Mphasis SOC – Information Security News

Date & Time Issued: 05-JUL-2024, 14:30 IST

Title

Mekotio Banking Trojan

Summary

- 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, 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.

Severity

Medium 🟩🟩🟨🟧⬜

Attack Vectors

- 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.

Indicator of Compromise

INDICATOR TYPE	INDICATORS
File Hash	• 5e92f0fcddc1478d46914835f012137d7ee3c217 • f68d3a25433888aa606e18f0717d693443fe9f5a • 3fe5d098952796c0593881800975bcb09f1fe9ed • 1087b318449d7184131f0f21a2810013b166bf37 • ef22c6b4323a4557ad235f5bd80d995a6a15024a
Domain	• hxxps://intimaciones[.]afip[.]gob[.]ar[.]kdental[.]cl/Documentos_Intimacion/ • hxxps://techpowerup[.]net/cgefacturacl/descargafactmayo/eletricidad/ • hxxps://christcrucifiedinternational[.]org/descargafactmayo/eletricidad/ • tudoprafrente[.]org • tudoprafrente[.]co:7958
IP	• 68[.]233[.]238[.]122:80

Recommendations

- Block all threat indicators at your respective controls.
- Search for indicators of compromise (IOCs) in your environment utilizing your respective security controls.
- Never trust or open links and attachments received from unknown sources/senders.
- Regularly monitor network activity for any unusual behavior, as this may indicate that a cyberattack is underway.
- Using email filters and anti-spam software, and ensuring they are up to date.

	• Reporting phishing attempts to IT and security teams when applicable. • Educating employees on security best practices, including phishing and social engineering tactics. **NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre -Prod or test environment before implementing. diligence and impact analysis.**
References	• https://www.trendmicro.com/en_us/research/24/g/mekotio-banking-trojan.html • https://securityonline.info/mekotio-banking-trojan-resurges-targeting-latin-american-financial-systems/ • https://thecyberexpress.com/surge-mekotio-banking-trojan-latin-america/