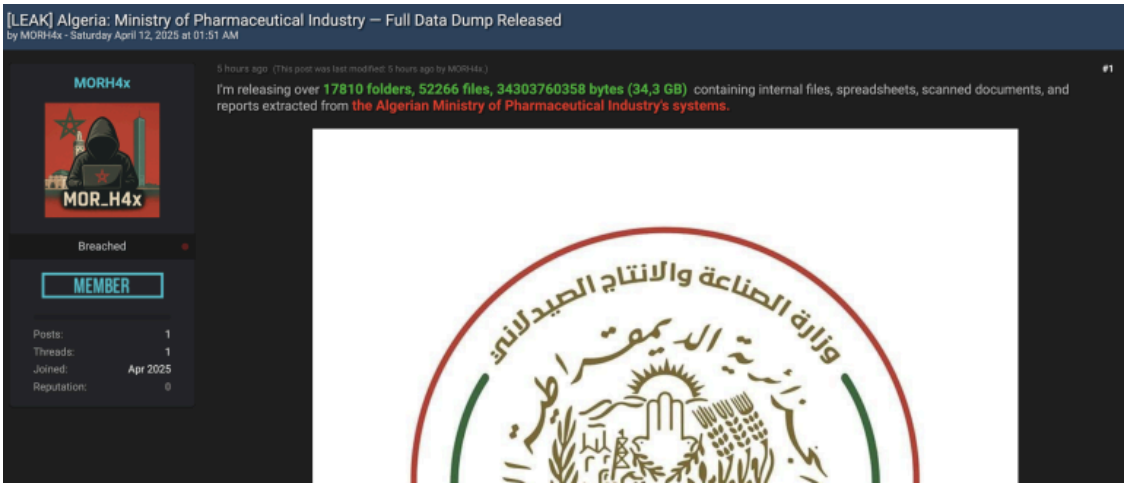
Algeria’s Ministry of Pharmaceutical Industry Data Leaked in Retaliatory Cyberattack - Cybersecurity88

By Chetna Sehgal

Published: 2025-04-12 · Archived: 2026-04-05 13:00:18 UTC

Today, we identified a new data breach involving the **Algerian Ministry of Pharmaceutical Industry**, with threat actor **MORH4x** listing **34.4GB** of internal data for sale on breach forums. The actor claims the breach includes extensive documentation related to Algeria’s pharmaceutical imports, personnel, inventory management, and psychotropic drug control.

The actor explicitly framed the breach as retaliation for the **April 8 CNSS breach in Morocco**, making this the latest move in a growing cycle of cyber escalation between Algeria and Morocco-while also aiming to expose the flow of medical imports into Algeria, identify which companies are profiting, and reveal how psychotropic medications are being distributed.



Context & Attribution

This breach is the third major incident in an escalating pattern of cyber activity involving Algerian and Moroccan entities as previously reported by us,

- **April 8, 2025:** Threat actor *Jabaroot* leaked extensive records from Morocco’s CNSS, exposing data of nearly **2 million employees** and over **499,000 companies**.
- **April 9, 2025:** Threat actor *Phantom Altars* released 13GB of internal files from Algeria’s MGPTT, reportedly in retaliation for the CNSS breach.
- **April 10, 2025:** *MORH4x* now targets the Algerian Ministry of Pharmaceutical Industry, citing the same motivation.

This series of events suggests a coordinated or ideologically-driven campaign of reciprocal cyberattacks, reflecting growing tensions between the two countries. Attribution remains uncertain, but indicators suggest

geopolitical motivations.

Related Reading: ***Algeria's MGPTT Data Listed for Sale After CNSS Breach***

The Listed Data

According to the listing, the leaked data spans from **2019 to 2025** and includes sensitive information across multiple areas of Algeria's pharmaceutical supply chain. The dataset includes:

- **3,368 folders:** Monthly records of imported medical devices and drugs (État mensuel des importations des dispositifs médicaux)
- Invoices and customs declarations: Product types, quantities, countries of origin, pricing, and importer details.
- **2,163 folders:** Files on commercial registers of pharmaceutical import firms.
- **804 folders:** Personnel data of company managers and technical directors, including criminal records, licenses, and ministry approval letters
- **64 folders:** Declarations of discrepancies in psychotropic drug inventories
- **1,754 folders:** Inventory declarations submitted by pharmaceutical distributors
- Drug stock reports, distribution lists for psychotropic substances, and official authorization documents

Additional files include internal notes on supply priorities by **Wilaya (province)**, employee names and contacts from both ministry staff and private pharmaceutical companies, and folders labeled Inventaire, Autorisation psychotrope, and Déclaration des écarts.

Note: While the threat actor also posted various documents as samples to validate the breach, we do not find it appropriate to share or republish those materials due to the sensitivity of the information involved. We also cannot independently verify the authenticity of the breach at this time.

Conclusion

This breach is the third major cyber event in what now appears to be a tit-for-tat campaign between threat actors operating in or aligned with Algeria and Morocco — a sequence we've actively reported on. These incidents highlight how **cyberwarfare** has become an extension of traditional geopolitical struggles, with political aspirations now fought on the digital front. As a result, the privacy of ordinary citizens is increasingly at risk, with sensitive personal data being exposed in the crossfire of these digital battles.
