Mekotio Banking Trojan Threatens Financial Systems in Latin America

By By: Trend Micro Research Jul 04, 2024 Read time: 2 min (627 words)

Published: 2024-07-04 · Archived: 2026-04-05 16:02:57 UTC

Introduction

The Mekotio banking trojan is a sophisticated piece of malware that has been active since at least 2015, primarily targeting Latin American countries with the goal of stealing sensitive information — particularly banking credentials — from its targets. Originating in the Latin American region, it has been particularly prolific in Brazil, Chile, Mexico, Spain, and Peru. Furthermore, Mekotio seems to share a common origin with other notable Latin American banking malware such as Grandoreiro, which was disrupted by law enforcement earlier this year. Mekotio is often delivered through phishing emails, employing social engineering to trick users into interacting with malicious links or attachments.

We've recently seen a surge in attacks involving Mekotio among our customers. In this blog entry, we'll provide an overview of the trojan and what it does.

How Mekotio Works

Figure 1 shows the attack chain for a Mekotio infection:

Mekotio typically arrives through emails that appear to be from tax agencies alleging that the user has unpaid tax obligations. These emails contain a ZIP file attachment or a link to a malicious site. Once the user interacts with the email, the malware is downloaded and executed on their system. In our analysis, the attachment is a PDF file that contains the malicious link.

Upon execution, Mekotio gathers system information and establishes a connection with a command- and-control (C&C) server. This server provides instructions and a list of tasks for the malware to perform.

Once inside the system, Mekotio performs the following malicious activities:

- **Credential Theft**: Mekotio's main goal is to steal banking credentials. It achieves this by displaying fake pop-ups that mimic legitimate banking sites, tricking users into entering their details, which the trojan then proceeds to harvest.
- **Information Gathering**: Mekotio can capture screenshots, log keystrokes, and steal clipboard data.
- **Persistence Mechanisms**: Mekotio employs various tactics to maintain its presence on the infected system, including adding itself to startup programs or creating scheduled tasks.

The stolen banking information is sent back to the C&C server, where it can be further used by malicious actors for fraudulent activities, such as unauthorized access to bank accounts.

Mitigation

By practicing proper security best practices, users can protect themselves from threats that are primarily delivered via email. These include the following:

- Being skeptical of unsolicited emails
- Users should verify the sender's email address, look for spelling and grammar mistakes, and scrutinize subject lines.
- Avoiding clicking on links and downloading attachments
- Users should hover over links to check URLs and avoid downloading attachments in general unless absolutely certain of the sender's identity.
- Verifying sender identity
- Users should directly contact the sender using known contact details and compare the email with previous correspondence if they suspect that the email might be malicious.
- Using email filters and anti-spam software
- Organizations should ensure that spam filters and other security tools are turned on and are up to date.
- Reporting phishing Attempts
- Users should report phishing attempts to their IT and security teams when applicable.
- Educating employees on security best practices
- Organizations should educate their employees on phishing and social engineering tactics, as well as conduct regular phishing awareness training.

Conclusion

The Mekotio banking trojan is a persistent and evolving threat to financial systems, especially in Latin American countries. It uses phishing emails to infiltrate systems, with the goal of stealing sensitive information while also maintaining a strong foothold on compromised machines. By adhering to recommended security practices, such as verifying email authenticity, avoiding suspicious links and attachments, and employing robust cybersecurity solutions, individuals and organizations can significantly reduce the risk of falling victim to this dangerous malware.

Indicators of Compromise

The indicators of compromise for this entry can be found here.

Source: https://www.trendmicro.com/en_us/research/24/g/mekotio-banking-trojan.html