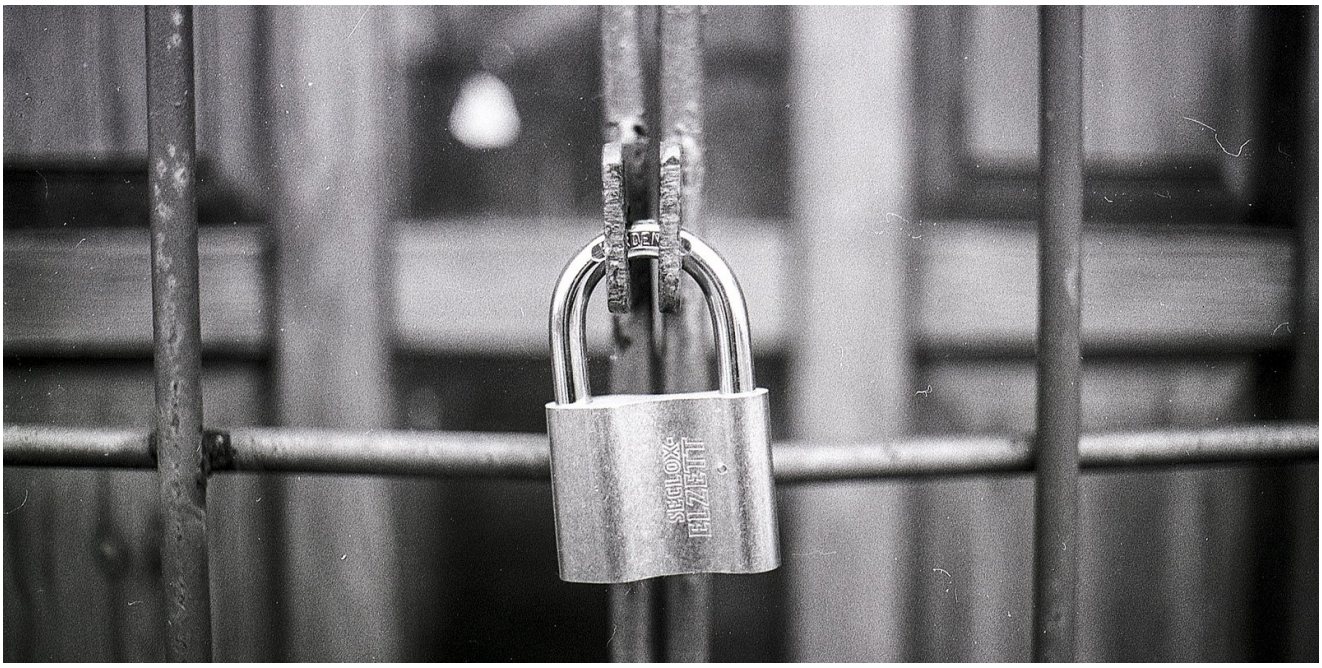
Ecuador's state-run CNT telco hit by RansomEXX ransomware

bleepingcomputer.com/news/security/ecuadors-state-run-cnt-telco-hit-by-ransomexx-ransomware/

Lawrence Abrams

By
Lawrence Abrams

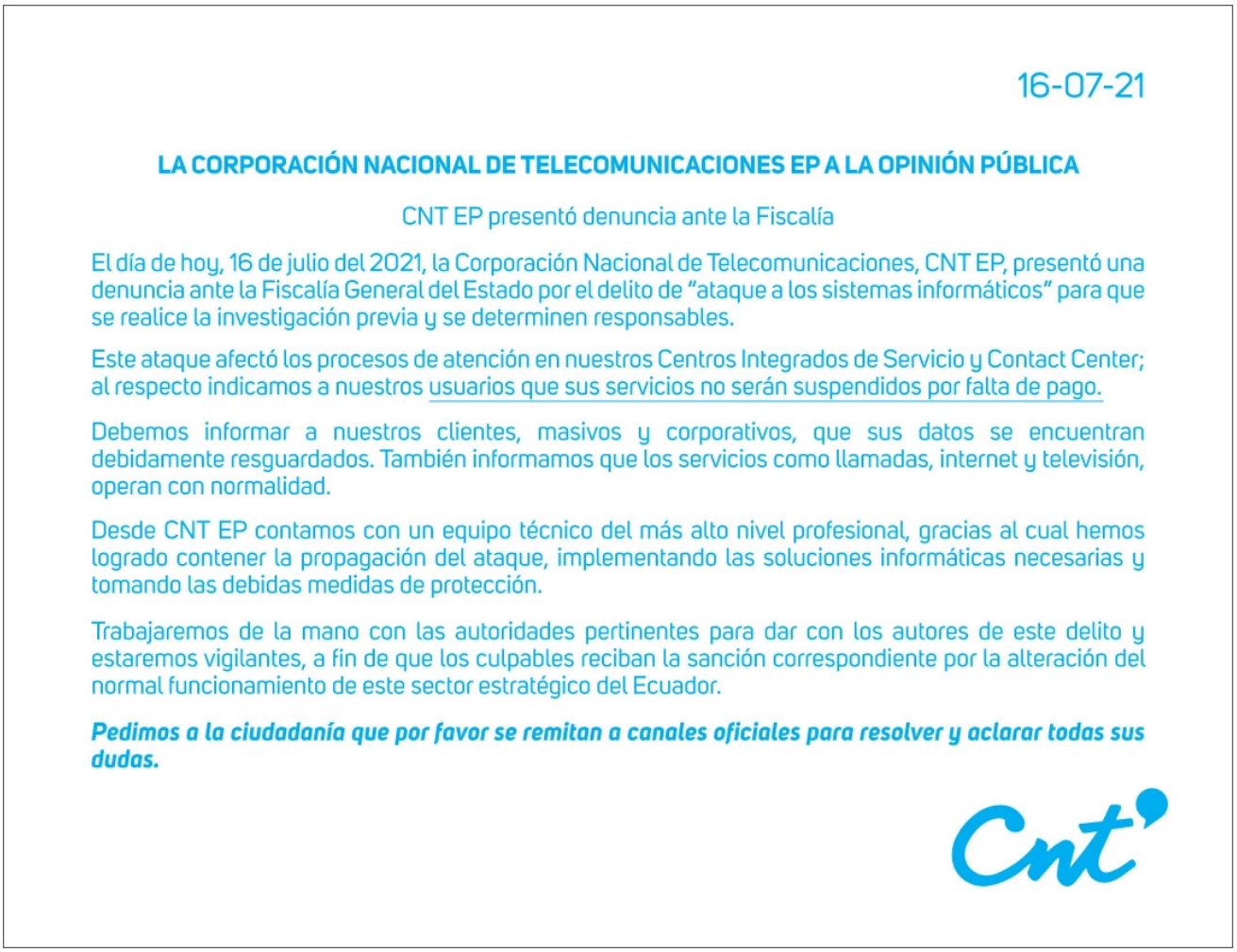
- July 17, 2021
- 09:53 AM
- 0



Ecuador's state-run Corporación Nacional de Telecomunicación (CNT) has suffered a ransomware attack that has disrupted business operations, the payment portal, and customer support.

CNT is Ecuador's state-run telecommunication carrier that offers fixed-line phone service, mobile, satellite TV, and internet connectivity.

Starting this week, the CNT website began displaying an alert warning that they suffered an attack and that customer care and online payment are no longer accessible.



16-07-21

LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES EP A LA OPINIÓN PÚBLICA

CNT EP presentó denuncia ante la Fiscalía

El día de hoy, 16 de julio del 2021, la Corporación Nacional de Telecomunicaciones, CNT EP, presentó una denuncia ante la Fiscalía General del Estado por el delito de "ataque a los sistemas informáticos" para que se realice la investigación previa y se determinen responsables.

Este ataque afectó los procesos de atención en nuestros Centros Integrados de Servicio y Contact Center; al respecto indicamos a nuestros usuarios que sus servicios no serán suspendidos por falta de pago.

Debemos informar a nuestros clientes, masivos y corporativos, que sus datos se encuentran debidamente resguardados. También informamos que los servicios como llamadas, internet y televisión, operan con normalidad.

Desde CNT EP contamos con un equipo técnico del más alto nivel profesional, gracias al cual hemos logrado contener la propagación del ataque, implementando las soluciones informáticas necesarias y tomando las debidas medidas de protección.

Trabajaremos de la mano con las autoridades pertinentes para dar con los autores de este delito y estaremos vigilantes, a fin de que los culpables reciban la sanción correspondiente por la alteración del normal funcionamiento de este sector estratégico del Ecuador.

Pedimos a la ciudadanía que por favor se remitan a canales oficiales para resolver y aclarar todas sus dudas.

Cnt

Announcement on the website about the cyberattack

"Today, July 16, 2021, the National Telecommunications Corporation, CNT EP, filed a complaint with the State Attorney General's Office for the crime of "attack on computer systems "so that the preliminary investigation is carried out and the responsible," read the alert translated into English.

"This attack affected the care processes in our Integrated Service Centers and Contact Center; In this regard, we indicate to our users that their services will not be suspended for non-payment."

"We must inform our clients, massive and corporate, that their data is They are duly protected. We also inform that services such as calls, internet and television, operate normally."

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

CNT suffers RansomEXX ransomware attack

While CNT has not officially stated that they suffered a ransomware attack, BleepingComputer has learned that the attack was conducted by a ransomware operation known as RansomEXX.

Security researcher Germán Fernández shared with BleepingComputer a hidden link to the group's data leak site that warns CNT that the gang would leak data stolen during the attack if CNT did not pay a ransom.

> "Your time is **LIMITED**!
> When this time will come to end, there are two ways: we will **RAISE** the ransom amount or **PUBLISH** your files.
> You will lose the opportunity to contact us after the data **PUBLICATION**.
> If you **REALLY WANT** to prevent data leak, contact us **RIGHT NOW**.
>
> We have downloaded 190GB+ of your files and we are ready to publish it." - RansomEXX.

Hidden RansomEXX data leak page for CNT

This page is currently hidden from the public and can only be accessed via the direct link. These hidden pages are commonly included in ransom notes to prove that a ransomware operation stole data during an attack.

In CNT's press statement, the company states that corporate and customer data are secure and have not been exposed.

However, the RansomEXX gang claims to have stolen 190 GB of data and shared screenshots of some of the documents on the hidden data leak page.

The screenshots seen by BleepingComputer, include contact lists, contracts, and support logs.

The ransomware operation originally launched under the name Defray in 2018 but became more active in June 2020 when it rebranded as RansomEXX and began to target large corporate entities.

Like other ransomware gangs, RansomEXX will compromise a network through purchased credentials, brute-forced RDP servers, or by utilizing exploits.

Once they gain access to a network, they will quietly spread throughout the network while stealing unencrypted files to be used for extortion attempts.

After gaining access to an administrator password, they deploy the ransomware on the network and encrypt all of its devices.

As is becoming common among ransomware operations, RansomEXX created a Linux version to ensure they can target all critical servers and virtual machines.

The RansomEXX gang's has a history of high-profile attacks, including Brazil's government networks, Texas Department of Transportation (TxDOT), Konica Minolta, IPG Photonics, and Tyler Technologies.

BleepingComputer has contacted CNT with further questions but has not received a response at this time.

Related Articles:

Luxury fashion house Zegna confirms August ransomware attack

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Google shut down caching servers at two Russian ISPs

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.