AL2024_13 Experts Warn of Mekotio Banking Trojan Targeting Latin American Countries (10th July 2024)

Description

Financial institutions across Latin America are facing a significant threat from the Mekotio banking trojan, also known as Melcoz, according to recent observations by Trend Micro. This malware, active since 2015, has intensified its cyber-attacks, primarily targeting countries such as Brazil, Chile, Mexico, Spain, Peru, and Portugal with the primary objective of stealing banking credentials.

Details

Mekotio was first documented by ESET in August 2020 and is part of a group of banking trojans—including Guildma, Javali, and Grandoreiro, focused on the Latin American region. Known for its use of Delphi programming language, Mekotio employs tactics such as fake pop-up windows, backdoor functionalities, and specifically targets Spanish and Portuguese speaking countries.

In July 2021, Spanish law enforcement arrested 16 individuals associated with a criminal network responsible for distributing Mekotio through social engineering campaigns. These campaigns leveraged tax-themed phishing emails containing malicious attachments or links leading to an MSI installer file. This file utilizes an AutoHotKey (AHK) script to execute the malware, differing slightly from previous infection methods involving obfuscated batch and PowerShell scripts.

Once installed, Mekotio gathers system information and establishes communication with a command and control (C&C) server to receive commands. Its main operations include harvesting banking credentials through fake pop-ups, mimicking legitimate banking websites, capturing screenshots, logging keystrokes, stealing clipboard data, and ensuring persistence on compromised systems via scheduled tasks.

Indicators of Compromise (IoCs)

The following link contains IoCs were provided by Trend Micro Research and includes file hashes for the malware, IP addresses for the malware's command and control (C&C) servers and malicious URLs that host the malware:
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/24/g/mekotio/mekotio-banking-trojan-threatens-financial-systems-in-latin-america.txt

Remediation

To mitigate the risk posed by Mekotio, organizations are advised to:

- Enhance email security to detect and block phishing attempts.
- Educate employees on identifying and avoiding suspicious emails.
- Implement robust endpoint protection to detect and respond to malware infections promptly.
- Monitor for unusual system behavior, such as unauthorized network connections and application activities.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Newsroom. (2024, July 8). Experts Warn of Mekotio Banking Trojan Targeting Latin American Countries. Retrieved from Hackers News. https://thehackernews.com/2024/07/experts-warn-of-mekotio-banking-trojan.html
- Trend Micro Research. (2024, July 4). Mekotio Banking Trojan Threatens Financial Systems in Latin America. Retrieved from Trend Micro. https://www.trendmicro.com/en_us/research/24/g/mekotio-banking-trojan.html