Trend Micro Collaborated with Interpol in Cracking Down Grandoreiro Banking Trojan

Published: 2024-04-24 · Archived: 2026-04-05 20:21:14 UTC

Malware

In this blog entry, we discuss Trend Micro's contributions to an Interpol-coordinated operation to help Brazilian and Spanish law enforcement agencies analyze malware samples of the Grandoreiro banking trojan.

By: Joshua Paul Ignacio, Paul Pajares, Paul John Bardon Apr 24, 2024 Read time: 3 min (681 words)

Last April 2023, the International Criminal Police Organization (Interpol) requested any indicators of compromise (IOCs) or information related to the banking trojan Grandoreiro, specifically for command-and-control (C&C) servers. Grandoreiro has evolved with new features and capabilities since it first appeared around 2018, and has been primarily targeting users in Latin America and Europe. Trend Micro was one of the partners involved in Interpol's operation to help Brazilian and Spanish law enforcement agencies (LEAs) analyze Grandoreiro malware samples as part of their national cybercrime investigations. The Interpol-coordinated operationopen on a new tab resulted in the arrest of five administrators behind a Grandoreiro operation, as announcedopen on a new tab by the Brazilian authorities.

Grandoreiro spreads through phishing emails, malicious attachments, or links leading to fake websites. These emails often impersonate legitimate organizations, such as banks or financial institutions, to trick users into downloading and executing the malware. Once installed on a victim's system, Grandoreiro operates as a typical banking trojan, aiming to steal sensitive financial information. Over time, Grandoreiro has undergone various updates and modifications, enhancing its evasion techniques and obfuscation methods to evade detection by antivirus software and security measures.

Trend's Contributions

Here's the summary of Trend's contributions to the operation:

- Trend threat intelligence data from January to April 2023 showed that Argentina recorded the highest number of detections related to Grandoreiro with 1,118 detections, followed by Turkey with 322 detections, and Mexico with 265 detections (Figure 1).

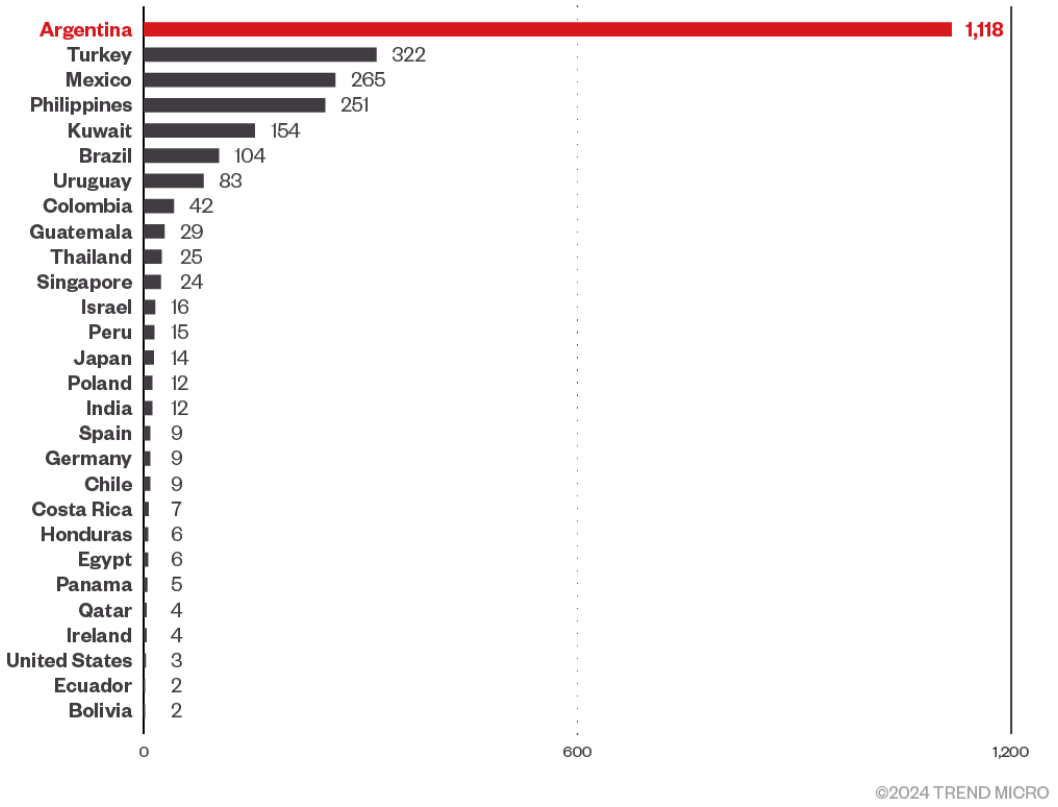

Figure 1. Highest number of Grandoreiro detections by country

- Trend provided an additional list of banks/strings found on a sample. These were utilized to monitor the browsing activity of the user by cross-referencing the window to check if it matches specific strings. The list of strings can be accessed at the end of this article.
- During the investigation, it was discovered that Grandoreiro utilized domain generation algorithms (DGAs) for its C&C communications. To gain further insights, Trend generated all possible domains from the list of strings and subdomains found on multiple samples. As a result, more than 4,000 DGAs were generated, providing valuable information to pivot to the C&C servers used by Grandoreiro at that time.
- The admin panel is crucial for investigation on the scale of attack of threat actors and the identification of victims. Using the open-source tool URLScan (urlscan.io), Trend recommended inspecting three active admin panels with their respective locations. The following were the URLs of the admin panels and the screenshot of login page (Figure 2):
- 185.191.228[.]227/autorizar.php (United States)
- 192.95.6[.]196/23112022new/autorizar.php (Canada)
- 51.77.193[.]20/eliteseguros/autorizar.php (France)

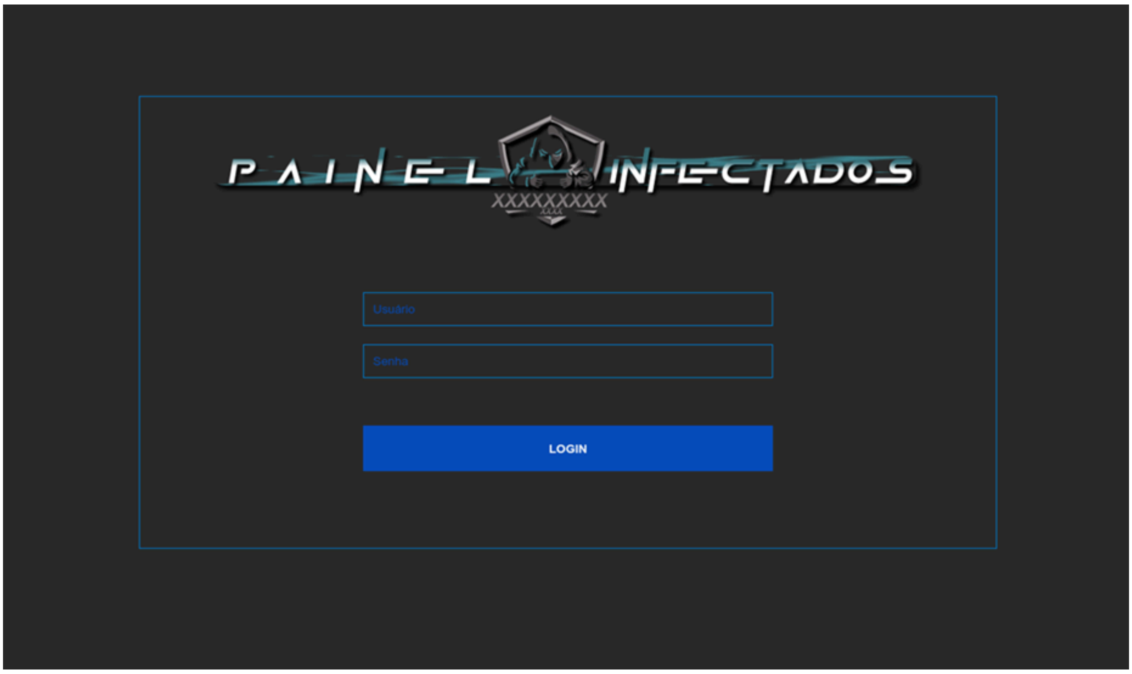

Figure 2. Screenshot of the login page

- Trend recommended to inspect the file storage Dropbox where the malicious email attachment was hosted and contained a name of the uploader. It was highly likely a fake name although we believe it can help in attribution. Figures 3 and 4 show the Dropbox accounts with the names "RITA MENDES" and "Nohemi Valdes", respectively:

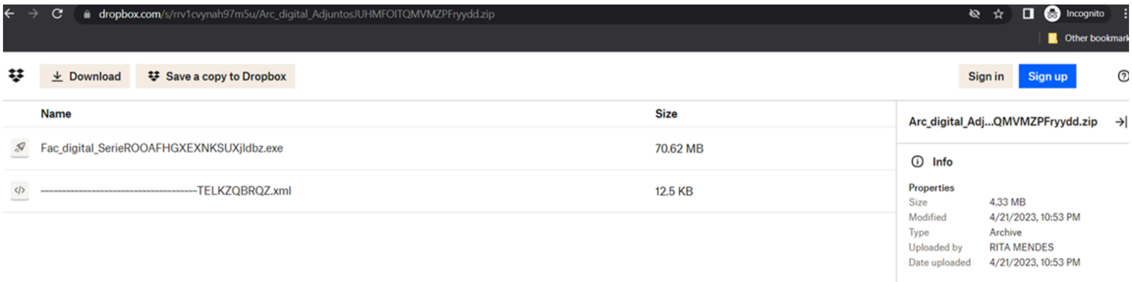

Figure 3. Dropbox storage with the uploader name "RITA MENDEZ"

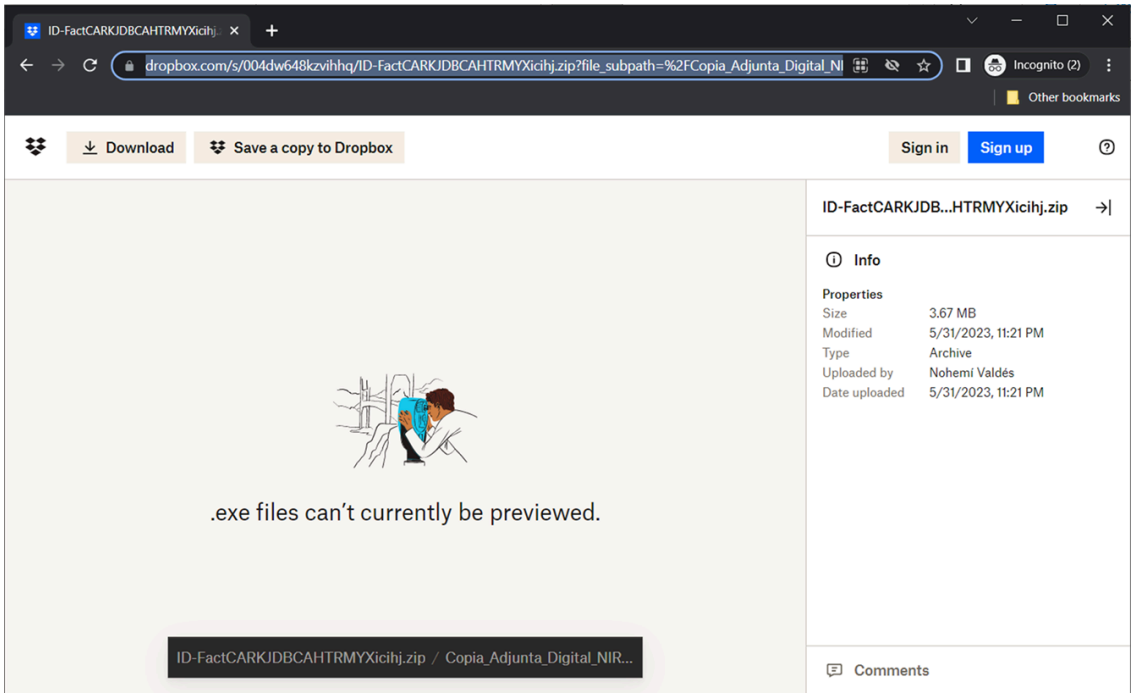

Figure 4. Dropbox storage with the uploader name "Nohemi Valdes"

- Trend provided an analysis of Grandoreiro's utilization of VBScript (VBS) for its malicious routine, as shown in Figure 5.

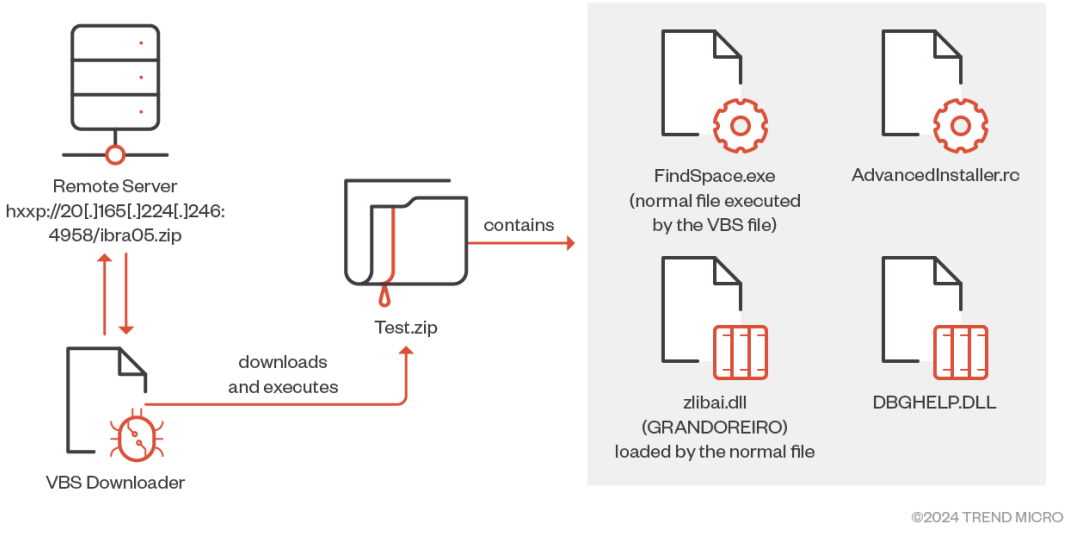

Figure 5. Infection chain of Grandoreiro using VBS

Cooperation with Interpol

These contributions are the latest in Trend's long track record of successful collaborations with international law enforcement. Collaborations between law enforcement and the private sector provide security organizations and industry specialists the opportunity to share their expertise, resources, and years-long experience with LEAs such

as Interpol to enhance their cybercrime combating efforts in effectively targeting and dismantling malicious actors.

Trend's ongoing cooperation with Interpol has been instrumental in a series of prominent crackdowns throughout the years: These include the dismantling of the 16shop phishing kitopen on a new tab and the disruption of African cybercrime networks during Africa Cyber Surge I and IIopen on a new tab in 2023, the apprehension of business email compromise (BEC) actors under Operation Killer Beeopen on a new tab in 2022, and the capture of REvil and Cl0p syndicate members as part of Operation Cycloneopen on a new tab in 2021. This partnership endures as Trend persists in its commitment to securing our increasingly connected world.

The list of banks/strings found on a sample can be viewed hereopen on a new tab.

Tags
