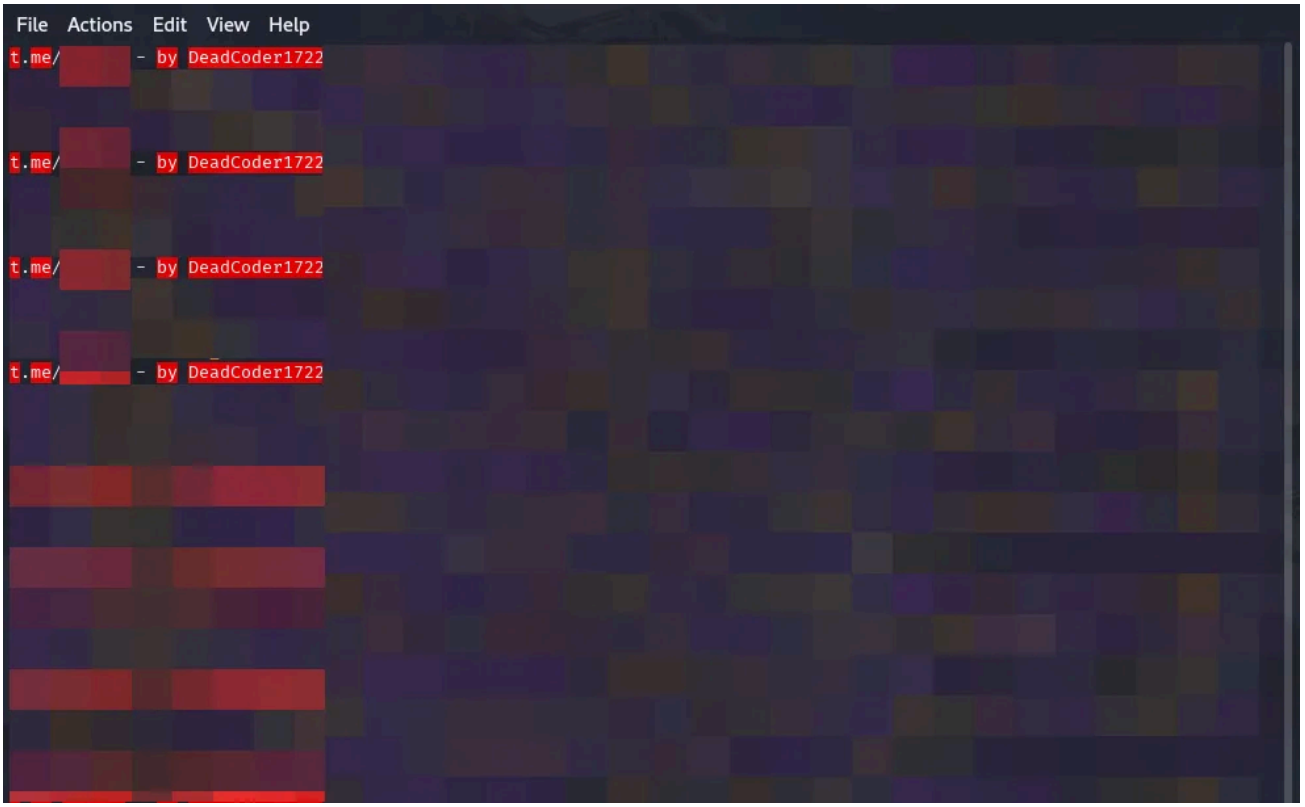

Figure 4.1.2. The string "by DeadCoder1722" was included in a data leak involving U.S. citizen information, released by Team 1722 after its restructuring.

سڵاوی خودا لە هەموو لایک بێت بە باشمان زانی چەند ڕوونکردنەوەیک بدەین دەربارەی هەندێک کێشە

لە زۆر لاوە پەیوەندی بە ئێمەوە ئەکرێت بۆ مەسەلەی کێشەکانی رابردووی تیمی 1722

DeadCoder , NoahByte , OblivionByte , Robot , BoldCoder , Lusiver , Devil , Virus , Mamosta Rayan , Ranj , mr helper , Other...

زۆری تریش ئێمە هەقمان بەوانەوە نیە کە پێشتر لە تیمی 1722 کاریان کردووە نامە بۆ ئێمە مەنێرن و هیچ کەسێک لەو کەسانە لە تیمی 1722 نماون و ناش بنەوە و تیمەکەمان لە ئێستادا هیچ کەسێکی دیاری نیە و تەنها ناوی تیم دیارە

Reported by Team D4rkn3ttz

A message above from Team 1722 during the restructuring phase stating that previous members are no longer affiliated with the group. The message also reveals names of individuals formerly involved with the group.Confirmed aliases include DeadCoder, NoahByte, OblivionByte, Robot, BoldCoder, Lusiver *(believed to be a misspelling of "Lucifer")*, Devil, Virus, Mamosta Rayan, Ranj, and mr helper.

In particular, the account DeadCoder(1722) appears to remain involved with the group. Even after Team 1722's declared restructuring, several messages advised users to contact this account, suggesting an ongoing role within the organization.

Notably, in early June 2025, when personally identifiable information (PII) of U.S. citizens was leaked, the data was explicitly published by the account DeadCoder1722. This strongly implies that the account remained operational despite the group's public announcement of suspended activity.

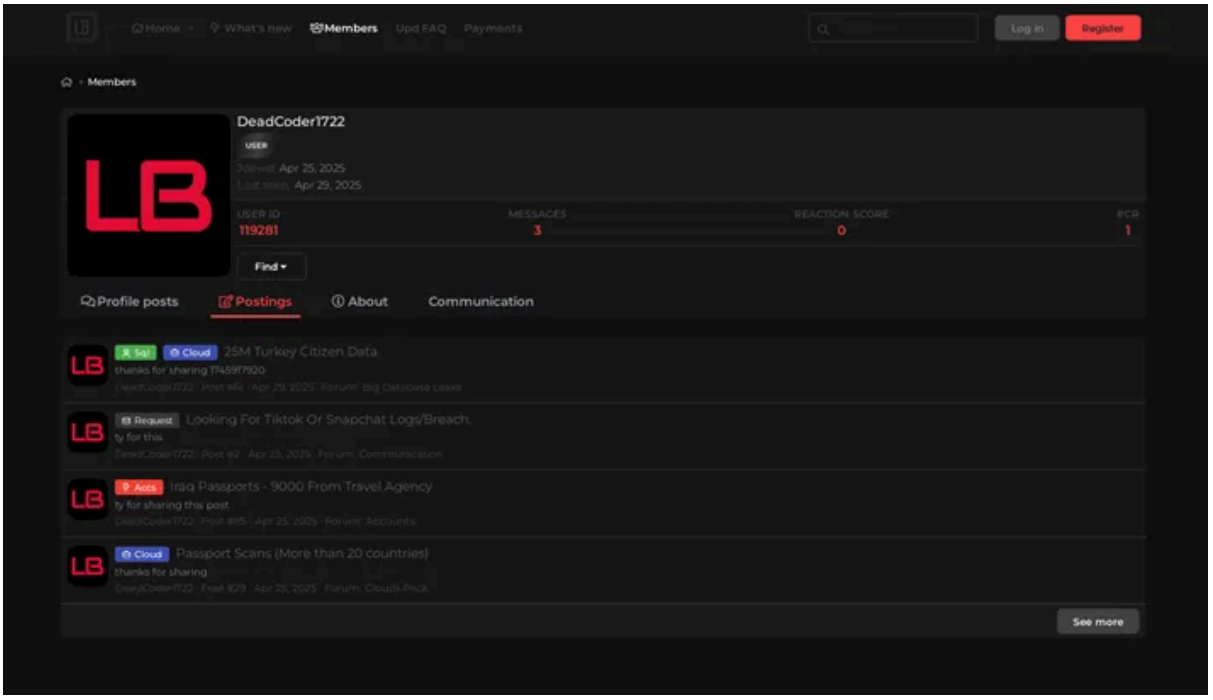

Figure 4.1.3. An account with the same name as DeadCoder1722 was found to be active on the cybercrime forum LeakBase (leakbase[.]la).

This account was observed posting leaked passport information of an Iraqi national. If the leaked data is authentic, it raises a contradiction—suggesting the threat actor may have exposed data from their own country. However, the same account also published data belonging to Turkish citizens, aligning with Team 1722's historical hostility toward Turkey, one of its primary adversary states.

This account appears to have been deactivated or removed from the forum following Team 1722’s official suspension of operations.

b. Identities revealed by another hacktivist group, Team 313

Figure 4.2.1. Although direct access to past Team 1722 messages is no longer available, some historical records can be found in materials published by a rival group, Team 313.

Given that some former members of Team 1722 remain active, there is still value in investigating the group's earlier operations. According to Team 313, Byte Blitz, a cyber threat group that previously collaborated with Team 1722, later turned against them due to allegations of embezzlement and extortion.

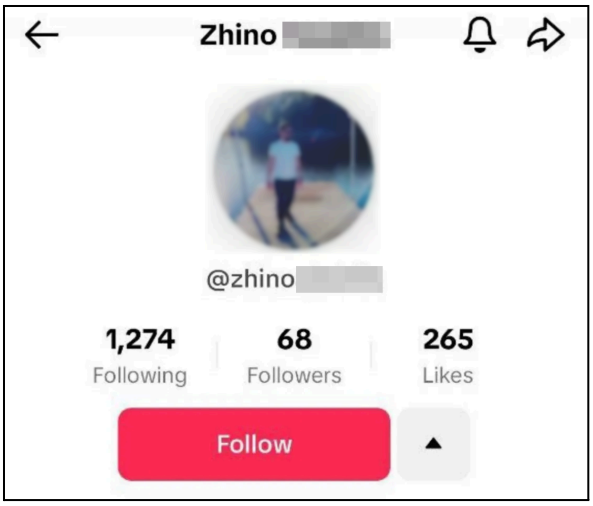

Figure 4.2.2. Team 313 also released information claiming to expose the real identity of LuciferCoder (1722).

Team 313 is an anti-Palestinian, pro-Iranian hacktivist group that remains active as of 2025. The group operates a Telegram channel titled "Team 1722 | Reveal identities," through which it has conducted a campaign to expose the internal structure and personal details of Team 1722 members.

Through this channel, sensitive personal information—including real names, contact details, and home addresses of specific members—was leaked. These disclosures provided insight into the internal conflict surrounding Team 1722's restructuring in late 2024.

Team 313 accused Team 1722 of embezzlement and deceiving donors during its previous affiliation with the BCID alliance. It referenced an incident in which Byte Blitz, another BCID-affiliated group, attacked Team 1722 in retaliation for these actions.

Team 313 also issued extortionate threats, stating that they would continue exposing Team 1722 members unless payments were made.

During this campaign, the real name, residence, and phone number of the member known as LuciferCoder (1722) were made public.

If these claims are accurate, Team 1722's declaration in late November 2024 of initiating a "new operation unrelated to the former team" can be interpreted not as a true restructuring, but rather as a result of ideological fragmentation within BCID—particularly stemming from value conflicts with Byte Blitz.

5. TTPs of Team 1722

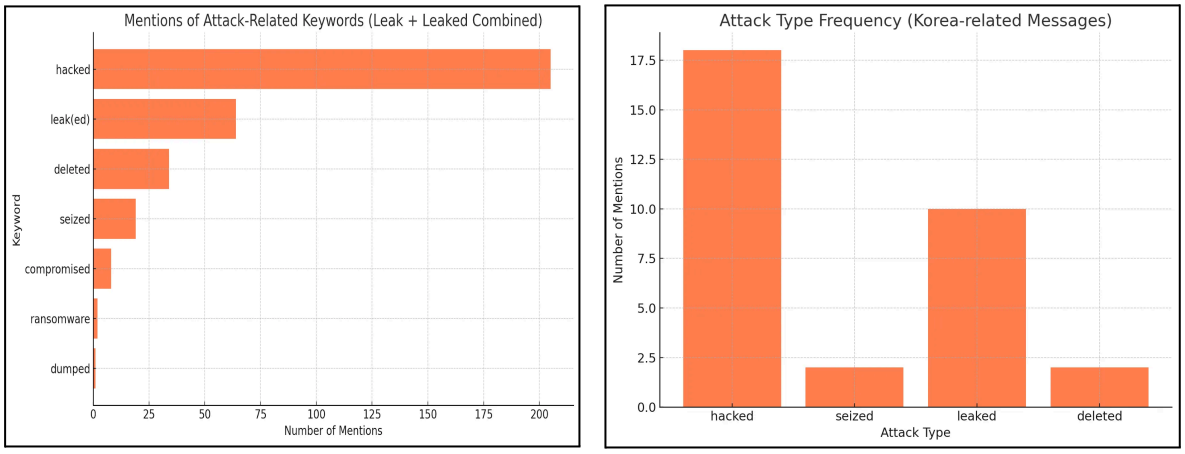

Figure 5.0.1. The following is an analysis of keywords used in Team 1722's Telegram announcements regarding completed attacks.

Most messages indicate unauthorized access to admin panels, using terms such as "Hacked" or "Seized." Additional actions include data exfiltration ("Leaked") and destruction ("Deleted"). Although there is a single mention of ransomware, the isolated nature of the claim makes it unreliable and likely exaggerated. The same pattern is observed in messages related to attacks against South Korea, showing similar keyword distributions and attack behaviors.

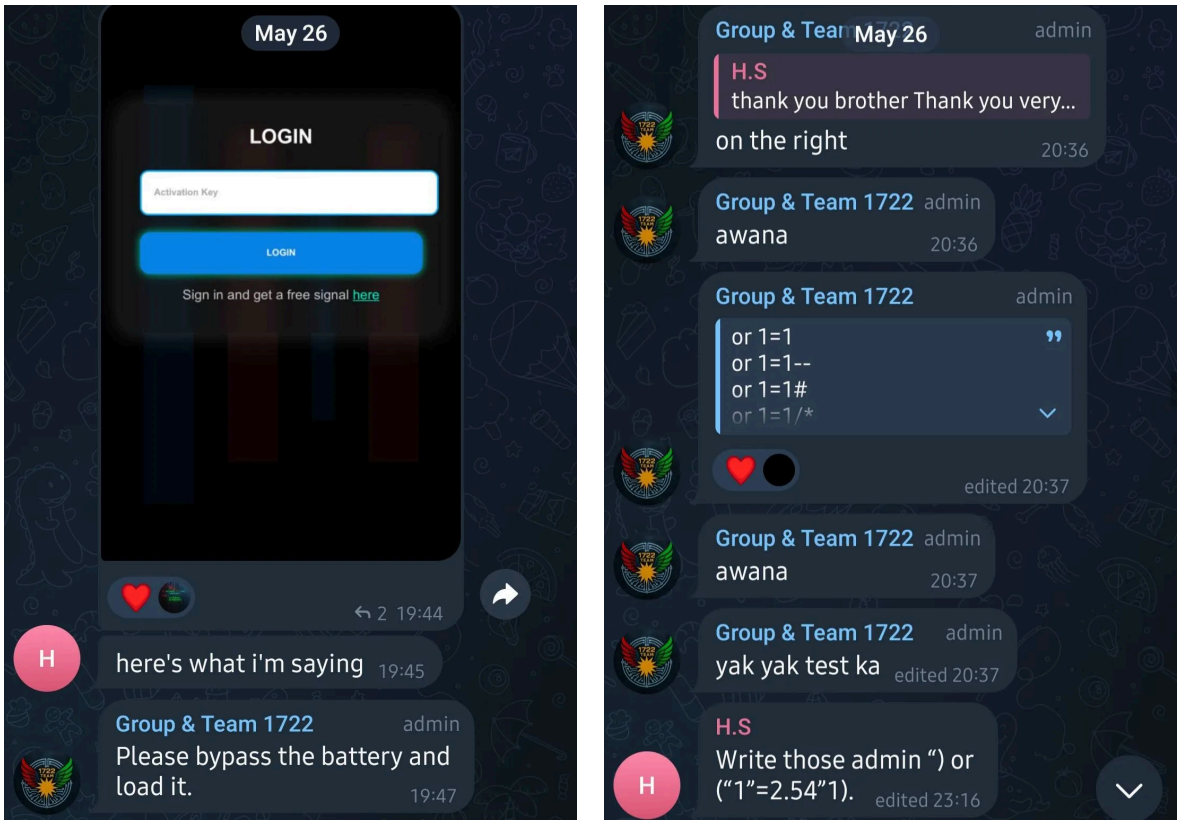

Figure 5.0.2. A message from the group in which a member responds to a technical inquiry by recommending SQLi (SQL injection) as the attack method.

The above image mentioned the list of suggested techniques that may have been used in automated attack scripts, indicating the use of basic but replicable exploitation tactics.

Team 1722's actual attack techniques can be inferred through materials the group has publicly shared—such as messages, videos, and conversations. In addition to their primary channel for publishing attack claims, they operated a separate channel for responding to user questions, occasionally providing insights into tools and methods used.

For example, in one interaction, a user posted a screenshot of a web input form and asked how to bypass the input restriction. Team 1722 responded with a list of SQL injection (SQLi)-vulnerable input values, suggesting that SQLi could be used on login or password fields. The group later shared a video demonstrating automated brute-force SQLi attacks using command-line scripts, confirming their reliance on automation rather than manual intrusion.

Reported by Team D4rkn3ttz

An analysis of websites targeted by Team 1722—including those in South Korea—suggests they primarily targeted sites with exposed /admin login pages. In one video, the group is seen manipulating input values on a foreign website's admin panel to influence system behavior. While there is no direct footage of attacks against South Korean targets, the similarity in patterns strongly indicates the same methods were used.

In one notable case involving a South Korean site (*e-rannet.com*), Team 1722 reportedly exfiltrated and leaked software via the admin panel. This site featured no layered security architecture, linking directly to its admin login from the homepage, and the admin interface was effectively the only functional component. This further supports the conclusion that Team 1722's primary attack vector was exploiting weakly secured admin interfaces.

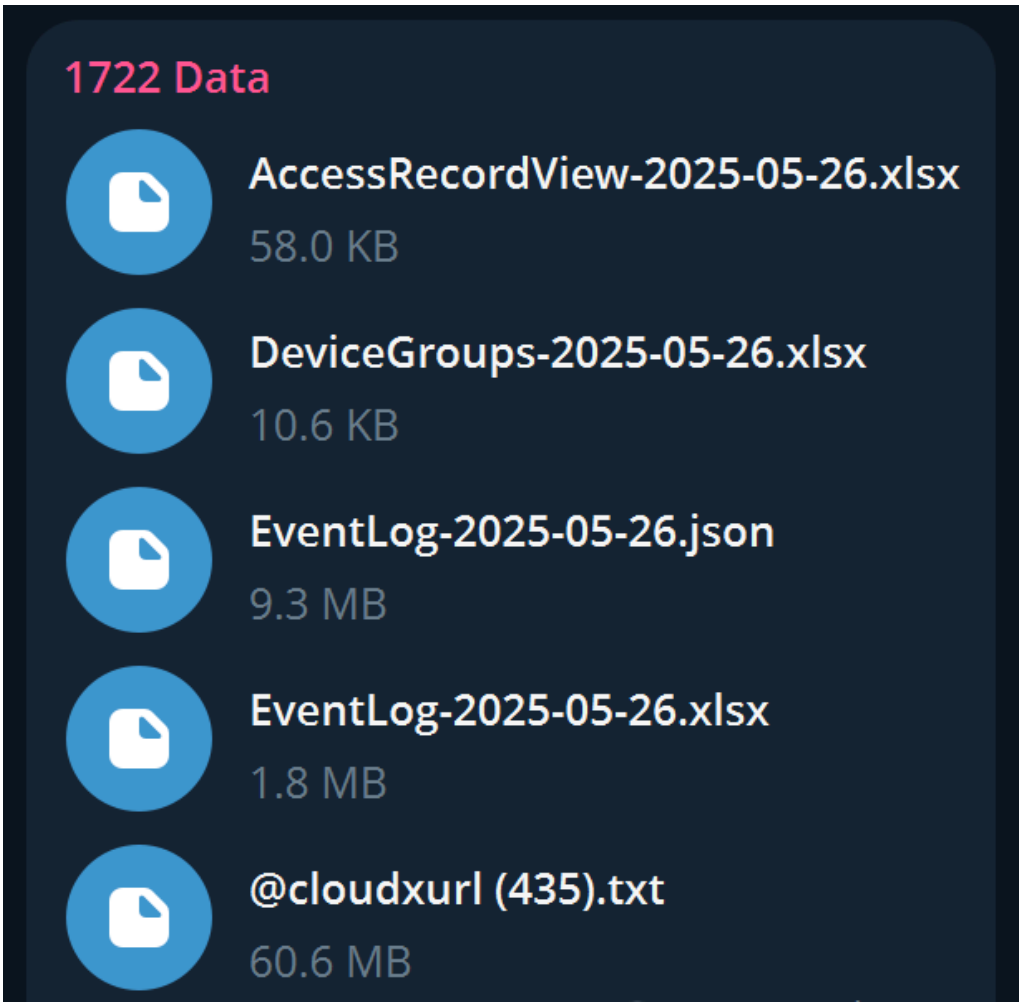

Figure 5.0.3. The leaked data disclosed by Team 1722 during the Wadiz breach included a combolist, whether intentionally or by mistake.

Published on July 16, 2025.

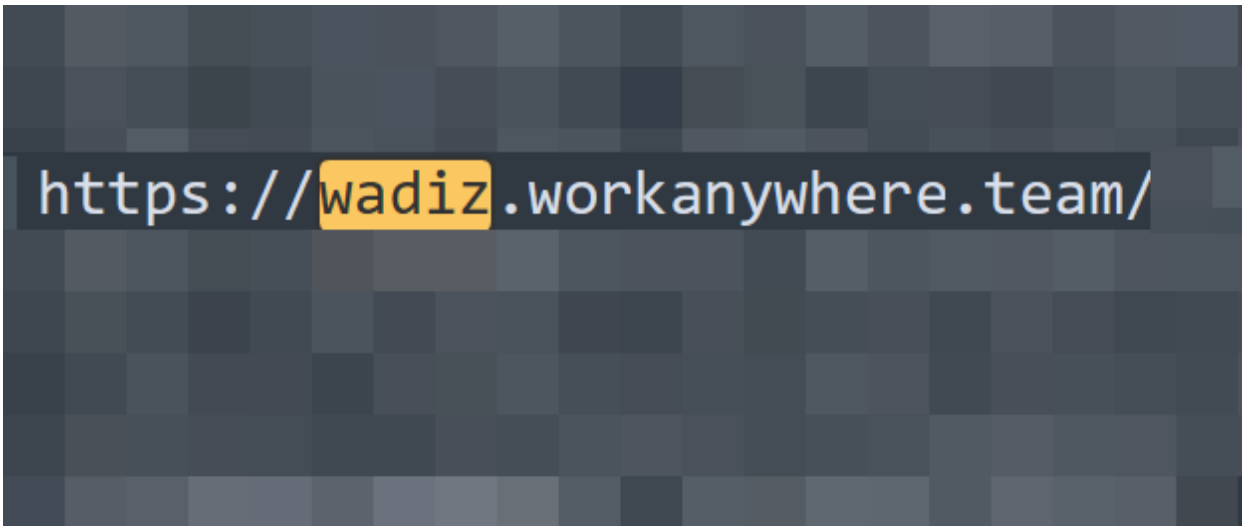

Figure 5.0.4. This combolist was found to contain login credentials for the Wadiz website, with approximately five valid entries identified.

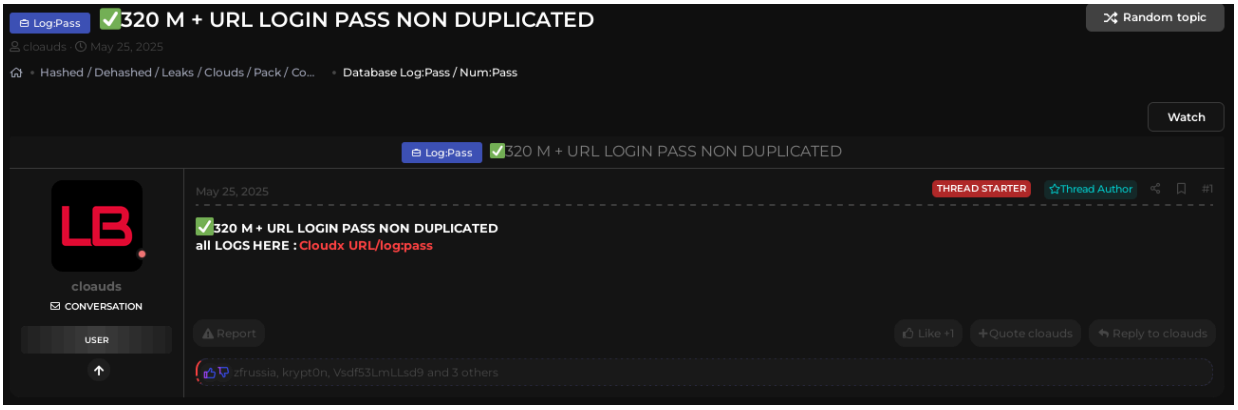

Figure 5.0.5. A combolist distribution channel with the same name as the leaked file was previously advertised on LeakBase, but the channel has since been taken offline.

Additionally, following their attack on the blog of the South Korean crowdfunding platform Wadiz, Team 1722 published exfiltrated data through their leak distribution channel. Among the leaked files was one named “@cloudxurl (435).txt”, which, upon analysis, was identified as a combolist—a file containing numerous email and password pairs that could be used to log in to the Wadiz blog. Notably, the file included credentials granting access to the blog’s admin panel, indicating a successful compromise of privileged accounts.

This strongly suggests that Team 1722 employs pre-compiled combolist to gain unauthorized access to administrator interfaces of vulnerable websites.

Reported by Team D4rkn3ttz

The file naming convention used—@cloudxurl (435).txt—is commonly associated with logs and credential packs (such as Logs Cloud, Combolists, and ULPs [User:Login:Password lists]) sold or shared through illicit Telegram channels. Although the specific Telegram channel in question has since been taken offline, a user named CloudXUrl was previously found promoting their Telegram leak channel on the cybercrime forum LeakBase (leakbase[.]la), suggesting a linkage between Team 1722's leaked data and broader infostealer and combolist trafficking ecosystems.

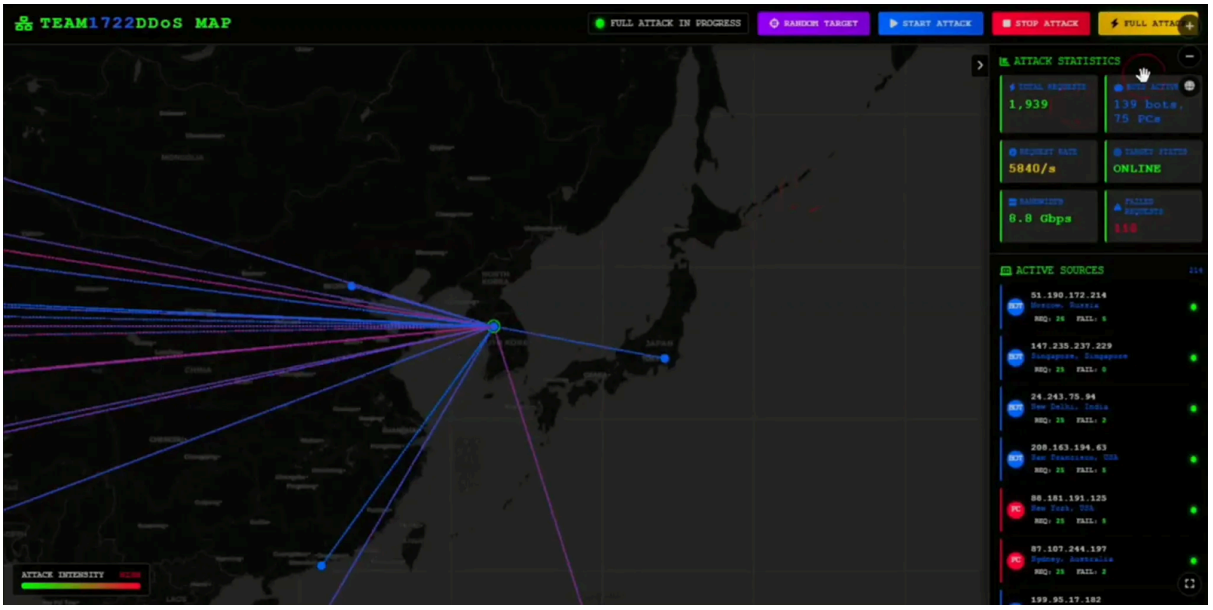

Figure 5.0.6. This is the DDoS GUI tool that Team 1722 previously showcased. The group later operated a private Telegram room where users could access the tool by paying approximately 20,000 to 30,000 KRW (around $15–$23 USD). However, not long after, the group announced its dissolution. (Source: https://x.com/abdul__alamri/status/1932046279770841454)

Team 1722 has also released a video demonstrating the use of a GUI-based DDoS attack tool. This tool is capable of directing traffic from multiple IP addresses around the world to a specific server simultaneously. Given that it was shared among group members in a graphical interface format, it suggests the group employed user-friendly, near-commercial-grade attack tools.

Overall, Team 1722 tends to rely on relatively low-sophistication techniques and tools—primarily SQL injection (SQLi) and DDoS attacks—while focusing on targets with weak or missing basic security protections. However, the group appears to possess at least a minimal

level of technical capability, such as writing automation scripts and developing GUI programs.

While they have previously claimed to offer advanced tools to internal administrators, the credibility of such claims remains uncertain. In practice, the attack techniques observed appear to remain at a fundamental level.

Table 2. TTPs of TEAM1722

Tactic	Technique ID	Technique Name	Explanation
Initial Access	T1190	Exploit Public-Facing Application	Exploitation of publicly known vulnerabilities such as CVE-2021-41773 (Apache Path Traversal) to infiltrate external web services
Collection	T1119	Automated Collection	Automated data harvesting from databases or file systems
Exfiltration	T1048.002	Exfiltration Over Alternative Protocol (TOR, DNS)	Exfiltration of collected data via TOR network or Telegram Bot API
Impact	T1491.001	Defacement	Exfiltration of collected data via TOR network or Telegram Bot API
	T1485	Data Destruction	Deployment of destructive payloads to damage parts of the target system

6. Conclusion

Despite its relatively low technical sophistication, Team 1722 has proven to be a tangible threat by causing multiple real-world security incidents. While the group primarily relied on basic techniques such as SQL injection and unauthorized access to admin pages, these attacks were effective against targets with inadequate baseline security—demonstrating how even low-skill threat actors can cause significant damage under the right conditions.

The group's motivations have shifted over time, driven less by consistent ideology and more by geopolitical developments, internal conflicts, or a desire for recognition. As of June 2025, the group appears to be largely disbanded, following internal whistleblower revelations and public infighting. However, in the past, Team 1722 had declared that *"our operations will never fully end,"* raising uncertainty as to whether the current shutdown is permanent or merely another phase of reorganization.

What remains certain is that their actions did cause measurable harm. For instance, an attack on Goyang Urban Management Corporation led to the exposure of sensitive user and vehicle data. This incident underscores the consequences of poor security awareness and vulnerable website architectures—factors that threat actors like Team 1722 can readily exploit.

7. Mitigations

- Restrict access to sensitive web paths
    - Block or control access to paths such as /admin, /login, /manager via IP filtering, CAPTCHA, or authentication gateways.
    - Remove these paths from search engine indexing using robots.txt or noindex tags.
- Defend against SQL Injection (SQLi)
    - Perform vulnerability scans using automated tools such as SQLMap or OWASP ZAP to detect SQLi risks.
    - Validate all user input on login forms and admin pages to prevent injection attacks.
    - Follow secure coding practices like Prepared Statements and ORM (Object-Relational Mapping) frameworks.
- Enforce password hygiene
    - Prohibit the use of default or weak passwords.
    - Prevent password reuse and maintain strict separation between user and administrator accounts.
- Engage with hosting providers
    - Request regular security assessments from your web hosting service providers to ensure server-side protection.
- Implement anomaly detection
    - Set up real-time alerts for unusual behavior, such as web defacement, suspicious admin logins, or abnormal traffic patterns.
- Prepare for DDoS attacks
    - Establish a DDoS response plan and consider deploying simple defenses like cloud-based solutions (e.g., Cloudflare, AWS Shield, or lightweight CDN services).