

Tracing an Underground Military Data Network

Archived: 2026-08-07 02:00:10 UTC



Underground data markets are filled with sellers offering stolen databases, compromised credentials, and confidential records. But military and defence-related data sits in a different category. Claims involving classified documents, military personnel, defence institutions, drone technology, or internal government communications naturally carry greater significance, while also raising an important question: who is actually behind these listings, and how many seemingly different sellers are truly independent?

ModernStealer emerged as one such identity, appearing across underground forums with posts advertising military and defence-related material from multiple countries. At first glance, the activity appeared to belong to a single forum user operating under a recognizable alias. But as the investigation moved beyond the username and into the contact details left behind in these posts, the picture became more complicated. The same identifiers began appearing alongside other accounts, other aliases, and similar offerings across different corners of the underground ecosystem.

Using StealthMole to follow these traces across dark web forums and Telegram, this investigation examines the digital footprint surrounding ModernStealer and the identities that appear to intersect with it. Rather than assuming that every matching alias belongs to the same person, the report follows the identifiers themselves, looking at where they reappear, how the connections develop, and what those overlaps can tell us about the network operating behind a series of military and government data offerings.

The Thread That Started It All

The investigation began with a post on DarkForums where **ModernStealer** was offering what appeared to be sensitive documents related to a defence agreement between Türkiye and Pakistan. The thread, titled "[PK] TUR-PAK DEFENSE DRONE DEAL," immediately stood out because the material being advertised was not a typical database or credential dump, but a document concerning defence cooperation and drone technology.

The post described a **23-page confidential document** titled "**TURKEY-PAKISTAN BAYKAR-NASTP COOPERATION: STRATEGIC DEFENSE INDUSTRIAL PARTNERSHIP, TECHNOLOGY TRANSFER PROSPECTS AND DRONE PROCUREMENT.**" According to the description provided in the listing, the document covered cooperation involving **Baykar Teknoloji** and Pakistan's **National Aerospace Science and Technology Park (NASTP)**, including areas such as unmanned systems, technology transfer, joint research and development, industrial collaboration, training, localization, and potential drone procurement.

- https://darkforums.*/Thread****PK-TUR-PAK-DEFENSE-DRONE-DEAL

The screenshot displays a web browser window with the URL https://darkforums.*/Thread****PK-TUR-PAK-DEFENSE-DRONE-DEAL. The browser's address bar shows the URL and the page title "[PK] TUR-PAK DEFENSE DRONE DEAL". The page is a snapshot from 2026-07-08 10:11:46. The sidebar on the left contains the following information:

- URL**: https://darkforums.*/Thread****PK-TUR-PAK-DEFENSE-DRONE-DEAL
- Scanned date**: 2026-07-08 10:11:46
- Content size**: 50,568 bytes
- Content HASH**: 40a700c498980e10d98621c9e1c6887927cfb596992476affab e778caa820ee5
- Text**: [View text in preview](#)

The main content area shows the thread title **DOCUMENTS [PK] TUR-PAK DEFENSE DRONE DEAL** by ModernStealer - 3 hours ago. Below the title is a placeholder image with a question mark. The user profile for ModernStealer is visible, showing 44 posts, 22 threads, joined in Mar 2026, and a reputation of 1. The thread is marked as #1 and was posted 3 hours ago.

The listing itself was enough to make **ModernStealer** worth a closer look. A seller claiming access to confidential defence material involving drone technology raised the question of whether this was an isolated offering or part of a broader pattern. At this point, however, there was no basis to assume that ModernStealer had personally obtained the document through a breach, or even that the advertised material was authentic. What the thread did provide was a clear starting point: an underground identity openly associated with the alleged sale of sensitive defence-related information.

More importantly, the post contained an artifact that could be followed beyond the thread itself. ModernStealer had included the following **Session ID** as a contact point:

- 05214b*****f6163



Unlike the claims surrounding the advertised documents, the Session ID provided something concrete that could be searched and compared across StealthMole's indexed data. What began with a single defence-related listing now had a potential trail to follow, and the next step was to find out where else the same identifier had appeared.

A Pattern Begins to Emerge

Before following the Session ID beyond ModernStealer's own activity, we first wanted to understand whether the TU-PAK drone deal was an isolated listing or part of something larger. Searching the keyword "**ModernStealer**" in StealthMole's **Leaked Monitoring** tool returned five listings detected between March and April 2026.

StealthMole				
Leaked Monitoring				
Sort				
DT				
CDF				
TT	5 victims			
FF				
CDS				
CB				
CL				
UB				
RM				
LM				
GM				
DA				
SO				
	Leak Title	Bad Actor	Detection Date (UTC+0)	Source URL
✓	PK Nuclear Regulatory Authority (PNRA) DATABASE	ModernStealer	2026-04-18 08:05:07	
+	DATA LEAK OF NUST PAKISTAN DEFENCE	ModernStealer	2026-04-06 12:05:25	
+	USA LOCKHEED MARTIN EMPLOYEES DATABASE	ModernStealer	2026-04-03 18:05:02	
+	Sri Lanka Air Force Database	ModernStealer	2026-04-02 12:05:50	
+	[CHINA] PLA BREACH EXPOSES SENSITIVE DATA	ModernStealer	2026-03-13 20:08:22	

Among the results were listings involving the **Pakistan Nuclear Regulatory Authority (PNRA)**, **Pakistan's National University of Sciences and Technology (NUST)**, and a database allegedly containing information belonging to **Lockheed Martin employees**. Another result concerned the **Sri Lanka Air Force**. While the nature and authenticity of these advertised datasets could not be established from the listings alone, their appearance under the same actor name suggested that the defence-related material seen in the TU-PAK thread was not an isolated occurrence.

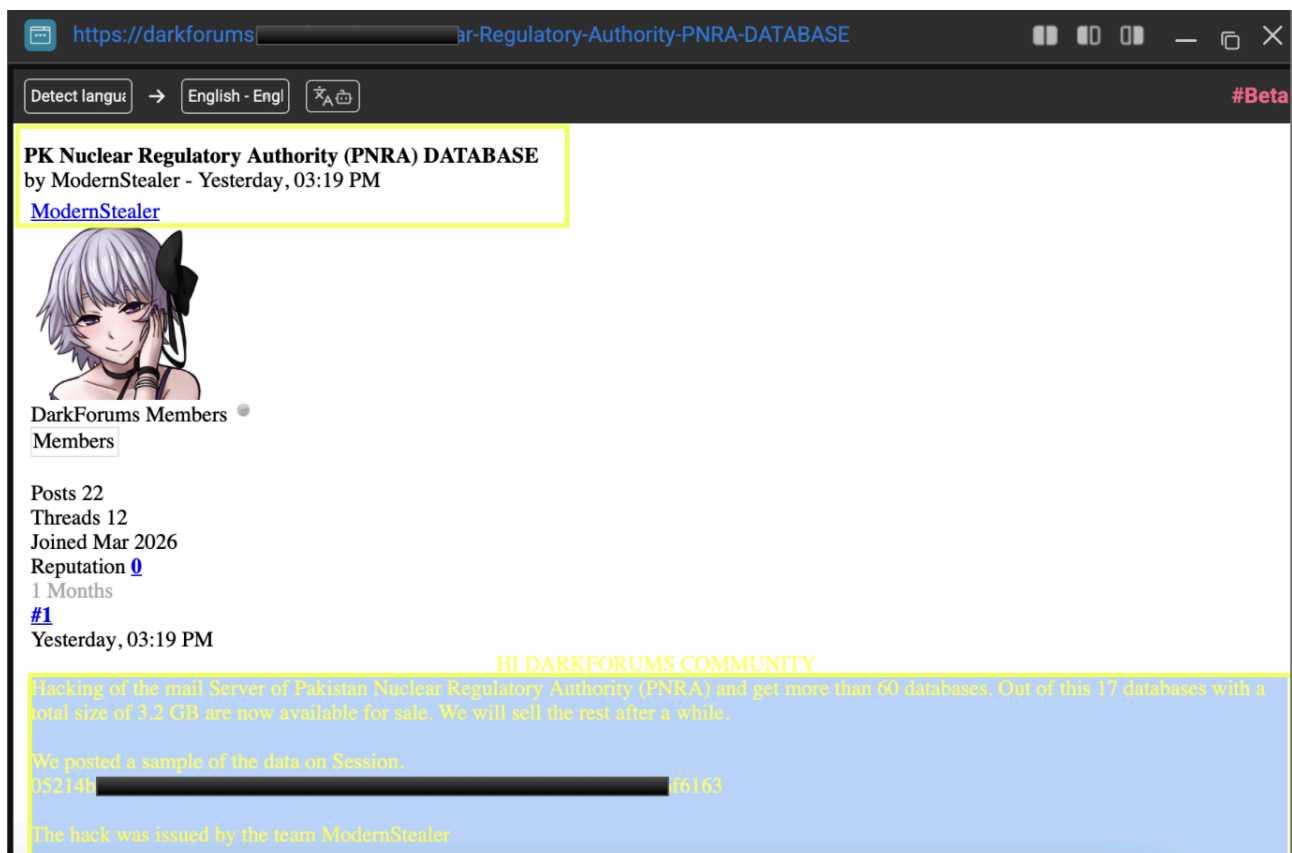
The search was then extended to StealthMole's **Government Monitoring** tool to see whether the same name appeared in connection with government entities. This returned eight listings associated with ModernStealer between March and July 2026. Among them were posts concerning alleged internal documents from the **Bangladesh military**, Pakistan's **SUPARCO and Ministry of Science and Technology**, and a listing referencing the **PLA, CIA, Department of Defense, and DARPA**.

StealthMole				
ModernStealer				
DT	Government Monitoring			
CDF				
TT	8 victims			
FF				
CDS				
CB				
CL				
UB				
RM				
LM				
GM				
DA				
SO				
	Leak Title	Bad Actor	Detection Date (UTC+0)	Source URL
+	PLA ARMY, USA CIA/DOD/DARPA AND MANY OTHERS	ModernStealer	2026-07-16 10:06:57	
+	Highly Classified Internal Documents of the Bangladesh Military	ModernStealer	2026-06-23 14:06:03	
+	[PK] SUPARCO AND MINISTRY OF SCIENCE & TECH	ModernStealer	2026-06-04 22:05:13	
+	PK GOVERNMENT AND MILITARY DEPARTMENTS	ModernStealer	2026-05-07 06:05:19	
+	DATABASE OF BANGLADESH ARMY	ModernStealer	2026-04-08 10:04:54	

Together, the results began to show a recurring theme around the ModernStealer identity. The listings repeatedly touched on military, defence, government, nuclear, aerospace, and science-related organizations. This did not establish that ModernStealer had personally breached each of these entities, nor did it confirm that every dataset being advertised was authentic. But it did show that the TU-PAK drone deal was part of a much broader pattern of sensitive data offerings associated with the same name.

One of those listings offered a particularly useful opportunity to look closer. The thread concerned an alleged database belonging to the **Pakistan Nuclear Regulatory Authority (PNRA)** and was available at:

- https://darkforums.*/Thr*****PK-Nuclear-Regulatory-Authority-PNRA-DATABASE



In the post, **ModernStealer** claimed to have compromised PNRA's mail server and obtained more than 60 databases, with 17 databases totaling approximately 3.2 GB being offered for sale. The actor claimed that the material included information related to nuclear reactor and chemical laboratory locations, employees, email addresses, sensitive documents, and infrastructure. These claims remained unverified, but one detail in the post was immediately familiar.

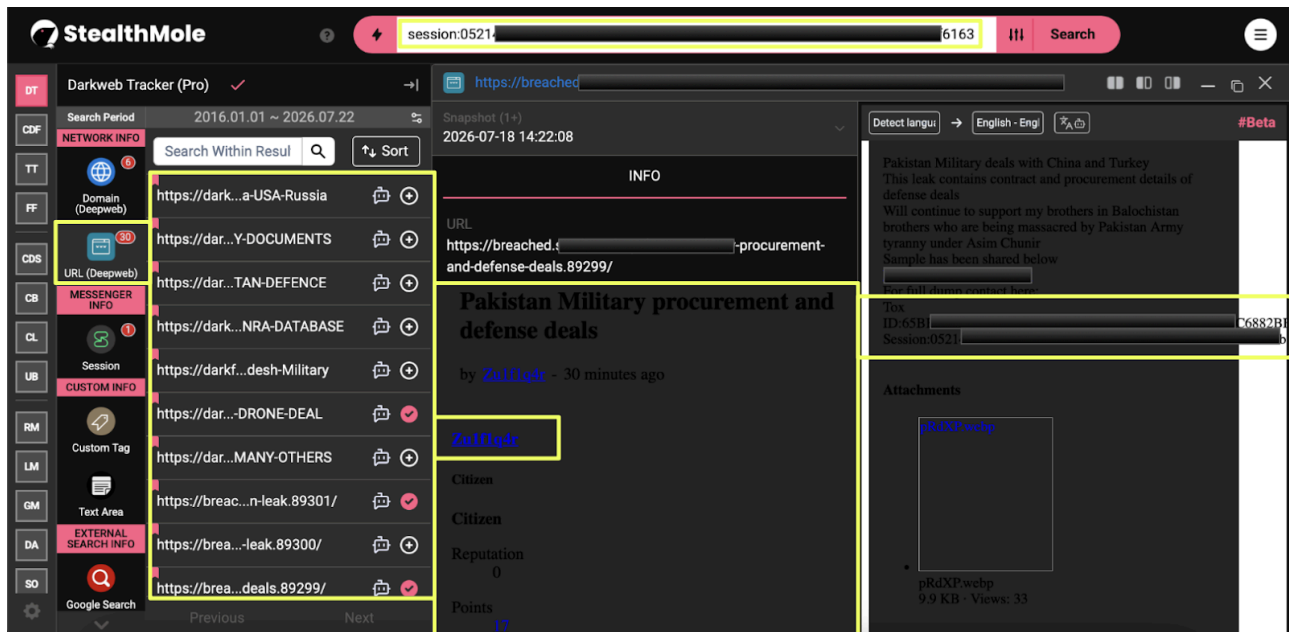
ModernStealer had again provided the same Session ID:

- 05214b*****f6163

The identifier first encountered in the TU-PAK drone deal was therefore not confined to a single listing. It has now appeared again in another sensitive post attributed to ModernStealer. With the same contact point recurring across separate offerings, the Session ID became more than a detail buried inside a forum post. It became the most promising artifact to follow beyond **ModernStealer's** own activity.

Following the Session ID

With the Session ID now appearing across more than one ModernStealer listing, the next step was to search the identifier directly in StealthMole's **Dark Web Tracker**. The results widened the investigation almost immediately. At least **30 indexed threads** contained the same identifier, suggesting that its use extended well beyond the ModernStealer posts examined so far.



Among those results was a thread on Breached titled "**Pakistan Military Procurement and Defense Deals**," posted by a user named **Zu1f1q4r**:

- https://breached.*/threads/pakistan-military-procurement****99/

The post concerned alleged contract and procurement information related to Pakistan's defence dealings with China and Türkiye. But it was the contact information at the bottom of the post that mattered most to the investigation. **Zu1f1q4r** had provided the exact same Session ID previously used by **ModernStealer**:

- **0521*****f6163**

Alongside it was another identifier that had not appeared in the ModernStealer posts examined so far, a Tox ID:

- **65BB*****BC9D**

The appearance of the same Session ID under a different username created the first clear overlap between **ModernStealer** and another underground identity. To understand whether this was a one-time occurrence, we looked further into **Zu1f1q4r**'s activity and identified the actor's Breached profile:

- https://breached.*/members/zu1f1q4*****8/

<https://breached.8/>

Snapshot (3+)
2026-07-18 14:22:58

INFO

URL
<https://breached.8/>

Scanned date
2026-07-18 14:22:58

Content size
408,891 bytes

Content HASH
9423fe7a04893cdacd28cd518c4d4a29d04a5680df68120d0fab82f01484fec5

Text
[View text in preview](#)

HTML
[View html in preview](#)

Source
[View source](#)

Detect language → English - Engl

[Report](#)

Zu1f1q4r

Citizen
Citizen

Joined
55 minutes ago

Last seen
22 minutes ago

Messages
3

Reputation
0

Reaction score
0

Points
17

[Follow](#) [Ignore](#)
[Send direct message](#)

The trail did not stop with the military procurement post. Another thread by **Zu1f1q4r** concerned an alleged leak involving Pakistan's **Intelligence Bureau**:

- https://breached.*/threads/intelligence-bureau-pakistan****1/

<https://breached-bureau-pakistan-leak.89301/>

Snapshot (1+)
2026-07-18 14:18:57

INFO

URL
<https://breached-bureau-pakistan-leak.89301/>

Scanned date
2026-07-18 14:18:57

Content size
441,937 bytes

Content HASH
3a5df2cda2b73773d9931909e9a62ce668ae045d681e3194869602b6498a21cc

Text
[View text in preview](#)

Detect language → English - Engl

Intelligence Bureau Pakistan leak

by [Zu1f1q4r](#) - 18 minutes ago

[Zu1f1q4r](#)
Citizen
Citizen
Reputation
0
Points
17

- [18 minutes ago](#)
- New

Once again, the post listed the same Session ID and the same Tox ID as contact points.

A third thread followed the same pattern, this time involving alleged documents from Pakistan's **Federal Investigation Agency (FIA)**:

- https://breached.**/threads/pakistan-fia-documents*****0/

Snapshot (1+)
2026-07-18 14:20:42

INFO

URL
https://breached.**/threads/pakistan-fia-documents-leak.89300/

Scanned date
2026-07-18 14:20:42

Content size
443,590 bytes

Content HASH
ab3b1ed04cdf9a772c1087f01aa43d8c2be9c5d98dbc05a0d71e175820e8f4a9

Text
[View text in preview](#)

Detect language → English - Engl

Pakistan FIA documents leak

by [Zu1f1q4r](#) - 24 minutes ago

[Zu1f1q4r](#)

Citizen

Citizen

Reputation
0

Points
[17](#)

- [24 minutes ago](#)
- New

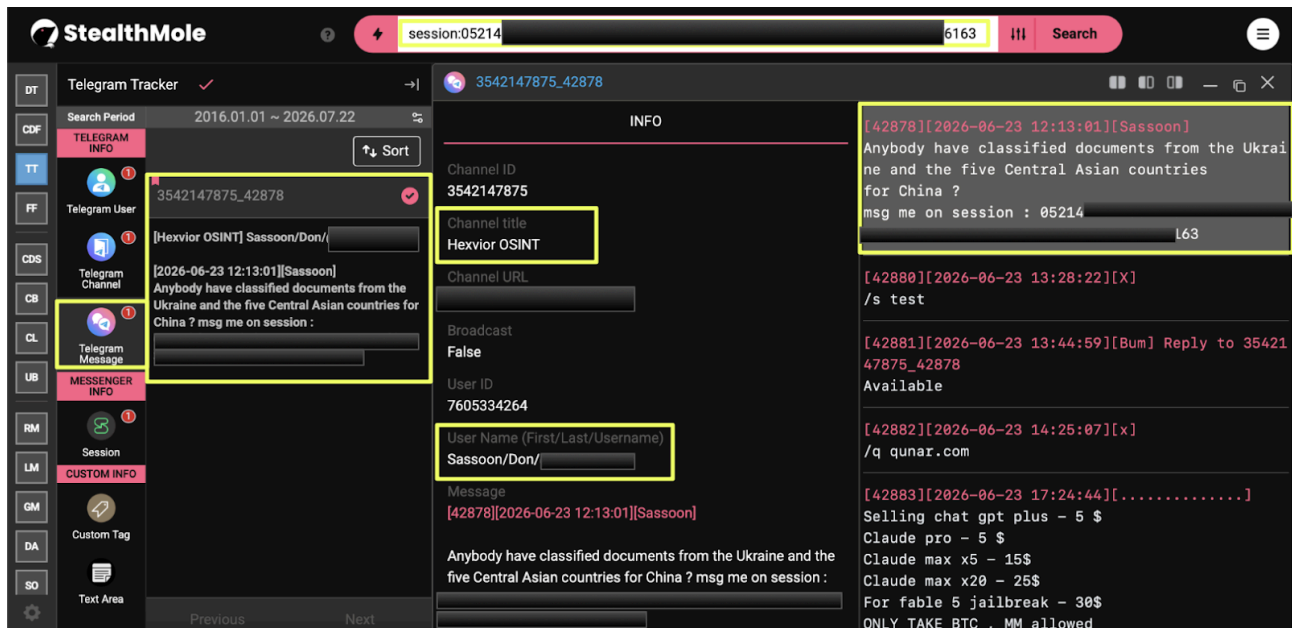
Here too, **Zu1f1q4r** provided the same pair of identifiers.

The repeated overlap was difficult to ignore. **ModernStealer** and **Zu1f1q4r** were operating under different names, but the same Session ID appeared as a contact point in posts associated with both identities. **Zu1f1q4r** then repeatedly paired that identifier with the same Tox ID across multiple Pakistan-focused listings.

At this stage, however, the evidence did not establish that **ModernStealer** and **Zu1f1q4r** were the same person. The Session ID could have been shared between members of a group or used as common contact infrastructure. The Tox ID also remained directly associated only with **Zu1f1q4r**, since it had not been observed in any **ModernStealer** post examined during the investigation.

From the Dark Web to Telegram

The Session ID had already connected **ModernStealer's** DarkForums activity with posts published by **Zu1f1q4r** on Breached. But underground actors rarely limit their activity to a single type of platform. To see whether the same identifier had travelled beyond dark web forums, we searched it again, this time using StealthMole's **Telegram Tracker**.



The search led to a message posted in the Telegram channel:

- https://t.me/Hexvi*****ach

The message came from a user identified as **Sassoon Don**, operating under the Telegram username **S*****n**. In it, the user was looking for classified documents related to **Ukraine and five Central Asian countries**, apparently for China, and asked anyone with access to such material to contact them through Session.

The Session ID provided in the message was immediately recognizable:

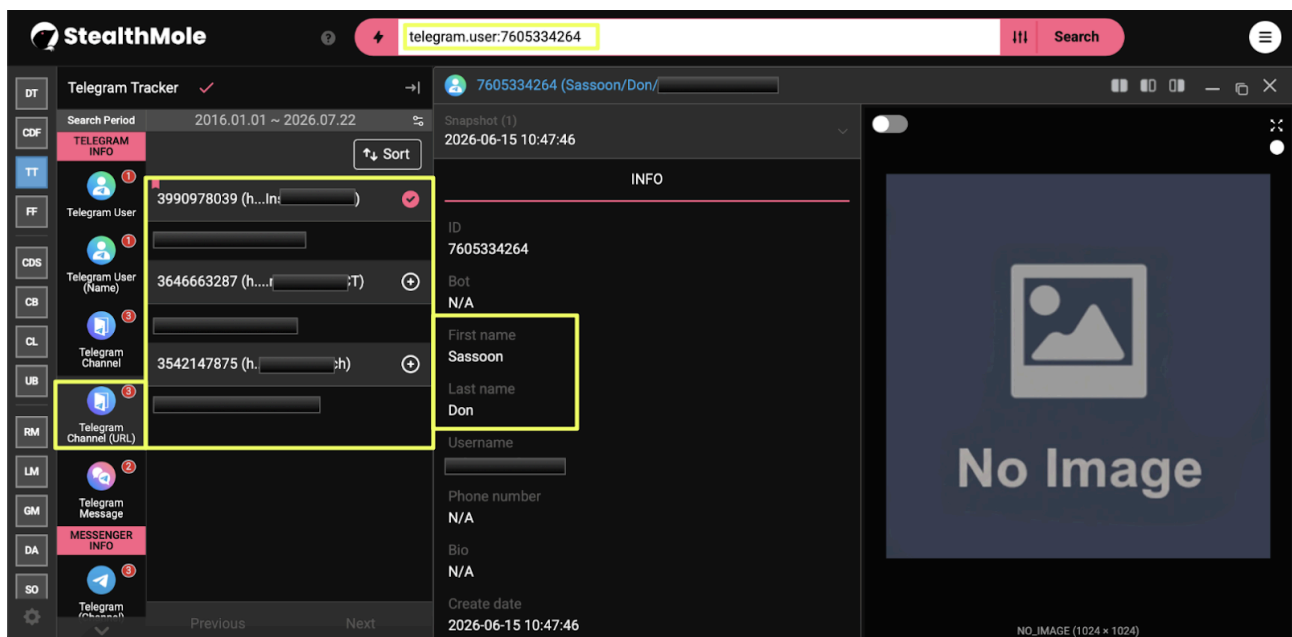
- **05214*****6163**

It was the exact same identifier that had already appeared in posts by **ModernStealer** and **Zu1f1q4r**.

This was an interesting shift in the investigation. Until this point, the Session ID had appeared alongside actors advertising alleged military and government data. The Telegram message showed an account using the same contact point while **actively seeking classified material**, adding another dimension to the activity surrounding the identifier. It did not establish how any of the previously advertised material had been obtained, but it raised the possibility that the network around the Session ID was interested not only in distributing sensitive information, but also in sourcing it.

StealthMole's Telegram data allowed the account itself to be examined further. The user **Sassoon Don** was associated with the immutable Telegram User ID:

- **7605334264**



Searching the user profile revealed only two indexed messages, leaving relatively little historical activity to work with. StealthMole also showed the account appearing across three Telegram channels:

- 3990978039: https://t.me/I*****d
- 3646663287: https://t.me/N*****T
- 3542147875: https://t.me/Hex*****h

These channel associations were useful as contextual information, but they were not treated as evidence of ownership or affiliation. Simply appearing in or being a member of a Telegram channel does not establish an operational relationship with the people running it.

More importantly, the investigation had not yet found another contact identifier in **Sassoon Don** limited Telegram history that could independently connect the account to ModernStealer. At this point in the investigation, the connection rested on one persistent artifact: the same Session ID.

The trail now involved three different identities across dark web forums and Telegram: **ModernStealer**, **Zu1f1q4r**, and **Sassoon Don**. Whether they represented separate actors sharing infrastructure, members of the same operation, or different identities controlled by one person was still unclear.

The Link Back to ModernStealer

The appearance of **Sassoon Don** on Telegram added another identity to the investigation, but at that point, the connection to ModernStealer still depended on the shared Session ID. To determine whether a more direct link existed, we returned to StealthMole's **Dark Web Tracker** and began looking more closely at other threads posted under the ModernStealer name.

One of those threads concerned the alleged sale of classified Pakistani military documents:

- https://darkforums.**/Th***PAKISTAN-CLASSIFIED-MILITARY-DOCUMENTS

https://darkforums.../CLASSIFIED-MILITARY-DOCUMENTS

Snapshot (1+)
2026-03-12 12:11:17

INFO

URL
https://darkforums.../AN-CLASSIFIED-MILITARY-DOCUMENTS

Scanned date

SELLING [PAKISTAN] CLASSIFIED MILITARY DOCUMENTS
by ModernStealer - 4 hours ago
[ModernStealer](#)


DarkForums Members
Members

Posts 2
Threads 2
Joined Mar 2026
Reputation 0
1 days
#1
4 hours ago

1 days
#1
4 hours ago

Hi, DarkForums Community

I sharing a collection of highly sensitive military documents, including correspondence from the COAS Secretariat, personnel information of officers, materials from the Senior Command and Staff Course, and reports related to the Composite Air Defence Task Force of Republic of PAKISTAN.

Sample data shared

For Complete database Contact

Session :05214-*****163

Telegram : *****n

Attached Files
Thumbnail(s)

[Email PM Find Rate](#)
[Reply Quote Report](#)

Enter Keywords Search Thread

« [Next Oldest](#) | [Next Newest](#) »

[New Reply](#)

This time, the contact details provided at the bottom of the post changed the picture considerably. ModernStealer had listed two ways to get in touch:

- Session: 05214*****88163
- Telegram: @S*****n

The Telegram account discovered through the Session ID search was therefore not simply another user who happened to mention the same identifier. **ModernStealer had directly listed Sassoon Don as a contact point in their own forum post.**

The same pairing appeared again in another ModernStealer thread:

- https://darkforums.***/T*****Military-Documents-of-Various-Countries-China-East-Asia-USA-Russia

https://darkforums.../Military-Documents-of-Various-Countries-China-East-Asia-USA-Russia

Snapshot (2+)
2026-03-11 10:44:27

INFO

URL
https://darkforums.../Military-Documents-of-Various-Countries-China-East-Asia-USA-Russia

SELLING Military Documents of Various Countries (China, East Asia, USA, Russia)
by ModernStealer - 4 hours ago
[ModernStealer](#)


DarkForums Members
Members

Posts 1
Threads 1
Joined Mar 2026
Reputation 0
Few hours
#1
4 hours ago

Hi, Darkforums community

Description

Various military documents from various countries (China, East Asia, USA, Russia, Ukraine, NOTA, North Korea)

Recently I have shared a compiling various military and defense documents from different regions. The collection includes materials and reports related to China, East Asia, the United States, Russia, Ukraine, NATO, and North Korea.

Contact

Session - 05214-*****163

Telegram - *****on

The post advertised what was described as military material from several countries and regions and again directed interested users to the same Session ID and the same Telegram account, **Sassoon Don**.

Another thread involving an alleged data leak from Pakistan's National University of Sciences and Technology provided further evidence of the Session ID's repeated use:

- https://darkforums.***Threa**DATA-LEAK-OF-NUST-PAKISTAN-DEFENCE

Here, ModernStealer once again used the same Session identifier as a contact point.

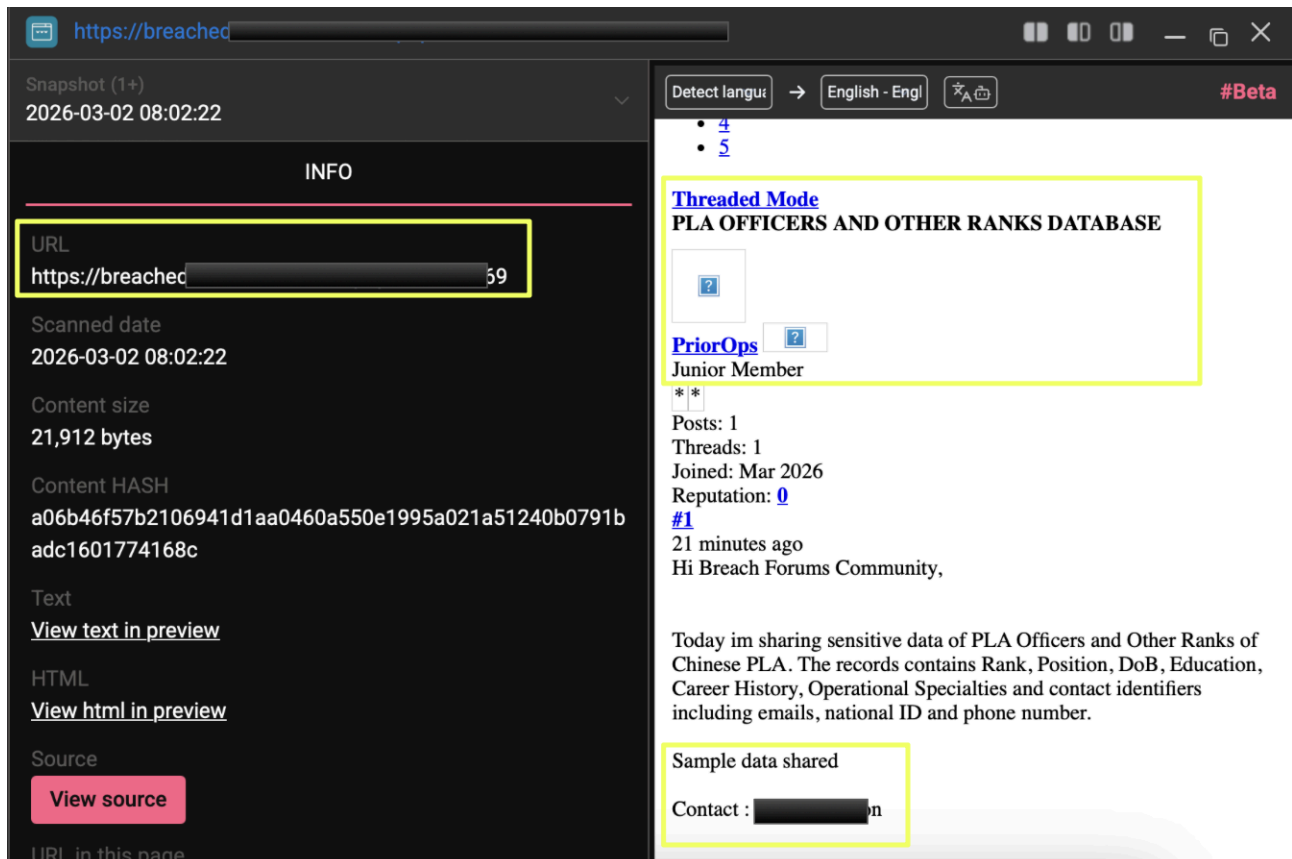
The repeated use of these identifiers provided a much clearer connection than the investigation had at the beginning. The Session ID could now be directly tied to multiple posts under the ModernStealer identity, while **Sassoon Don** had also been explicitly presented by ModernStealer as a Telegram contact across separate listings.

This did not necessarily mean that the person operating the **Sassoon Don** Telegram account and the person posting as ModernStealer were the same individual. Shared accounts and contact infrastructure remain possible, particularly if ModernStealer represents a team rather than a single operator. But the evidence now establishes a **direct operational association** between the ModernStealer forum activity and **Sassoon Don**.

One Contact, Another Name

With **Sassoon Don** now directly connected to ModernStealer's forum activity, the Telegram username became the next artifact to investigate. Searching "**SassoonDon**" in StealthMole's **Dark Web Tracker** surfaced another forum thread, this time on Breached.live:

- https://breached.*****/showt*****669



The thread, titled "**PLA OFFICERS AND OTHER RANKS DATABASE**," was not posted by ModernStealer. Instead, the account behind the listing was operating under a different name: **PriorOps**.

According to the post, PriorOps was offering what was described as a database containing information related to officers and other ranks within China's **People's Liberation Army (PLA)**. The advertised records were said to include details such as rank, position, date of birth, education, career history, operational specialties, and contact information. As with the other listings examined during the investigation, these claims could not be independently verified from the post alone.

But once again, the most useful part of the listing was not necessarily what the actor claimed to possess. It was how they asked to be contacted.

The post listed:

- **Contact:** @S*****n

The same Telegram username that ModernStealer had explicitly provided in military-related DarkForums posts was now being used as a contact point by **PriorOps**, another forum identity advertising alleged military data.

This created a more direct overlap than the one previously observed with **Zu1f1q4r**. In that case, the connection to ModernStealer came through the shared Session ID. Here, both ModernStealer and PriorOps had independently published the exact same Telegram username as their contact point.

By this stage, a pattern was beginning to take shape around the identifiers rather than the names themselves. **ModernStealer** was directly connected to both the Session ID and **Sassoon Don**. **Zu1f1q4r** repeatedly used the

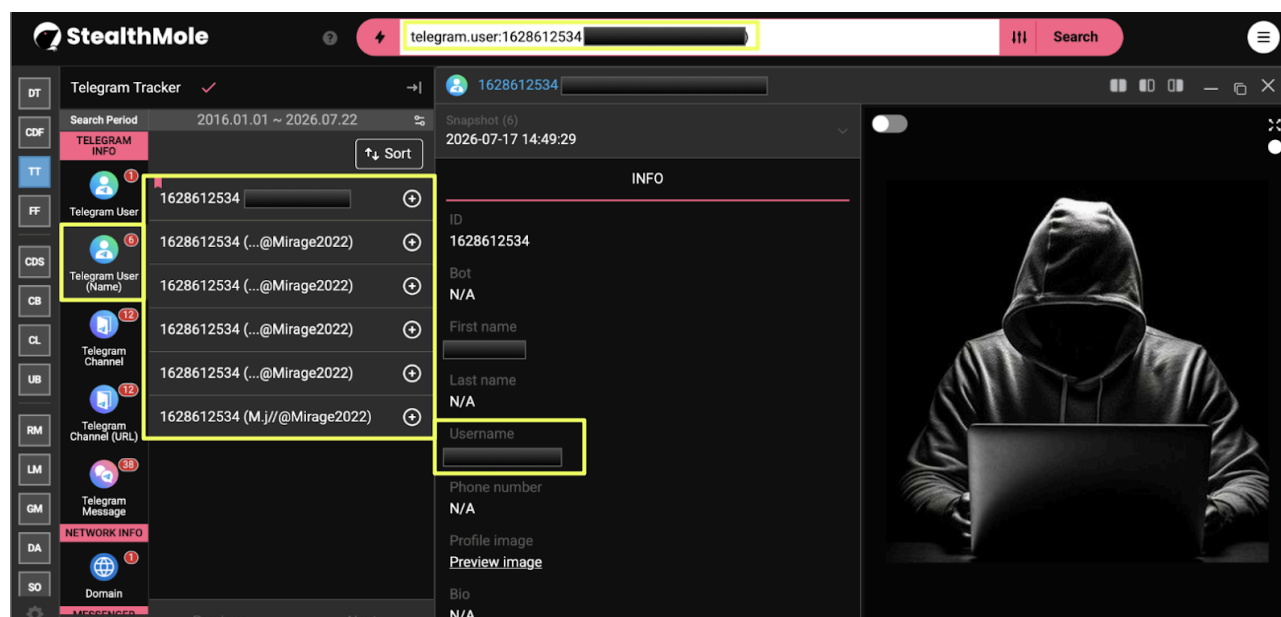
same Session ID across several Pakistan-focused listings, while **PriorOps** used the same **Sassoon Don** Telegram account in a post involving alleged PLA personnel data.

The overlaps raised an obvious possibility: **ModernStealer**, **Zu1f1q4r**, and **PriorOps** could represent different aliases used by the same operator. But the evidence also allowed for another explanation. The identities could belong to multiple individuals using shared contact infrastructure or operating as part of the same group. The available artifacts were strong enough to establish an operational connection between the identities, but not strong enough to conclusively determine who was sitting behind each account.

What was becoming increasingly clear, however, was that following usernames alone would have missed much of this picture. The names changed from one forum to another, but the contact points did not. The Session ID and **Sassoon Don** account provided the connective tissue between accounts that, at first glance, appeared to be unrelated.

A Second ModernStealer?

The connections uncovered so far had all developed from contact points that could be traced from one identity to another. But there was another, more obvious lead worth examining. Searching the keyword "**ModernStealer**" directly in StealthMole's **Telegram Tracker** surfaced a user using the name **ModernStealer**.



At first glance, the match appeared significant. But a closer look at the account's history showed why matching usernames alone can be misleading in underground investigations.

StealthMole associated the account with the immutable Telegram User ID:

- 1628612534

Historical records showed that the same user ID had changed its username multiple times over the years, with **six username changes** observed in the available data. Among the account's previous identities was **@Mirage2022**, appearing under names including **Myles** and **Haven**.

Looking through the account's older messages revealed one detail that stood out in the context of the investigation. On 3 February 2026, while appearing as **Myles / @Mirage2022**, the user posted a message asking:

- “Who knows where I can get drone leaks and blueprints”

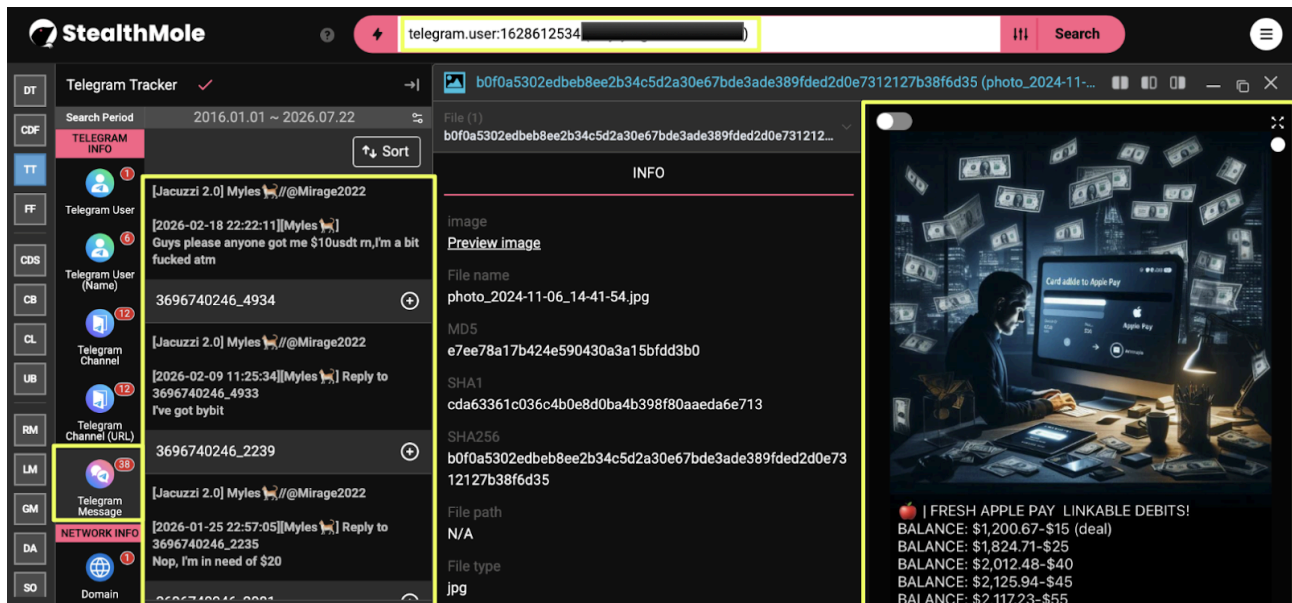
The screenshot shows the StealthMole Telegram Tracker interface. The search bar at the top contains 'telegram.user:1628612534'. The left sidebar lists various search filters like DT, CDF, TT, FF, CDS, CB, CL, UB, RM, LM, GM, DA, and SO. The main area displays a list of Telegram users and channels. The selected user is 3696740246_3891, with channel ID 3696740246 and channel title 'Jacuzzi 2.0'. The right-hand pane shows a chat history with messages from Myles (@Mirage2022) and others. The message 'Who knows where I can get drone leaks and blueprints' is highlighted in yellow.

The message was difficult to ignore. The investigation itself had begun with ModernStealer advertising documents related to a Türkiye-Pakistan drone deal, and there was a Telegram account that would later use the same username with a documented historical interest in obtaining drone-related leaks and blueprints.

Other messages provided glimpses into the account's broader activity. Historical records showed the user asking others for money, while one conversation included the statement:

- “No, I’m not Indian, lol”

The comment offered little in the way of reliable attribution. It was a self-reported statement made by the user and could not be used to establish nationality or location.



StealthMole also preserved images associated with the account's historical Telegram activity. Among them were screenshots showing payment-related information and material referring to **Apple Pay-linkable debit cards**, alongside purported balances and prices. While these images added context to the type of underground activity surrounding the account, they did not establish that the user owned the financial accounts shown, controlled the advertised cards, or personally carried out any related fraud.

Taken together, the findings made Telegram User ID **1628612534** an interesting lead. The later use of the exact name and the earlier interest in drone leaks created a notable resemblance to the activity examined elsewhere in the investigation.

But unlike **Sassoon Don**, this account could not be tied back to ModernStealer through the Session ID or another contact point directly published in the actor's forum posts. No overlap was found with Telegram User ID **7605334264**, and the investigation did not uncover another persistent identifier connecting the two accounts.

For that reason, the account remains an **unconfirmed branch of the investigation**. It may represent another identity connected to ModernStealer, or the username may have been adopted independently. The similarities make the account worth documenting, but they are not enough to merge it into the stronger attribution chain built around the Session ID and **Sassoon Don**.

Conclusion

What began with a single DarkForums listing involving an alleged **Türkiye-Pakistan defence drone** deal quickly developed into a much broader investigation. **ModernStealer's** activity extended across a series of listings involving military, government, nuclear, defence, and aerospace-related material, but it was the contact information left behind in those posts that ultimately proved more revealing than the names attached to them.

By following the Session ID and **Sassoon Don** across StealthMole's indexed dark web and Telegram data, the investigation uncovered connections that would have been difficult to identify through username searches alone. The same Session ID used by **ModernStealer** appeared repeatedly in posts by **Zu1f1q4r**, while the Telegram account directly advertised by **ModernStealer** was also used as a contact point by **PriorOps**. These overlaps

establish a clear operational relationship between the identities, although the evidence does not conclusively determine whether they represent one person operating under multiple aliases, members of the same group, or separate actors sharing communication infrastructure.

The investigation also surfaced a separate Telegram account using the **ModernStealer** name, whose historical activity included an interest in obtaining drone leaks and blueprints. Despite the apparent similarities, no persistent identifier was found connecting that account to the stronger attribution trail surrounding the known Session ID and **Sassoon Don**. It therefore remains an unresolved lead rather than a confirmed part of the cluster.

Ultimately, the ModernStealer investigation shows why the identity displayed beside a forum post is often only the beginning of the story. Usernames changed as the investigation moved between platforms, but certain contact points continued to reappear. Following those identifiers allowed a single military data listing to develop into a wider picture of interconnected underground activity, while also leaving an important question unresolved: whether the many faces surrounding ModernStealer belong to one operator or to a network working behind shared infrastructure.

Editorial Note

Attribution in cyber and dark web investigations is rarely absolute. Shared accounts, reused identifiers, changing usernames, and common infrastructure can create strong connections without necessarily proving that the same individual is behind every identity. This investigation reflects that uncertainty: StealthMole made it possible to follow persistent artifacts across forums and Telegram and uncover relationships that were not immediately visible, while the available evidence still required each connection to be assessed on its own strength rather than treated as definitive attribution.

To access the unmasked report or full details, please reach out to us separately.

Contact us: support@stealthmole.com

Labels: [Featured](#), [Threat Actor](#)

Source: <https://stealthmole-intelligence-hub.blogspot.com/2026/07/the-many-faces-of-modernstealer-tracing.html>