Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

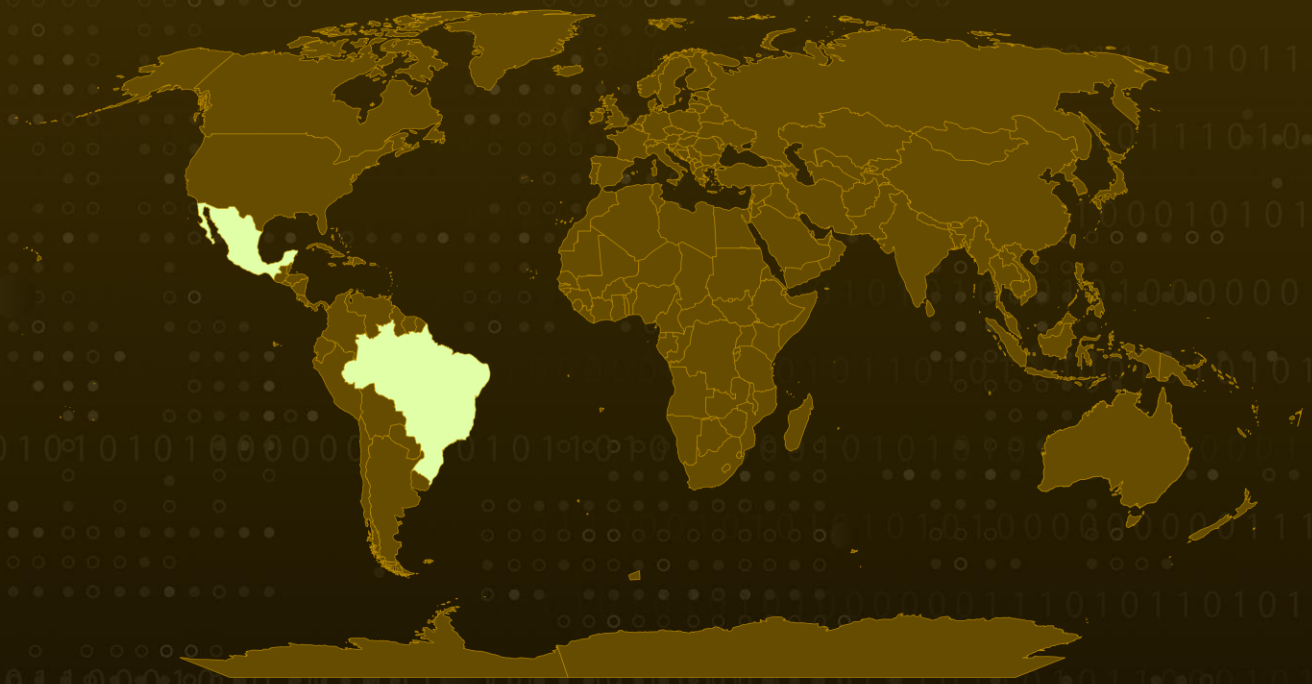
CHAVECLOAK Banking Trojan Sneaks into Brazil's Financial Hub

Date of Publication	Admiralty Code	TA Number
March 6, 2024	A1	TA2024087

Summary

Malware: CHAVECLOAK
Attack Region: Brazil and Mexico
Targeted Industry: Financial, Cryptocurrency, Banking
Affected Platforms: Microsoft Windows
Attack: The CHAVECLOAK banking trojan is purposefully crafted to target the banking credentials of individuals in Brazil, highlighting the ongoing focus of cyber criminals on the nation's financial sector.

Attack Regions



Attack Details

#1 The recently identified CHAVECLOAK malware is strategically crafted to pilfer banking credentials from individuals in Brazil, highlighting an ongoing focus of cyber criminals on the nation's financial sector. This sophisticated banking trojan, known as CHAVECLOAK, employs a nefarious method of propagation through a corrupted PDF file, cleverly concealing its malicious intent.

#2 After infection, victims may notice the unauthorized extraction of their banking credentials. The malevolent PDF claims to contain contractual documents, with instructions meticulously composed in Portuguese, enticing victims to engage by clicking a button for the review and signing of the attached files.

#3 Upon interaction, the PDF initiates the download of a ZIP file, utilizing DLL side-loading techniques to execute the final stage of the malware. A discreetly embedded link within the stream object serves as a gateway to a malicious downloader, revealing its decoded URL. This URL undergoes processing through a free link-shortening service.

#4 CHAVECLOAK orchestrates a range of malevolent actions aimed at credential theft, including the ability to impede the victim's screen, log keystrokes surreptitiously, and present deceptive pop-up windows. Notably, it not only monitors the victim's interactions with specific financial portals but also actively seeks connections to Mercado Bitcoin, a prominent cryptocurrency exchange encompassing both traditional banking and cryptocurrency functionalities.

Recommendations

Email Filtering and Monitoring: Strengthen email filtering systems to detect and quarantine phishing attempts, especially those involving malicious PDFs. Regularly monitor email communications for potential threats and provide timely alerts to users.

Network Traffic Monitoring and Anomaly Detection: Implement robust network traffic monitoring systems with anomaly detection capabilities to identify and respond promptly to any unusual activities, especially those related to compromised network infrastructure used by threat actors.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0011 Command and Control
TA0010 Exfiltration	TA0040 Impact	T1204.001 Malicious Link	T1574.002 DLL Side-Loading
T1056.001 Keylogging	T1555 Credentials from Password Stores	T1041 Exfiltration Over C2 Channel	T1584 Compromise Infrastructure
T1053.005 Scheduled Task	T1204.002 Malicious File	T1140 Deobfuscate/Decode Files or Information	T1562 Impair Defenses
T1036.004 Masquerade Task or Service	T1027.007 Dynamic API Resolution	T1027.009 Embedded Payloads	T1056 Input Capture
T1033 System Owner/User Discovery	T1071.001 Web Protocols	T1657 Financial Theft	T1598.002 Spearphishing Attachment

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	64[.]225[.]32[.]24
URLs	hxxps://webattach.mail.yandex.net/message_part_real/NotaFiscalEsdeletronicasufactrub66667kujhdfdjrWEWGFG09t5H6854JHGJUUR[.]zip, hxxps://goo[.]su/FTD9owO
Hostnames	mariashow[.]ddns[.]net, comunidadebet20102[.]hopto[.]org
SHA256	51512659f639e2b6e492bba8f956689ac08f792057753705bf4b9273472c72c4, 48c9423591ec345fc70f31ba46755b5d225d78049cfb6433a3cb86b4ebb5a028, 4ab3024e7660892ce6e8ba2c6366193752f9c0b26beedca05c57dcb684703006, 131d2aa44782c8100c563cd5febf49fcb4d26952d7e6e2ef22f805664686ffff, 8b39baec4b955e8dfa585d54263fd84fea41a46554621ee46b769a706f6f965c, 634542fdd6581dd68b88b994bc2291bf41c60375b21620225a927de35b5620f9, 2ca1b23be99b6d46ce1bbd7ed16ea62c900802d8efff1d206bac691342678e55

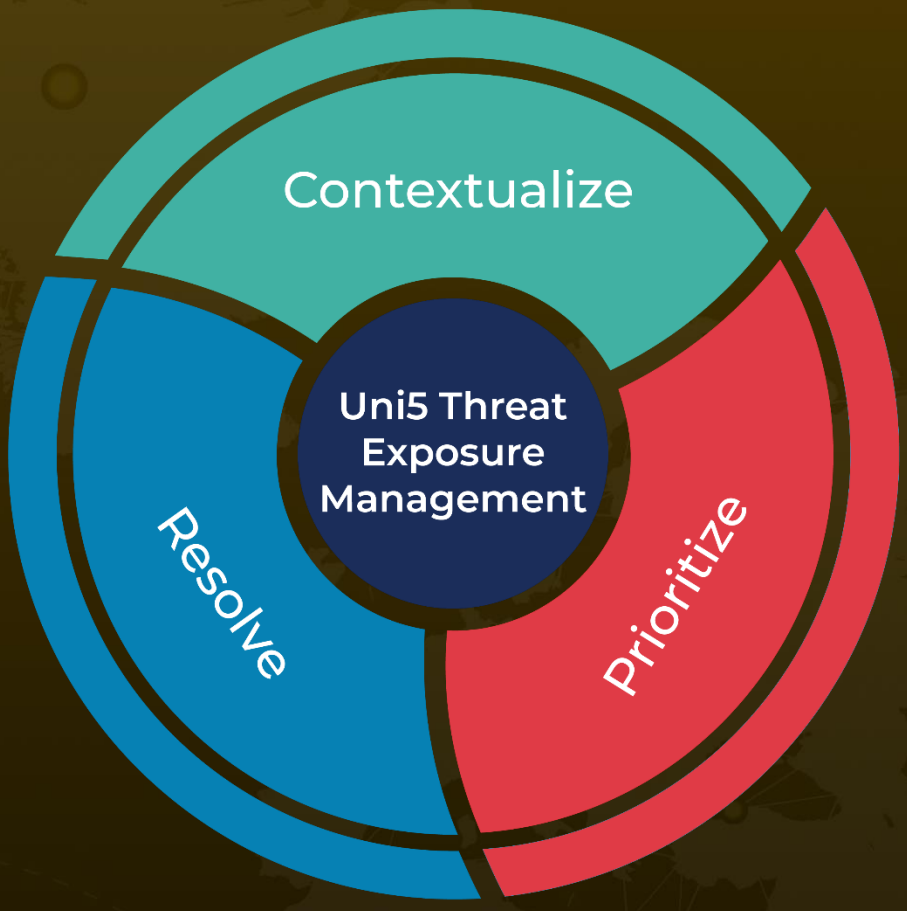
References

https://www.fortinet.com/blog/threat-research/banking-trojan-chavecloak-targets-brazil

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

March 6, 2024 • 3:00 AM

More at www.hivepro.com