The Threat of Brazilian Grandoreiro Banking Malware | Proofpoint US

By October 23, 2023 Jared Peck

Published: 2023-10-09 · Archived: 2026-04-05 16:09:59 UTC

Key Takeaways

- A new version of Grandoreiro malware from TA2725 targets both Mexico and Spain. Previously this malware has only targeted victims in Brazil and Mexico.

Overview

Proofpoint researchers have long tracked clusters of malicious activity using banking malware to target users and organizations in Brazil and surrounding countries. Recently, researchers observed multiple threat clusters targeting Spain from threat actors and malware that have traditionally targeted Portuguese and Spanish speakers in Brazil, Mexico, and other parts of the Americas. While the targeting of victims in the Americas has been common for some time, recent clusters targeting Spain have been unusual in frequency and volume compared to previous activity.

Brazilian Cyber Threat Landscape

The Brazilian cyber threat landscape has changed rapidly over the last several years becoming more complicated and diverse. More people than ever are online in the country meaning the potential victim base has increased. According to third-party reporting, Brazil is among the most highly-targeted countries for information stealers and other malware, and its broad adoption of online banking offers potential for threat actors to social engineer people eager to conduct financial activity online.

Brazilian Banking Malware

Brazilian banking malware comes in many varieties, but, based on Proofpoint observations, most of them appear to have a common ancestor written in Delphi with source code reused and modified over many years. This base malware has spawned many varieties of Brazilian malware including Javali, Casabeniero, Mekotio, and Grandoreiro. Some malware strains like Grandoreiro are still in active development (both the loader and the final payload). Grandoreiro has capabilities to both steal data through keyloggers and screen-grabbers as well as steal bank login information from overlays when an infected victim visits pre-determined banking sites targeted by the threat actors. Based on recent Proofpoint telemetry, Grandoreiro is typically delivered with an attack chain beginning with a URL in an email with various lures including shared documents, Nota Fiscal Electronicos (NF-e, a tax form required to be used by organizations in Brazil), and utility bills. Once a victim clicks the URL, they are delivered a zip file containing the loader, usually an MSI, HTA or exe file. If the user runs the loader, the malicious file will use DLL injection to add malicious behavior to an otherwise legitimate but vulnerable program

included in the zip file with the loader. The loader will then download and run the final Grandoreiro payload and check in with a command and control (C2) server.

Previously, bank customers targeted by Grandoreiro overlays have been in Brazil and Mexico, but recent Grandoreiro campaigns show that this capability has been expanded to banks in Spain as well. Two campaigns attributed to TA2725 spanning from 24 through 29 August 2023 shared common infrastructure and payload while targeting both Mexico and Spain simultaneously. This development means that the Grandoreiro bank credential stealing overlays now include banks in both Spain and Mexico in the same version so that the threat actors can target victims in multiple geographic regions without modification of the malware.

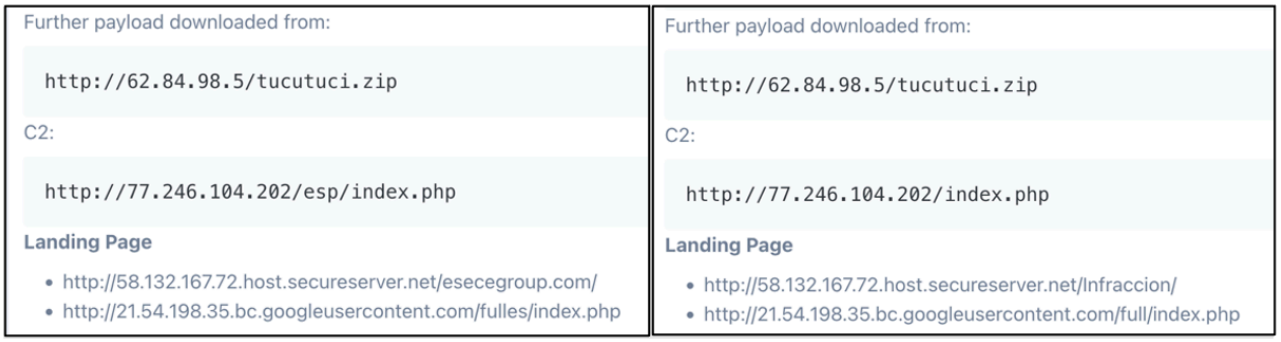

Figure 1. Common C2 and payload download for both campaigns.

Threat actors from the Americas have previously targeted organizations in Spain but have typically used more generic malware or phishing campaigns that were unique to Spain. In this case, the threat actors have expanded this version of Grandoreiro that had previously only targeted the Americas to include other parts of the world.

Figure 2. Example of TA2725 targeting of victims in Spain in August and September by spoofing ÉSECÈ Group, a Spanish manufacturing company.

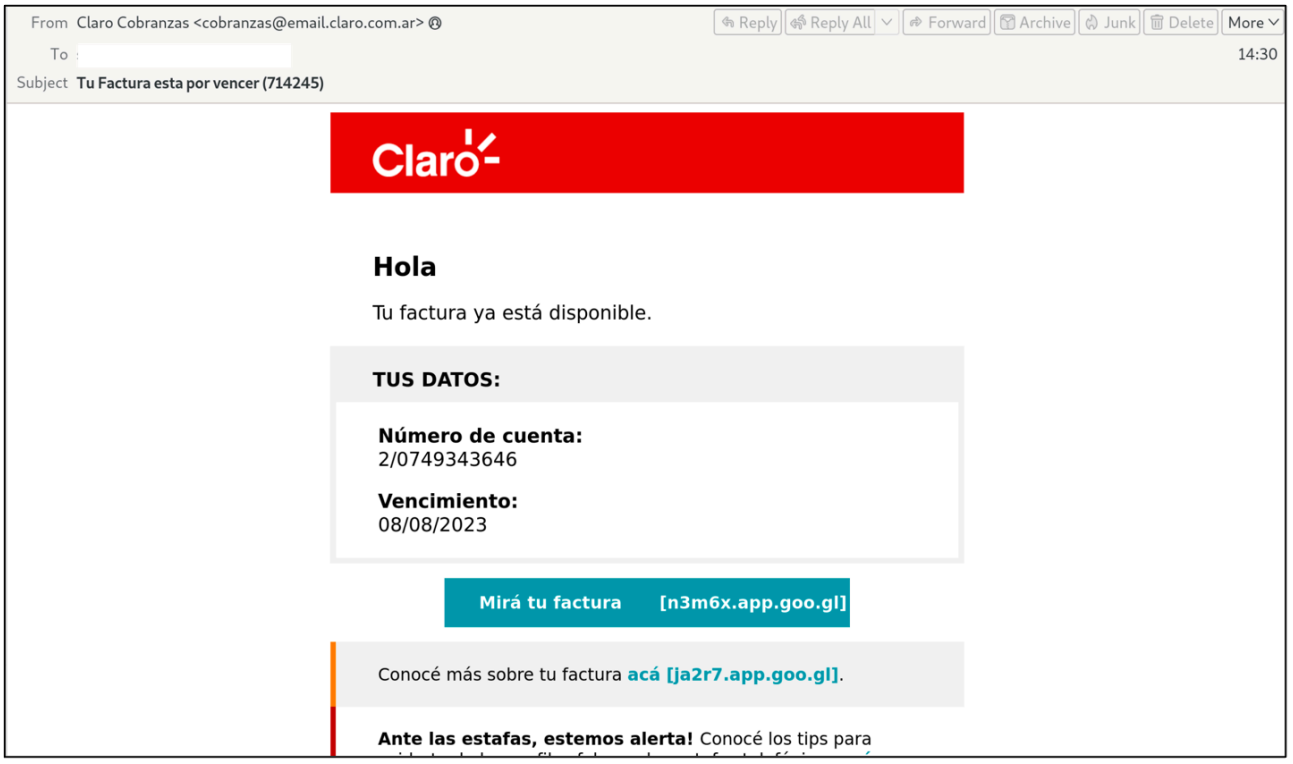

Figure 3. Example of an unattributed Grandoreiro cluster targeting Spain with a mobile phone bill lure spoofing Claro.

TA2725

TA2725 is a threat actor Proofpoint has tracked since March 2022 that is known for using Brazilian banking malware and phishing to target organizations mainly in Brazil and Mexico. The actor has been observed targeting credentials for banks in those countries as well as targeting consumer credentials and payment information for Netflix and Amazon accounts. TA2725 typically hosts their URL redirector on GoDaddy virtual hosting and redirects users to a zip file hosted on legitimate cloud hosting providers such as Amazon AWS, Google Cloud, or Microsoft Azure.

Conclusion

Given the rapid malware development and tenacity of threat actors in Latin America and South America, we expect to see an increase in targets of opportunity outside that region who share a common language. As the global supply chain continues to evolve and rely on suppliers around the world, the targeting of organizations outside of a company's normal service region will continue to be an increasing threat to all organizations worldwide.

Subscribe to the Proofpoint Blog
