Netwalker ransomware hits Argentinian government, demands $4 million

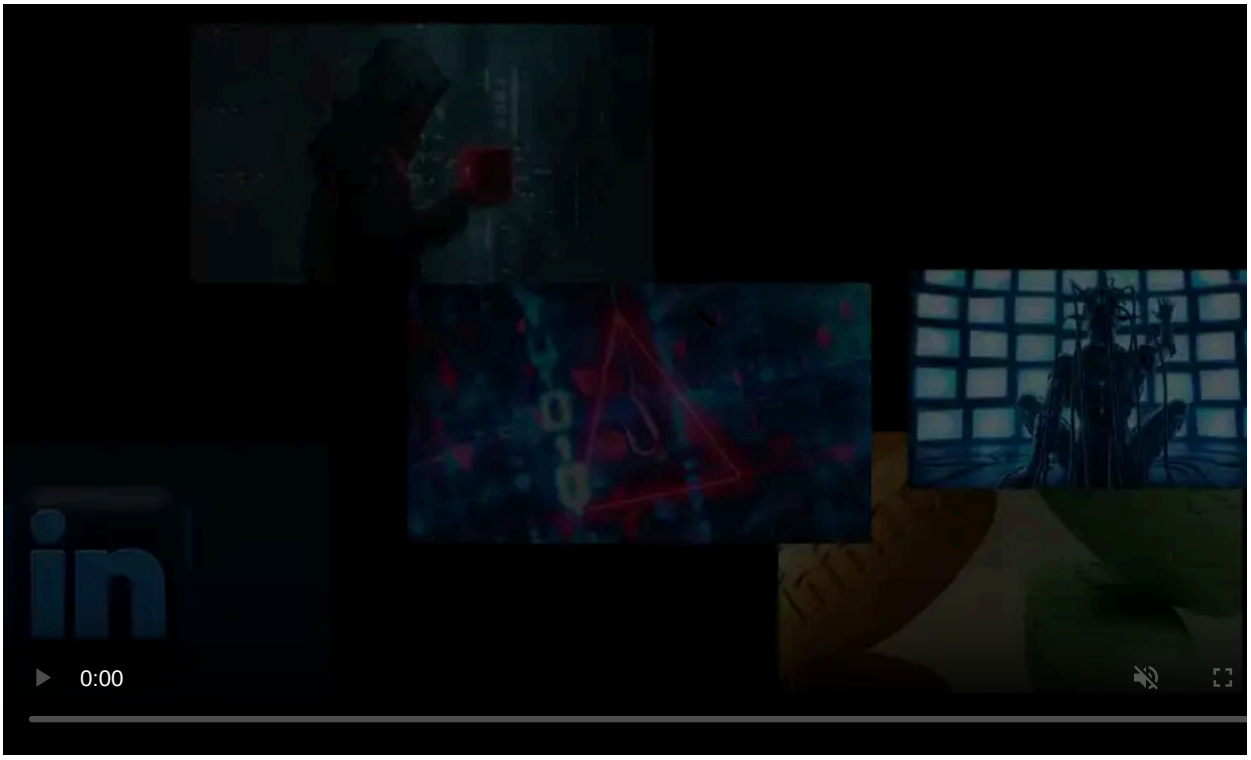
By Lawrence Abrams

Published: 2020-09-06 · Archived: 2026-04-05 18:10:53 UTC

Argentina's official immigration agency, Dirección Nacional de Migraciones, suffered a Netwalker ransomware attack that temporarily halted border crossing into and out of the country.

While ransomware attacks against cities and local agencies have become all too common, this may be a first known attack against a federal agency that has interrupted a country's operations.

According to a criminal complaint published by Argentina's cybercrime agency, Unidad Fiscal Especializada en Ciberdelincuencia, the government first learned of the ransomware attack after receiving numerous tech support calls from checkpoints at approximately 7 AM on August 27th.


0:00

"Being approximately 7 a.m. of the day indicated in the paragraph above, the Directorate of Technology and Communications under the Directorate General Information Systems and Technologies of this Organization received numerous calls from various checkpoints requesting technical support."

"This realized that it was not an ordinary situation, so it was evaluated the situation of the infrastructure of the Central Data Center and Servers Distributed, noting activity of a virus that had affected the systems MS Windows based files (ADAD SYSVOL and SYSTEM CENTER DPM mainly) and Microsoft Office files (Word, Excel, etc.) existing in users' jobs and shared folders," a translation of the complaint stated.

To prevent the ransomware from infecting further devices, the computer networks used by the immigration offices and control posts were shut down.

According to Argentinian news site Infobae, this led to a temporary suspension of border crossings for four hours while the servers were brought back online.

"The Comprehensive Migration Capture System (SICaM) that operates in international crossings was particularly affected, which caused delays in entry and exit to the national territory," the National Directorate of Migration (DNM) stated.

Government sources told Infobae that "they will not negotiate with hackers and neither they are too concerned with getting that data back."

If you have first-hand information about this attack or know of other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731.

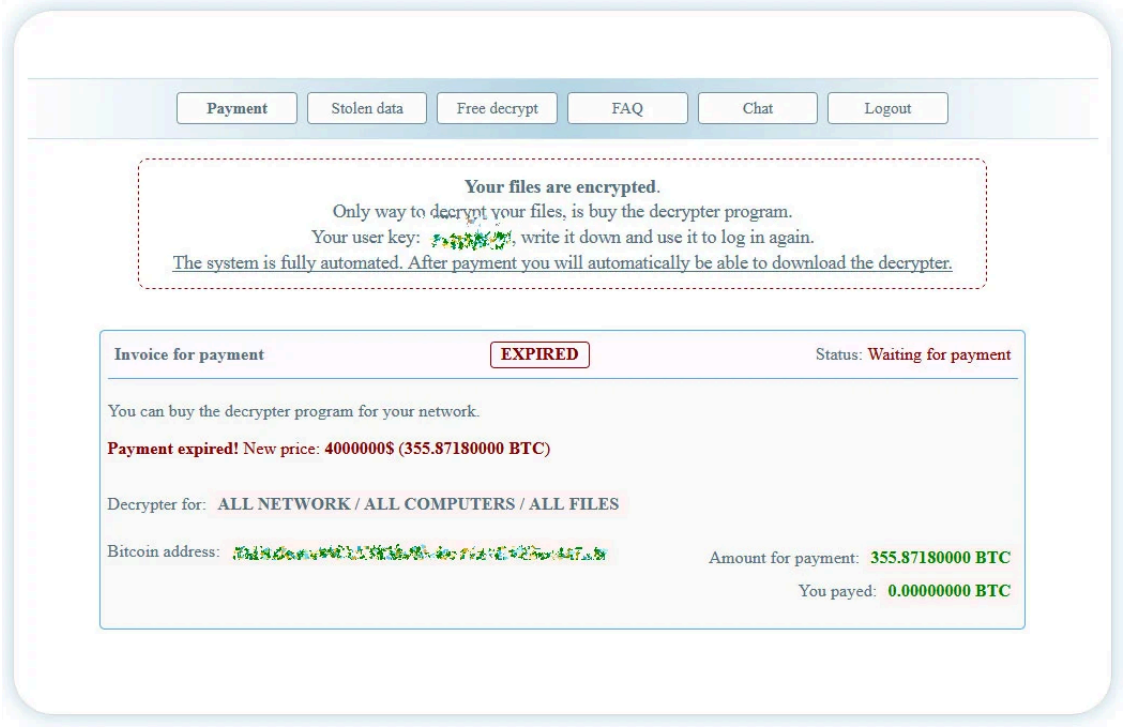
Netwalker demands a $4 million ransom

When the Netwalker performs a ransomware attack, ransom notes will be left on devices that have been encrypted.

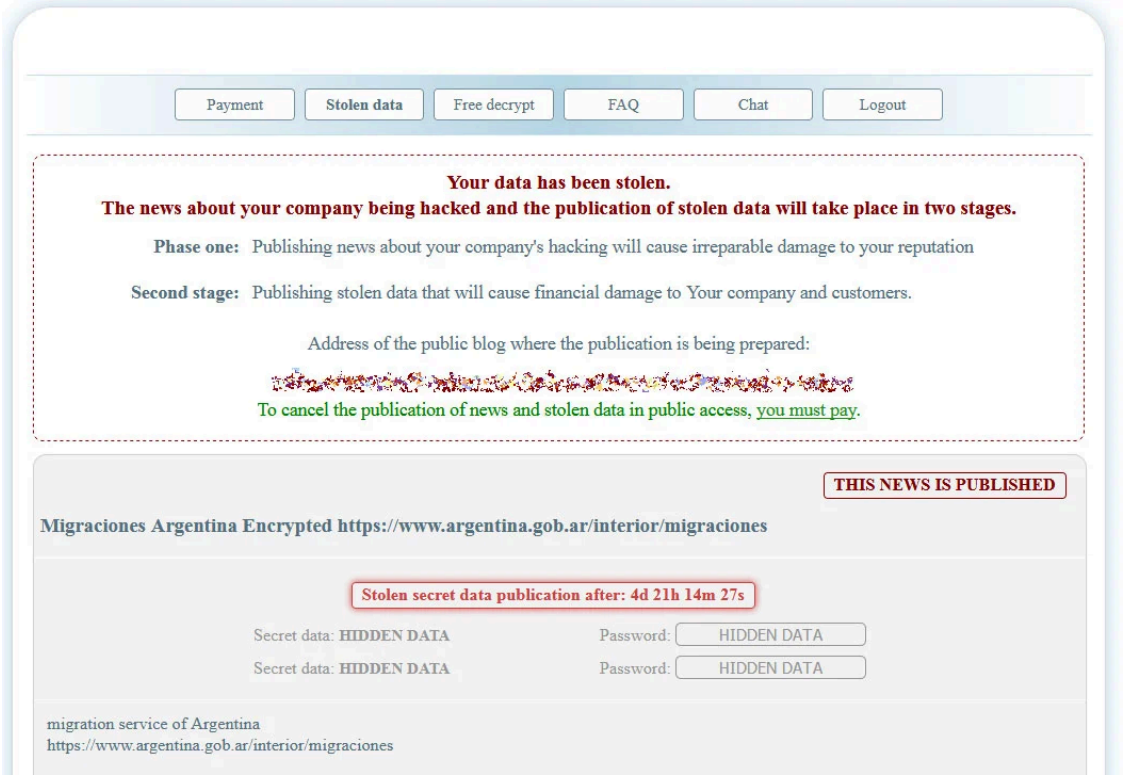
These ransom notes contain links to a dark web payment site that contains information on how to purchase a decryptor, the ransom amount, and information about any unencrypted files that were stolen during the attack.

From a Netwalker Tor payment page shared with BleepingComputer, we have learned that the ransomware actors initially demanded a $2 million ransom.

After seven days passed, the ransom increased to $4 million, or approximately 355 bitcoins, as shown below in the image of Dirección Nacional de Migraciones's ransom page.



This Tor site also includes a 'Stolen Data' page that displays a screenshot of data stolen from "Migraciones Argentina" during this attack.



Due to this leaked data's potentially sensitive nature, BleepingComputer has decided not to post the data leak screenshots.

Source: https://www.bleepingcomputer.com/news/security/netwalker-ransomware-hits-argentinian-government-demands-4-million/