Ransomware gang demands $7.5 million from Argentinian ISP

By Catalin Cimpanu

Published: 2020-07-20 · Archived: 2026-04-05 21:43:01 UTC

A ransomware gang has infected the internal network of Telecom Argentina, one of the country's largest internet service providers, and is now asking for a $7.5 million ransom demand to unlock encrypted files.

The incident took place over the weekend, on Saturday, July 18, and is considered one of Argentina's biggest hacks.

Sources inside the ISP said hackers caused extensive damage to the company's network after they managed to gain control over an internal Domain Admin, from where they spread and installed their ransomware payload to more than 18,000 workstations.

The incident did not cause internet connectivity to go down for the ISP's customers, nor did it affect fixed telephony or cable TV services; however, many of Telecom Argentina's official websites have been down since Saturday.

Since the attack's onset, multiple Telecom employees have now also taken to social media to share details about the incident, and how the ISP has been managing the crisis.

According to images shared online, the ISP appears to have detected the intrusion right away and has been actively warning employees through internal alerts to limit their interaction with the corporate network, not to connect to its internal VPN network, and not open emails containing archive files.


telecom-revil-internal-alert.jpg
Image source: [protected]


telecom-revil-warning.jpg
Image source: [protected]

The attackers have also been identified as the REvil (Sodinokibi) ransomware group, according to a now-deleted tweet showing the ransomware gang's dark web portal -- the page where victims are directed to make payments.

This web page currently shows a ransom demand of 109345.35 Monero coins (~$7.53 million), a sum that will double after three days, making this one of the largest ransom demands requested in a ransomware attack this year.


telecom-revil-page.png
Image source: [unknown]

Telecom Argentina has not commented on the incident, when contacted by local press, and did not say if it intends to pay the ransom demand.

Local media has also reported that the ISP believes the hacker's point of entry is a malicious email attachment received by one of its employees, but this does not generally fit with the REvil gang's normal modus operandi.

According to a report from security firm Advanced Intel, for the past year, the REvil gang has specialized in carrying out network-based intrusions, targeting unpatched networking equipment as the entry point into victim organizations, and before spreading laterally through a company's network.

In the past, REVil operators have targeted Pulse Secure and Citrix VPN and enterprise gateway systems as entry points.

In a conversation on Sunday, threat intelligence company Bad Packets has told ZDNet that Telecom Argentina not only ran Citrix VPN servers, but had also ran a Citrix instance vulnerable to the CVE-2019-19781 security bug months after a patch had been made available.

Some security researchers have pointed the finger at two files uploaded on the VirusTotal web antivirus scanner as being used in the Telecom Argentina attack, although we could not immediately verify this claim.

The REvil ransomware gang also maintains a dark web portal where it leaks data it stole from infected hosts in case the companies don't pay. At the time of writing, the REvil "leak site" did not list Telecom Argentina as one of the victim organizations the REvil gang planned to leak files from.

This is also the REvil gang's second attack against the network of an internet service provider. The REvil gang also targeted Sri Lanka Telecom, the largest fixed telephony provider in Sri Lanka, in May.
