Informe Código Dañino
CCN-CERT ID-15/20

Snake Locker

Mayo 2020

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

centro criptológico nacional

Fecha de Edición: mayo de 2020

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. RESUMEN EJECUTIVO

El presente documento recoge el análisis de la muestra de código dañino identificada por la firma **MD5 47EBE9F8F5F73F07D456EC12BB49C75D**, perteneciente a la familia de ransomware **Snake Locker**. El principal objetivo de esta muestra es cifrar los ficheros de todos los dispositivos conectados al equipo para, posteriormente, solicitar el pago de un rescate en bitcoins a cambio de la herramienta de descifrado. Durante el análisis se han encontrado evidencias que relacionan esta muestra de código dañino con el ataque ransomware sufrido por el grupo alemán del sector sanitario **Fresenius.**

3. SNAKE LOCKER

3.1 DETALLES GENERALES

La muestra analizada en este apartado es un ejecutable de 32 bits, sin firma digital y con el siguiente hash MD5:

NOMBRE FICHERO	MD5
Desconocido	47EBE9F8F5F73F07D456EC12BB49C75D

La fecha de compilación es nula, por esta razón el valor representado es 1 enero de 1970, 00:00:00 (UTC):

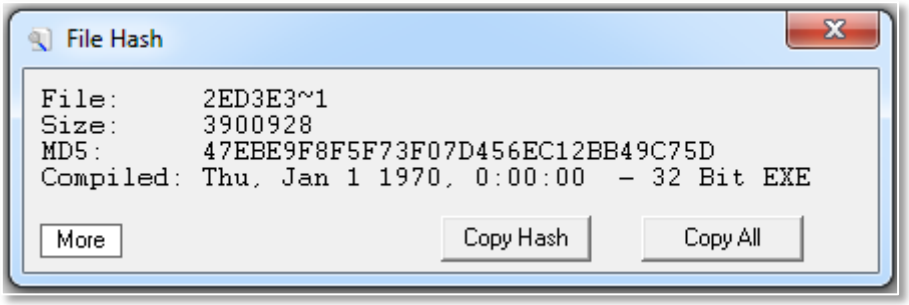


Figura 1. Fechas de compilación de la muestra.

La muestra no presenta propiedades del fichero.

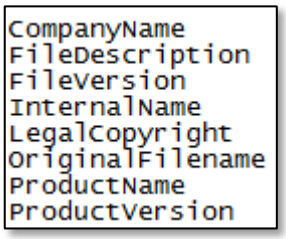


Figura 2. Las propiedades de los ficheros están vacías.

3.2 ANÁLISIS TÉCNICO

El código dañino ha sido desarrollado mediante el lenguaje de programación **GoLang (Go 1.10)**. Aunque no es un lenguaje comúnmente utilizado para el desarrollo de código dañino, últimamente está siendo más utilizado por los atacantes, especialmente en RaaS (Ransomware as a Service). El código dañino contiene un alto grado de rutinas de ofuscación, lo que lo hace difícil de analizar.

```
File: 2ed3e37608e65be8b6e8c59f8c93240bd0efe9a60c08c21f4889c00eb6082d74.exe
MD5:  47ebe9f8f5f73f07d456ec12bb49c75d
Size: 3900928

Ascii Strings:
------------------------------------------------------------------------------
0000004D  !This program cannot be run in DOS mode.
00000178  .text
0000019F  `.data
000001C8  .idata
000001F0  .symtab
00000401  Go build ID: "SPlES9E155q_V-b330Fx/tblnamFk-AFuyVtAqkB6/L8WLP6oE3GX
FUGixfAITrn2V"
```

Figura 3. Código dañino programado en GoLang.

El código dañino comienza su ejecución resolviendo la dirección IP de "**ADS.FRESENIUS.COM**". **Fresenius** es un gran grupo alemán del sector sanitario, que se ha visto afectado por un ataque de ransomware recientemente. Con base a esta información, se puede afirmar que esta muestra de SNAKE es la utilizada en este ataque.

```
.text:00545760                jbe     loc_5458A4
.text:00545766                sub     esp, 4Ch
.text:00545769                lea     eax, aAdsFreseniusCo ; "ADS.FRESENIUS.COM"
.text:0054576F                mov     [esp+4Ch+var_4C], eax
.text:00545772                mov     [esp+4Ch+var_48], 11h
.text:0054577A                call    net_LookupIP
.text:0054577F                mov     eax, [esp+4Ch+var_40]
```

Figura 4. Resolución de ADS.FRESENIUS.COM.

La IP resultante de la resolución DNS es comparada con "**10.2.10.41**", que como se puede observar se trata de una IP privada. No se han encontrado referencias públicas de IP pública asociada a la dirección "**ADS.FRESENIUS.COM**", por lo que lo más seguro es que se trate de una dirección interna de la compañía, solo accesible desde su intranet. Seguramente los atacantes ya disponían de acceso a la red interna de la compañía antes de lanzar el ataque de ransomware. El atacante ha utilizado este método a modo de "**killswitch**", con la finalidad de limitar su ataque a equipos de la propia compañía, ya que solo equipos conectados a su red interna serán capaces de resolver "**ADS.FRESENIUS.COM**" a la dirección IP ("**10.2.10.41**"). Si la dirección no puede resolverse o la IP no coincide con "**10.2.10.41**", el código dañino terminará su ejecución, pero antes descifrará en memoria la siguiente cadena de texto "**There can be only one**", pero no la utilizará para nada. El proceso de descifrado es el siguiente:

- Cada byte es incrementado en **0x2A**
- La cadena resultante es descifrada mediante XOR y la siguiente clave:
  31 0C A3 60 37 5A A7 C1 38 06 10 31 6D 6C 70 0F B0 CB C0 1D 4D 2D

Este algoritmo de descifrado es utilizado para el descifrado de todas las cadenas de texto utilizadas durante la ejecución del código dañino, pero cada cadena utiliza una clave XOR diferente. El apéndice IV contiene un script en IdaPython que permite descifrar todas las cadenas cifradas del código dañino.

```
runtime_stringtoslicebyte(&v26, data_enc, 0x1C);
v33 = v8;
runtime_stringtoslicebyte(&v18, xor_key_, 0x1C);
v32 = v8;
fillmem___(0, &v11);
v1 = v32;
v2 = v33;
for ( i = 0; (int)i < v9; ++i )
{
  if ( i >= v0 || i >= 0x1C )
    runtime_panicindex(
      v5,
      v6,
      v7,
      v8,
      v9,
      v10,
      v9,
      v11,
      v12,
      v13,
      v14,
      v15,
      v16,
      v17,
      v18,
      v19,
      v20,
      v21,
      v22,
      v23,
      v24,
      v25,
      v26,
      v27,
      v28,
      v29,
      v30,
      v31);
  *((_BYTE *)&v11 + i) = *(_BYTE *)(v1 + i) ^ (*(_BYTE *)(v2 + i) + 0x2A);
}
runtime_slicebytetostring(0, &v11, 28, 28);
```

Figura 5. Algoritmo de cifrado de las cadenas de texto.

Seguidamente el código dañino utiliza Windows Management Interface (WMI) para ejecutar el comando "**select DomainRole FROM Win32_ComputerSystem**" con el fin de identificar si el equipo pertenece a un dominio o no y el tipo de role que tiene

dentro de ese dominio. El código dañino solo continuará su ejecución si se trata de un **Servidor del dominio**, un **Controlador Primario del dominio** o un **Controlador Secundarios de dominio**. Lo que significa que cualquier Workstation del dominio o no asociado a ningún dominio, no será infectada.

Siguiendo con su ejecución, el código dañino crea el siguiente mutex: **Global\EKANS.** Si el mutex ya existe en el sistema, el código dañino finalizará su ejecución, por lo que la creación de un mutex en el sistema podría utilizarse para bloquear la infección de este código dañino.

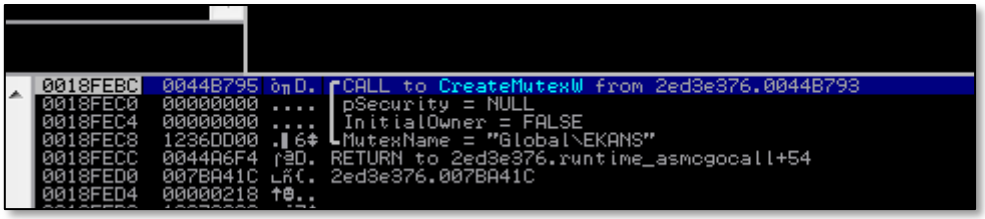


Figura 6. Creación del Mutex.

El código dañino contiene embebido en su código la siguiente clave pública RSA:

RSA CLAVE PÚBLICA
-----BEGIN RSA PUBLIC KEY-----
MIIBCgKCAQEAuMBx+hZWQFjyOGwHtb13JhGJS6FohQRzg4ouAuFPC59VydRSfcWp
0YCwSMR4NbJw38/527eGeG3vPeSg1aqz4fFEISm3GR9i2bLWxl7r7gQx2iuwQbZJ
jzSm7ymwc7P9rOERdgTHFltz+x1JIa/pUEUdjpSgJMrcEYeix4TDVUjKMPFZbvAo
wU/wTRJmb6/Cv0ibyEfyDNUazP+jdqojgI9egCmRTX56LmH41Q1Y3pQQFLFx0pge
MOizcr4c0HAqUJw9lu2/a4ATQ/DS/nk3J2DF+1RPhDXWrYJY3iIK6NldZTa2ZWx4
ZDfceIe2t/4GcgpBdSTU9Q+fBmbcyY3qvQIDAQAB
-----END RSA PUBLIC KEY-----

El código dañino contiene una extensa lista de nombres de servicios. Esta lista, debido a su extensión, se ha incluido en el apéndice II. Si el servicio existe en el sistema y está activo, el código dañino detendrá su ejecución.

```
text:0055ADF6                   mov     eax, 0
text:0055ADFB                   lea     edi, [esp+13ACh+var_9F8]
text:0055AE02                   call    fillmem_____
text:0055AE07                   call    main_decrypt_Acronis_VSS_Prov ; Acronis VSS Provider
text:0055AE0C                   mov     eax, [esp+13ACh+var_13A8]
text:0055AE10                   mov     [esp+13ACh+var_115C], eax
text:0055AE17                   mov     ecx, [esp+13ACh+var_13AC]
text:0055AE1A                   mov     [esp+13ACh+var_C98], ecx
text:0055AE21                   call    main_decrypt_Enterprise_Clien ; Enterprise Client Service
text:0055AE26                   mov     eax, [esp+13ACh+var_13A8]
text:0055AE2A                   mov     [esp+13ACh+var_1160], eax
text:0055AE31                   mov     ecx, [esp+13ACh+var_13AC]
text:0055AE34                   mov     [esp+13ACh+var_C9C], ecx
text:0055AE3B                   call    main_decrypt_Sophos_Agent ; Sophos Agent
text:0055AE40                   mov     eax, [esp+13ACh+var_13A8]
text:0055AE44                   mov     [esp+13ACh+var_1164], eax
text:0055AE4B                   mov     ecx, [esp+13ACh+var_13AC]
text:0055AE4E                   mov     [esp+13ACh+var_CA0], ecx
text:0055AE55                   call    main_decrypt_Sophos_AutoUpdat ; Sophos AutoUpdate Service
text:0055AE5A                   mov     eax, [esp+13ACh+var_13A8]
text:0055AE5E                   mov     [esp+13ACh+var_1168], eax
text:0055AE65                   mov     ecx, [esp+13ACh+var_13AC]
text:0055AE68                   mov     [esp+13ACh+var_CA4], ecx
text:0055AE6F                   call    main_decrypt_Sophos_Clean_Ser ; Sophos Clean Service
text:0055AE74                   mov     eax, [esp+13ACh+var_13A8]
```

Figura 7. Ejemplo de los nombres de servicios a detener.

También contiene una lista de nombres de procesos, incluida en el apéndice III, que el código dañino utilizará como lista negra, de forma que si el proceso se encuentra en ejecución, el código dañino detendrá su ejecución mediante **TerminateProcess()**.

```
text:00547D59                   mov     [esp+4658h+var_2320], eax
text:00547D60                   mov     [esp+4658h+var_231C], eax
text:00547D67                   call    main_decrypt_ccflic0_exe ; ccflic0.exe
text:00547D6C                   mov     eax, [esp+4658h+var_4654]
text:00547D70                   mov     [esp+4658h+var_34C0], eax
text:00547D77                   mov     ecx, [esp+4658h+var_4658]
text:00547D7A                   mov     [esp+4658h+var_232C], ecx
text:00547D81                   call    main_decrypt_ccflic4_exe ; ccflic4.exe
text:00547D86                   mov     eax, [esp+4658h+var_4654]
text:00547D8A                   mov     [esp+4658h+var_34C4], eax
text:00547D91                   mov     ecx, [esp+4658h+var_4658]
text:00547D94                   mov     [esp+4658h+var_2330], ecx
text:00547D9B                   call    main_decrypt_healthservice_ex ; healthservice.exe
text:00547DA0                   mov     eax, [esp+4658h+var_4654]
text:00547DA4                   mov     [esp+4658h+var_34C8], eax
text:00547DAB                   mov     ecx, [esp+4658h+var_4658]
text:00547DAE                   mov     [esp+4658h+var_2334], ecx
text:00547DB5                   call    main_decrypt_ilicensesvc_exe ; ilicensesvc.exe
text:00547DBA                   mov     eax, [esp+4658h+var_4654]
text:00547DBE                   mov     [esp+4658h+var_34CC], eax
text:00547DC5                   mov     ecx, [esp+4658h+var_4658]
text:00547DC8                   mov     [esp+4658h+var_2338], ecx
text:00547DCF                   call    main_decrypt_nimbus_exe ; nimbus.exe
text:00547DD4                   mov     eax, [esp+4658h+var_4654]
text:00547DD8                   mov     [esp+4658h+var_34D0], eax
text:00547DDF                   mov     ecx, [esp+4658h+var_4658]
text:00547DE2                   mov     [esp+4658h+var_233C], ecx
text:00547DE9                   call    main_decrypt_prlicensemgr_exe ; prlicensemgr.exe
```

Figura 8. Ejemplo de los nombres de procesos a terminar.

Muchos de estos procesos y servicios están relacionados con sistemas SCADA, máquinas virtuales, sistemas de control industrial, sistemas de administración remota, aplicaciones de administración de red, etc.

Nuevamente utiliza Windows Management Interface (WMI) para obtener información de las copias de seguridad "Shadow", mediante el siguiente comando: **"SELECT * FROM Win32_ShadowCopy"**. Una vez obtenida la lista de las copias "Shadow", procederá a borrarlas todas.

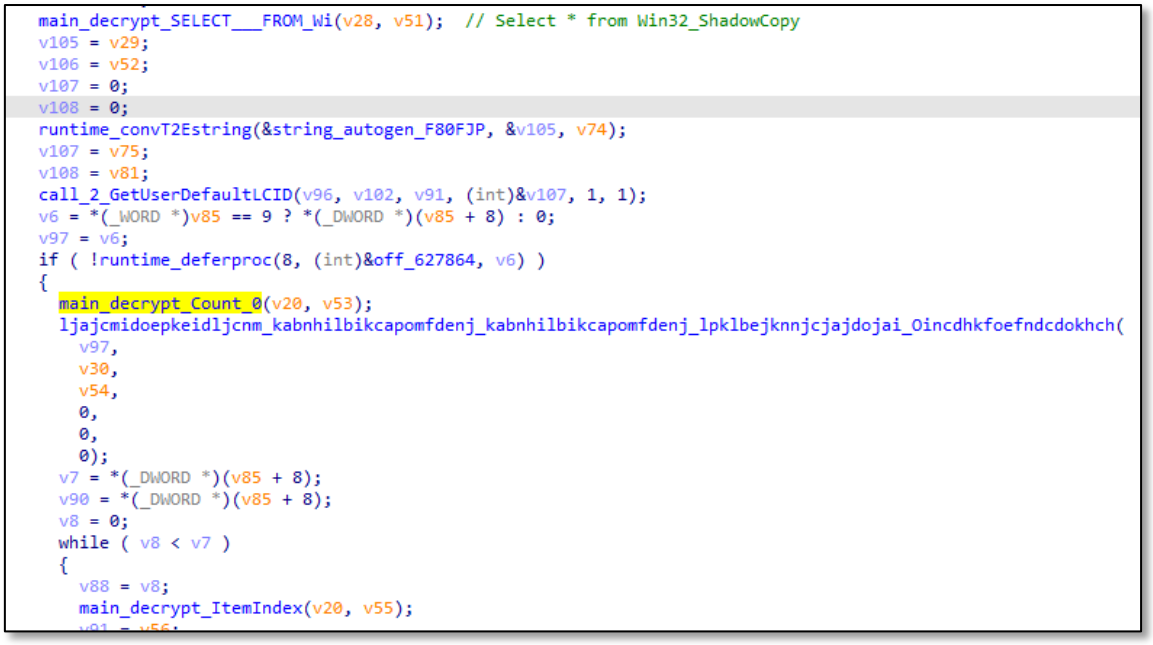


Figura 9. Borrado de las copias de seguridad "Shadow".

El código dañino excluirá del cifrado cualquiera de los ficheros del directorio Windows (excepto el directorio Temp) y también los siguientes ficheros, independientemente de su localización.

FICHEROS EXCLUIDOS	
Ntldr	NTDETECT.COM
boot.ini	Bootfont.bin
Bootsect.bak	Desktop.ini
Ctfmon.exe	Iconcache.db
Ntuser.dat	Ntuser.dat.log
Ntuser.ini	Thumbs.db

Los siguientes ficheros y extensiones tampoco serán cifrados si se encuentran en alguno de los siguientes directorios (incluida una expresión regular):

FICHEROS EXCLUIDOS	
Desktop.ini	Iconcache.db
Ntuser.dat	Ntuser.ini
Ntuser.dat.log1	Ntuser.dat.log2
Usrclass.dat	Usrclass.dat.log1
Usrclass.dat.log2	Bootmgr
Bootnxt	

EXTENSIONES EXCLUIDAS					
.dll	.exe	.sys	.mui	.tmp	.lnk
.config	.settingcontent-ms	.tlb	.olb	.blf	.ico
.regtrans-ms	.devicemetadata-ms	.manifest	.bat	.cmd	.ps1

DIRECTORIOS EXCLUIDOS
:\$Recycle.Bin
:\ProgramData
:\Users\All Users
:\Program Files
:\Local Settings
:\Boot
:\System Volume Information
:\Recovery\
\AppData\
\Temp\
.+\\Microsoft\\(User Account Pictures|Windows\\(Explorer|Caches)|Device Stage\\Device|Windows)\\

Aunque el código dañino contiene la siguiente lista de extensiones de fichero, no está clara su funcionalidad, ya que el código dañino parece no utilizarla y cifra ficheros con extensiones que no están incluidas en esta lista.

LISTA DE EXTENSIONES		
.docx	.sql	.bkp
.accdb	.py	.db
.accde	.ppam	.db-journal
.accdr	.pps	.csproj
.accdt	.ppsm	.sln
.asp	.ppsx	.md
.aspx	.ppt	.pl
.back	.pptm	.js
.backup	.pptx	.html
.backupdb	.hpp	.htm
.bak	.java	.dbf
.mdb	.jsp	.rdo
.mdc	.php	.arc
.mdf	.doc	.vhd
.war	.docm	.vmdk
.xls	.pst	.vdi
.xlsx	.psd	.vhdx
.xlsm	.dot	.edb
.xlr	.dotm	.c
.zip	.cpp	.h
.rar	.cs	
.sqlitedb	.csv	

Durante el proceso de cifrado, el código dañino cifra los ficheros mediante **AES en modo CTR**, con una clave de **0x20 bytes** y un **IV de 0x10 bytes**, ambos generados aleatoriamente.

```
v35 = v12;
v34 = v10;
runtime_makeslice64(&uint8, 16, 0, 16, 0, v19, v23);
v33 = v27;
IV_size_ = IV_size;
IV_ = IV;
crypto_rand_Read(IV, IV_size);
main_dasfasd(AES_key_size, IV);
runtime_makeslice(&uint8);
v30 = AES_key_size;
IV__ = IV;
AES_key_ = AES_key;
crypto_rand_Read(AES_key, AES_key_size);
main_dasfasd(AES_key_size, IV);
if ( v34 > 0x9C4000 && v35 == 0 || v35 > 0 )
{
  main_encrypt_file(v39, AES_key, AES_key_size, IV, IV, IV_size, v27, v27);
  v49 = v27;
  v4 = 2;
}
```

Figura 10. Generación de la clave AES y del IV.

La clave AES es cifrada mediante **RSA-OAEP** y **ripemd160** como función hash. La clave pública utilizada es la extraída del cuerpo del código dañino.

```
runtime_newobject(&sha1_digest);
*ripemd160_hash_func = 0x67452301;
ripemd160_hash_func[1] = 0xEFCDAB89;
ripemd160_hash_func[2] = 0x98BADCFE;
ripemd160_hash_func[3] = 0x10325476;
ripemd160_hash_func[4] = 0xC3D2E1F0;
ripemd160_hash_func[21] = 0;
ripemd160_hash_func[22] = 0;
ripemd160_hash_func[23] = 0;
crypto_rsa_EncryptOAEP(
  (int)&off_6BACC0,
  (int)ripemd160_hash_func,
  dword_7B9640,
  dword_7B9644,
  a1,
  aes_key,
  a3,
  a4,
  0,
  0,
  0);
```

Figura 11. Cifrado de la clave AES.

El código dañino utiliza la codificación **GOB** (propia del lenguaje GO) para incluir la clave AES cifrada, el IV y el nombre del fichero al final del fichero cifrado.

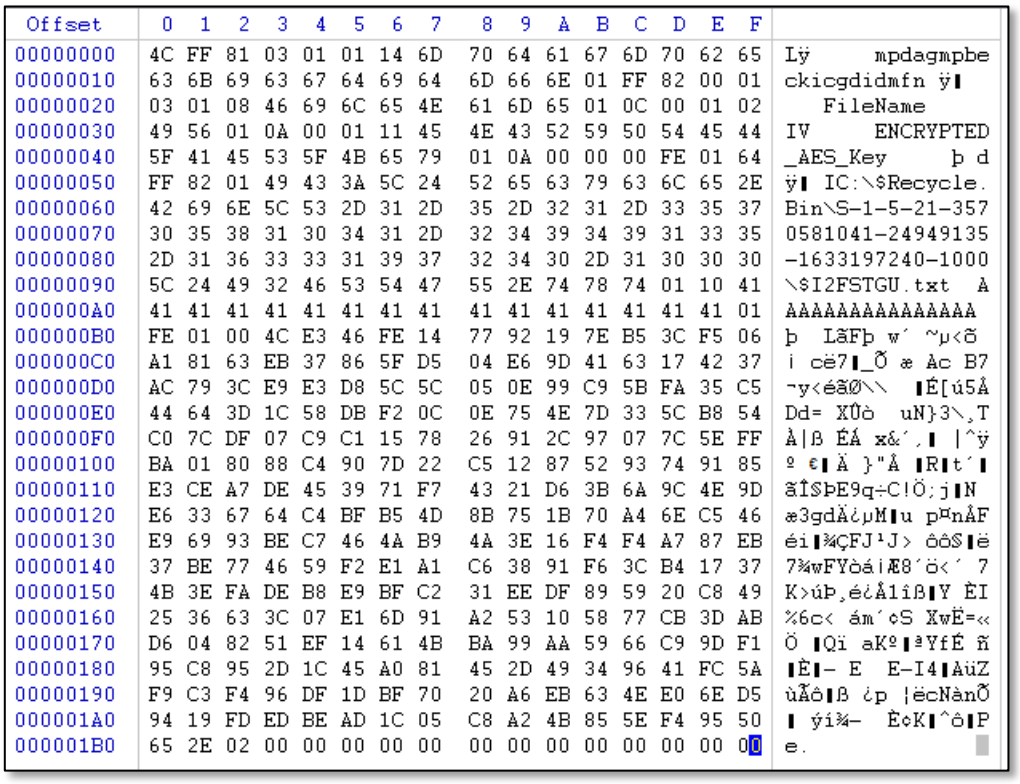
```
runtime_newobject(&bytes_Buffer);
v28 = v15;
((void (__cdecl *)(interfaceType **))encoding_gob_NewEncoder)(&off_6BA260);
v27 = v17;
((void (*)(void))loc_44B376)();
runtime_convT2E(&main_mpdagmpbeckicgdidmfn, &v34);
encoding_gob__ptr_Encoder_Encode(v17, v17, v18);
result = v18;
if ( !v18 )
{
  os___File__Seek(a10, 0, 0);
  if ( v21 )
  {
    main_decrypt__v__1(v13, v16);
    sub_545470();
    result = v22;
  }
```

Figura 12. Codificación **GOB** de la clave AES.

La estructura utilizada para la codificación **GOB** es la siguiente:

GOB ESTRUCTURA

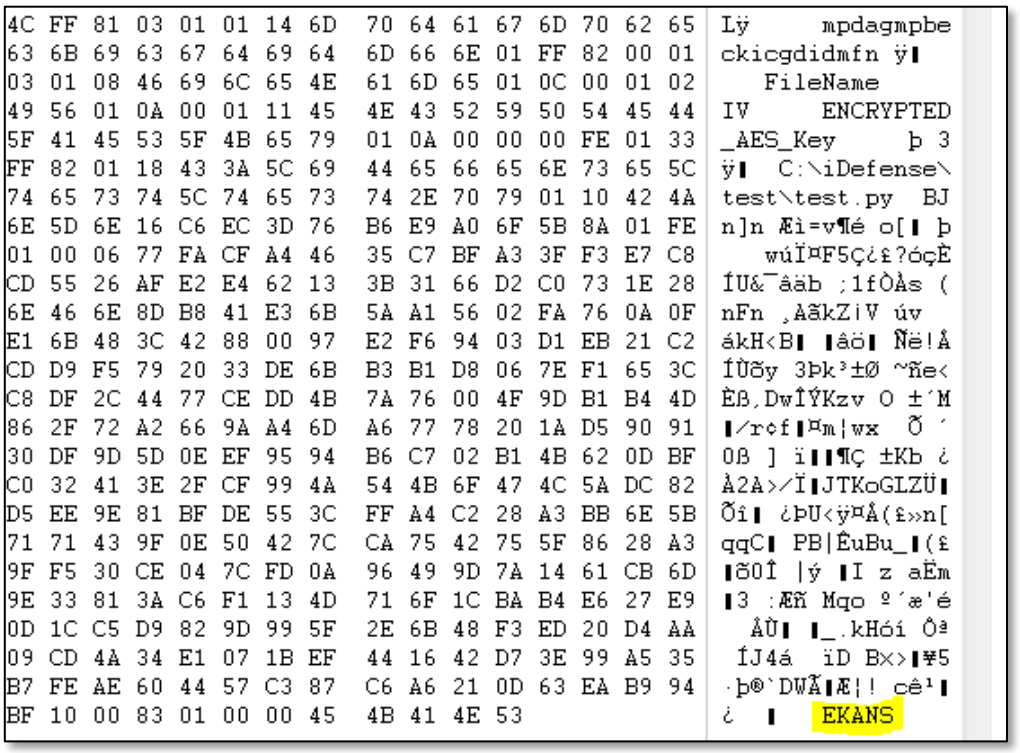
// Decoded gob 1
 	
//Types
// type ID: 65
type mpdagmpbeckicgdidmfn struct {
FileName string
IV []byte
ENCRYPTED_AES_Key []byte
 	
}



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	4C	FF	81	03	01	01	14	6D	70	64	61	67	6D	70	62	65	Lÿ mpdagmpbe
00000010	63	6B	69	63	67	64	69	64	6D	66	6E	01	FF	82	00	01	ckicgdidmfn ÿ‚
00000020	03	01	08	46	69	6C	65	4E	61	6D	65	01	0C	00	01	02	FileName
00000030	49	56	01	0A	00	01	11	45	4E	43	52	59	50	54	45	44	IV ENCRYPTED
00000040	5F	41	45	53	5F	4B	65	79	01	0A	00	00	00	FE	01	64	_AES_Key þ d
00000050	FF	82	01	49	43	3A	5C	24	52	65	63	79	63	6C	65	2E	ÿ‚ IC:\$Recycle.
00000060	42	69	6E	5C	53	2D	31	2D	35	2D	32	31	2D	33	35	37	Bin\S-1-5-21-357
00000070	30	35	38	31	30	34	31	2D	32	34	39	34	39	31	33	35	0581041-24949135
00000080	2D	31	36	33	33	31	39	37	32	34	30	2D	31	30	30	30	-1633197240-1000
00000090	5C	24	49	32	46	53	54	47	55	2E	74	78	74	01	10	41	\$I2FSTGU.txt A
000000A0	41	41	41	41	41	41	41	41	41	41	41	41	41	41	41	01	AAAAAAAAAAAAAAA
000000B0	FE	01	00	4C	E3	46	FE	14	77	92	19	7E	B5	3C	F5	06	þ LãFþ w' ~µ<õ
000000C0	A1	81	63	EB	37	86	5F	D5	04	E6	9D	41	63	17	42	37	¡‚cë7†_Õ æ Ac B7
000000D0	AC	79	3C	E9	E3	D8	5C	5C	05	0E	99	C9	5B	FA	35	C5	¬y<éãØ\\ ™É[ú5Å
000000E0	44	64	3D	1C	58	DB	F2	0C	0E	75	4E	7D	33	5C	B8	54	Dd= XÛò uN}3\¸T
000000F0	C0	7C	DF	07	C9	C1	15	78	26	91	2C	97	07	7C	5E	FF	À|ß ÉÁ x&',— |^ÿ
00000100	BA	01	80	88	C4	90	7D	22	C5	12	87	52	93	74	91	85	º €ˆÄ }"Å ‡R“t'…
00000110	E3	CE	A7	DE	45	39	71	F7	43	21	D6	3B	6A	9C	4E	9D	ãÎ§ÞE9q÷C!Ö;jœN
00000120	E6	33	67	64	C4	BF	B5	4D	8B	75	1B	70	A4	6E	C5	46	æ3gdÄ¿µM‹u p¤nÅF
00000130	E9	69	93	BE	C7	46	4A	B9	4A	3E	16	F4	F4	A7	87	EB	éi“¾ÇFJ¹J> ôô§‡ë
00000140	37	BE	77	46	59	F2	E1	A1	C6	38	91	F6	3C	B4	17	37	7¾wFYòá¡Æ8‘ö<´ 7
00000150	4B	3E	FA	DE	B8	E9	BF	C2	31	EE	DF	89	59	20	C8	49	K>úÞ¸é¿Â1îß‰Y ÈI
00000160	25	36	63	3C	07	E1	6D	91	A2	53	10	58	77	CB	3D	AB	%6c< ám'¢S XwË=«
00000170	D6	04	82	51	EF	14	61	4B	BA	99	AA	59	66	C9	9D	F1	Ö ‚Qï aKº™ªYfÉ ñ
00000180	95	C8	95	2D	1C	45	A0	81	45	2D	49	34	96	41	FC	5A	•È•- E E-I4–AüZ
00000190	F9	C3	F4	96	DF	1D	BF	70	20	A6	EB	63	4E	E0	6E	D5	ùÃô–ß ¿p ¦ëcNànÕ
000001A0	94	19	FD	ED	BE	AD	1C	05	C8	A2	4B	85	5E	F4	95	50	” ýí¾- È¢K…^ô•P
000001B0	65	2E	02	00	00	00	00	00	00	00	00	00	00	00	00	00	e.

Figura 13. Ejemplo de datos codificados en **GOB**.

Todo fichero cifrado es marcado con la cadena de texto "**EKANS**" al final del fichero. EKANS es SNAKE al revés. Por esta razón este código dañino es conocido de las dos formas: SNAKE/EKANS.



4C	FF	81	03	01	01	14	6D	70	64	61	67	6D	70	62	65	Lÿ	mpdagmpbe
63	6B	69	63	67	64	69	64	6D	66	6E	01	FF	82	00	01	ckicgdidmfn	ÿ‚
03	01	08	46	69	6C	65	4E	61	6D	65	01	0C	00	01	02	FileName	
49	56	01	0A	00	01	11	45	4E	43	52	59	50	54	45	44	IV	ENCRYPTED
5F	41	45	53	5F	4B	65	79	01	0A	00	00	00	FE	01	33	_AES_Key	þ 3
FF	82	01	18	43	3A	5C	69	44	65	66	65	6E	73	65	5C	ÿ‚	C:\iDefense\
74	65	73	74	5C	74	65	73	74	2E	70	79	01	10	42	4A	test\test.py	BJ
6E	5D	6E	16	C6	EC	3D	76	B6	E9	A0	6F	5B	8A	01	FE	n]n	Æì=v¶é o[Š þ
01	00	06	77	FA	CF	A4	46	35	C7	BF	A3	3F	F3	E7	C8		wúÏ¤F5Ç¿£?óçÈ
CD	55	26	AF	E2	E4	62	13	3B	31	66	D2	C0	73	1E	28	ÍU&¯âäb ;1fÒÀs	(
6E	46	6E	8D	B8	41	E3	6B	5A	A1	56	02	FA	76	0A	0F	nFn ¸AãkZ¡V ú	v
E1	6B	48	3C	42	88	00	97	E2	F6	94	03	D1	EB	21	C2	ákH<B ˆâö” Ñë!Â	
CD	D9	F5	79	20	33	DE	6B	B3	B1	D8	06	7E	F1	65	3C	ÍÙõy 3Þk³±Ø ~ñe<	
C8	DF	2C	44	77	CE	DD	4B	7A	76	00	4F	9D	B1	B4	4D	ÈB,DwÎÝKzv O ±´M	
86	2F	72	A2	66	9A	A4	6D	A6	77	78	20	1A	D5	90	91	†/r¢fš¤m¦wx	Õ ‘
30	DF	9D	5D	0E	EF	95	94	B6	C7	02	B1	4B	62	0D	BF	0ß] ï•”¶Ç ±Kb	¿
C0	32	41	3E	2F	CF	99	4A	54	4B	6F	47	4C	5A	DC	82	À2A>/Ï™JTKoGLZÜ‚	
D5	EE	9E	81	BF	DE	55	3C	FF	A4	C2	28	A3	BB	6E	5B	Õî‚ ¿ÞU<ÿ¤Â(£»n[	
71	71	43	9F	0E	50	42	7C	CA	75	42	75	5F	86	28	A3	qqC Ÿ PB|ÊuBu_†(£	
9F	F5	30	CE	04	7C	FD	0A	96	49	9D	7A	14	61	CB	6D	Ÿõ0Î |ý –I z aËm	
9E	33	81	3A	C6	F1	13	4D	71	6F	1C	BA	B4	E6	27	E9	ž3 :Æñ Mqo º´æ'é	
0D	1C	C5	D9	82	9D	99	5F	2E	6B	48	F3	ED	20	D4	AA	ÅÙ‚ _.kHóí Ô	ª
09	CD	4A	34	E1	07	1B	EF	44	16	42	D7	3E	99	A5	35	ÍJ4á ïD B×>™¥5	
B7	FE	AE	60	44	57	C3	87	C6	A6	21	0D	63	EA	B9	94	·þ®`DWÃ‡Æ¦! cê¹”	
BF	10	00	83	01	00	00	45	4B	41	4E	53					¿ ƒ	EKANS

Figura 14. Marca de fichero cifrado.

Los ficheros cifrados son renombrados añadiendo 5 caracteres aleatorios al final, sin embargo, el renombrado no se realiza al mismo tiempo del cifrado. El código dañino primero selecciona todos los ficheros que quiere cifrar, a continuación, comienza el proceso de cifrado y finalmente procede a renombrarlos. Esto hace que el ataque sea más lento, pero más efectivo, ya que renombrar lo ficheros al final, evitará que el usuario sea alertado durante el proceso de cifrado, lo que permitiría al usuario detener el código dañino antes de que cifrara todos los ficheros.

Tras finalizar el renombrado de los ficheros, el código dañino crea el fichero con la nota de rescate en los siguientes directorios, finalizando su ejecución:

- **C:\Users\Public\Desktop\Decrypt-Your-Files.txt**
- **C:\Decrypt-Your-Files.txt**

```
main_decrypt_ransom_note();
v36 = v12;
v39 = v3;
v44 = a1;
v45 = a2;
v46 = 0;
v47 = 0;
runtime_convT2Estring(&string_autogen_F80FJP, &v44, v21);
v46 = v22;
v47 = v26;
fmt_Sprintf(v39, v36, &v46, 1, 1);
runtime_stringtoslicebyte(0, v30, v31);
main_decrypt_public(v4, v13);
os_Getenv(v5, v14, v23, v27);
v35 = v28;
v38 = v24;
main_decrypt_systemdrive(v6, v15);
os_Getenv(v7, v16, v24, v28);
v37 = v25;
v34 = v29;
main_decrypt_pub___v_root___v(v8, v17);
v42 = v38;
v43 = v35;
v40 = v25;
v41 = v29;
v48 = &string_autogen_F80FJP;
v49 = &v42;
v50 = &string_autogen_F80FJP;
v51 = &v40;
sub_545470();
if ( v35 > 0 )
{
  main_decrypt__Desktop_(v9, v18);
```

Figura 15. Creación de la nota de rescate.

La nota de rescate, extraída del cuerpo del código dañino, se ha incluido en el apéndice I y contiene una variable, dirección email de contacto, que es resuelta en tiempo de ejecución. La nota contiene instrucciones para ponerse en contacto por email, con el fin de obtener las instrucciones para el descifrado de los ficheros. La dirección de correo utilizada en esta muestra es la siguiente: **alfredmir@protonmail.com**.

EMAIL DE CONTACTO EN NOTA DE RESCATE
---------- | How to contact us to get your files back? ---------- The only way to restore your files is by purchasing a decryption tool loaded with a private key we created specifically for your network. Once run on an effected computer, the tool will decrypt all encrypted files - and you can resume day-to-day operations, preferably with better cyber security in mind. If you are interested in purchasing the decryption tool contact us at **%s**
---------- | How to contact us to get your files back? ---------- The only way to restore your files is by purchasing a decryption tool loaded with a private key we created specifically for your network. Once run on an effected computer, the tool will decrypt all encrypted files - and you can resume day-to-day operations, preferably with better cyber security in mind. If you are interested in purchasing the decryption tool contact us at **alfredmir@protonmail.com**

4. PERSISTENCIA

Esta muestra de código dañino no presenta ningún sistema de persistencia.

5. YARA

La siguiente regla Yara puede utilizarse para detectar el código dañino en un equipo infectado.

SNAKE

SNAKE

import "pe"
 	
rule snake_locker {
meta:
description = "Ransomware snake Locker"
date = "2020-05-25"
hash1 = "47EBE9F8F5F73F07D456EC12BB49C75D"
 	
strings:
$s1 = { 6D 70 64 61 67 6D 70 62 65 63 6B 69 63 67 64 69 64 6D 66 6E }
$s2 = { 8D 05 ?? ?? ?? 00 89 44 24 04 c7 44 24 08 ?? ?? ?? 00 e8 ?? ?? e? ff 8b 44 24 0c [25-25] 89 54 24 04 c7 44 24 08 ?? ?? ?? 00 e8 }
 	
condition:
uint16(0) == 0x5a4d and
filesize < 5MB and
($s1 or $s2 or
pe.imphash() == "96c44fa1eee2c4e9b9e77d7bf42d59e6")
}

6. IOCS

Los siguientes IOCs pueden ser utilizados para detectar equipos infectados con este código dañino.

	IOCs
MD5	47EBE9F8F5F73F07D456EC12BB49C75D
Nombre de fichero	C:\Users\Public\Desktop\Decrypt-Your-Files.txt C:\Decrypt-Your-Files.txt
Email	alfredmir@protonmail.com
DNS	ADS.FRESENIUS.COM
Mutex	Global\EKANS Este mutex puede ser utilizado para detener la infección, ya que, si el mutex existe en el sistema, el código dañino detiene su ejecución.

7. APÉNDICE I

El código dañino presenta el siguiente mensaje de rescate.

MENSAJE DE RESCATE
---------- | What happened to your files?   ----------   We breached your corporate network and encrypted the data on your computers. The encrypted data includes documents, databases, photos and more -   all were encrypted using a military grade encryption algorithms (AES-256 and RSA-2048). You cannot access those files right now. But dont worry!   You can still get those files back and be up and running again in no time.   ---------- | How to contact us to get your files back?   ----------   The only way to restore your files is by purchasing a decryption tool loaded with a private key we created specifically for your network.   Once run on an effected computer, the tool will decrypt all encrypted files - and you can resume day-to-day operations, preferably with   better cyber security in mind. If you are interested in purchasing the decryption tool contact us at %s   ---------- | How can you be certain we have the decryption tool?   ----------   In your mail to us attach up to 3 non critical files (up to 3MB, no databases or spreadsheets).   We will send them back to you decrypted.   ---------- | What happens if you dont contact us within 48 hours or refuse payment?   ----------   We publish sensitve databases and documents we collected from your network.   ----------

8. APÉNDICE II

Lista de Servicios que el código dañino detendrá.

LISTA DE SERVICIOS	
Acronis VSS Provider	NtLmSspNtmsSvc
AcrSch2Svc	ntrtscanPOP3Svc
AdobeARMservice	odservTlntSvr
AlerterERSvc	oracleservice
Antivirus	OracleService
ArcserveUDPPS	PDVFSService
ArcserveUDPPS	ProLiantMonitor
ARSMbedbgDCAgent	ReportServer
ASLogWatch	ReportServer$TPSRESvc
avast! AntivirusaswBccmfewc	ReportServer$TPSSQLBrowserAVP
avbackupNetSvc	RSCDsvcLRSDRVX
BackupExecAgentAccelerator	RumorServer
BackupExecAgentBrowser	sacsvr
BackupExecDeviceMediaService	SamSs
bcrservice	SAVServiceSAVAdminService
CAARCAppSvc	SDD_Service
CAARCUpdateSvc	SDRSVCShMonitor
CASAD2DwebSvc	SentinelAgent
CASARPSWebSVC	SepMasterServiceSmcinstSMTPSvc
CASDatastoreSvc	SmcService
ccEvtMgrccSetMgrCSAdmin	SNACSntpService
CSAuth	Sophos AgentSophos MCS AgentAcronisAgent
CSDbSyncCSLog	Sophos AutoUpdate Service
CSMon	Sophos Clean Service
CSRadiusCSTacacsSymantecVGAuthService	Sophos Device Control Service
Cylance	Sophos File Scanner Service
DB2INST2myAgtSvcIBMDataServerMgrIBMDSServer41	Sophos Health Service
DB2LICD_DB2COPY1DB2DAS00DB2-0	Sophos MCS Client
Enterprise Client Service	Sophos Message Router
EPUpdateService	Sophos Safestore Service
EraserSvc11710	Sophos System Protection ServiceSophos Web
EsgShKernel	Control Service
ESHASRV	sophosspsSstpSvcSQLAgent$ECWDB2
EventlogNetDDE	SophosVeeam
FA_Scheduler	SplunkForwarder
gupdatemHealthService	SQL Backups
IDriverTMSMQMMS	SQLAgent$CXDB
IISAdminIMAP4Svcmacmnsvcmasvc	SQLAgent$ITRIS
ImapiService	SQLAgent$NET2
KAVFSmfefire	SQLAgent$PROD
klnagentMSSQL$SOPHOS	SQLAgent$PROD
MBAMService	SQLAgent$SOPHOS
MBEndpointAgent	SQLAgent$SOPHOS
McAfeeFramework	SQLAgent$TPS
McShieldmfemms	SQLAgent$TPSAMA
McTaskManager	SQLBrowser
mfevtpMSOLAP$TPSmozyprobackup	SQLsafe Backup Service
MsDtsServer	SQLsafe Filter Service
MsDtsServer100	SQLSERVERAGENT
MsDtsServer110	SQLTELEMETRY
MsDtsServer130	SQLWriter

LISTA DE SERVICIOS	
MSExchangeES	SSISTELEMETRY130epredlineTmPfw
MSExchangeIS	svcGenericHost
MSExchangeMGMT	swi_filterTmCCSFswi_service
MSExchangeMTA	swi_update
MSExchangeSA	swi_update_64
MSExchangeSRS	Symantec System Recovery
msftesql$PROD	sysdown
msftesql$PROD	System
MSOLAP$SQL_2008	Telemetryserver
MSOLAP$TPSAMA	tmlistenTrueKey
MSSQL$BKUPEXEC	tpautoconnsvc
MSSQL$ECWDB2	TPVCGateway
MSSQL$EPOSERVER	TrueKeySchedulerUI0DetectW3Svc
MSSQL$ITRIS	VeeamBackupSvc
MSSQL$NET2	VeeamBrokerSvc
MSSQL$PROD	VeeamCatalogSvc
MSSQL$SHAREPOINTMSSQL$SQL_2008	VeeamCloudSvc
MSSQL$SQLEXPRESSkavfsslpKAVFSGT	VeeamDeploySvc
MSSQL$SYSTEM_BGCMSSQL$TPSMySQL57MSSQL$TPSA	VeeamMountSvc
MA	VeeamNFSSvc
MSSQLFDLauncher	VeeamRESTSvc
MSSQLMySQLmssql	VMTools
MSSQLSERVER	VMware
msvsmon90	wbengineWRSVC
MySQL80nxlogSAP	WdNisSvcBITSepagWinDefend
Net2ClientSvc	WebClientWinVNC4CissesrvCpqRcmc3gupdate
NetMsmqActivatorEhttpSrvekrn	Zoolz 2 Service

9. APÉNDICE III

Lista de procesos que el código dañino detendrá.

LISTA DE PROCESOS				
a2guard.exe	cwbunnav.exe	mcshld9x.exe	ravxp.exe	rdrcef.exe
a2service.exe	cylancesvc.exe	mcsvhost.exe	rcsvcmon.exe	realmon.exe
a2start.exe	cylanceui.exe	mcsysmon.exe	mcshell.exe	redirsvc.exe
aawservice.exe	dao_log.exe	mctray.exe	mcshield.exe	regmech.exe
acaas.exe	dbeng50.exe	mctskshd.exe	mcshld9x.exe	remupd.exe
acaegmgr.exe	dbserv.exe	mcui32.exe	mcsvhost.exe	repmgr64.exe
acaif.exe	dbsnmp.exe	mcuimgr.exe	mcsysmon.exe	reportersvc.exe
acais.exe	dbsrv9.exe	mcupdate.exe	mctray.exe	reportsvc.exe
acctmgr.exe	defwatch.exe	mcupdmgr.exe	mctskshd.exe	retinaengine.exe
aclient.exe	defwatchrnav.exe	mcvsftsn.exe	mcui32.exe	rfwmain.exe
aclntusr.exe	deloeminfs.exe	mcvsrte.exe	mcuimgr.exe	rfwproxy.exe
ad-aware2007.exe	deteqt.agent.exe	mcvsshld.exe	mcupdate.exe	rfwsrv.exe
adminserver.exe	diskmon.exe	mcwce.exe	mcupdmgr.exe	rfwstub.exe
aexnsagent.exe	djsnetcn.exe	mcwcecfg.exe	mcvsftsn.exe	rnreport.exe
aexnsrcvsvc.exe	dlservice.exe	mfeann.exe	mcvsrte.exe	routernt.exe
aexsvc.exe	dltray.exe	mfecanary.exe	mcvsshld.exe	rpcserv.exe
aexswdusr.exe	dolphincharge.exe	mfeesp.exe	mcwce.exe	rscdsvc.exe
aflogvw.exe	doscan.exe	mfefire.exe	mcwcecfg.exe	rsnetsvr.exe
afwserv.exe	dpmra.exe	mfefw.exe	mfeann.exe	rssensor.exe
agntsvc.exe	drwagntd.exe	mfehcs.exe	mfecanary.exe	ravstub.exe
ahnrpt.exe	drwagnui.exe	mfemactl.exe	mfeesp.exe	ravtask.exe

LISTA DE PROCESOS				
ahnsd.exe	drweb.exe	mfemms.exe	mfefire.exe	ravtray.exe
ahnsdsv.exe	drweb32.exe	mfetp.exe	mfefw.exe	ravupdate.exe
alert.exe	drweb32w.exe	mfevtps.exe	mfehcs.exe	ravxp.exe
alertsvc.exe	drweb386.exe	mfewc.exe	mfemactl.exe	rcsvcmon.exe
almon.exe	drwebcgp.exe	mfewch.exe	mfemms.exe	rstray.exe
alogserv.exe	drwebcom.exe	mgavrtcl.exe	mfetp.exe	rtvscan.exe
alsvc.exe	drwebdc.exe	mghtml.exe	mfevtps.exe	rulaunch.exe
alunotify.exe	drwebmng.exe	mgntsvc.exe	mfewc.exe	safeservice.exe
alupdate.exe	drwebscd.exe	monsvcnt.exe	mfewch.exe	sahookmain.exe
amsvc.exe	drwebupw.exe	monsysnt.exe	mgavrtcl.exe	saservice.exe
amswmagtcaf.exe	drwebwcl.exe	mpcmdrun.exe	mghtml.exe	sav32cli.exe
anvir.exe	drwebwin.exe	mpf.exe	mgntsvc.exe	savfmsectrl.exe
aphost.exe	drwinst.exe	mpfagent.exe	monsvcnt.exe	savfmselog.exe
appsvc32.exe	drwupgrade.exe	mpfconsole.exe	monsysnt.exe	savfmsesjm.exe
aps.exe	dsmcad.exe	mpfservice.exe	mpcmdrun.exe	savfmsesp.exe
apvxdwin.exe	dsmcsvc.exe	mpfsrv.exe	mpf.exe	savfmsesrv.exe
ashavast.exe	dwarkdaemon.exe	mpftray.exe	mpfagent.exe	savfmsetask.exe
ashbug.exe	dwengine.exe	mps.exe	mpfconsole.exe	savfmseui.exe
ashchest.exe	dwhwizrd.exe	mpsevh.exe	mpfservice.exe	savmain.exe
ashcmd.exe	dwnetfilter.exe	mpsvc.exe	mpfsrv.exe	savroam.exe
ashdisp.exe	dwrcst.exe	mrf.exe	mpftray.exe	savscan.exe
ashenhcd.exe	dwwin.exe	msaccess.exe	mps.exe	savservice.exe
ashlogv.exe	edisk.exe	msascui.exe	mpsevh.exe	savui.exe
ashmaisv.exe	eeyeevnt.exe	mscifapp.exe	mpsvc.exe	sbamsvc.exe
ashpopwz.exe	egui.exe	msdtssrvr.exe	mrf.exe	scan32.exe
ashquick.exe	ehttpsrv.exe	msftesql.exe	msaccess.exe	scanfrm.exe
ashserv.exe	ekrn.exe	mskagent.exe	msascui.exe	scanmsg.exe
ashsimp2.exe	elogsvc.exe	mskdetct.exe	mscifapp.exe	scansbserv.exe
ashsimpl.exe	emlproui.exe	msksrver.exe	msdtssrvr.exe	scanwscs.exe
ashskpcc.exe	emlproxy.exe	msksrvr.exe	msftesql.exe	scfagent_64.exe
ashskpck.exe	encsvc.exe	msmdsrv.exe	mskagent.exe	scfmanager.exe
ashupd.exe	engineserver.exe	msmpeng.exe	mskdetct.exe	scfservice.exe
ashwebsv.exe	entitymain.exe	mspmspsv.exe	msksrver.exe	scftray.exe
asupport.exe	epmd.exe	mspub.exe	msksrvr.exe	schdsrvc.exe
aswdisp.exe	era.exe	msscli.exe	msmdsrv.exe	schupd.exe
aswregsvr.exe	erlsrv.exe	msseces.exe	msmpeng.exe	sdrservice.exe
aswserv.exe	esecservice.exe	msssrv.exe	mspmspsv.exe	sdtrayapp.exe
aswupdsv.exe	esmagent.exe	myagttry.exe	mspub.exe	seccenter.exe
aswwebsv.exe	etagent.exe	mydesktopqos.exe	msscli.exe	seestat.exe
atrshost.exe	etconsole3.exe	mysqld.exe	msseces.exe	semsvc.exe
atwsctsk.exe	etcorrel.exe	mysqld-nt.exe	msssrv.exe	sesclu.exe
aupdrun.exe	etreporter.exe	mysqld-opt.exe	myagttry.exe	setloadorder.exe
aus.exe	etrssfeeds.exe	n.exe	mydesktopqos.exe	setupguimngr.exe
auth8021x.exe	etscheduler.exe	nailgpip.exe	mysqld.exe	sevinst.exe
autoup.exe	euqmonitor.exe	naprdmgr.exe	mysqld-nt.exe	sgbhp.exe
avadmin.exe	eventparser.exe	navapsvc.exe	mysqld-opt.exe	shstat.exe
avagent.exe	evtarmgr.exe	navapw32.exe	n.exe	sidebar.exe
avastsvc.exe	evtmgr.exe	navectrl.exe	nailgpip.exe	siteadv.exe
avastui.exe	ewidoctrl.exe	navelog.exe	naprdmgr.exe	slee81.exe
avcenter.exe	ewidoguard.exe	navesp.exe	navapsvc.exe	smc.exe
avconfig.exe	excel.exe	navshcom.exe	navapw32.exe	smcgui.exe
avconsol.exe	execstat.exe	navw32.exe	navectrl.exe	smex_activeupda.exe
avengine.exe	explicit.exe	navwnt.exe	navelog.exe	smex_master.exe
avesvc.exe	fameh32.exe	ncdaemon.exe	navesp.exe	smex_remoteconf.exe
avfwsvc.exe	fcappdb.exe	nd2svc.exe	navshcom.exe	smex_systemwatc.exe
avgam.exe	fcdblog.exe	ndetect.exe	navw32.exe	sms.exe

LISTA DE PROCESOS				
avgamsvr.exe	fch32.exe	ndrvs.exe	navwnt.exe	smsectrl.exe
avgas.exe	fchelper64.exe	ndrvx.exe	ncdaemon.exe	smselog.exe
avgcc.exe	fcsms.exe	neotrace.exe	nd2svc.exe	smsesjm.exe
avgcc32.exe	fcssas.exe	nerosvc.exe	ndetect.exe	smsesp.exe
avgcefrend.exe	fih32.exe	netcfg.exe	ndrvs.exe	smsesrv.exe
avgchsvx.exe	firefox.exe	networkagent.exe	ndrvx.exe	smsetask.exe
avgcmgr.exe	firesvc.exe	ngctw32.exe	neotrace.exe	smseui.exe
avgcsrva.exe	firetray.exe	ngserver.exe	nerosvc.exe	smsx.exe
avgcsrvx.exe	firewallgui.exe	nimbus.exe	netcfg.exe	snac.exe
avgctrl.exe	fmon.exe	nimcluster.exe	networkagent.exe	sndmon.exe
avgdiag.exe	forcefield.exe	nip.exe	ngctw32.exe	sndsrvc.exe
avgemc.exe	fortiesnac.exe	nipsvc.exe	ngserver.exe	snhwsrv.exe
avgemca.exe	fortifw.exe	nisoptui.exe	nimbus.exe	snicheckadm.exe
avgemcx.exe	fortiproxy.exe	nisserv.exe	nimcluster.exe	snichecksrv.exe
avgfws.exe	fortitray.exe	nissrv.exe	nip.exe	snicon.exe
avgfws8.exe	fortiwf.exe	nisum.exe	nipsvc.exe	snsrv.exe
avgfws9.exe	fpavserver.exe	njeeves.exe	nisoptui.exe	spbbcsvc.exe
avgfwsrv.exe	fprottray.exe	nlclient.exe	nisserv.exe	spideragent.exe
avgidsagent.exe	frameworkservice.exe	nlsvc.exe	nissrv.exe	spiderml.exe
avgidsui.exe	frzstate2k.exe	nmagent.exe	nisum.exe	spidernt.exe
avginet.exe	fsaa.exe	nmain.exe	njeeves.exe	spiderui.exe
avgmfapx.exe	fsaua.exe	nod32.exe	nlclient.exe	spntsvc.exe
avgmsvr.exe	fsav32.exe	nod32krn.exe	nlsvc.exe	spooler.exe
avgnsa.exe	fsavgui.exe	nod32kui.exe	nmagent.exe	spyemergency.exe
avgnsx.exe	fscuif.exe	nod32view.exe	nmain.exe	sqlagent.exe
avgnt.exe	fsdfwd.exe	npfmntor.exe	nod32.exe	sqlbrowser.exe
avgregcl.exe	fsgk32.exe	npfmsg.exe	nod32krn.exe	sqlservr.exe
avgrsa.exe	fsgk32st.exe	npfmsg2.exe	nod32kui.exe	sqlwriter.exe
avgrssvc.exe	fsguidll.exe	npfsvice.exe	nod32view.exe	srvload.exe
avgrsx.exe	fsguiexe.exe	npmdagent.exe	npfmntor.exe	srvmon.exe
avgscanx.exe	fshdll32.exe	nprotect.exe	npfmsg.exe	sschk.exe
avgserv.exe	fshoster32.exe	npscheck.exe	npfmsg2.exe	ssm.exe
avgserv9.exe	fshoster64.exe	npssvc.exe	npfsvice.exe	ssp.exe
avgsvc.exe	fsm32.exe	nrmenctb.exe	npmdagent.exe	ssscheduler.exe
avgsystx.exe	fsma32.exe	nscsrvce.exe	nprotect.exe	starta.exe
avgtray.exe	fsmb32.exe	nsctop.exe	npscheck.exe	steam.exe
avguard.exe	fsorsp.exe	nsmdemf.exe	npssvc.exe	stinger.exe
avgui.exe	fspex.exe	nsmdmon.exe	nrmenctb.exe	stopa.exe
avgupd.exe	fsqh.exe	nsmdreal.exe	nscsrvce.exe	stopp.exe
avgupdln.exe	fwcfg.exe	nsmdsch.exe	nsctop.exe	stwatchdog.exe
avgupsvc.exe	fwinst.exe	nsmdtr.exe	nsmdemf.exe	svcgenerichost.exe
avgvv.exe	fws.exe	ntcaagent.exe	nsmdmon.exe	svcharge.exe
avgw.exe	gcascleaner.exe	ntcadaemon.exe	nsmdreal.exe	svcntaux.exe
avgwb.dat	gcasdtserv.exe	ntcaservice.exe	nsmdsch.exe	svdealer.exe
avgwdsvc.exe	gcasnotice.exe	ntevl.exe	nsmdtr.exe	svframe.exe
avgwizfw.exe	gcasserv.exe	ntrtscan.exe	ntcaagent.exe	svtray.exe
avkproxy.exe	GDDServer.exe	ntservices.exe	ntcadaemon.exe	swc_service.exe
avkservice.exe	gdfwsvc.exe	nvcoas.exe	ntcaservice.exe	swdsvc.exe
avktray.exe	gdscan.exe	nvcsched.exe	ntevl.exe	sweepsrv.sys
avkwctl.exe	ghost_2.exe	nymse.exe	ntrtscan.exe	swi_service.exe
avltmain.exe	ghosttray.exe	oasclnt.exe	ntservices.exe	swnetsup.exe
avmailc.exe	googleupdate.exe	ocautoupds.exe	nvcoas.exe	swnxt.exe
avmcdlg.exe	guard.exe	ocomm.exe	nvcsched.exe	swserver.exe
avnotify.exe	guardgui.exe	ocssd.exe	nymse.exe	symlcsvc.exe
avp.exe	gziface.exe	oespamtest.exe	oasclnt.exe	symproxysvc.exe
avpcc.exe	gzserv.exe	ofcdog.exe	ocautoupds.exe	symsport.exe

LISTA DE PROCESOS				
avpdtagt.exe	hasplmv.exe	ofcpfwsvc.exe	ocomm.exe	symtray.exe
avpexec.exe	hdb.exe	okclient.exe	ocssd.exe	symwsc.exe
avpm.exe	hpqwmiex.exe	olfsnt40.exe	oespamtest.exe	synctime.exe
avpncc.exe	hwapi.exe	omniagent.exe	ofcdog.exe	sysdoc32.exe
avps.exe	icepack.exe	omtsreco.exe	ofcpfwsvc.exe	system.exe
avpui.exe	idsinst.exe	onenote.exe	okclient.exe	taskhostw.exe
avpupd.exe	iface.exe	onlinent.exe	olfsnt40.exe	tbirdconfig.exe
avscan.exe	igateway.exe	onlnsvc.exe	omniagent.exe	tbmon.exe
avscc.exe	ilicensesvc.exe	op_viewer.exe	omtsreco.exe	tclproc.exe
avserver.exe	inet_gethost.exe	opscan.exe	onenote.exe	tdimon.exe
avshadow.exe	infopath.exe	oracle.exe	onlinent.exe	tfgui.exe
avsynmgr.exe	inicio.exe	outlook.exe	onlnsvc.exe	tfservice.exe
avtask.exe	inonmsrv.exe	outpost.exe	op_viewer.exe	tftray.exe
avwebgrd.exe	inorpc.exe	paamsrv.exe	opscan.exe	tfun.exe
basfipm.exe	inort.exe	padfsvr.exe	oracle.exe	thebat.exe
bavtray.exe	inotask.exe	pagent.exe	outlook.exe	thebat64.exe
bcreporter.exe	inoweb.exe	pagentwd.exe	outpost.exe	thunderbird.exe
bcrservice.exe	isafe.exe	pasystemtray.exe	paamsrv.exe	tiaspn~1.exe
bdagent.exe	isafinst.exe	patch.exe	padfsvr.exe	tmas.exe
bdc.exe	isntsmtp.exe	patrolagent.exe	pagent.exe	tmlisten.exe
bdlite.exe	isntsysmonitor.exe	patrolperf.exe	pagentwd.exe	tmntsrv.exe
bdmcon.exe	ispwdsvc.exe	pavbckpt.exe	pasystemtray.exe	tmpfw.exe
bdredline.exe	isqlplussvc.exe	pavfires.exe	patch.exe	tmproxy.exe
bdss.exe	isscsf.exe	pavfnsvr.exe	patrolagent.exe	tnbutil.exe
bdsubmit.exe	issdaemon.exe	pavjobs.exe	patrolperf.exe	tnslsnr.exe
bhipssvc.exe	issvc.exe	pavkre.exe	pavbckpt.exe	tpsrv.exe
bka.exe	isuac.exe	pavmail.exe	pavfires.exe	traflnsp.exe
blackd.exe	iswmgr.exe	pavprot.exe	pavfnsvr.exe	trjscan.exe
blackice.exe	itmrt_trace.exe	pavprsrv.exe	pavjobs.exe	trupd.exe
blupro.exe	itmrtsvc.exe	pavreport.exe	pavkre.exe	tsansrf.exe
bmrt.exe	ixaptsvc.exe	pavsched.exe	pavmail.exe	tsatisy.exe
bullguard.exe	ixavsvc.exe	pavsrv50.exe	pavprot.exe	tscutynt.exe
bwgo0000fspc.exe	ixfwsvc.exe	pavsrv51.exe	pavprsrv.exe	tsmpnt.exe
ca.exe	kabackreport.exe	pavsrv52.exe	pavreport.exe	ucservice.exe
caav.exe	kaccore.exe	pavupg.exe	pavsched.exe	udaterui.exe
caavcmdscan.exe	kanmcmain.exe	pccclient.exe	pavsrv50.exe	uiseagnt.exe
caavguiscan.exe	kansgui.exe	pccguide.exe	pavsrv51.exe	uiwatchdog.exe
cafw.exe	kansvr.exe	pcclient.exe	pavsrv52.exe	umxagent.exe
caissdt.exe	kastray.exe	pccnt.exe	pavupg.exe	umxcfg.exe
calogdump.exe	kav.exe	pccntmon.exe	pccclient.exe	umxfwhlp.exe
capfaem.exe	kav32.exe	pccntupd.exe	pccguide.exe	umxpol.exe
capfasem.exe	kavfs.exe	pccpfw.exe	pcclient.exe	unsecapp.exe
capfsem.exe	kavfsgt.exe	pcctlcom.exe	pccnt.exe	unvet32.exe
capmuamagt.exe	kavfsrcn.exe	pcscan.exe	pccntmon.exe	up2date.exe
casc.exe	kavfsscs.exe	pcscm.exe	pccntupd.exe	update_task.exe
caunst.exe	kavfswp.exe	pcscnsrv.exe	pccpfw.exe	updaterui.exe
cavrep.exe	kavisarv.exe	pcsws.exe	pcctlcom.exe	updtnv28.exe
cavrid.exe	kavmm.exe	pctsauxs.exe	pcscan.exe	upfile.exe
cavscan.exe	kavshell.exe	pctsgui.exe	pcscm.exe	uplive.exe
cavtray.exe	kavss.exe	pctssvc.exe	pcscnsrv.exe	uploadrecord.exe
ccap.exe	kavstart.exe	pctstray.exe	pcsws.exe	upschd.exe
ccapp.exe	kavsvc.exe	pep.exe	pctsauxs.exe	url_response.exe
ccemflsv.exe	kavtray.exe	persfw.exe	pctsgui.exe	urllstck.exe
ccenter.exe	kb891711.exe	pmgreader.exe	pctssvc.exe	usbguard.exe
ccevtmgr.exe	keysvc.exe	pmon.exe	pctstray.exe	useractivity.exe
ccflic0.exe	kis.exe	pnmsrv.exe	pep.exe	useranalysis.exe

LISTA DE PROCESOS				
ccflic4.exe	kislive.exe	pntiomon.exe	persfw.exe	usergate.exe
cclaw.exe	kissvc.exe	pop3pack.exe	pmgreader.exe	usrprmpt.exe
ccnfagent.exe	klnacserver.exe	pop3trap.exe	pmon.exe	v2iconsole.exe
ccprovsp.exe	klnagent.exe	poproxy.exe	pnmsrv.exe	v3clnsrv.exe
ccproxy.exe	klserver.exe	powerpnt.exe	pntiomon.exe	v3exec.exe
ccpxysvc.exe	klswd.exe	ppclean.exe	pop3pack.exe	v3imscn.exe
ccsetmgr.exe	klwtblfs.exe	ppctlpriv.exe	pop3trap.exe	v3lite.exe
ccsmagtd.exe	kmailmon.exe	ppppwallrun.exe	poproxy.exe	v3main.exe
ccsvchst.exe	knownsvr.exe	pqibrowser.exe	powerpnt.exe	v3medic.exe
cctray.exe	knupdatemain.exe	pqv2isvc.exe	ppclean.exe	v3sp.exe
ccupdate.exe	kpf4gui.exe	pralarmmgr.exe	ppctlpriv.exe	v3svc.exe
cdm.exe	kpf4ss.exe	prconfigmgr.exe	ppppwallrun.exe	vetmsg.exe
cfftplugin.exe	kpfw32.exe	preventmgr.exe	pqibrowser.exe	vettray.exe
cfnotsrvd.exe	kpfwsvc.exe	prevsrv.exe	pqv2isvc.exe	visio.exe
cfp.exe	krbcc32s.exe	prftpengine.exe	pralarmmgr.exe	vmacthlp.exe
cfpconfg.exe	kswebshield.exe	prgateway.exe	prconfigmgr.exe	vmtoolsd.exe
cfpconfig.exe	kvdetech.exe	printdevice.exe	preventmgr.exe	vmwaretray.exe
cfplogvw.exe	kvmonxp.kxp	prlicensemgr.exe	prevsrv.exe	vpatch.exe
cfpsbmit.exe	kvmonxp_2.kxp	procexp.exe	prftpengine.exe	vpc32.exe
cfpupdat.exe	kvolself.exe	proficysts.exe	prgateway.exe	vpdn_lu.exe
cfsmsmd.exe	kvsrvxp.exe	proutil.exe	printdevice.exe	vprosvc.exe
checkup.exe	kvsrvxp_1.exe	prproficymgr.exe	prlicensemgr.exe	vprot.exe
chrome.exe	kvxp.kxpfssm32.exe	prrds.exe	procexp.exe	vptray.exe
cis.exe	kwatch.exe	prreader.exe	proficysts.exe	vrv.exe
cistray.exe	kwsprod.exe	prrouter.exe	proutil.exe	vrvmail.exe
cka.exe	kxeserv.exe	prstubber.exe	prproficymgr.exe	vrvmon.exe
clamscan.exe	leventmgr.exe	prsummarymgr.exe	prrds.exe	vrvnet.exe
clamtray.exe	livesrv.exe	prunsrv.exe	prreader.exe	vshwin32.exe
clamwin.exe	lmon.exe	prwriter.exe	prrouter.exe	vsmain.exe
client.exe	log_qtine.exe	psanhost.exe	prstubber.exe	vsmon.exe
client64.exe	loggetor.exe	psctris.exe	prsummarymgr.exe	vsserv.exe
clps.exe	luall.exe	psctrls.exe	prunsrv.exe	vsstat.exe
clpsla.exe	lucoms.exe	psh_svc.exe	prwriter.exe	vstskmgr.exe
clpsls.exe	lucoms~1.exe	pshost.exe	psanhost.exe	webproxy.exe
clshield.exe	lucomserver.exe	psimreal.exe	psctris.exe	webscanx.exe
cmdagent.exe	lwdmserver.exe	psimsvc.exe	psctrls.exe	webtrapnt.exe
cmdinstall.exe	macmnsvc.exe	pskmssvc.exe	psh_svc.exe	wfxctl32.exe
cmgrdian.exe	macompatsvc.exe	psuamain.exe	pshost.exe	wfxmod32.exe
cntaosmgr.exe	mantispm.exe	psuaservice.exe	psimreal.exe	wfxsnt40.exe
collwrap.exe	masalert.exe	pthosttr.exe	psimsvc.exe	win32sysinfo.exe
comhost.exe	massrv.exe	pview.exe	pskmssvc.exe	winlog.exe
console.exe	masvc.exe	pviewer.exe	psuamain.exe	winroute.exe
cpd.exe	mbamservice.exe	pwdfilthelp.exe	psuaservice.exe	winvnc4.exe
cpdclnt.exe	mbamtray.exe	pxemtftp.exe	pthosttr.exe	winword.exe
cpf.exe	mcagent.exe	pxeservice.exe	pview.exe	wordpad.exe
cpntsrv.exe	mcapexe.exe	qclean.exe	pviewer.exe	wrctrl.exe
cramtray.exe	mcappins.exe	qdcsfs.exe	pwdfilthelp.exe	wrsa.exe
crashrep.exe	mcconsol.exe	qhsafetray.exe	pxemtftp.exe	wrspysetup.exe
crdm.exe	mcdash.exe	qhwatchdog.exe	pxeservice.exe	wscntfy.exe
crssvc.exe	mcdetect.exe	qoeloader.exe	qclean.exe	wssfcmai.exe
csacontrol.exe	mcepoc.exe	qserver.exe	qdcsfs.exe	xagt.exe
csadmin.exe	mcepocfg.exe	rapapp.exe	qhsafetray.exe	xcommsvr.exe
csauth.exe	mcinfo.exe	rapuisvc.exe	qhwatchdog.exe	xfilter.exe
csdbsync.exe	mcmnhdlr.exe	ras.exe	qoeloader.exe	xfssvccon.exe
csinject.exe	mcmscsvc.exe	rasupd.exe	qserver.exe	zanda.exe
csinsm32.exe	mcnasvc.exe	rav.exe	rapapp.exe	zapro.exe

LISTA DE PROCESOS				
csinsmnt.exe	mcods.exe	ravalert.exe	rapuisvc.exe	zavaux.exe
cslog.exe	mcpalmcfg.exe	ravmon.exe	ras.exe	zavcore.exe
csmon.exe	mcpromgr.exe	ravmond.exe	rasupd.exe	zillya.exe
csradius.exe	mcproxy.exe	ravservice.exe	rav.exe	zlclient.exe
csrss_tc.exe	mcregwiz.exe	ravstub.exe	ravalert.exe	zlh.exe
cssauth.exe	mcsacore.exe	ravtask.exe	ravmon.exe	zonealarm.exe
cstacacs.exe	mcshell.exe	ravtray.exe	ravmond.exe	zoolz.exe
ctdataload.exe	mcshield.exe	ravupdate.exe	ravservice.exe	

10. APÉNDICE IV

Script de IdaPython para el descifrado de todas las cadenas de texto del código dañino. El resultado será escrito a un fichero TXT.

SCRIPT IDAPYTHON DE DESCIFRADO DE CADENAS DE TEXTO

```
import re

def decrypt(ea, data, key, size):
 print(hex(data))
 print(hex(key))
 print(hex(ea))

 result=""
 for i in range(0,size):
  aux = ( ( (get_wide_byte(data+i) + 0x2A) & 0xFF ) ^ get_wide_byte(key+(i%size) ) )
  result = result + chr(aux)


 f.write(hex(ea) + " - " + get_func_name(ea) + "\n")
 f.write("------------------------------------------------------------\n")
 f.write(result + "\n")
 f.write("------------------------------------------------------------\n\n")

 refs=XrefsTo(ea, 0)
 for ea_refs in refs:
  #print(ea_refs.frm)
  if len(result) >= 0x100:
    comment=result[0:0x100]
  else:
    comment=result[0:len(result)]

  if len(result) >= 0x10:
    functionName=result[0:0x10]
  else:
    functionName=result[0:len(result)]

  set_cmt(ea_refs.frm, comment, 0)

 set_name(ea, "main_decrypt_" + functionName , SN_NOCHECK | SN_FORCE)

 #print(result)

f=open("c:\\\\temp\\\\strings.txt","w")
```

SCRIPT IDAPYTHON DE DESCIFRADO DE CADENAS DE TEXTO

```
#ea=get_screen_ea()
#functionName = get_func_name(ea)
for segea in Segments():
 for funcea in Functions(segea, get_segm_end(segea)):
   for (startea, endea) in Chunks(funcea):
      i=0
      flags=0
      for head in Heads(startea, endea):
         if ( (i==0x07 or i==0x08) and print_insn_mnem(head) == "lea" and print_operand(head,0) ==
"eax"):
            data_addr=get_operand_value(head,1)
            #print(hex(data_addr))
            flags=flags+1
         if ( (i==0x11 or i==0x12) and print_insn_mnem(head) == "lea" and print_operand(head,0) ==
"edx"):
            key_addr=get_operand_value(head,1)
            #print(hex(key_addr))
            flags=flags+1
         if (flags==0x02 and print_insn_mnem(head) == "cmp" and print_operand(head,0) == "ebp" and
get_operand_type(head,1) == 5):
            size=get_operand_value(head,1)
            #print(get_operand_type(head,1))
            print_operand(head,1)
            flags=flags+1
         if flags == 3:
            decrypt(startea, data_addr, key_addr, size)
            break
         i=i+1

f.close()
```