Mar 08 2024

NETMANAGEIT

Intelligence Report

New Banking Trojan Targets Brazil

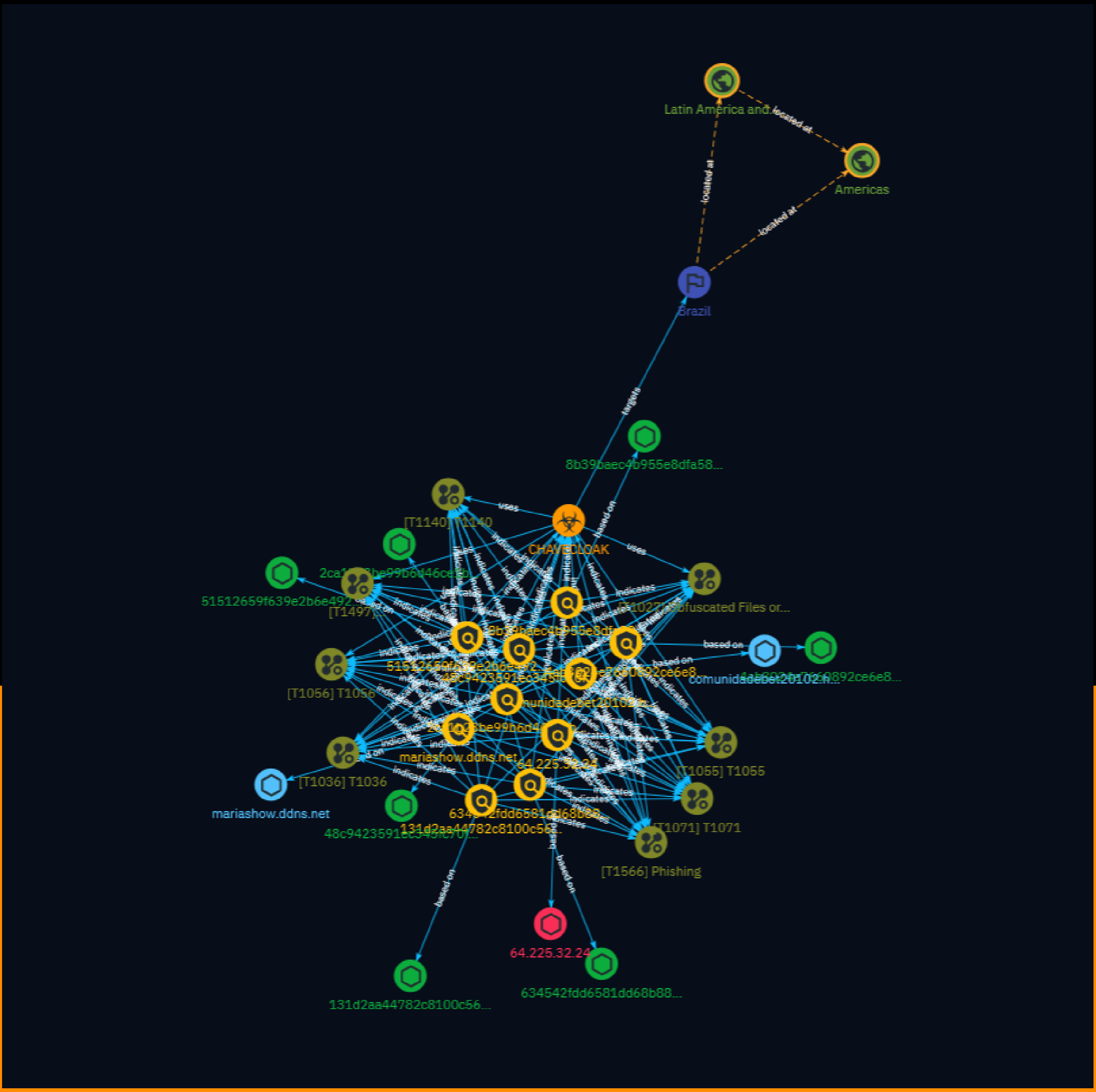

Table of contents

Overview

Entities

Observables

External References

Overview

Description

FortiGuard Labs recently uncovered a threat actor employing a malicious PDF file to propagate the banking Trojan CHAVECLOAK in Brazil. This intricate attack involves the PDF downloading a ZIP file and subsequently utilizing DLL side-loading techniques to execute the final malware. CHAVECLOAK is specifically designed to target users in Brazil, aiming to steal sensitive information linked to financial activities. It employs Portuguese language settings, indicating a strategic approach to the region, and actively monitors victims' interactions with financial portals. CHAVECLOAK exemplifies the sophistication of contemporary banking trojans, necessitating continual vigilance and proactive cybersecurity measures to safeguard against evolving threats within the financial landscape of South America.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Indicator

Name
comunidadebet20102.hopto.org
Pattern Type
stix
Pattern
[hostname:value = 'comunidadebet20102.hopto.org']
Name
mariashow.ddns.net
Pattern Type
stix
Pattern
[hostname:value = 'mariashow.ddns.net']
Name
8b39baec4b955e8dfa585d54263fd84fea41a46554621ee46b769a706f6f965c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8b39baec4b955e8dfa585d54263fd84fea41a46554621ee46b769a706f6f965c']

Name

634542fdd6581dd68b88b994bc2291bf41c60375b21620225a927de35b5620f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '634542fdd6581dd68b88b994bc2291bf41c60375b21620225a927de35b5620f9']

Name

51512659f639e2b6e492bba8f956689ac08f792057753705bf4b9273472c72c4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '51512659f639e2b6e492bba8f956689ac08f792057753705bf4b9273472c72c4']

Name

4ab3024e7660892ce6e8ba2c6366193752f9c0b26beedca05c57dcb684703006

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4ab3024e7660892ce6e8ba2c6366193752f9c0b26beedca05c57dcb684703006']

Name

2ca1b23be99b6d46ce1bbd7ed16ea62c900802d8efff1d206bac691342678e55

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2ca1b23be99b6d46ce1bbd7ed16ea62c900802d8efff1d206bac691342678e55']

Name

48c9423591ec345fc70f31ba46755b5d225d78049cfb6433a3cb86b4ebb5a028

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '48c9423591ec345fc70f31ba46755b5d225d78049cfb6433a3cb86b4ebb5a028']

Name

64.225.32.24

Description

- **Zip Code:** N/A - **ISP:** Digital Ocean - **ASN:** 14061 - **Organization:** Digital Ocean - **Is Crawler:** False - **Timezone:** America/Los_Angeles - **Mobile:** False - **Host:** 64.225.32.24 - **Proxy:** True - **VPN:** True - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** True - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** US - **Region:** California - **City:** Santa Clara - **Latitude:** 37.34170151 - **Longitude:** -121.97530365

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.225.32.24']

Name

131d2aa44782c8100c563cd5febf49fcb4d26952d7e6e2ef22f805664686ffff

Pattern Type

stix

Pattern

```
[file:hashes.'SHA-256' =
'131d2aa44782c8100c563cd5febf49fcb4d26952d7e6e2ef22f805664686ffff']
```

Malware

Name
CHAVECLOAK

Attack-Pattern

Name
T1056
ID
T1056
Description
Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).
Name
Obfuscated Files or Information
ID
T1027
Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Virtualization/Sandbox Evasion

ID

T1497

Description

Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness) Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox.(Citation: Unit 42 Pirpi July 2015)

Name

T1055

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/

T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1140

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Name

T1071

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Country

Name
Brazil

Region

Name
Latin America and the Caribbean

Name
Americas

Hostname

Value
mariashow.ddns.net
comunidadebet20102.hopto.org

StixFile

Value
8b39baec4b955e8dfa585d54263fd84fea41a46554621ee46b769a706f6f965c
634542fdd6581dd68b88b994bc2291bf41c60375b21620225a927de35b5620f9
51512659f639e2b6e492bba8f956689ac08f792057753705bf4b9273472c72c4
4ab3024e7660892ce6e8ba2c6366193752f9c0b26beedca05c57dcb684703006
48c9423591ec345fc70f31ba46755b5d225d78049cfb6433a3cb86b4ebb5a028
2ca1b23be99b6d46ce1bbd7ed16ea62c900802d8efff1d206bac691342678e55
131d2aa44782c8100c563cd5febf49fcb4d26952d7e6e2ef22f805664686ffff

IPv4-Addr

Value
64.225.32.24

External References

- https://www.fortinet.com/blog/threat-research/banking-trojan-chavecloak-targets-brazil
- https://otx.alienvault.com/pulse/65eb4a6e81789f86b903f4b7