

Ransomware

Ecopetrol confirms ransomware attempt, data stolen from 3,300 accounts

July 20, 2026

 Share

By SC Staff



(Adobe Stock)

Ecopetrol, a Latin American energy producer, has confirmed a ransomware attack where attackers stole data from 3,300 user accounts but were prevented from deploying an encryptor due to security controls, according to a recent report by Tech Radar.

The incident involved an unidentified threat actor accessing **Ecopetrol**'s IT infrastructure and exfiltrating pseudonymous data from 3,300 user accounts. While the attackers attempted to install an encryptor, the

Cookies

This website uses cookies to improve your experience, provide social media features and deliver advertising offers that are relevant to you. If you continue without changing your settings, you consent to our use of cookies in accordance with our [privacy policy](#). You may disable cookies.

[Accept Cookies](#)

publicly disclosed thus far. The stolen files are reported to be pseudonymous, potentially limiting their utility to the attackers.

Source: [Tech Radar](#)

An In-Depth Guide to Ransomware

Get essential knowledge and practical strategies to protect your organization from ransomware attacks.

[Learn More](#)



[SC Staff](#)

Related

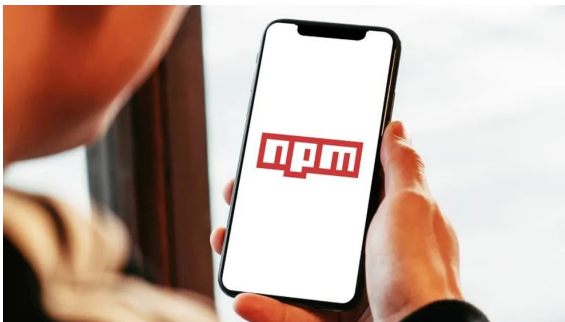


BREACH

Craneware confirms customer and employee data exposed in security incident

[SC Staff](#) July 20, 2026

The breach, which occurred on July 20, saw a significant volume of file names viewed and exfiltrated by unauthorized individuals.



SUPPLY CHAIN

New npm malware cluster targets Vite ecosystem

[SC Staff](#) July 20, 2026

The ViteVenom campaign, attributed to the threat actor SuccessKey, builds upon the tactics seen in the earlier ChainVeil attack.

Cookies

This website uses cookies to improve your experience, provide social media features and deliver advertising offers that are relevant to you. If you continue without changing your settings, you consent to our use of cookies in accordance with our [privacy policy](#). You may disable cookies.



[SC Staff](#) July 17, 2026

Microsoft has detailed two primary intrusion chains used by ACR Stealer.

Related Events

CYBERCAST

Ransomware reloaded: Finding resilience when attackers wield AI

On-Demand Event

VIRTUAL CONFERENCE

Ransomware Resilience: Strategies to Defend, Mitigate, and Recover

On-Demand Event

GET DAILY EMAIL UPDATES

SC Media's daily must-read of the most current and pressing daily news

Business Email*

By clicking the Subscribe button below, you agree to SC Media [Terms of Use](#) and [Privacy Policy](#).

SUBSCRIBE



ABOUT US

[SC Media](#) | [CyberRisk Alliance](#) | [Contact Us](#) | [Careers](#) | [Privacy](#)

Cookies

This website uses cookies to improve your experience, provide social media features and deliver advertising offers that are relevant to you. If you continue without changing your settings, you consent to our use of cookies in accordance with our [privacy policy](#). You may disable cookies.



Cookies

This website uses cookies to improve your experience, provide social media features and deliver advertising offers that are relevant to you. If you continue without changing your settings, you consent to our use of cookies in accordance with our [privacy policy](#). You may disable cookies.