Spanish railway infrastructure manager ADIF infected with ransomware

By Pierluigi Paganini

Published: 2020-07-24 · Archived: 2026-04-05 12:34:42 UTC

ADIF, a Spanish state-owned railway infrastructure manager under the responsibility of the Ministry of Development, was hit by REVil ransomware operators.

Administrador de Infraestructuras Ferroviarias (ADIF), a Spanish state-owned railway infrastructure manager was hit by REVil ransomware operators.

ADIF (*Administrador de Infraestructuras Ferroviarias*) is charged with the management of most of Spain's railway infrastructure, that is the track, signaling and stations. It was formed in 2005 in response to European Union requirements to separate the natural monopoly of infrastructure management from the competitive operations of running train services.

The company has over 13,000 employees for a revenue of around $8 Billion.

The hackers claimed to have stolen 800GB of data including correspondence and contracts.

The incident was confirmed by Spanish media and security firms, including threat intelligence company Cyble.

As proof of the attack, REVil ransomware operators have posted a sample of data files exfiltrated from the company. If ADIF will refuse to pay the ransom, REvil ransomware operators will leak their confidential data online.

"Simultaneously with the publication, the third attack will follow," the reads a message posted on their leak site. "We will continue to download your data until you contact us."

Adif confirmed to IRJ that it has suffered a ransomware attack and added that its internal security services immediately mitigated it.

"The infrastructure has not been affected at any time, and the correct functioning of all its services has been guaranteed," the company says. "Adif, aware of being the manager of a critical infrastructure such as the exploitation of the railway network, considers cybersecurity as one of the pillars of comprehensive security."

"As per Cyble Research Team, the operators may have downloaded, what seems to be the company's confidential data such as ADIF's high-speed hiring committee contracts, property records, field works reports, project action plans, documents about customers, and much more." reads the post published by Cyble.

Below one of the sample data leaked by the threat actors:

This week REVil ransomware operators also hit Telecom Argentina, one of the largest internet service providers in Argentina, infecting roughly 18,000 computers during the weekend and now are asking for a $7.5 million ransom.

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

Pierluigi Paganini

(SecurityAffairs – hacking, ADIF)

[adrotate banner="5″]

[adrotate banner="13″]

Source: https://securityaffairs.co/wordpress/106304/cyber-crime/adif-revil-ransomware-attack.html