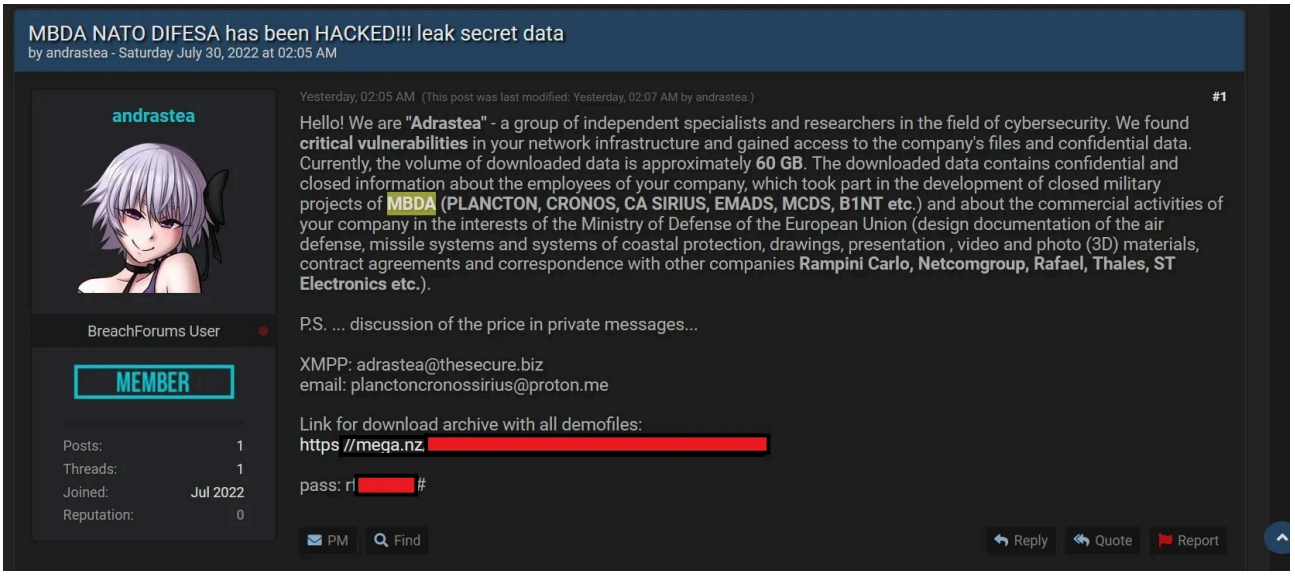
Threat actor claims to have hacked manufacturer of missiles MBDA

By Pierluigi Paganini

Published: 2022-07-31 · Archived: 2026-04-05 12:44:02 UTC



Threat actors that go online with the moniker Adrastea claim to have hacked the multinational manufacturer of missiles MBDA.

MBDA is a European multinational developer and manufacturer of missiles that was the result of the merger of the main French, British and Italian missile systems companies (Aérospatiale–Matra, BAE Systems, and Finmeccanica (now Leonardo). The name MBDA comes from the initialism of the names missile companies: Matra, BAe Dynamics and Alenia.

A threat actor that goes online with the moniker **Adrastea**, and that defines itself as a group of independent cybersecurity specialists and researchers, claims to have hacked **MBDA**.

Adrastea said that they have found critical vulnerabilities in the company infrastructure and have stolen 60 GB of confidential data.

The attackers said that the stolen data includes information about the employees of the company involved in military projects, commercial activities, contract agreements and correspondence with other companies.

*“Hello! We are **“Adrastea”** – a group of independent specialists and researchers in the field of cybersecurity. We found **critical vulnerabilities** in your network infrastructure and gained access to the company’s files and confidential data. Currently, the volume of downloaded data is approximately **60 GB**.” reads the adv published by the group on a popular hacker forum. “The downloaded data contains confidential and closed information about*

*the employees of your company, which took part in the development of closed military projects of **MBDA (PLANCTON, CRONOS, CA SIRIUS, EMADS, MCDS, B1NT etc**.) and about the commercial activities of your company in the interests of the Ministry of Defense of the European Union (design documentation of the air defense, missile systems and systems of coastal protection, drawings, presentation , video and photo (3D) materials, contract agreements and correspondence with other companies **Rampini Carlo, Netcomgroup, Rafael, Thales, ST Electronics etc.**).”*

As a proof of the hack Adrastea shared a link to a password-protected linked archive containing internal documents related to projects and correspondence.
At this time it is not clear if the threat actors have breached only one of the national divisions of the company, they did not disclose details about the attack.

Update: August 1 st, 2022

MBDA published the following press release confirming that its systems were not hacked. The origin of the data has already been ascertained, as they were acquired from an external hard drive. It has been confirmed that there has been no violation and / or compromise of the corporate networks. At present, the company’s internal verification processes indicate that the data that has been made available online are neither classified nor sensitive.

Follow me on Twitter: **@securityaffairs** and **Facebook**

[adrotate banner=”9″]	[adrotate banner=”12″]

Pierluigi Paganini

(SecurityAffairs – hacking, MBDA)

[adrotate banner=”5″]

[adrotate banner=”13″]

Source: https://securityaffairs.co/wordpress/133881/data-breach/mbda-alleged-data-breach.html