

ModernStealer Threat Actor Linked to Government and Defense Data-Leak Claims

By Tushar Subhra Dutta

Published: 2026-08-03 · Archived: 2026-08-07 02:00:20 UTC

ModernStealer is the name behind underground posts claiming to offer military, government, nuclear, and aerospace material.

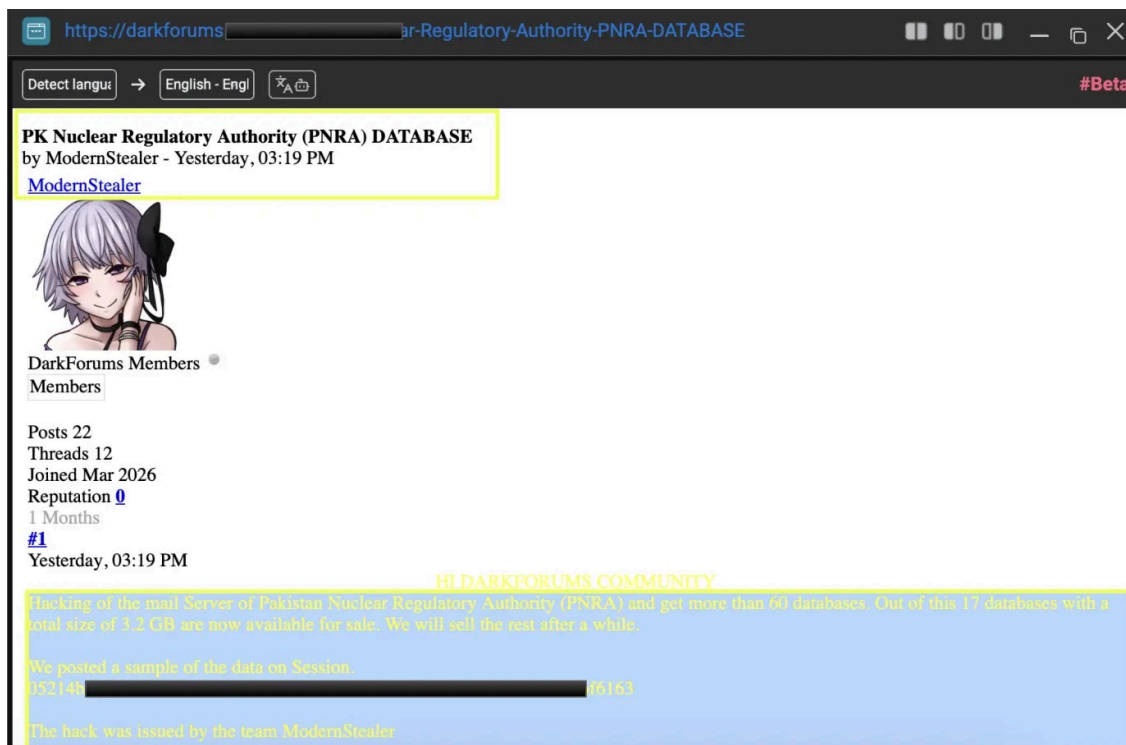
The posts appeared on dark web forums and Telegram, making a single alias a concern for public-sector and defence teams.

The activity is not a confirmed malware campaign or proof that every named organization was breached.

It involves alleged data sales and claims with reused contact details. Sellers can exaggerate, recycle records, or offer material they did not steal.

Analysts at StealthMole identified a recurring trail behind the postings. Their review connected ModernStealer to a Session contact identifier and a Telegram account called Sassoon Don, then found those artifacts linked to other identities advertising sensitive material.

[StealthMole said in a report](#) shared with Cyber Security News (CSN) that the apparent attack path is a marketplace and messaging ecosystem, not a disclosed software exploit.



ModernStealer had included the following Session ID (Source – StealthMole)

Listings can create pressure before verification, forcing organizations to assess samples and decide whether a claim signals compromise.

ModernStealer Threat Actor

The investigation began with a DarkForums post advertising an alleged document about a Türkiye-Pakistan drone partnership.

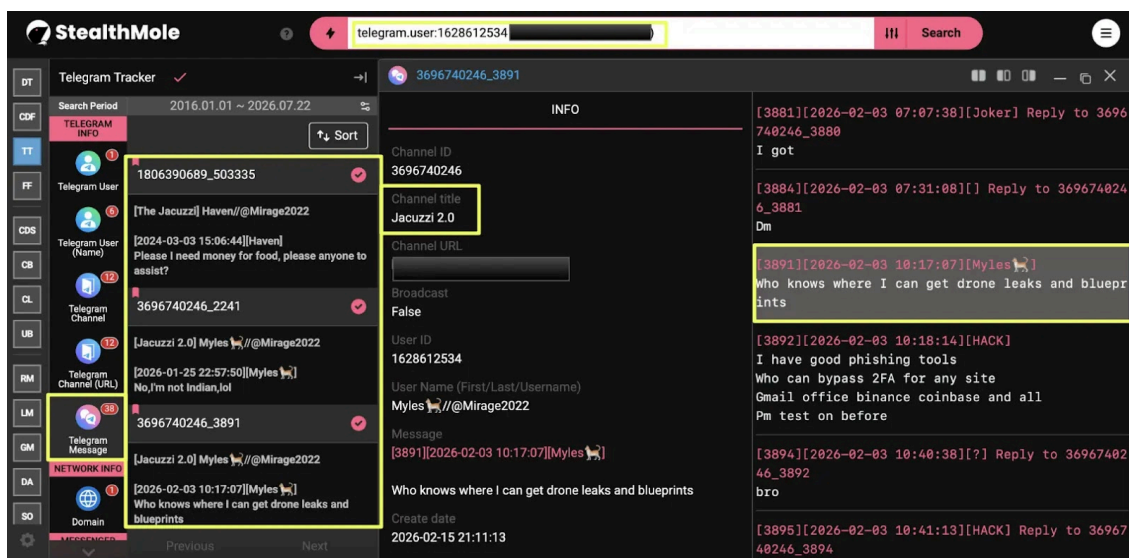
It cited Baykar Teknoloji, Pakistan's National Aerospace Science and Technology Park, technology transfer, training, joint research, localization, and procurement.

That post did not show who obtained the document, whether it was authentic, or whether a breach occurred.

Yet it gave researchers a useful starting point: a contact identifier that appeared again in a ModernStealer listing advertising an alleged Pakistan Nuclear Regulatory Authority database.

The searches found five ModernStealer listings and eight government-related listings. The posts named Pakistan's NUST and SUPARCO, Bangladesh's military, and US defence bodies.

The report stresses that these are claims, not confirmed intrusions. That caution is important because [dark web brokers repackaging](#) older or mixed data as new leaks, creating false urgency while defenders separate an incident from a sales pitch.



Drone leaks and blueprints (Source – StealthMole)

A recurring Session identifier widened the picture. It appeared in 30 indexed threads, including Zu1f1q4r posts advertising Pakistan military procurement, Intelligence Bureau material, and Federal Investigation Agency documents.

The shared identifier establishes an operational overlap, but it does not prove that ModernStealer and Zu1f1q4r are one person.

They could be separate operators sharing infrastructure or group members, so attribution should remain measured and evidence-led.

Telegram ties and response steps

The trail also reached a Telegram account identified as Sassoon Don. A message from that account used the same Session contact while seeking classified documents about Ukraine and Central Asian countries, and ModernStealer later listed the account directly as a contact option in military-document posts.

PriorOps used the same Telegram handle in a post claiming to offer a database of People's Liberation Army personnel.

This shows why [Telegram for initial access](#) and underground activity merit monitoring alongside forums: aliases may change, while operational contacts stay the same.

Researchers also noted a different Telegram user that later adopted the ModernStealer name and had previously asked about drone leaks and blueprints.

However, no persistent artifact connected it to the stronger ModernStealer, Sassoon Don, and Zu1f1q4r cluster, leaving it an unconfirmed lead rather than a proven alias.

For affected organizations, the practical response is to validate before escalating. Teams should preserve logs, compare samples with their records, reset exposed credentials when evidence supports it, and avoid amplifying unverified posts.

That discipline complements [evidence-based leak claim checks](#) when adversaries use visibility and uncertainty as leverage.

Defence and government organizations should review remote access, enforce phishing-resistant multi-factor authentication, remove unused accounts, and watch for unusual logins.

These measures matter where stolen credentials are brokered quickly, as shown in reporting on [low-cost infostealer malware](#) targeting high-value environments.

ModernStealer illustrates the value of following durable identifiers instead of trusting a forum name.

The evidence supports links among several accounts, but not a final conclusion about a single operator, and every advertised leak still requires independent verification.

Indicators of Compromise (IoCs):-

Type	Indicator	Description
Session ID	05214b*****f6163	Reused contact identifier in ModernStealer-linked listings;

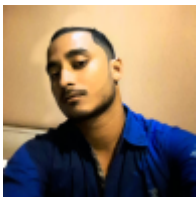
Type	Indicator	Description
		middle characters were redacted in the source.
Tox ID	65BB*****BC9D	Contact identifier listed in posts attributed to Zu1f1q4r; middle characters were redacted in the source.
Telegram username	@S*****n	Telegram contact linked to the Sassoon Don identity; username was redacted in the source.
Telegram User ID	7605334264	Immutable user identifier associated with the Sassoon Don account.
Telegram User ID	1628612534	Identifier for a separate account that later used the ModernStealer name.
Telegram channel ID	3990978039	Channel association listed for the Sassoon Don account.

Type	Indicator	Description
Telegram channel ID	3646663287	Channel association listed for the Sassoon Don account.
Telegram channel ID	3542147875	Channel association listed for the Sassoon Don account.
Defanged URL	https://darkforums.**/Thread****PK-TUR-PAK-DEFENSE-DRONE-DEAL	DarkForums listing concerning the alleged Türkiye-Pakistan defence drone deal.
Defanged URL	https://darkforums.**/Thr*****PK-Nuclear-Regulatory-Authority-PNRA-DATABASE	DarkForums listing claiming a Pakistan Nuclear Regulatory Authority database.
Defanged URL	https://breached.**/threads/pakistan-military-procurement****99/	Breached forum thread associated with Zu1f1q4r.
Defanged URL	https://breached.**/threads/intelligence-bureau-pakistan****1/	Breached thread claiming Pakistan Intelligence Bureau material.
Defanged URL	https://breached.**/threads/pakistan-fia-documents*****0/	Breached thread claiming

Type	Indicator	Description
		Pakistan Federal Investigation Agency documents.
Defanged URL	<code>https://t.me/Hexvi*****ach</code>	Telegram channel where the shared Session contact appeared.
Defanged URL	<code>https://breached.*****/showt*****669</code>	Breached.live thread associated with the PriorOps identity.

Note: IP addresses and domains are intentionally defanged (e.g., [.]) to prevent accidental resolution or hyperlinking. Re-fang only within controlled threat intelligence platforms such as MISP, VirusTotal, or your SIEM.

Building Resilience Against Phishing & Malware and Analyze it in a safe environment – [Power your SOC with ANY.RUN](#)



[Tushar Subhra Dutta](#)

Tushar is a senior cybersecurity and breach reporter. He specializes in covering cybersecurity news, trends, and emerging threats, data breaches, and malware attacks. With years of experience, he brings clarity and depth to complex security topics.

Source: <https://cybersecuritynews.com/modernstealer-threat-actor/>