Retail giant Cencosud hit by Egregor Ransomware attack, stores impacted

bleepingcomputer.com/news/security/retail-giant-cencosud-hit-by-egregor-ransomware-attack-stores-impacted/

Lawrence Abrams

By
Lawrence Abrams

- November 14, 2020
- 07:07 PM
- 0

Chilean-based multinational retail company Cencosud has suffered a cyberattack by the Egregor ransomware operation that impacts services at stores.

Cencosud is one of the largest retail companies in Latin America, with over 140,000 employees and $15 billion in revenue for 2019. Cencosud manages a wide variety of stores in Argentina, Brazil, Chile, Colombia, and Peru, including Easy home goods, Jumbo supermarkets, and the Paris department stores.

This weekend, Cencosud was hit with a ransomware attack that encrypted devices throughout their retail outlets and impacted the company's operations.

According to Argentinian publisher Clarín, retail stores are still open, but some services are impacted.

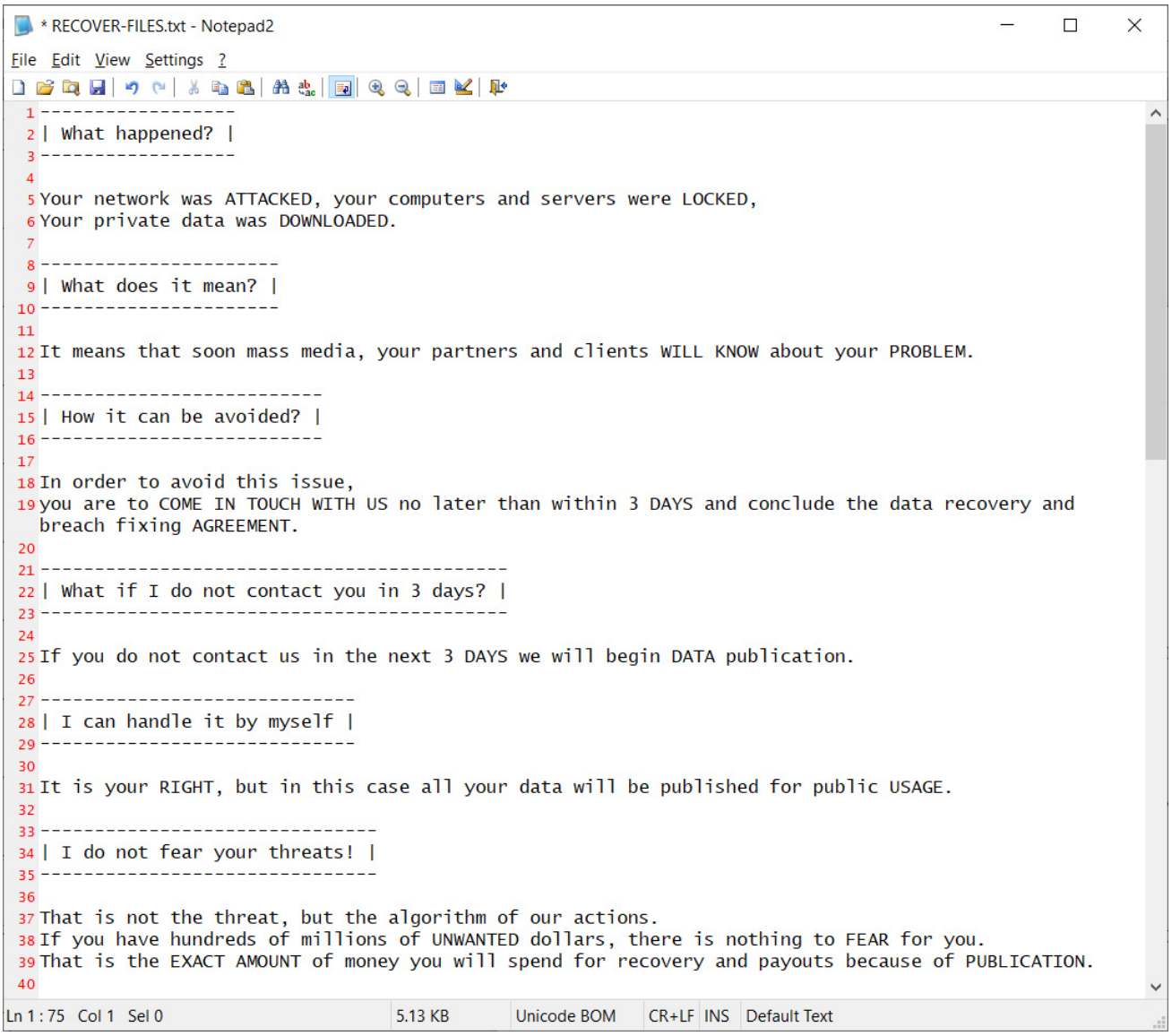
For example, an Easy store in Buenos Aires is displaying a sign warning customers that they are not accepting the 'Cencosud Card' credit card, accepting returns, or allowing the pickup of web purchases due to technical problems.

Sign outside Easy store in Buenos Aires
Source: Daniel Monastersky

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.

Egregor behind ransomware attack

After learning of the attack, BleepingComputer obtain the ransom note and can confirm it was conducted by Egregor and targeted the 'Cencosud' Windows domain.



Cencosud's Egregor ransom note

Egregor is a ransomware-as-a-service operation that began operating in the middle of September, just as another ransomware group known as Maze started shutting down their operation. BleepingComputer has learned from threat actors that many hackers who partnered with Maze are now working with Egregor.

Clarín also reported that printers in numerous retail outlets in Chile and Argentina, such as Easy home goods stores, began printing out ransom notes as devices are encrypted.

This function is a known "feature" of the Egregor ransomware software, which will automatically print ransom notes to attached printers after the files on a device have been encrypted. For network-wide attacks, this could potentially lead to thousands of ransom notes being printed throughout the organization.

The ransom note does not provide links to proof of stolen data, but Egregor has a history of stealing unencrypted files before deploying their ransomware.

Egregor has been responsible for other high profile attacks on Crytek, Ubisoft, and Barnes and Noble.

BleepingComputer has contacted Cencosud with further questions but has not heard back.

Related Articles:

Windows 11 KB5014019 breaks Trend Micro ransomware protection

Industrial Spy data extortion market gets into the ransomware game

New ‘Cheers’ Linux ransomware targets VMware ESXi servers

SpiceJet airline passengers stranded after ransomware attack

US Senate: Govt’s ransomware fight hindered by limited reporting

- Cencosud
- Egregor
- Latin America
- Ransomware

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.

- Previous Article
- Next Article

You may also like: