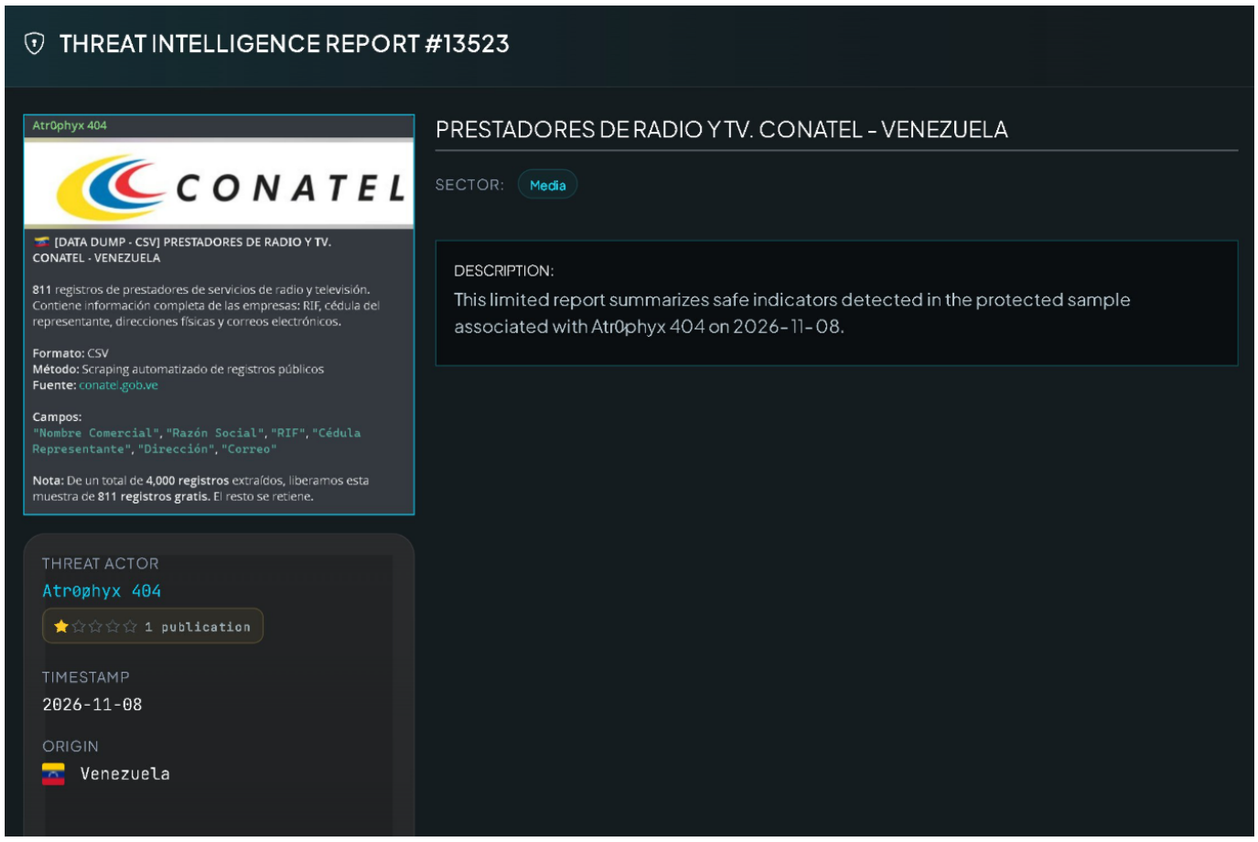
Filtran presuntos datos de miles de proveedores de radio y televisión registrados en Conatel

Una presunta filtración de datos relacionados con proveedores de servicios de radio y televisión registrados en la Comisión Nacional de Telecomunicaciones (Conatel) fue reportada el pasado sábado por el observador de ciberseguridad VECERT Analyzer, que atribuyó el incidente al actor identificado como “Y3rk404”, integrante del grupo de piratas informáticos “Atr0phyx 404 Crew”.

De acuerdo con la alerta difundida por la plataforma, el actor habría publicado una muestra de 811 registros en un archivo CSV denominado “prestadores_venezuela_completo.csv”. El grupo asegura que obtuvo aproximadamente 4.000 registros en total y que mantiene bajo su control el resto de la información.

La muestra contendría datos de empresas operadoras y titulares de permisos registrados ante Conatel, entre ellos nombres comerciales, razones sociales, números de identificación fiscal (RIF), cédulas de identidad de representantes legales, direcciones físicas y correos electrónicos corporativos.

Según el reporte, la extracción de estos datos se habría realizado mediante técnicas de “scraping” (“extraer”, “arrastrar”), un procedimiento automatizado que permite recopilar información disponible en páginas web y directorios públicos.



Piratas informáticos filtran presuntos datos de miles de proveedores de radio y televisión registrados en Conatel.

Riesgos de exposición de información

Aunque la información descrita estaría vinculada con registros institucionales, la eventual divulgación masiva de estos datos podría generar riesgos para las empresas y sus representantes legales, especialmente ante posibles intentos de suplantación de identidad, fraude e ingeniería social.

La exposición de números de identificación fiscal, documentos de identidad, direcciones físicas y correos electrónicos podría facilitar la elaboración de comunicaciones fraudulentas dirigidas a operadores de radio y televisión o a sus responsables administrativos.

Ante este escenario, VECERT Analyzer recomendó revisar los mecanismos de acceso a los directorios públicos de Conatel e implementar medidas de protección frente a la extracción automatizada de información. También planteó alertar a los representantes legales de las empresas que pudieran estar involucradas.

?? ?? ? ?? PREVENTIVE ALERT — ALLEGED DATA EXFILTRATION REGARDING CONATEL SERVICE PROVIDERS IN VENEZUELA (ACTOR: Y3RK404 / ATR0PHYX 404)

[STATUS: ALLEGED / UNCONFIRMED / THREAT ACTOR: Y3RK404 / ATR0PHYX 404 CREW / DATE: NOVEMBER 7, 2026]

Centralized cyber-intelligence systems have intercepted a post on clandestine channels (recorded on November 7, 2026) regarding a data exfiltration and dump by the actor Y3rk404, representing the group Atr0phyx 404 Crew. The report announces the alleged release of a sample containing 811 records of radio and television service providers registered with the National Telecommunications Commission (CONATEL) in Venezuela (https://t.co/YJ9cDdPFbA), obtained through automated data extraction (scraping) from public records.

The actor states that the total extracted repository amounts to approximately 4,000 records, with the remainder currently being withheld. The released sample, in CSV format (`prestadores_venezuela_completo.csv`), contains detailed information regarding the operating companies and permit holders.

It is strictly noted that the veracity of this intrusion, the method used to obtain the data, and the overall authenticity of the exposed records have not been officially confirmed by CONATEL or any incident response centers in Venezuela.

Threat Actor: Y3rk404 (Atr0phyx 404 Crew).

Victim / Target: CONATEL (National Telecommunications Commission) / Radio and Television Service Providers – ?? Venezuela.

Sector: ? Telecommunications, Broadcasting, Media, and Government Regulation.

Publication Date: November 7, 2026.

Reported Volume: A sample of 811 records (from an estimated total of 4,000 records in the repository).

Nature of the Incident: Alleged mass data extraction via scraping of institutional portals, involving the exfiltration of tax information, contact details, and data pertaining to legal representatives.

? TECHNICAL BREAKDOWN OF THE COMPROMISED INFORMATION (ALLEGED)

Based on the field structure provided by the author in the CSV file, the exposed data includes:

Corporate and Tax Data: Trade name, legal business name of the operating entity, and Tax Identification Number (RIF).

Representation and Contact Information: Identification number

(national ID) of the legal representative, physical addresses of stations or offices, and corporate or institutional email addresses.

CSV File Field Schema:

“Trade Name”
“Legal Business Name”
“Tax ID (RIF)”
“Representative’s ID”
“Address”
“Email”

?? TECHNICAL PREVENTIVE AND CONTAINMENT RECOMMENDATIONS (SOC / CSIRT / INSTITUTIONAL)

Audit and Restriction of Public Endpoints: CONATEL’s technical teams should review access control policies and anti-scraping mechanisms (protections against automated data extraction) applied to their online directories and public registries.

Protection Against Fraud and Impersonation: Given the exposure of corporate Tax IDs (RIFs), physical addresses, and email addresses belonging to media outlets and broadcasters, it is advised to alert legal representatives to help prevent social engineering attempts or institutional impersonation.

?? CENTRALIZED THREAT MONITORING SYSTEM

Intelligence System: https://t.co/wk9bZJ2Nli

Quickly check your security at: https://t.co/QZhWp0kFrO

Quotes and services: https://t.co/sx3BM5zbnK

#Venezuela #CONATEL #RadioTV #DataLeak #DataBreach #BreachAlert #DarkWeb #Hacking #ThreatIntel #ThreatIntelligence #InfoSec #CyberAlert #VECERT #SOC #CSIRT #Unconfirmed #SecurityAlert #CyberDefense #CyberRisk

— VECERT Analyzer (@VECERTRadar) November 8, 2026

Incidente sin confirmación oficial

VECERT Analyzer subrayó que la presunta intrusión, el método utilizado para obtener los registros y la autenticidad de los

datos divulgados no han sido confirmados oficialmente por Conatel ni por algún centro de respuesta a incidentes de Venezuela.

Por tanto, tampoco existe confirmación independiente sobre la totalidad de los aproximadamente 4.000 registros que el actor asegura haber obtenido.

La alerta constituye, por ahora, un reporte preventivo sobre una posible exposición de información vinculada con el sector de telecomunicaciones venezolano.

la Patilla