Maze ransomware group hacks oil giant; leaks data online

By Deeba Ahmed

Published: 2020-04-06 · Archived: 2026-04-05 22:31:33 UTC

On April 1st, 2020, Berkine became a victim of cyber-attack by the notorious Maze ransomware group that is known for its unique blackmailing practices.

The attackers managed to steal the entire database containing over 500MB of confidential documents related to budgets, organizational strategies, production quantities, and similar sensitive data.

The Maze ransomware group leaked the database containing information about the Sonatrach oil firm.

See: Terabytes of OnlyFans data being sold on hacking forum

Berkine is a joint venture of Algeria's state-owned oil firm Sonatrach and Anadarko Algeria Company, a subsidiary of a US-based firm previously known as Anadarko Petroleum Corp. and currently Oxy Occidental.

Discover more

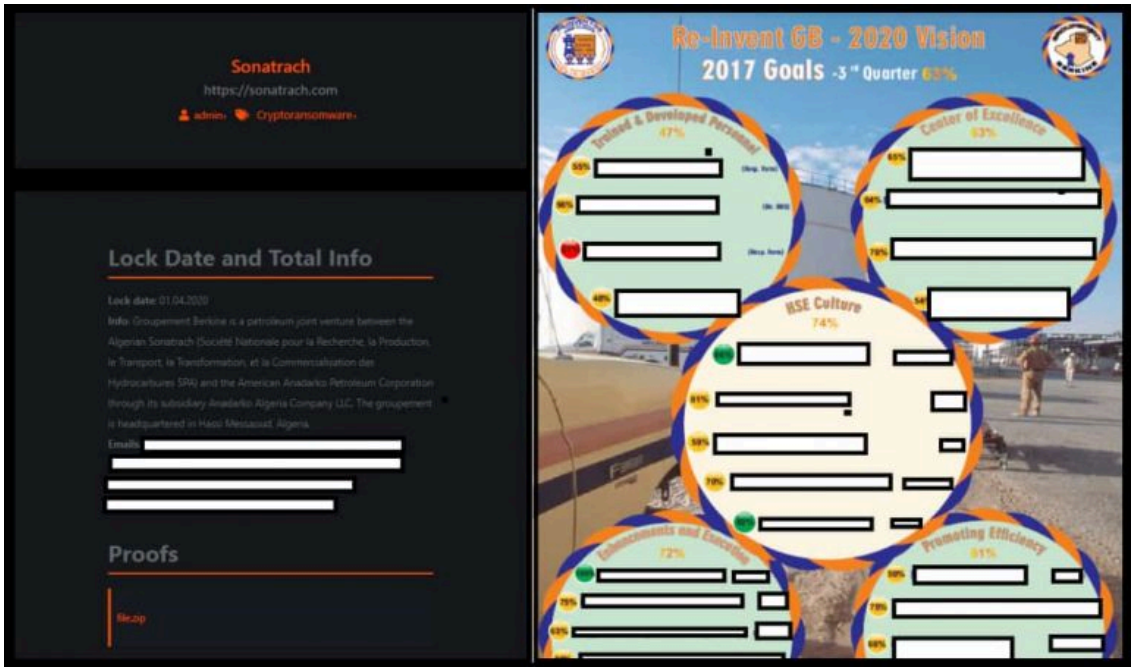
Hacking news portal

Penetration testing services

VPN subscriptions

According to Under the Breach, a service that exclusively monitors data breaches and works for its prevention stated that the documents posted online are related to financial details and investment plans of the company.

The leaked data includes the Berkine group's cost price per barrel, organizational goals for the year 2020, and budgets allocated for various missions of the two owners of Berkine. The database also contains a list of Berkine employees including their contact details and travel documents of some of them.



The screenshot shows leaked data on Maze ransomware group's website (Via Under The Breach)

The maze ransomware group has quickly become the biggest threat to organizations around the world. The French National Agency for Security of Information Systems (ANSSI) examined this group after it attacked a subsidiary of Bouygues in January 2020.

See: Digital wallet app leaks millions of users' credit cards & Govt IDs

As per the ANSSI, the group has been active since May 2019 and "is mainly known to be associated with Internet disclosures of information presented as originating from compromised information systems".

Discover more

Apple security patches

Internet & Telecom

Identity Theft Protection

The Maze ransomware, assessed ANSSI, is a variant of the ChaCha20 cryptographic algorithm, which is one of the most feared data encryption software.

The agency also identified that the group employs extreme tactics to pressurize the victims who refuse to pay the ransom or delay the payment. They, not only encrypt the data but also exfiltrate it prior to encrypting it and later use it to blackmail the victim into paying their desired ransom.

Moreover, the group keeps releasing some of the data and even post it on hacker forums for phishing purposes if the victim doesn't give in to their demands.

Did you enjoy reading this article? Like our page on Facebook and follow us on Twitter.

Source: https://www.hackread.com/maze-ransomware-group-hacks-oil-giant-leaks-data/