The new maxtrilha trojan is being disseminated and targeting several banks

seguranca-informatica.pt/the-new-maxtrilha-trojan-is-being-disseminated-and-targeting-several-banks/

September 10, 2021

The new maxtrilha trojan is being disseminated and targeting several banks around the world.

A new banking trojan dubbed **maxtrilha** (due to its encryption key) has been discovered in the last few days and targeting customers of European and South American banks. Criminals are constantly creating variants of popular banking trojans, keeping in mind the same *modus operandi* but changing the malware internals and its capabilities making it a fully undetectable (FUD) weapon.

Overview

The recent campaign have been disseminated in Latin America but also extended to Europe and Portugal. The campaign has been leveraged by Brazilian criminals' gangue, who use customized phishing templates to spread the trojan maxtrilha according to the target country.

The malware samples disseminated in Portugal open a legitimate webpage from Autoridade Tributária e Aduaneira – Finanças to lure the victims during the execution of the 1st stage. After that, the malware creates persistence, **disables Internet Explorer security settings** to facilitate the download of the 2nd stage from the Internet. In short, the 2nd stage – maxtrilha trojan – checks or creates persistence when executed on the target machine, uses a mechanism of capturing details from opened foreground windows matching its name with specific hardcoded strings related to banking companies, launches banking windows overlay, can deploy new payloads and communicates with the C2 server in real-time.

The maxtrilha trojan was developed in Delphi language, it's an x64 binary, and it can bypass AV and EDRs systems – at least until the moment of its analysis.

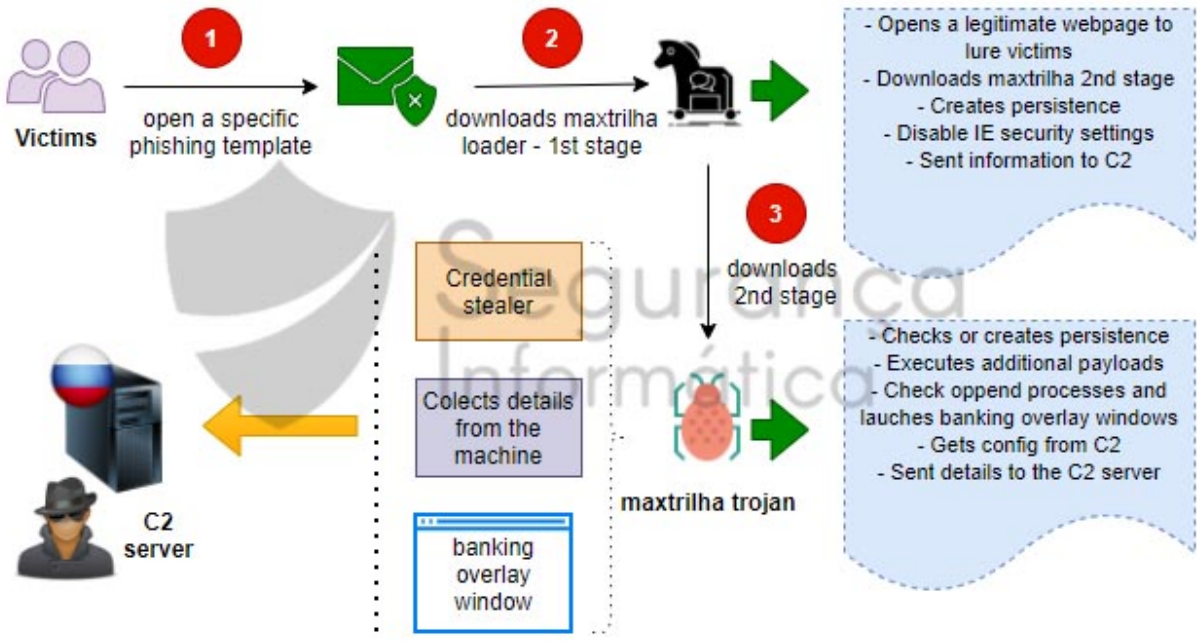

Figure 1: *High-level diagram of maxtrilha banking trojan.*

Key findings

- Maxtrilha has been disseminated via crafted phishing templates by country.
- The maxtrilha 1st stage – the loader – opens a legitimate service previously presented on the phishing template to lure victims during its execution.
- The 1st stage creates persistence on the infected machine, disables Internet Explorer security settings and accepted extensions to facilitate the download of the 2nd stage.
- Maxtrilha trojan – 2nd stage – checks or creates persistence on the machine, installs or modifies Windows trusted certificates, checks by opening windows to perform banking windows overlay to steal credentials and can deploy additional payloads executed via DLL injection technique.
- The victims' data is encrypted and sent to the C2 server geolocated in Russia.

Maxtrilha trojan analysis in-depth

In this section, we are going through the details of maxtrilha malware, analyzing step-by-step this banking trojan, how it operates, and what kind of data is exfiltrated. Figure 2 shows the phishing template disseminated in Portugal that impersonates the Autoridade Tributária e Aduaneira – Finanças to lure victims to download the maxtrilha 1st stage (the loader).

Figure 2: *Maxtrilha phishing template disseminated in Portugal and impersonating the Autoridade Tributária e Aduaneira – Finanças | h/t* ***@MiguelSantareno***

As observed below, the **"cld.]pt"** domain have been used to host several malicious campaigns during 2021, including the maxtrilha malware wave. The full list can be found at the end of the analysis.

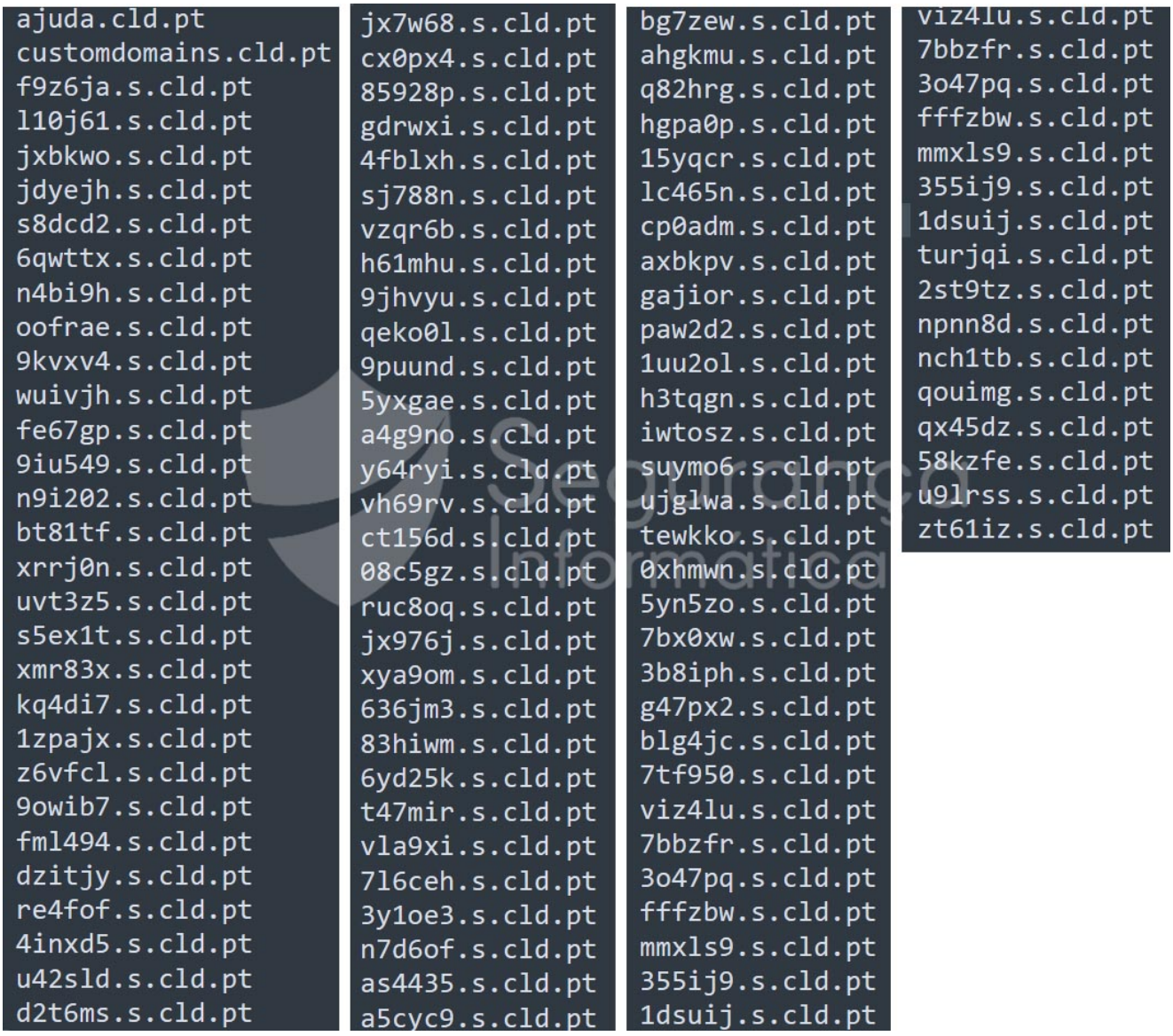

Figure 3: *Malicious .PT domain used to distribute campaigns in the wild during 2021, including the maxtrilha malware wave.*

Maxtrilha loader– the 1st stage

Filename: PdF.exe / MSITrueColor.exe
MD5:a6f3e35760bc2848cd258b786c1fd247
Creation date: 2021-09-06 09:20:49

The first alert on this banking trojan was triggered on the **0xSI_f33d**.The maxtrilha loader is customized by criminals according to the target country, and it performs some tasks in advance, namely:

- Opens a target legitimate page during its execution via a hardcoded short URL
- Creates persistence on the target machine
- Disables IE security settings; and
- Downloads the maxtrilha 2nd stage.

As presented in Figure 4, several samples have been distributed in the wild last few days, impersonating different organizations in different countries.

Scanned	Detections	Type	Name
2021-09-09	15 / 67	Win32 EXE	ChromaTune.exe
2021-09-09	13 / 65	Win32 EXE	606.exe
2021-09-09	14 / 67	Win32 EXE	561.exe
2021-09-09	9 / 67	Win32 EXE	582.exe
2021-09-09	3 / 68	Win32 EXE	278.exe
2021-09-08	36 / 68	Win32 EXE	CoreSync
2021-09-08	34 / 67	Win32 EXE	CoreSync
2021-09-09	19 / 68	Win32 EXE	master.mp4
2021-09-08	18 / 67	Win32 EXE	CriadorUOL.exe
2021-09-08	19 / 67	Win32 EXE	CoreSync
2021-09-09	7 / 57	Win32 EXE	iLovePDF
2021-09-08	5 / 68	Win32 EXE	ChromaTune.exe
2021-09-08	23 / 68	Win32 EXE	CoreSync
2021-09-08	19 / 67	Win32 EXE	AnyDesk
2021-09-09	6 / 67	Win32 EXE	E-Factura.exe
2021-09-08	25 / 68	Win32 EXE	CoreSync
2021-09-08	20 / 68	Win32 EXE	CoreSync
2021-09-09	14 / 67	Win32 EXE	payload_1.bin
2021-09-08	3 / 68	Win32 EXE	track003[1].mp3
2021-09-08	41 / 67	Win32 EXE	CriadorFINAL.exe
2021-09-09	0 / 67	Win32 EXE	276.exe

Scanned	Detections	Type	Name
2021-09-09	0 / 67	Win32 EXE	140.exe
2021-09-08	0 / 68	Win32 EXE	Skype.exe
2021-09-08	0 / 67	Win32 EXE	efactura.exe
2021-09-09	2 / 67	Win32 EXE	facturación.exe
2021-09-08	0 / 68	Win32 EXE	ccleaner
2021-09-08	0 / 68	Win32 EXE	Telegram Desktop
2021-09-09	0 / 66	Win32 EXE	WinRAR
2021-09-08	0 / 67	Win32 EXE	ccleaner
2021-09-08	0 / 65	Win32 EXE	WinRAR
2021-09-08	3 / 66	Win32 EXE	electron.exe
2021-09-08	0 / 66	Win32 EXE	Skype.exe
2021-09-08	0 / 65	Win32 EXE	ccleaner
2021-09-08	10 / 69	Win32 EXE	facturaeletronica.exe
2021-09-09	7 / 67	Win32 EXE	Finanzas.exe
2021-09-08	13 / 66	Win32 EXE	iLovePDF
2021-09-08	1 / 67	Win32 EXE	Financas.exe
2021-09-08	0 / 67	Win32 EXE	ccleaner
2021-09-08	0 / 66	Win32 EXE	efatura.exe
2021-09-08	0 / 67	Win32 EXE	tributo.exe

Segurança Informática

Figure 4: *Maxtrilha samples disseminated in August and September 2021.*

As mentioned, a specific short URL is hardcoded inside each loader, depending on the target country. In the case of the maxtrilha loader disseminated in Portugal, it uses the TinyURL online service, which is opened during the malware execution by the default web browser installed and available on the victim machine. The short URL points to a specific page related to the phishing template (see Figure 2) to lure victims.

```
.text:0000000000CEA7E0 nShowCmd        = dword ptr -10h
.text:0000000000CEA7E0
.text:0000000000CEA7E0                 sub     rsp, 38h
.text:0000000000CEA7E4                 xor     ecx, ecx        ; hwnd
.text:0000000000CEA7E6                 lea     rdx, aOpen_0    ; "open"
.text:0000000000CEA7ED                 lea     r8, File        ; lpFile
.text:0000000000CEA7F4                 lea     r9, Parameters  ; lpParameters
.text:0000000000CEA7FB                 lea     rax, Parameters
.text:0000000000CEA802                 mov     [rsp+38h+lpDirectory], rax ; lpDirectory
.text:0000000000CEA807                 mov     [rsp+38h+nShowCmd], 1 ; nShowCmd
.text:0000000000CEA80F                 call    ShellExecuteW
.text:0000000000CEA814                 add     rsp, 38h
.text:0000000000CEA818                 retn
.text:0000000000CEA818 sub_CEA7E0      endp
.text:0000000000CEA818
.text:0000000000CEA818 ; ---------------------------------------------------------------------------
.text:0000000000CEA819 algn_CEA819:                            ; DATA XREF: .pdata:0000000000EF
.text:0000000000CEA819                 align 4
.text:0000000000CEA81C ; const WCHAR aOpen_0
.text:0000000000CEA81C aOpen_0:                                ; DATA XREF: sub_CEA7E0+6↑o
.text:0000000000CEA81C                 text "UTF-16LE", 'open',0
.text:0000000000CEA826 ; const WCHAR File
.text:0000000000CEA826 File            dd offset loc_740068    ; DATA XREF: sub_CEA7E0+D↑o
.text:0000000000CEA82A                 dw 74h, 70h, 73h
.text:0000000000CEA830 aTinyurlComFlex:
.text:0000000000CEA830                 text "UTF-16LE", '://tinyurl.com/flexibiliza',0
.text:0000000000CEA866 ; const WCHAR Parameters
.text:0000000000CEA866 Parameters      dw 0                    ; DATA XREF: sub_CEA7E0+14↑o
.text:0000000000CEA866                                         ; sub_CEA7E0+1B↑o
.text:0000000000CEA868                 align 10h
```

```
1 HINSTANCE sub_CEA7E0()
2 {
3   return ShellExecuteW(0i64, L"open", &File, &Parameters, &Parameters, 1);
4 }
```

```
Payload: "%ProgramFiles%\Internet Explorer\iexplore.exe" https://tinyurl.com/tributodashboard

Target: https://www.acesso.gov.pt/v2/loginForm?partID=PFAP&path=/geral/dashboard

Payload: "C:\Program Files\Internet Explorer\iexplore.exe" https://tinyurl.com/flexibiliza

Target: https://www.acesso.gov.pt/v2/loginForm;flexpinter_JSessionID=JybB4aq8bkjva-sDnu9c8c6vq30SQhB8sfdh1bpuEyt84qUL1Rg5!1514316675!1580723171?partID=FLXP&path=/flexibiliza/
```

Segurança Informática

```
Payload: "%ProgramFiles%\Internet Explorer\iexplore.exe" https://tinyurl.com/
tributodashboard

Target: https://www.acesso.gov.pt/v2/loginForm?partID=PFAP&path=/geral/
dashboard


Payload: "C:\Program Files\Internet Explorer\iexplore.exe"
https://tinyurl.com/flexibiliza

Target: https://www.acesso.gov.pt/v2/loginForm;flexpinter_JSessionID=JybB4aq8
bkjva-sDnu9c8c6vq30SQhBBsfdh1bpuEyt84qUL1Rg5!1514316675!1580723171?partID=FLX
P&path=/flexibiliza/
```

Figure 5: *A short URL is opened via a default web browser which redirects the victim to a legitimate service.*

In another sample also disseminated in Portugal, we found a different hardcoded string instead of the short URL. This specific domain is cached on Google and redirects the victim to the authentication page. With this trick in place, criminals can bypass some security agents.

Figure 6: *Specific hardcoded URL found inside the maxtrilha samples disseminated in Portugal.*

In detail, we found some samples distributing the threat in Portugal, Spain, and Mexico as observed below.

Figure 7: *Legitimate portals used to lure the victims during the maxtrilha execution in Portugal, Spain, and Mexico.*

After running the executable, it opens the target page to lure victims while it creates persistence, disables IE security settings, and downloads the 2nd stage into the **%Public%** folder.

As mentioned, the bait page is opened based on the TinyURL short URLs hardcoded inside each binary.

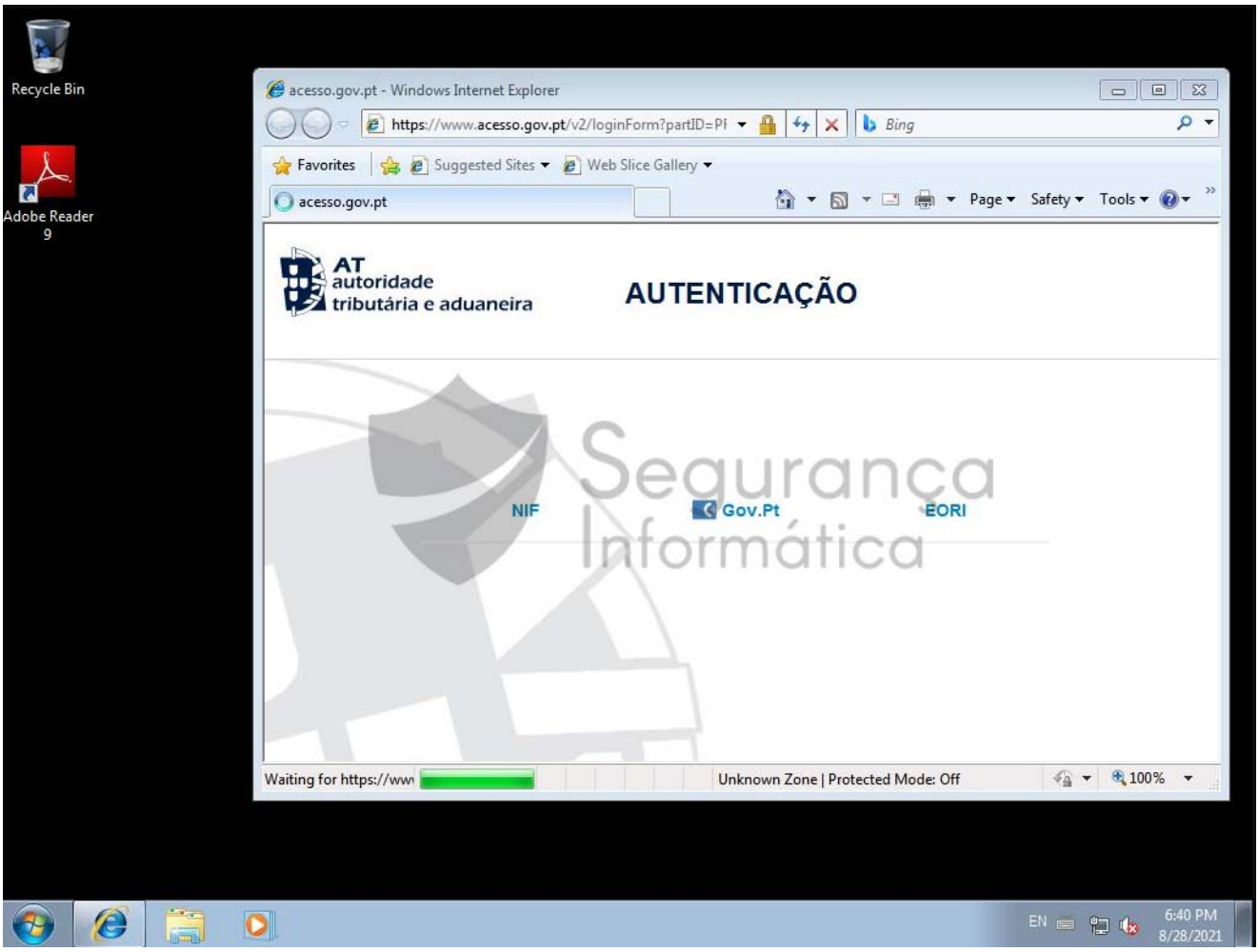

Figure 8: *Legitimate page opened during the malware execution (Portuguese sample).*

After showing the authentication page, the trojan performs specific tasks in the background. The first step is to modify software policy settings, namely the Windows trusted certificates to acts later as a proxy agent. Both the binaries, 1st stage, and 2nd stage perform this operation at runtime:

```
"PdF.exe" (Access type: "CREATE"; Path:
"SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\CA")
"PdF.exe" (Access type: "CREATE"; Path:
"SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED")
"PdF.exe" (Access type: "CREATE"; Path:
"SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUST")
"PdF.exe" (Access type: "CREATE"; Path:
"SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE")
"PdF.exe" (Access type: "CREATE"; Path:
"SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\ROOT")
"MSITrueColor.exe" (Access type: "CREATE"; Path:
"SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\CA")
"MSITrueColor.exe" (Access type: "CREATE"; Path:
"SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\DISALLOWED")
"MSITrueColor.exe" (Access type: "CREATE"; Path:
"SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\ROOT")
"MSITrueColor.exe" (Access type: "CREATE"; Path:
"SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUSTEDPEOPLE")
"MSITrueColor.exe" (Access type: "CREATE"; Path:
"SOFTWARE\POLICIES\MICROSOFT\SYSTEMCERTIFICATES\TRUST")
```

Next, also the **Internet Explorer security settings** are changed to facilitate the download of the 2nd stage without any restriction:

```
Queries sensitive IE security settings:
"iexplore.exe" (Path: "HKCU\SOFTWARE\MICROSOFT\INTERNET EXPLORER\SECURITY"; Key:
"DISABLESECURITYSETTINGSCHECK")
"IEXPLORE.EXE" (Path: "HKCU\SOFTWARE\MICROSOFT\INTERNET EXPLORER\SECURITY"; Key:
"DISABLESECURITYSETTINGSCHECK")


Queries the display settings of system associated file extensions:
"iexplore.exe" (Access type: "QUERYVAL"; Path:
"HKLM\SOFTWARE\CLASSES\SYSTEMFILEASSOCIATIONS\.EXE"; Key: "NEVERSHOWEXT")
"iexplore.exe" (Access type: "QUERYVAL"; Path:
"HKLM\SOFTWARE\CLASSES\SYSTEMFILEASSOCIATIONS\.EXE"; Key: "ALWAYSSHOWEXT")
```

The loader has the capacity of selecting the name of the target file to download; these names are hardcoded in a list with well-known music songs as observed in Figure 9 below. Finally, the 2nd stage is download from the “**sageprototypego.]pt/sept/cult.mp4**” domain path into the %Public% folder and the binary path added to the Windows registry.

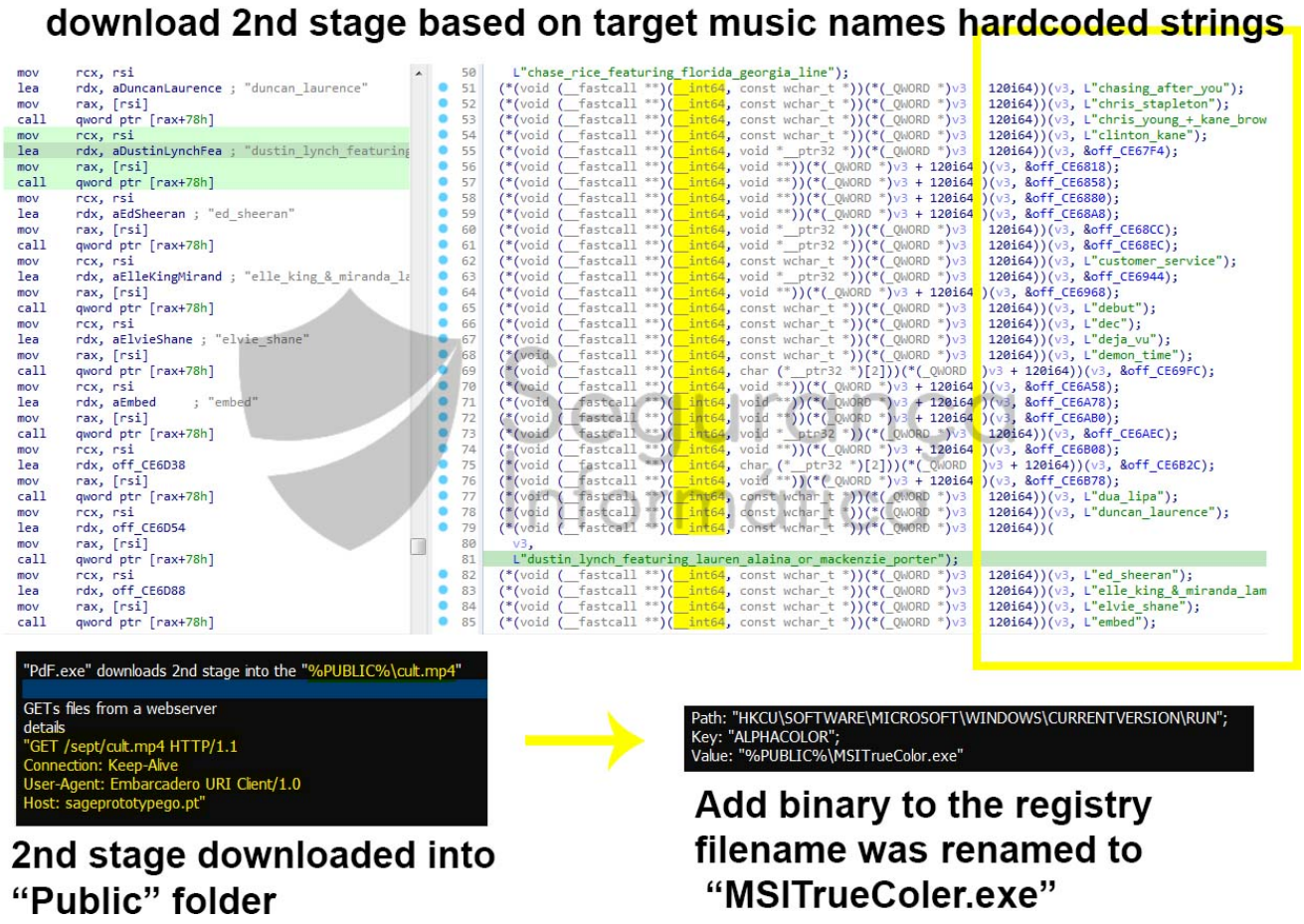

Figure 9: *Maxtrilha 2nd stage downloaded from the Internet based on target hardcoded strings.*

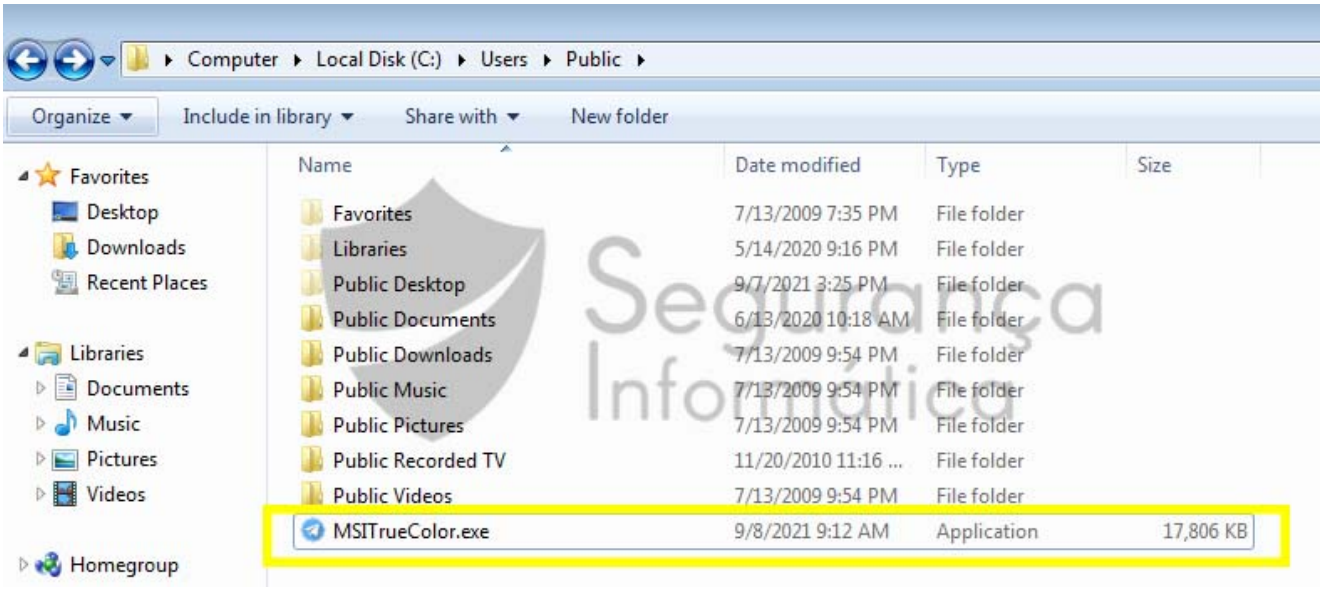

Figure 10: *Maxtrilha 2nd stage is launched every time from the Windows* ***%Public%*** *folder.*

Maxtrilha campaign – A possible kill switch

As a way of preventing further infections through this campaign, the domain from which the 2nd stage is downloaded has been decommissioned, and when the loader tries to unload the binary, it will go into an error loop because it cannot find and inject the new binary into memory (**sageprototypego.]pt**).

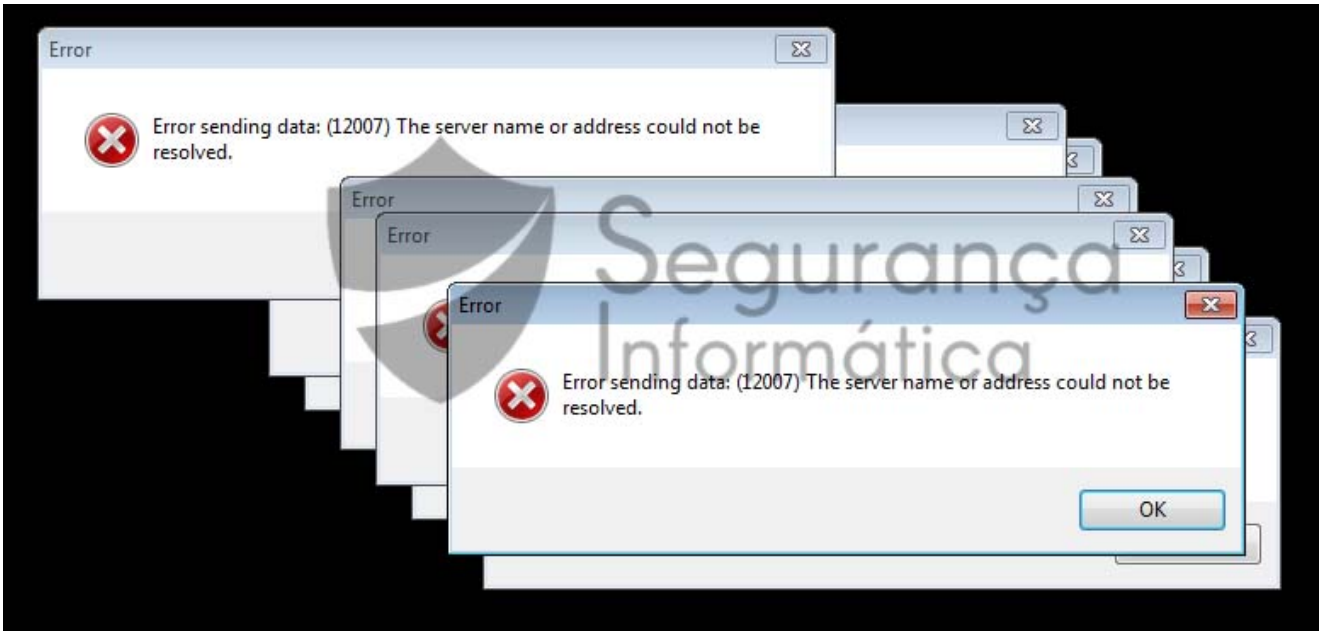

Figure 11: *Possible kill switch of maxtrilha trojan (1st stage – loader).*

Maxtrilha trojan banker – the final stage

Filename: Telegram.exe / MSITrueColor.exe /cult.mp4 / roddy_ricch.mp3
MD5: ea30c0dc58f71a1720990021fda92d1e
Creation date: 2021-09-06 09:06:20

Criminals are constantly creating new ways to make their malicious arsenal FUD. In this case, the maxtrilha trojan, an x64 Delphi binary is not detected as malicious on VirusTotal, allowing to infect a large volume of machines around the world during this campaign.

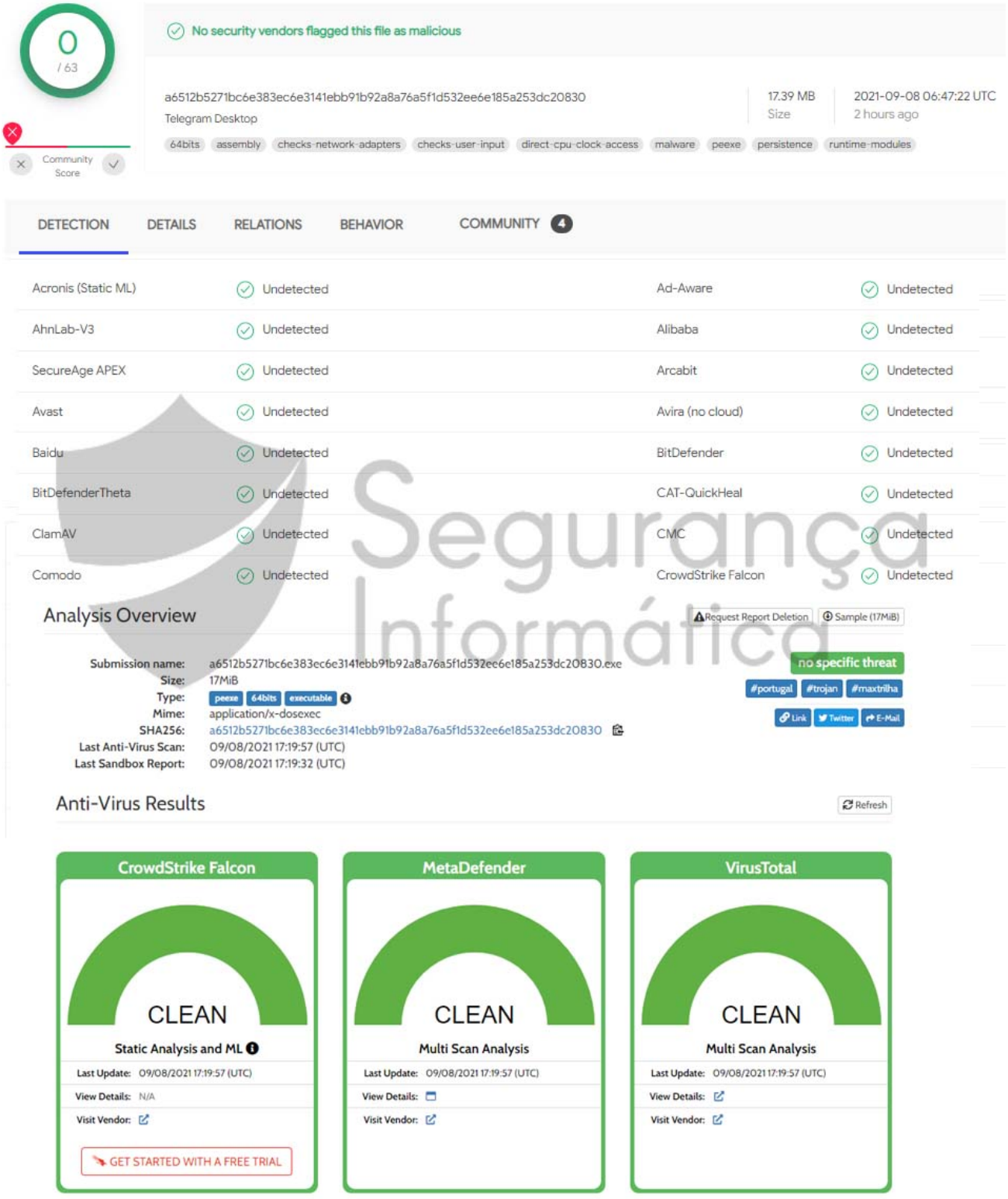

Figure 12: *Maxtrilha trojan 100% FUD, bypassing, thus part of the AVs and EDR systems.*

When the binary is executed, it performs some tasks, including:

- Uses the invertexto.]com online service to check the Internet connection and to get the victims' IP address and their geolocation. Then, it creates the PHP files dynamically on the C2 served based on the victims' IP addresses.
- Checks or creates persistence on the Windows registry.
- Performs monitoring on the user navigation finding by targeting banking portals hardcoded inside the binary.
- Retrieve commands from the C2 server and sent the gathered data.
- It can also deploy additional payloads executed via the DLL injection technique.

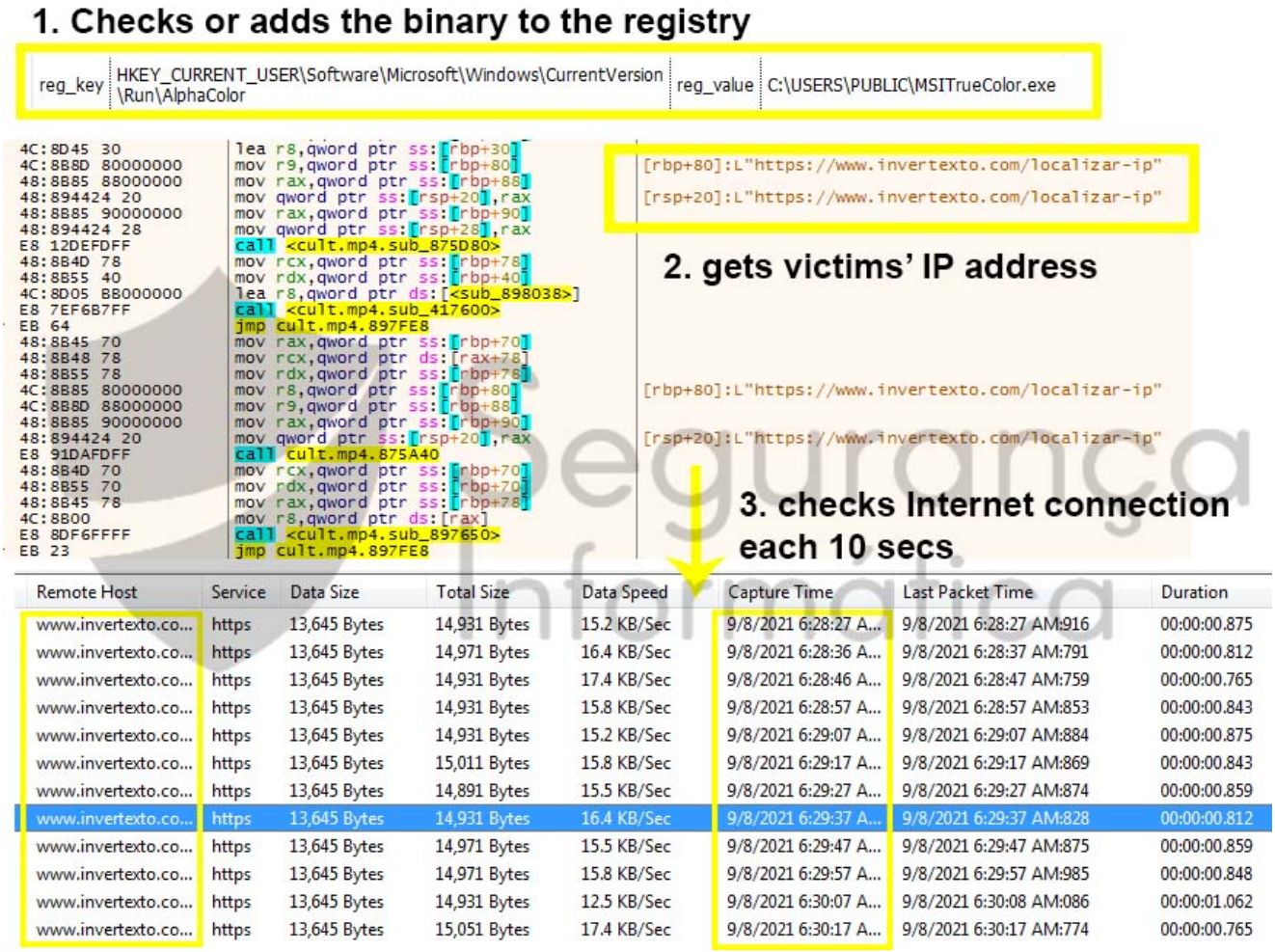

Figure 13: *Maxtrilha checks by Internet connection and adds the binary path to the Windows registry (persistence technique).*

Interestingly, the invertexto.]com service is being used by the maxtrilha trojan creators to obtain victims' IP addresses and at the same time to check by Internet connection. **On a VirusTotal screen**, we can see maxtrilha samples communicating with this address in the last few days.

Passive DNS Replication

Date resolved	Resolver	Domain
2021-09-08	VirusTotal	ec2-54-207-65-61.sa-east-1.compute.amazonaws.com
2019-12-12	VirusTotal	www.invertexto.com
2019-11-22	VirusTotal	invertexto.com
2016-01-26	VirusTotal	getnotifiq.com

Communicating Files

Scanned	Detections	Type	Name
2021-09-09	1 / 67	Win32 EXE	311.exe
2021-09-09	1 / 66	Win32 EXE	100.exe
2021-09-09	3 / 67	Win32 EXE	262.exe
2021-09-09	10 / 67	Win32 EXE	032.exe
2021-09-09	1 / 67	Win32 EXE	222.exe
2021-09-09	10 / 66	Win32 EXE	348.exe
2021-09-09	13 / 66	Win32 EXE	309.exe
2021-09-09	15 / 67	Win32 EXE	ChromaTune.exe
2021-09-09	13 / 65	Win32 EXE	606.exe
2021-09-09	14 / 67	Win32 EXE	561.exe
2021-09-09	9 / 67	Win32 EXE	582.exe
2021-09-09	3 / 68	Win32 EXE	278.exe
2021-09-08	16 / 58	JavaScript	931835777f4c70c5748dd088c6ee7da6e58ec6aeb154f8dc112edb1f7f8f9e3c.js
2021-09-08	36 / 68	Win32 EXE	CoreSync
2021-09-08	34 / 67	Win32 EXE	CoreSync
2021-09-09	19 / 68	Win32 EXE	master.mp4
2021-09-09	21 / 68	Win32 EXE	CriadorUOL.exe
2021-09-08	19 / 67	Win32 EXE	CoreSync
2021-09-09	7 / 57	Win32 EXE	iLovePDF
2021-09-09	5 / 68	Win32 EXE	ChromaTune.exe

Figure 14: *Maxtrilha samples communicating with the legitimate service to validate Internet connection and get the victims' IP addresses.*

During the malware activity, the binary is in a thread loop monitoring Internet browser windows, and matching the opened pages with hardcoded strings, namely substrings related to banks in Latin America and Europe, including Portugal.

```
func_0x31D690( *data_0xD5AE18 );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "abanca" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "accesoempresasbanca" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "acessoonlinebankingabancapt" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "activobank" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "azteca" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "bancanet" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "bancobest" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "bancobpi" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "bancoctt" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "bancodecomerciohome" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "bancomer" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "bankia" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "bankinter" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "bankofireland" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "barclaysonlinebanking" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "b" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "caixabank" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "caixadirecta" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "citibanamex" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "crditoagrcola" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "eurobic" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "halifax" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "halifaxwelcometoonlinebanking"
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "homebank" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "h" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "internetbanking" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "logintodigitalbanking" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "logintoonlinebanking" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "loyds" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "metrobank" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "millenniumbcp" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "montepio24" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "nationwideinternetbank" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "natwestonline" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "novobanco" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "openbank" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "santander" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "scotiaenlinea" );
(*(*data_0xD7DD70 + 120))( data_0xD7DD70, "t" );
```

Figure 15: *Target banks impacted by maxtrilha trojan.*

When the string matches, then the malware communicates with the C2 server geolocated in Russia to perform the following operations:

- It sends initial data related to the machine (hostname) and IP address.
- C2 server receives this information from the **index.php** page, and creates some PHP pages that will allow communication (each victim have specific pages based on their IP address)

With this trick in place, criminals can maintain the thread more invisible as each victim has its specific pages hosted on the same IP addresses.

In detail, some configurations are also obtained from a “webcindario.]com” subdomain, not available at the moment of analyzis.

Figure 16: *Additional configuration retrieved from the webcindario.com sub domain.*

The next image shows the moment the trojan gets the windows name via “**GetWindowsTextW()**” call, and the beginning of the C2 communication with the strings fully encrypted.

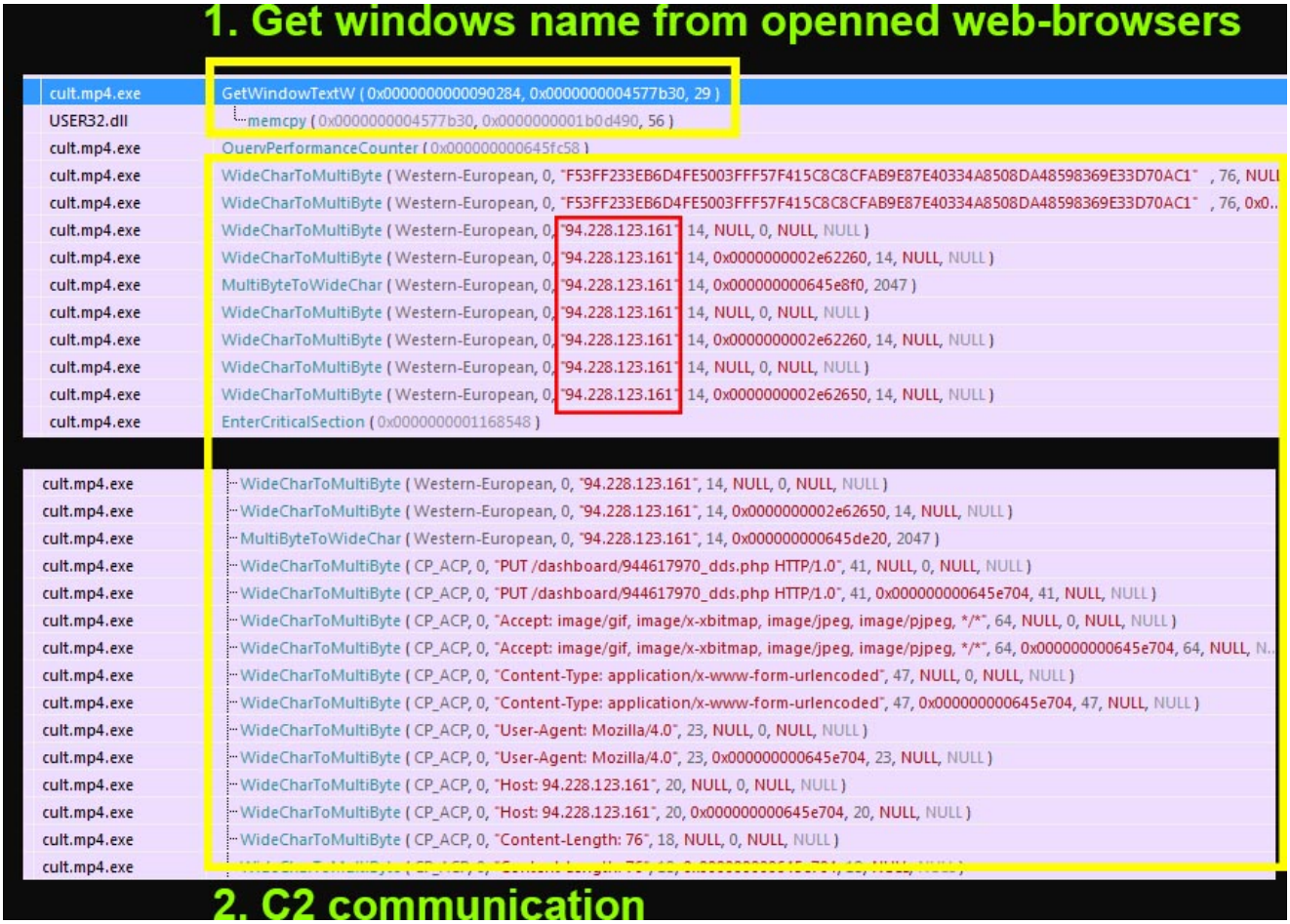

Figure 17: *Maxtrilha C2 communication.*

In detail, the "**maxtrilha123**" key is used to encrypt the clear-text strings in a binary operation each time the trojan sends information to the C2 server.

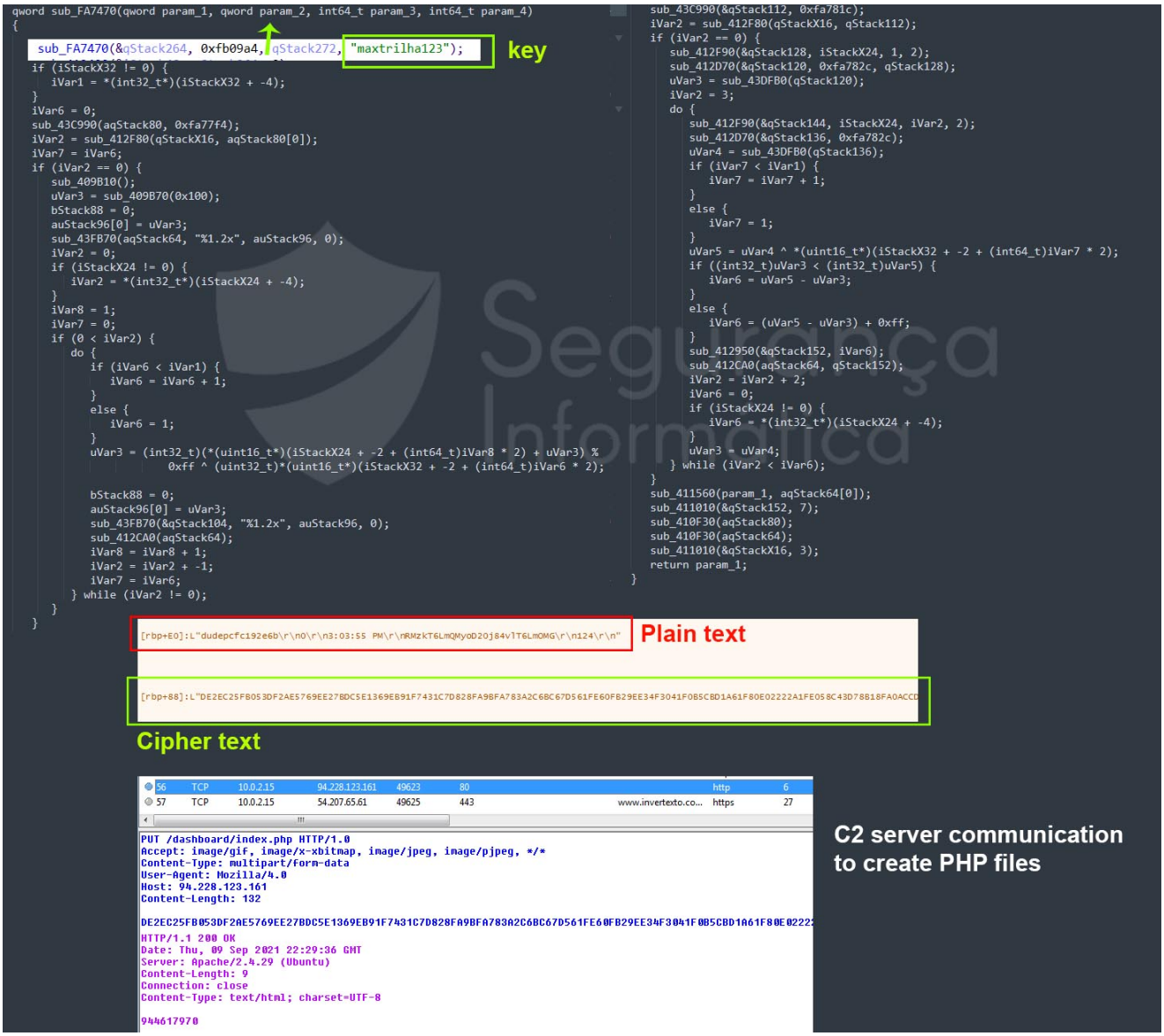

Figure 18: *Pseudo-code of the encryption algorithm used by maxtrilha.*

In another attempt to run the binary, we can see that a similar string is sent; different due to the timestamp the request was sent. This first server request then creates PHP pages on the server-side based on the victim's IP address.

Additional data is sent to the C2 server related to the page the victim is browsing.

Figure 19: *Maxtrilha trojan creating the victim's PHP pages on the C2 server to perform further communication.*

Maxtrilha uses API hashing and introduces well-known calls to perform DLL injection. This technique is then used to deploy additional payloads during the malware execution.

I

```
qword sub_FA5DD0()
{
   qword qVar1;
   if (qword_117DC00 == 0) {
      qword_117DC00 = _GetModuleHandleW("kernel32.dll");
      if (qword_117DC00 != 0) {
         qword_117DC08 = sub_427C00(qword_117DC00, "CreateToolhelp32Snapshot");
         qword_117DC10 = sub_427C00(qword_117DC00, "Heap32ListFirst");
         qword_117DC18 = sub_427C00(qword_117DC00, "Heap32ListNext");
         qword_117DC20 = sub_427C00(qword_117DC00, "Heap32First");
         qword_117DC28 = sub_427C00(qword_117DC00, "Heap32Next");
         qword_117DC30 = sub_427C00(qword_117DC00, "Toolhelp32ReadProcessMemory");
         qword_117DC48 = sub_427C00(qword_117DC00, "Process32First");
         qword_117DC50 = sub_427C00(qword_117DC00, "Process32Next");
         qword_117DC58 = sub_427C00(qword_117DC00, "Process32FirstW");
         qword_117DC60 = sub_427C00(qword_117DC00, "Process32NextW");
         qword_117DC38 = sub_427C00(qword_117DC00, "Process32FirstW");
         qword_117DC40 = sub_427C00(qword_117DC00, "Process32NextW");
         qword_117DC68 = sub_427C00(qword_117DC00, "Thread32First");
         qword_117DC70 = sub_427C00(qword_117DC00, "Thread32Next");
         qword_117DC88 = sub_427C00(qword_117DC00, "Module32First");
         qword_117DC90 = sub_427C00(qword_117DC00, "Module32Next");
         qword_117DC98 = sub_427C00(qword_117DC00, "Module32FirstW");
         qword_117DCA0 = sub_427C00(qword_117DC00, "Module32NextW");
         qword_117DC78 = sub_427C00(qword_117DC00, "Module32FirstW");
         qword_117DC80 = sub_427C00(qword_117DC00, "Module32NextW");
      }
```

Segurança Informática

DLL injection via rundll32.exe

```
if (param_3 == 2) {
   sub_412EA0(&qStack72, 3, "C:\Users\Public\", qStackX8, ".dll");
   cVar1 = sub_FA8BF0(qStackX16, qStack72);
   if (cVar1 == '\x01') {
      sub_412EA0(&qStack80, 5, "RunDll32.exe C:\Users\Public\", qStackX8, 0xfa989c, qStackX32, 0);
      sub_412400(&qStack88, qStack80, 0);
      qVar4 = sub_4122A0(qStack88);
      _WinExec(qVar4, 1);
      sub_412EA0(&qStack96, 5, "RunDll32.exe C:\Users\Public\", qStackX8, 0xfa989c, qStackX32, " - opcao = 2");
      sub_FB1180(*qword_1159AF8, qStack96);
```

Figure 20: *API hashing calls and DLL injection technique found on the binary to probably execute additional payloads at runtime based on specific operations listed below.*

```
- opcao = 1 -
- opcao = 2 -
- opcao = 3 -
- opcao = 4 -
- opcao = 5 -
```

The malware will also send the name of the foreground windows the user is opened to the C2 server. In this case, if for example some of those windows are on a blacklist (x64db, IDA, etc), the trojan may terminate its execution.

As observed below, the two C2 servers hardcoded inside the maxtrilha binary are geolocated in Russia.

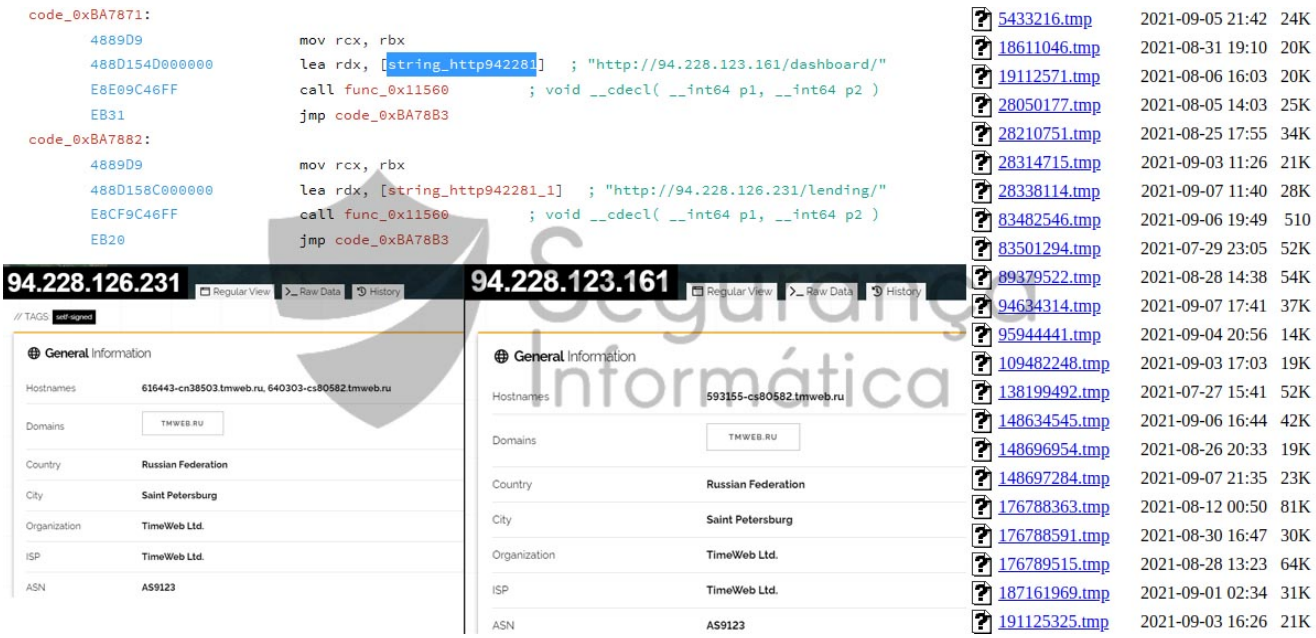

Figure 21: *Maxtrilha C2 servers geolocated in Russia.*

Final Thoughts

Nowadays, we are facing a growing of Brazilian trojans at a very high speed. Each one of them with its peculiarities, TTPs, etc. With this in mind, criminals achieve a FUD condition that allows them to avoid detection and impact a large number of users around the world.

In this sense, monitoring these types of IoCs is a crucial point now, as it is expected that in the coming weeks or months new infections or waves can appear.

Thank you to all who have contributed:

@JAMESWT_MHT
@MiguelSantareno

Mitre Att&ck Matrix

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1	Process Injection 1	Process Injection 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1
Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Rootkit	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Multi-hop Proxy 1
At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2
At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3
Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Proxy 1
Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Ingress Tool Transfer 1

Indicators of Compromise (IOCs)

```
--- .PT domain / phishing ---
ajuda.cld].pt
customdomains.cld].pt
f9z6ja.s.cld].pt
l10j61.s.cld].pt
jxbkwo.s.cld].pt
jdyejh.s.cld].pt
s8dcd2.s.cld].pt
6qwttx.s.cld].pt
n4bi9h.s.cld].pt
oofrae.s.cld].pt
9kvxv4.s.cld].pt
wuivjh.s.cld].pt
fe67gp.s.cld].pt
9iu549.s.cld].pt
n9i202.s.cld].pt
bt81tf.s.cld].pt
xrrj0n.s.cld].pt
uvt3z5.s.cld].pt
s5ex1t.s.cld].pt
xmr83x.s.cld].pt
kq4di7.s.cld].pt
1zpajx.s.cld].pt
z6vfcl.s.cld].pt
9owib7.s.cld].pt
fml494.s.cld].pt
dzitjy.s.cld].pt
re4fof.s.cld].pt
4inxd5.s.cld].pt
u42sld.s.cld].pt
d2t6ms.s.cld].pt
sq26oz.s.cld].pt
jx7w68.s.cld].pt
cx0px4.s.cld].pt
85928p.s.cld].pt
gdrwxi.s.cld].pt
4fblxh.s.cld].pt
sj788n.s.cld].pt
vzqr6b.s.cld].pt
h61mhu.s.cld].pt
9jhvyu.s.cld].pt
qeko0l.s.cld].pt
9puund.s.cld].pt
5yxgae.s.cld].pt
a4g9no.s.cld].pt
y64ryi.s.cld].pt
vh69rv.s.cld].pt
ct156d.s.cld].pt
08c5gz.s.cld].pt
ruc8oq.s.cld].pt
jx976j.s.cld].pt
xya9om.s.cld].pt
636jm3.s.cld].pt
83hiwm.s.cld].pt
6yd25k.s.cld].pt
```

t47mir.s.cld].pt
vla9xi.s.cld].pt
7l6ceh.s.cld].pt
3y1oe3.s.cld].pt
n7d6of.s.cld].pt
as4435.s.cld].pt
a5cyc9.s.cld].pt
bg7zew.s.cld].pt
ahgkmu.s.cld].pt
q82hrg.s.cld].pt
hgpa0p.s.cld].pt
15yqcr.s.cld].pt
lc465n.s.cld].pt
cp0adm.s.cld].pt
axbkpv.s.cld].pt
gajior.s.cld].pt
paw2d2.s.cld].pt
1uu2ol.s.cld].pt
h3tqgn.s.cld].pt
iwtosz.s.cld].pt
suymo6.s.cld].pt
ujglwa.s.cld].pt
tewkko.s.cld].pt
0xhmwn.s.cld].pt
5yn5zo.s.cld].pt
7bx0xw.s.cld].pt
3b8iph.s.cld].pt
g47px2.s.cld].pt
blg4jc.s.cld].pt
7tf950.s.cld].pt
viz4lu.s.cld].pt
7bbzfr.s.cld].pt
3o47pq.s.cld].pt
fffzbw.s.cld].pt
mmxls9.s.cld].pt
355ij9.s.cld].pt
1dsuij.s.cld].pt
turjqi.s.cld].pt
2st9tz.s.cld].pt
npnn8d.s.cld].pt
nch1tb.s.cld].pt
qouimg.s.cld].pt
qx45dz.s.cld].pt
58kzfe.s.cld].pt
u9lrss.s.cld].pt
zt61iz.s.cld].pt

-- domain used to get config ---
https://abrilprorock2018.]webcindario.]com/br/
https://abrilprorock2018.]webcindario.]com/nt/
https://abrilprorock2018.]webcindario.]com/baby/
https://abrilprorock2018.]webcindario.]com/hs/
https://abrilprorock2018.]webcindario.]com/jf/
https://abrilprorock2018.]webcindario.]com/hass/

```
-- C2 server --
94.228.123.]161
94.228.126.]231
sageprototypego.]pt/sept/cult.mp4" /]

-- samples--
1st stage: 043f535f68678652c50ff49cf03ee4b63fdbd03b76c732adfe83074335fbbb3b
2nd stage: a6512b5271bc6e383ec6e3141ebb91b92a8a76a5f1d532ee6e185a253dc20830

--short URLs--
https://tinyurl.]com/flexibiliza
https://tinyurl.]com/tributodashboard
http://tinyurl.]com/yjsfpjau
https://tinyurl.]com/ye65hycr
https://tinyurl.]com/tabloide01
http://tinyurl.]com/yh3mhn8o
https://tinyurl.]com/y6hkrtv6
```

Online Sandbox URLs

–https://app.any.run/tasks/b734235a-b6e1-4dbe-8d13-2709b9e282a0/
–https://www.joesandbox.com/analysis/847611
-https://capesandbox.com/analysis/186437/#

Samples

https://bazaar.abuse.ch/browse/tag/abrilprorock2018.webcindario.com/
https://bazaar.abuse.ch/browse/tag/54.207.65.61/
https://bazaar.abuse.ch/browse/tag/sageprototypego.pt/
https://bazaar.abuse.ch/sample/a6512b5271bc6e383ec6e3141ebb91b92a8a76a5f1d532ee6e185a253dc20830/

Yara Rule

```
import "pe"
rule maxtrilha_banking_trojan_loader_2021 {
meta:
    description = "Yara rule for maxtrilha trojan banker (loader) - September 2021
version"
    author = "SI-LAB - https://seguranca-informatica.pt"
    last_updated = "2021-09-10"
    tlp = "white"
    category = "informational"

    strings:
    $s_a = {68 00 74 00 74 00 70 00 73 00 3A 00 2F 00 2F 00 77 00 77 00 77 00 2E 00
69 00 6E 00 76 00 65 00 72 00 74 00 65 00 78 00 74 00 6F 00 2E 00 63 00 6F 00 6D 00
2F 00 6C 00 6F 00 63 00 61 00 6C 00}
    $s_b = {73 00 61 00 67 00 65 00 70 00 72 00 6F 00 74 00 6F 00 74 00 79 00 70 00
65 00 67 00 6F 00 2E 00 70 00 74 00 2F 00 73 00 65 00 70 00 74 00 2F 00 63 00 75 00
6C 00 74 00 2E 00 6D 00 70 00 33 00}
    condition:
        filesize < 20000KB
        and all of ($s_*)
}



rule maxtrilha_banking_trojan_2nd_stage_2021 {
meta:
    description = "Yara rule for maxtrilha trojan banker (2nd stage) - September 2021
version"
    author = "SI-LAB - https://seguranca-informatica.pt"
    last_updated = "2021-09-10"
    tlp = "white"
    category = "informational"

    strings:
    $s_a = {62 00 72 00 69 00 6C 00 70 00 72 00 6F 00 72 00 6F 00 63 00 6B 00 32 00
30 00 31 00 38 00 2E 00 77 00 65 00 62 00 63 00 69 00 6E 00 64 00 61 00 72 00 69 00
6F 00 2E 00 63 00 6F 00 6D 00 2F 00}
    $s_b = {68 00 74 00 74 00 70 00 73 00 3A 00 2F 00 2F 00 77 00 77 00 77 00 2E 00
69 00 6E 00 76 00 65 00 72 00 74 00 65 00 78 00 74 00 6F 00 2E 00 63 00 6F 00 6D 00
2F 00 6C 00 6F 00 63 00 61 00 6C 00}
    $s_c = {00 34 00 2E 00 32 00 32 00 38 00 2E 00 31 00 32 00 33 00 2E 00 31 00 36
00 31 00 2F 00 64 00 61 00}
    condition:
        filesize < 20000KB
        and all of ($s_*)
}
```

The Yara rules are also **available on GitHub**.

Pedro Tavares

Pedro Tavares is a professional in the field of information security working as an Ethical Hacker/Pentester, Malware Researcher and also a Security Evangelist. He is also a founding member at CSIRT.UBI and Editor-in-Chief of the security computer blog seguranca-informatica.pt.

In recent years he has invested in the field of information security, exploring and analyzing a wide range of topics, such as pentesting (Kali Linux), malware, exploitation, hacking, IoT and security in Active Directory networks. He is also Freelance Writer (Infosec. Resources Institute and Cyber Defense Magazine) and developer of the 0xSI_f33d – a feed that compiles phishing and malware campaigns targeting Portuguese citizens.

Read more here.