Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

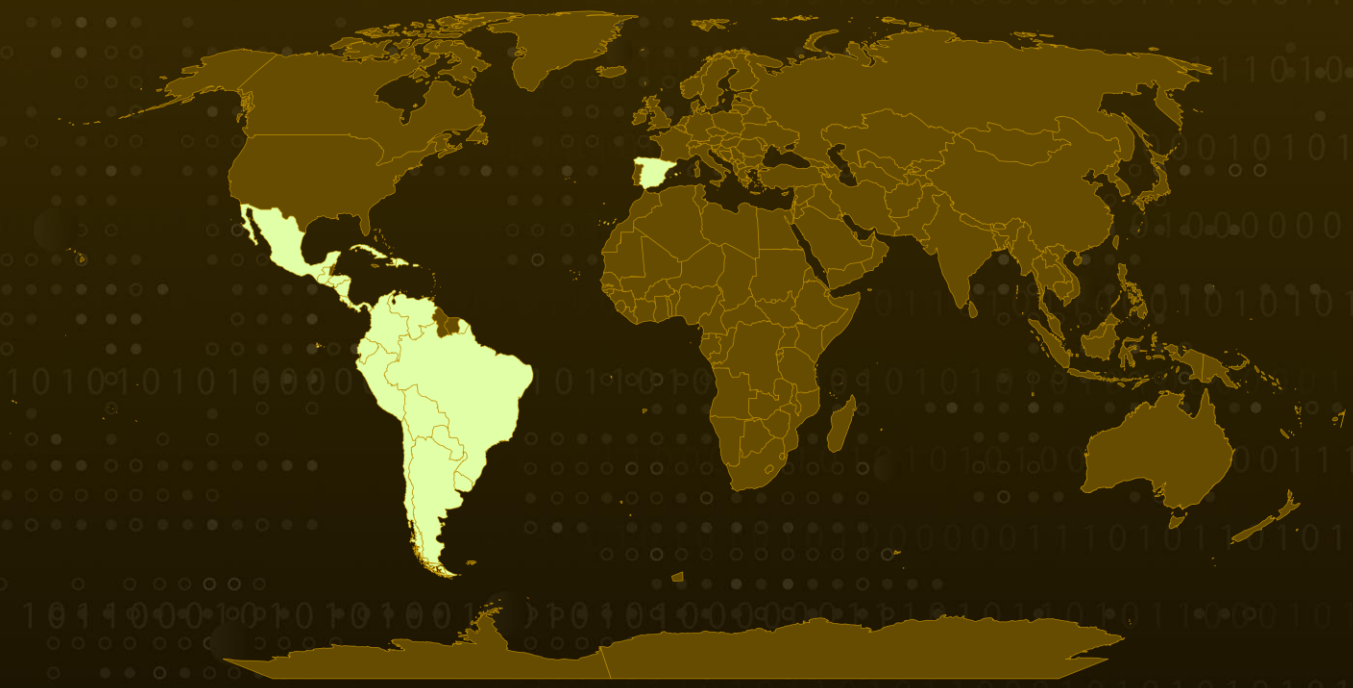
Mekotio Trojan Targets the Latin American Financial Sector

Date of Publication	Admiralty Code	TA Number
July 5, 2024	A1	TA2024260

Summary

Active Since: 2015
Malware: Mekotio banking trojan
Attack Regions: Latin America, Spain
Targeted Industries: Banking, Financial
Attack: The Mekotio banking trojan, a highly sophisticated malware active since at least 2015, primarily targets Latin American countries to steal sensitive information, particularly banking credentials. Mekotio shares a common lineage with other prominent Latin American banking malware, such as Grandoreiro, which was disrupted by law enforcement earlier this year.

Attack Regions



Attack Details

#1 A surge in attacks involving the Mekotio banking trojan, a sophisticated malware active since at least 2015, primarily targets Latin American countries to steal sensitive information, especially banking credentials.

#2 Mekotio employs fake pop-ups that mimic legitimate banking sites to deceive users into entering their details, which the trojan subsequently harvests. This malware is often distributed through phishing emails, utilizing social engineering techniques to lure users into interacting with malicious links or attachments.

#3 Mekotio appears to share a common origin with other notable Latin American banking malware such as **Grandoreiro**, which was disrupted by law enforcement earlier this year.

#4 Mekotio typically arrives via emails that seem to come from tax agencies, alleging unpaid tax obligations. Once the user interacts with the email, the malware is downloaded and executed on their system.

#5 Upon execution, Mekotio gathers system information and establishes a connection with a command-and-control (C&C) server. Mekotio persists by adding itself to startup programs or creating scheduled tasks. It can capture screenshots, log keystrokes, and steal clipboard data.

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

Recommendations

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

Implement Network Segmentation: Segment your network to isolate critical systems and sensitive data from general user access and potential malware spread. Use intrusion detection and prevention systems (IDPS) to monitor and analyze network traffic for abnormal behavior.

User Education and Awareness: Educate users about the dangers of opening suspicious documents or files received via email or other channels. Encourage them to be cautious and vigilant when interacting with unknown or unexpected content.

Content Filtering and Application Control: Enforce application control to prevent unauthorized app installations and executions, reducing the risk of downloading and running malicious files. This integrated strategy safeguards against downloadable threats by proactively blocking access to harmful content and preventing the execution of malicious code.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**TA0040** Impact	**T1566** Phishing	**T1566.001** Spearphishing Attachment
T1566.002 Spearphishing Link	**T1053** Scheduled Task/Job	**T1053.005** Scheduled Task	**T1204** User Execution
T1204.001 Malicious Link	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1656** Impersonation
T1036 Masquerading	**T1059.010** AutoHotKey & AutoIT	**T1056** Input Capture	**T1056.001** Keylogging
T1082 System Information Discovery	**T1560** Archive Collected Data	**T1115** Clipboard Data	**T1113** Screen Capture
T1041 Exfiltration Over C2 Channel	**T1657** Financial Theft	**T1480** Execution Guardrails	**T1204.002** Malicious File

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	5e92f0fcddc1478d46914835f012137d7ee3c217, f68d3a25433888aa606e18f0717d693443fe9f5a, 3fe5d098952796c0593881800975bcb09f1fe9ed, 1087b318449d7184131f0f21a2810013b166bf37, ef22c6b4323a4557ad235f5bd80d995a6a15024a
IPv4:Port	23[.]239[.]4[.]149[:]80, 68[.]233[.]238[.]122[:]80, 34[.]117[.]186[.]192[:]80, 68[.]221[.]121[.]160[:]9095, 68[.]221[.]121[.]160[:]80
Domain	tudoprafrente[.]org, tudoprafrente[.]co[:]7958
URL	hxxps[:]//intimaciones[.]afip[.]gob[.]ar[.]kdental[.]cl/Documentos_Intimacion/, hxxps[:]//techpowerup[.]net/cgefacturacl/descargafactmayo/eletricidad/, hxxps[:]//christcrucifiedinternational[.]org/descargafactmayo/eletricidad/

References

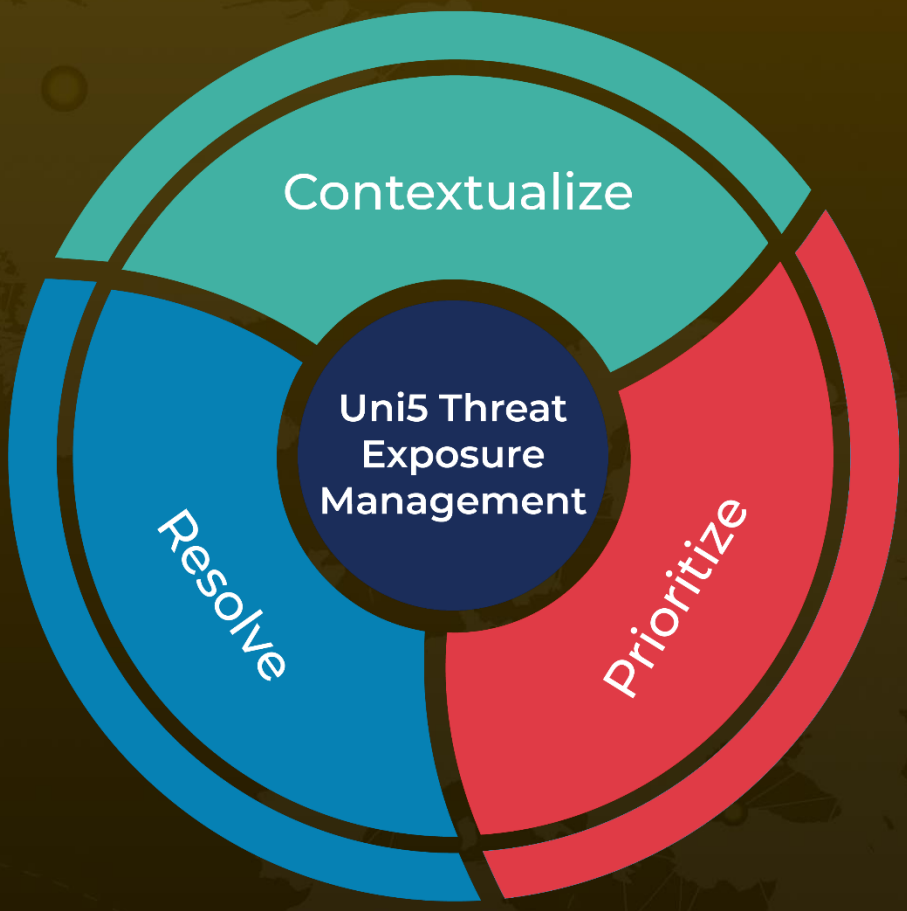
https://www.trendmicro.com/en_us/research/24/g/mekotio-banking-trojan.html

https://www.hivepro.com/threat-advisory/grandoreiro-trojan-an-evolving-threat-to-global-banking/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

July 5, 2024 • 6:00 AM

More at www.hivepro.com