Informe Código Dañino
CCN-CERT ID-19/20

RobbinHood

Junio 2020

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Fecha de Edición: junio de 2020

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

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

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

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

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

2. RESUMEN EJECUTIVO

El presente documento recoge el análisis de la muestra de código dañino perteneciente a la familia de **ransomware RobbinHood**, identificada por la firma SHA256 67d8888c4ef9b58a9f17b8afe5ec6dd9155dd334ef60729fc8bb7c6f6f144b6a.

El objetivo del binario es **cifrar los ficheros de los sistemas infectados**, para posteriormente, **solicitar el pago de un rescate a cambio de la herramienta de descifrado**.

El ransomware RobbinHood protagonizó los titulares de mayo de 2019, en lo que respecta a los incidentes causados por el despliegue masivo de ransomware, cuando la red interna del gobierno de Baltimore se vio afectada por esta variante. Esta tendencia de desplegar ransomware en las etapas de **post-explotación** se ha convertido en una de las principales actividades de numerosos grupos cibercriminales, que, junto con la **exfiltración de información** y consecuente la **extorsión**, están poniendo a prueba los planes de continuidad de negocio y recuperación ante desastres de compañías de todos los rincones del mundo.

Una peculiaridad observada en el código dañino y que denota que el adversario se encontraba dentro de la red de forma previa al despliegue del ransomware, es que la propia **clave de cifrado es leída de un fichero adicional que habría sido colocado por el atacante como paso previo a desencadenar el cifrado**. El binario objeto de análisis no realiza exfiltración de información, pero con el adversario dentro de la red, la exfiltración se ha podido desarrollar a través de cualquier otro procedimiento, siendo el despliegue de ransomware el punto final de la actividad en la red comprometida por parte del grupo criminal.

En puntos posteriores del informe se entra en detalles técnicos sobre la muestra analizada. Además, se proporcionan una regla YARA e indicadores de compromiso con los que identificar la amenaza.

3. DETALLES GENERALES

El binario analizado, es un ejecutable para sistemas Windows de 32-bit, reduce su tamaño mediante el uso del *packer open source* UPX, susceptible de ser descomprimido con la propia herramienta que permite la compresión. El binario original y resultado del *unpacking* se identifican con las firmas SHA256 listadas a continuación.

Fichero	SHA256
winlogon.exe	67d8888c4ef9b58a9f17b8afe5ec6dd9155dd334ef60729fc8bb7c6f6f144b6a
payload.exe	f431c0d492eb29159fc0a92deb2a029ec3f5a40340b1e3ba52f6bc20a8842e79

Desarrollado en GoLang en su versión 1.11, el payload analizado se corresponde con una muestra de ransomware de la familia **RobbinHood**, en la versión **6.1** del código dañino.

```
55+aCUsersUserGoSr_1 db 'C:/Users/User/go/src/Robbinhood6.1/main.go',0
                     align 10h
55+aCUsersUserGoSr_2 db 'C:/Users/User/go/src/Robbinhood6.1/functions.go',0
```

Figura 1. Trazas con el nombre original del proyecto y versión

A fecha del desarrollo del presente documento, el binario objeto de análisis no se conoce fecha de primera aparición y la fecha de compilación del mismo muestra un valor nulo. Cabe destacar que la variante de ransomware funciona de forma offline, leyendo la clave pública del par RSA de un fichero adicional, como se detallará en el siguiente apartado del informe.

4. PROCESO DE INFECCIÓN

Para el correcto funcionamiento del código dañino, la clave pública RSA-4096 debe encontrarse en formato PEM en el fichero listado a continuación.

```
C:\Windows\Temp\key.pub
```

En caso de no existir mencionado fichero, el código dañino finaliza ejecución. Que la clave se lea de un fichero adicional que debe haber sido situado en una ruta determinada, de forma independiente a la ejecución del malware responsable del cifrado, es un claro indicio del compromiso de la red. El adversario, de forma previa al despliegue del ransomware, habría distribuido por los equipos objetivo de ser cifrados, la clave pública RSA cuya pareja privada mantiene en un lugar seguro. La clave privada RSA en manos del atacante garantiza que sólo a través de la negociación por la herramienta y clave de descifrado, se pueda proceder a recuperar la información.

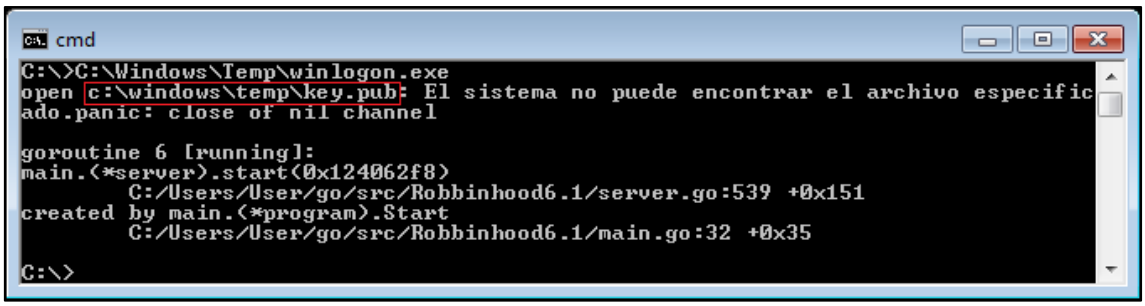

Figura 2. Error mostrado tras no encontrar la clave pública del par RSA.

No se realiza control de instancias por parte del código dañino, por tanto, si se ejecuta múltiples veces, varios procesos coexistirán simultáneamente. En caso de encontrar la clave pública RSA en la localización mencionada, se inicia el proceso de infección, cuyas fases principales se desglosan en detalle en los siguientes subapartados.

4.1 SELECCIÓN DE FICHEROS

En el mismo directorio donde se debe encontrar la clave pública del par RSA, se crean tres ficheros que el código dañino emplea para listar los ficheros del equipo en base a determinadas condiciones, recogidas en la siguiente tabla.

Fichero	Utilidad
C:\Windows\Temp\r_f_l_2	Fichero vacío para los test realizados
C:\Windows\Temp\r_f_s_2	Ficheros susceptibles de ser cifrados
C:\Windows\Temp\r_o_s_2	Ficheros con extensiones que no se encuentran en el objetivo del cifrado

Las rutas a los ficheros recogidas por los listados de la tabla anterior, muestran un *encoding* base64, además de invertir el orden de los caracteres de cada localización.

En esta misma etapa, después de listar los ficheros a cifrar, se eliminan todos los ficheros cuya extensión coincida entre las recogidas en la tabla a continuación.

Extensiones de ficheros a eliminar			
bk	backup	bkz	fbw
acp	backupdb	blend1	fh
adi	bakup	ctf	nbk
ajl	bakx	dim	rec
ast	bckup	dir	sbf
back	bkup	dsb	sv2i

La lista de las 564 extensiones objetivo del cifrado se incluye en el **anexo A**.

Además, como suele ser habitual en las implementaciones de ransomware, los siguientes ficheros se encontrarían excluidos del cifrado.

Ficheros exentos del cifrado	
boot.ini	ntuser.dat
bootsect.bak	ntuser.ini
bootmgr	desktop.ini
ntdetect.com	recycle.bin
ntldr	pagefile.sys

bootmgr	swapfile.sys
bootnxt	_Readme_Decrypt__Files.html
utoexec.bat	_Readme_Help_Important.html
ntds.dit	

Y por su parte, el contenido de los siguientes directorios también se encontraría exento del cifrado.

Directorios exentos del cifrado	
Windows	Windows.old
WINDOWS	Temp
bootmgr	tmp
Boot	$Recycle.Bin
$WINDOWS.~BT	System Volume Information

4.2 FINALIZACIÓN DE PROCESOS Y SERVICIOS

Con el objetivo de liberar ficheros para su posterior cifrado, debido a que se puedan encontrar bloqueados por su uso por parte de determinado proceso o servicio, el código dañino incluye un listado de 447 procesos y 131 servicios que finalizar. Debido a las dimensiones de los listados, los procesos a finalizar se incluyen en el **anexo B** y los servicios en el **anexo C**.

4.3 CAMBIO DE CONTRASEÑA

Como último paso antes de proceder al cifrado, se tratará de cambiar la contraseña de los usuarios de los sistemas afectados a **robbin_B_f00@D1263**. El cambio de la contraseña se realiza a través del siguiente comando.

```
cmd.exe /c net user <usuario> robbin_B_f00@D1263
```

4.4 ESQUEMA DE CIFRADO

En el directorio en que se ejecute el código dañino, se crea el fichero **rub.s** indicando el inicio del proceso de cifrado. El esquema de cifrado se basa en criptografía simétrica, **AES en modo CTR** con claves de 256-bit y vectores de inicialización de 128-bit para el cifrado de los ficheros, y criptografía asimétrica, **RSA-4096**, para asegurar que las claves simétricas AES solo puedan ser recuperadas a través de la negociación del rescate. Para cada fichero, se sigue el proceso descrito a continuación.

- Generación de la clave AES de 256-bit (32 bytes).
- Generación del vector de inicialización de 128-bit (16 bytes).
- Cifrado del contenido del fichero con AES en modo CTR.
- Añadido del delimitador indicando el tamaño del contenido cifrado.
- Cifrado del vector de inicialización AES con la clave pública RSA.
- Cifrado de la clave AES con la clave pública RSA.
- Cifrado del nombre original del fichero con AES en modo CTR y después con la clave pública RSA.
- Cifrado del nombre del equipo con la clave pública RSA.

El resultado de la aplicación del proceso de cifrado sobre un fichero se resume en el siguiente diagrama.

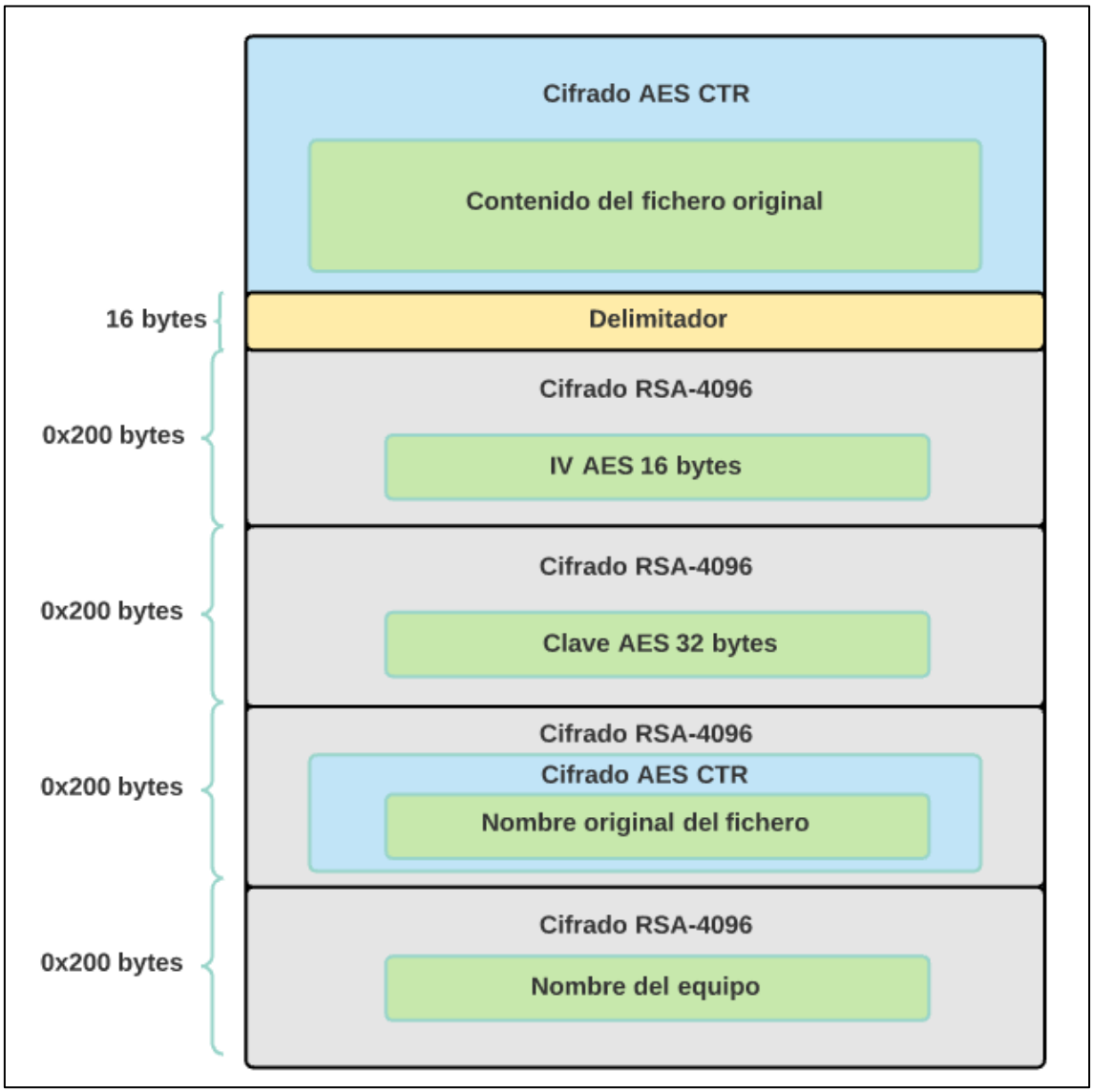

Figura 3. Desglose del resultado de la aplicación del proceso de cifrado sobre un fichero

En cuanto al delimitador con el tamaño del contenido cifrado, la mencionada cadena de 16 bytes indica en decimal el contenido a descifrar posteriormente,

añadiendo tantos ceros a la izquierda como sean necesarios hasta completar los 16 bytes. Para un fichero de 1.134 bytes, el delimitador se muestra en la siguiente imagen, marcado en rojo.

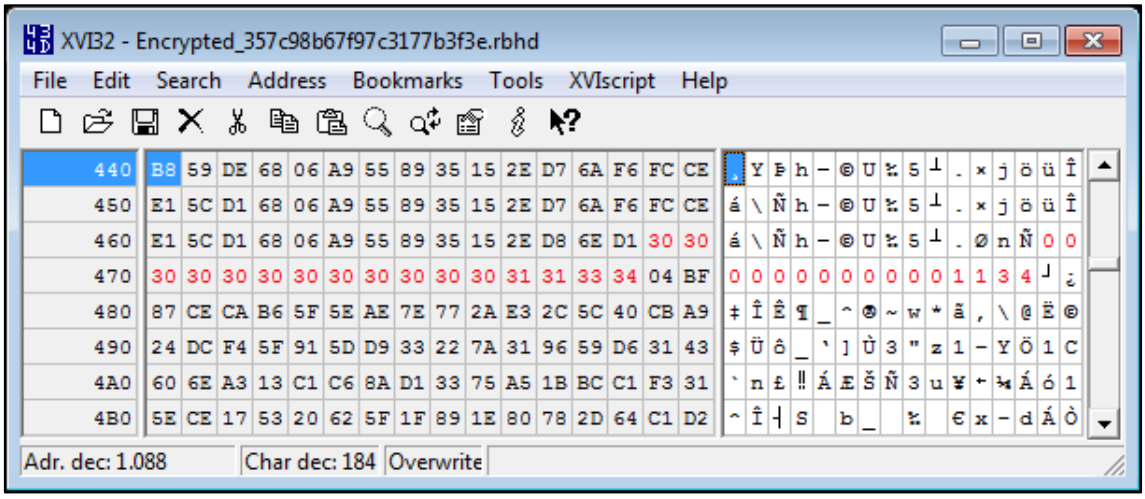

Figura 4. Ejemplo de delimitador para un fichero de 1.134 bytes

Finalmente, el nombre para el fichero con el contenido cifrado se genera de acuerdo al formato **Encrypted_[A-F0-9]{22}.rbhd**.

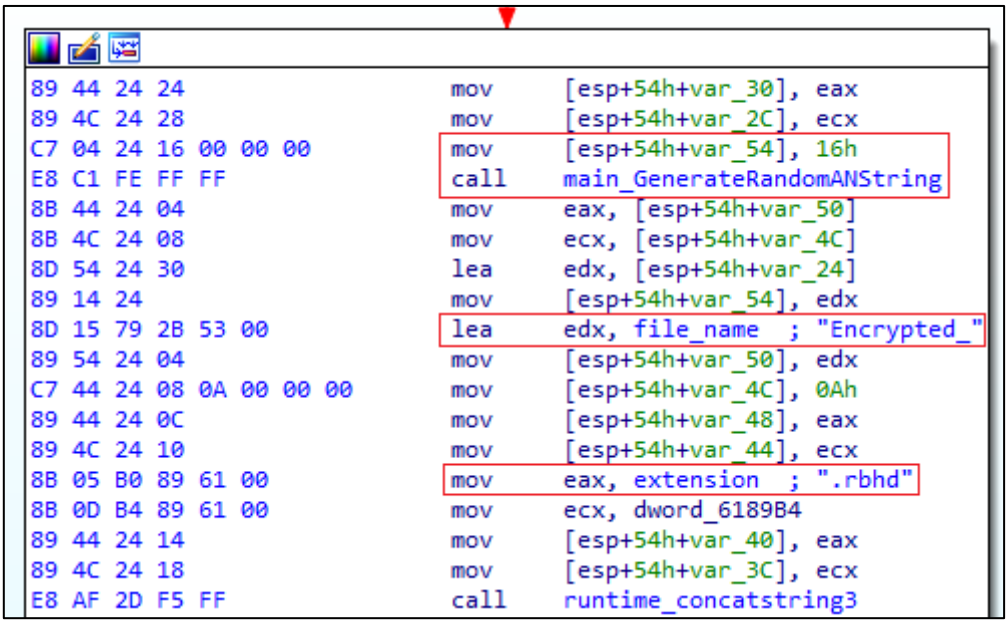

Figura 5. Generación de nombres para los ficheros con el contenido cifrado

Tras concluir el proceso de cifrado de ficheros, en el directorio en que se ejecutó el código dañino se escribe el fichero **rub.done**, indicando la finalización del proceso de cifrado.

4.5 ELIMINADO DE LAS SHADOW COPIES Y LOGS

Tras finalizar el proceso de cifrado, el código dañino tratará de asegurar que no se pueda devolver el sistema a un estado anterior a través del borrado de las ***shadow***

copies y configurará el sistema para deshabilitar reparaciones automáticas e ignorar posibles errores al inicio o apagado del equipo. Con este propósito, el binario analizado ejecuta los siguientes comandos.

```
cmd.exe /c vssadmin resize shadowstorage /for=C: /on=C: /maxsize=389MB
cmd.exe /c vssadmin resize shadowstorage /for=C: /on=C: /maxsize=unbounded
cmd.exe /c vssadmin.exe delete shadows /all /Quiet
cmd.exe /c WMIC.exe shadowcopy delete
cmd.exe /c bcdedit.exe /set {default} recoveryenabled no
cmd.exe /c bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
```

Además, se tratarán de eliminar todos los eventos del equipo listados con el comando **wevtutil.exe el**.

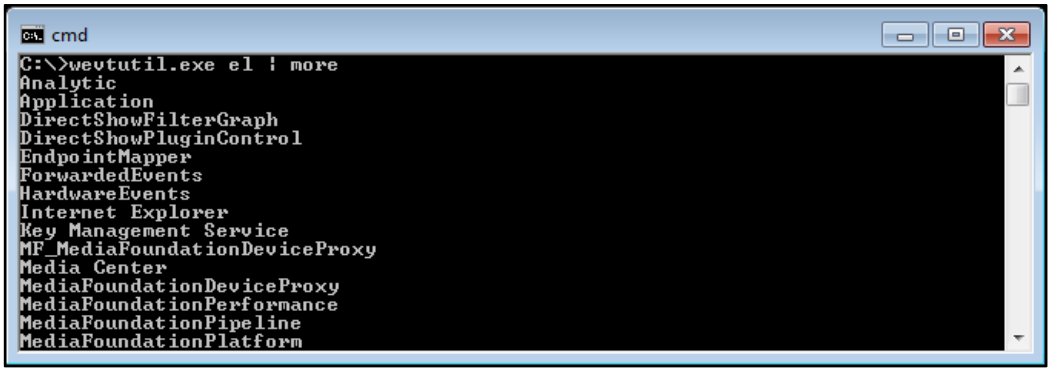

Figura 6. Ejemplo de listado de eventos a eliminar por el código dañino

Cada evento de la lista obtenida en cada equipo como resultado de la ejecución del comando anterior se tratará de eliminar mediante el comando **wevtutil cl**.

4.6 AUTO-ELIMINACIÓN

Cuando concluye el proceso de cifrado, tanto la clave pública como los ficheros que asisten en la enumeración de los archivos a cifrar se eliminan del equipo.

Ficheros eliminados tras concluir el proceso de cifrado
C:\Windows\Temp\key.pub
C:\Windows\Temp\r_f_l_2
C:\Windows\Temp\r_f_s_2
C:\Windows\Temp\r_o_s_2

Para eliminar el binario responsable del proceso de infección y cifrado, en el mismo directorio en que se inició la ejecución, se genera el fichero **RCleanUpBin.bat** con el siguiente contenido.

```
tasklist /v
tasklist /v
tasklist /v
del /f /q <localización del binario responsable del cifrado>
del /f /q <directorio del binario responsable del cifrado>\RCleanUpBin.bat
```

Dado que el binario se elimina, esta variante de ransomware no adquiere persistencia en el equipo.

5. RESCATE

En cada directorio donde se cifren archivos, en el directorio donde se ejecute el ransomware y en el escritorio, se podrán encontrar dos notas con las instrucciones para el rescate, ambas idénticas, en los ficheros **_Readme_Decrypt__Files.html** y **_Readme_Help_Important.html**.

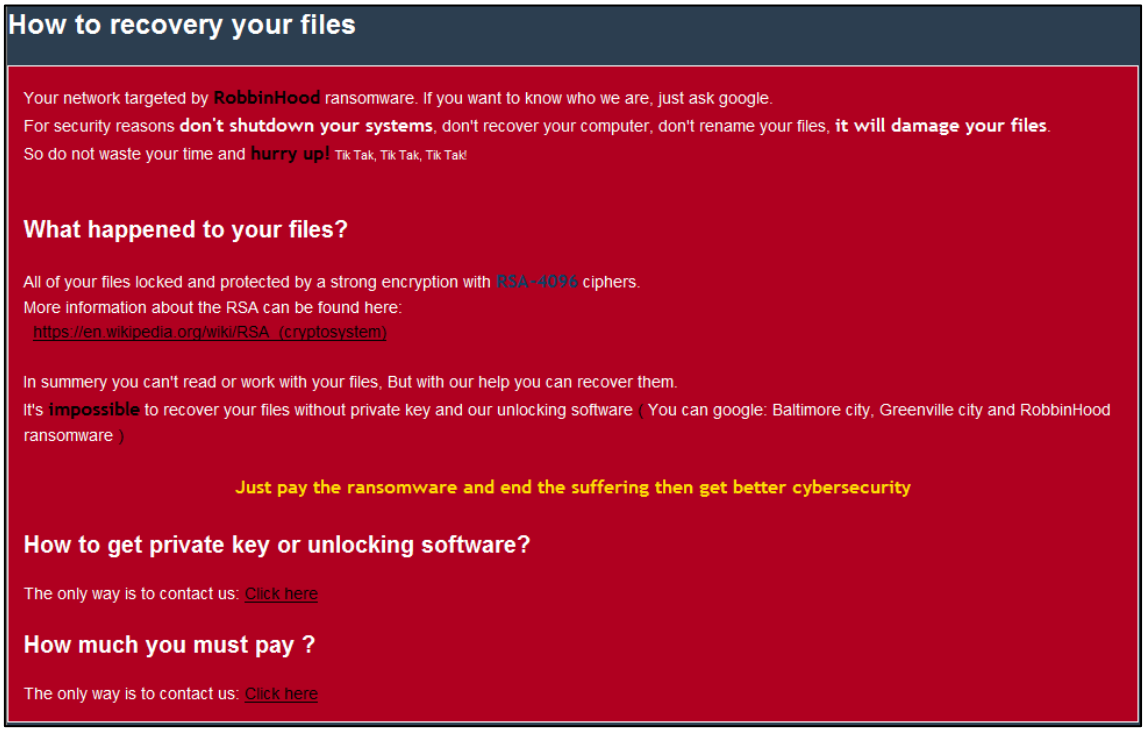

Figura 7. Instrucciones para recuperar los ficheros

En las notas se sugieren unas recomendaciones con el objetivo de no dañar los ficheros y se facilitan los pasos para establecer el contacto con el grupo cibercriminal.

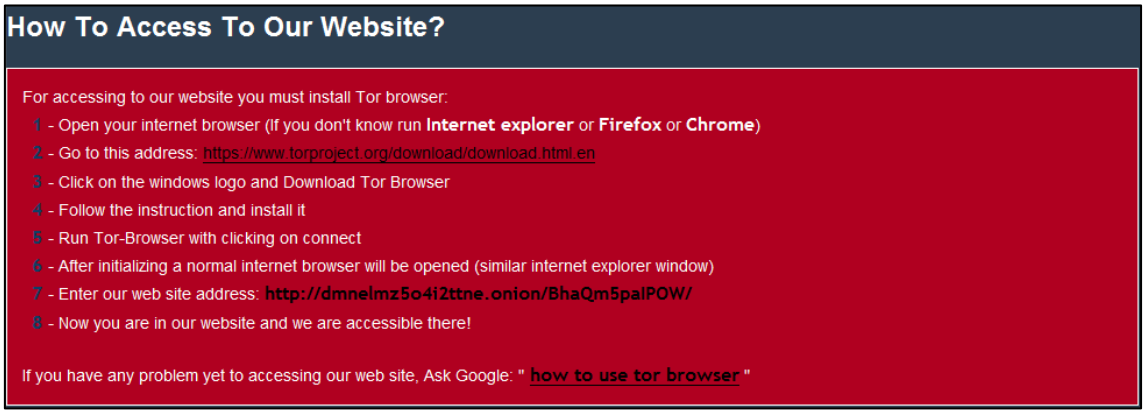

Figura 8. Instrucciones para contactar al grupo ciber-criminal

Como se observa en la nota de rescate, el portal para la negociación es accesible a través de TOR en la dirección:

http://dmnelmz5o4i2ttne.onion/BhaQm5paIPOW/

Dentro del portal, se aclaran una serie de conceptos sobre el funcionamiento del mismo y se establecen unos periodos en los que proceder con el pago a riesgo de que se incremente el importe o se eliminen las claves de descifrado.

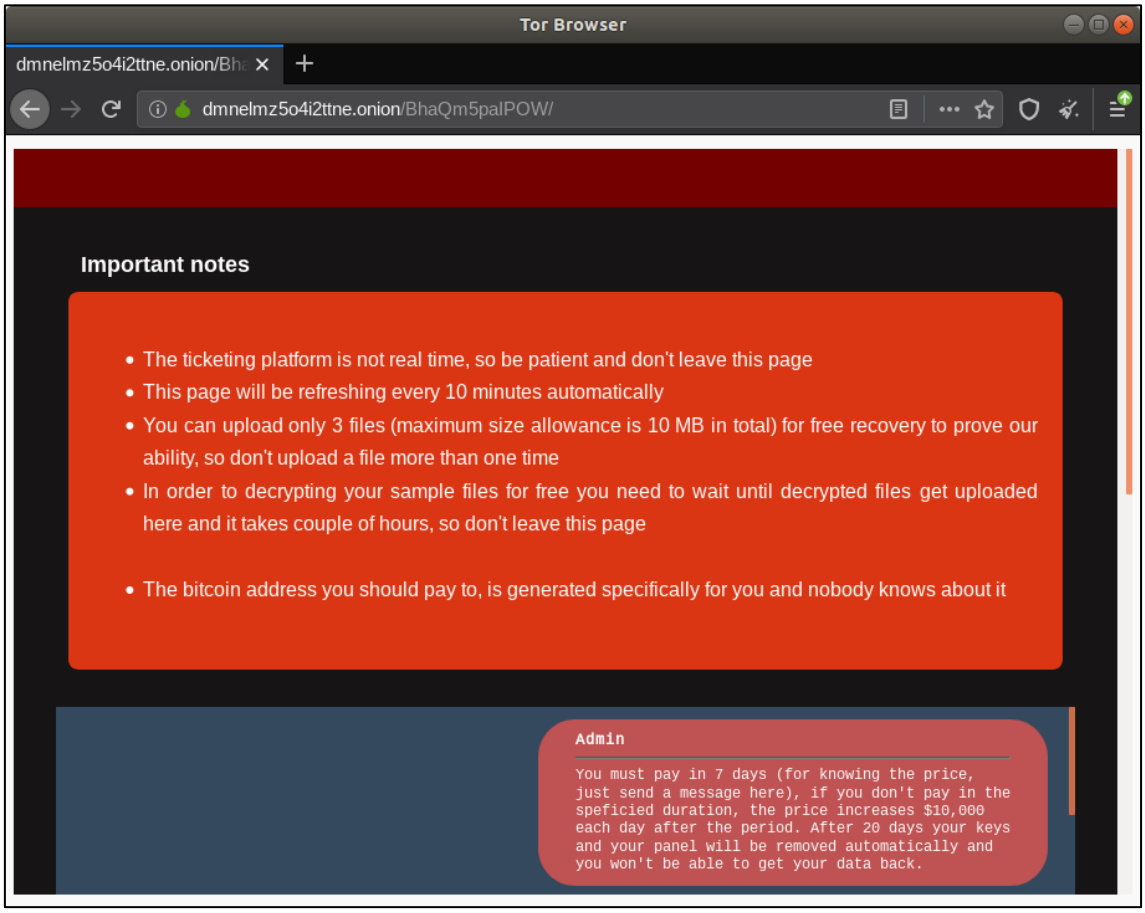

Figura 9. Notas importantes en el portal de pago

Para el incidente provocado por el binario objeto de análisis, el precio establecido es de 9 BTC a depositar en el *wallet*:

1CQkVWZFhYeWt4wbme4xL93BfKxFiYveAQ

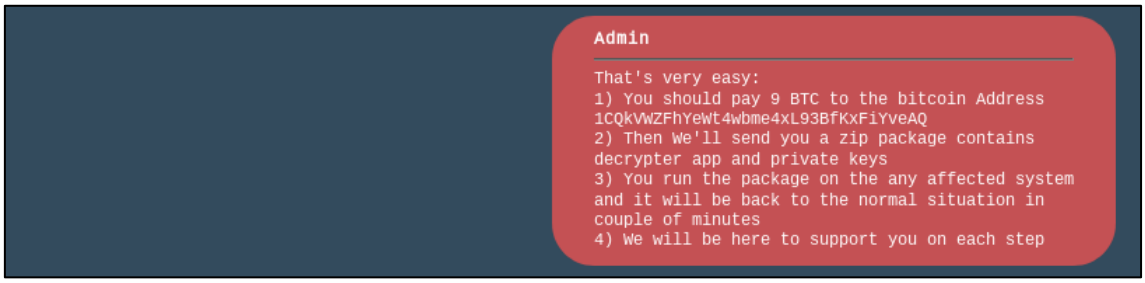

Figura 10. Precio establecido para el software y claves de descifrado.

6. DESINFECCIÓN

Dada la naturaleza del código dañino, no se requiere de un proceso de desinfección, puesto que no adquiere persistencia. Además, tras concluir ejecución el binario se auto-elimina, por lo que no existiría riesgo de volver a infectar el sistema accidentalmente.

En el caso del cifrado de los ficheros, el modelo de criptografía utilizado garantiza que el descifrado sea únicamente posible mediante el uso de la clave privada del par RSA, que se encuentra en poder del grupo cibercriminal.

7. REGLAS DE DETECCIÓN

7.1 REGLA YARA

```
rule RobbinHood
{
   meta:
      author = "CCN-CERT"
      date = "2020-06-15"
   strings:
      $path = "C:/Users/User/go/src/Robbinhood" ascii
      $main_0 = "main.Base64Decode" ascii
      $main_1 = "main.CoolMaker" ascii
      $main_2 = "main.doit" ascii
      $main_3 = "main.GenerateRandomANString" ascii
      $main_4 = "main.GetDrives" ascii
      $main_5 = "main.HelpMaker" ascii
      $main_6 = "main.NewKiller" ascii
      $main_7 = "main.RandomFileName" ascii
```

```
        $main_8 = "main.Reverse" ascii
        $main_9 = "main.RsaEncrypt" ascii
        $main_10 = "main.Walker" ascii
    condition: (uint16(0) == 0x5A4D and
            $path and
            all of ($main*))
}
```

8. INDICADORES DE COMPROMISO

Fichero	SHA256
winlogon.exe	67d8888c4ef9b58a9f17b8afe5ec6dd9155dd334ef60729fc8bb7c6f6f144b6a
payload.exe	f431c0d492eb29159fc0a92deb2a029ec3f5a40340b1e3ba52f6bc20a8842e79

Artefactos
C:\Windows\Temp\key.pub
C:\Windows\Temp\r_f_l_2
C:\Windows\Temp\r_f_s_2
C:\Windows\Temp\r_o_s_2
rub.s
rub.done
RCleanUpBin.bat

Nota de rescate
_Readme_Decrypt__Files.html
_Readme_Help_Important.html

Ficheros cifrados
Encrypted_[A-F0-9]{22}.rbhd

9. Anexo A. EXTENSIONES OBJETIVO DEL CIFRADO.

Extensiones objetivo del cifrado			
3dm	djvu	menu	rtf
3ds	dmp	mfw	rvt
3fr	dng	mid	rw2
3g2	doc	mkv	rwl
3gp	docb	mlb	rwz
3pr	docm	mlx	s3db
602	docx	mml	safe
7z	dot	mmw	sas7bdat
7zip	dotm	mny	sav
aac	dotx	moneywell	save
ab4	drf	mos	say
accdb	drw	mov	sb
accde	drwdot	mp3	sc2save
accdr	dst	mp4	sch
accdt	dtd	mpa	sd0
ach	dwf	mpeg	sda
acr	dwg	mpg	sdf
act	dws	mpqge	sh
adb	dxb	mrw	sid
adp	dxf	mrwref	sidd
ads	dxg	ms11	sidn
aes	dxt	msg	sie
agdl	dxx	myd	sis
ai	edb	myi	sldm

Extensiones objetivo del cifrado			
aif	eml	n64	sldx
aiff	epk	ncf	slk
ait	eps	nd	slm
al	epub	ndd	sln
aoi	erbsql	ndf	snx
apj	erf	nef	sql
apk	esm	NEF	sqlite
ARC	exf	nes	sqlite3
arch00	fdb	nk2	sqlitedb
arw	ff	nop	sr2
asc	ffd	nrw	srf
asf	fff	ns2	srt
asm	fh	ns3	srw
asp	fhd	ns4	st4
aspx	fla	nsd	st5
asset	flac	nsf	st6
asx	flf	nsg	st7
avi	flv	nsh	st8
awg	flvv	ntl	stc
bank	fmb	nvram	std
ibank	forge	nwb	sti
bar	fos	nx2	stm
bat	fpk	nxl	stw
bay	fpx	nyf	stx
bc6	frm	oab	sum

Extensiones objetivo del cifrado			
bc7	fsh	obj	suo
bdb	fxg	odb	svg
bgt	gam	odc	swf
big	gdb	odf	sxc
bik	gho	odg	sxd
bin	gif	odm	sxg
blend	go	odp	sxi
blob	gpg	ods	sxm
bmp	gray	odt	sxw
bpw	grey	ogg	syncdb
brd	groups	oil	t12
bsa	gry	onetoc2	t13
bz2	gz	orf	tar
c	h	ost	tarbz2
cab	hbk	otg	tax
cas	hdd	oth	tbk
catdrawing	hkdb	otp	tex
catpart	hkx	ots	tga
catproduct	hplg	ott	tgz
cc	hpp	p12	thm
cddx	htm	p7b	tif
cdf	html	p7c	tiff
cdr	hvpl	pab	tlg
cdr3	hwp	pages	tmp
cdr4	ibd	pak	tor

Extensiones objetivo del cifrado			
cdr5	ibz	paq	txt
cdr6	ico	pas	unity3d
cdrw	icxs	pat	uop
cdx	idx	pbl	uot
ce1	iif	pcd	upk
ce2	iiq	pct	vb
cer	incpas	pdb	vbox
cfg	indd	pdd	vbs
cfp	ini	pdf	vcf
cfr	itdb	pef	vdf
cgm	itl	pem	vdi
chm	itm	pfx	vfs0
cib	iwd	php	vhd
class	iwi	pif	vhdx
cls	jar	pkpass	vmdk
cmd	java	pl	vmem
cmt	jin	plc	vmsd
cnf	jnt	plus_muhd	vmsn
conf	jpe	pm	vmx
config	jpeg	png	vmxf
contact	jpg	pot	vob
cpi	js	potm	vpk
cpp	jse	potx	vpp_pc
cr2	jsp	ppam	vsd
craw	kc2	pps	vsdx

Extensiones objetivo del cifrado			
crt	kdb	ppsm	vtf
crw	kdbx	ppsx	w3x
cs	kdc	ppt	wab
csh	key	PPT	wad
csl	kf	pptm	wallet
csr	kpdx	pptx	walletdat
css	kwm	prf	war
csv	laccdb	ps	wav
d3dbsp	lay	psafe3	wb2
dac	lay6	psd	wk1
das	layout	psk	wks
dat	lbf	pspimage	wma
data	ldf	pst	wmo
dazip	lit	ptw	wmv
db	litemod	ptx	wotreplay
db-journal	litesql	pwm	wpd
db0	log	py	wps
db3	lrf	qba	x11
db_journal	ltx	qbb	x3f
dba	lua	qbm	xf
dbf	lvl	qbr	xis
dbfv	m	qbw	xla
dbx	m2	qbx	xlam
dc2	m2ts	qby	xlc
dch	m3u	qcow	xlk

Extensiones objetivo del cifrado			
dcr	m4a	qcow2	xlm
dcs	m4p	qdf	xlr
ddd	m4u	qed	xls
ddoc	m4v	qic	XLS
ddrw	map	r3d	xlsb
dds	mapimail	raf	xlsm
dem	max	rar	xlsx
der	mbx	rat	xlt
des	mcgame	raw	xltm
desc	mcmeta	rb	xltx
design	md	rdb	xlw
dfs	mdb	re4	xml
dgc	mdbackup	rgss3a	xxx
dif	mdc	rim	ycbcra
dip	mddata	rm	yuv
dit	mdf	rofl	zip
djv	mef	rom	ztmp

10. Anexo B. PROCESOS A FINALIZAR.

Procesos a finalizar			
acrord32.exe	inodemon.exe	rdfsnap.exe	tdfchart_l1.exe
acrotray.exe	ipoverusbsvc.exe	rdfsnapupdate.exe	tdfserver2_l1.exe
adb.exe	jenkins.exe	rdrcef.exe	tdfserver2_l2.exe
afterfx.exe	kbasesrv.exe	redgate.client.service.exe	tdfserver_all.exe
agmservice.exe	kernelupdate.exe	redgate.sqlprompt.trayapp.exe	tdfserver_l1_internal.exe
agsservice.exe	ksafesvc.exe	redis-server.exe	tdfserver_l2_internal.exe
aliwssv.exe	ksafetray.exe	regtool.exe	teambition.exe
alphasex.exe	linqpad.exe	reportingservicesservice.exe	teamviewer_service.exe
apirecv.exe	lockapp.exe	reverseproxy_windows_amd64.exe	tenpayserver.exe
appsubproc.exe	mad.exe	reviewassistantserver.exe	testfundcounter.exe
armsvc.exe	memcached.exe	rhs.exe	testhost.x86.exe
arpradio.exe	microsoft.exchange.imap4.exe	rinst3.exe	tfsjobagent.exe
ARSMxmind.exe	microsoft.exchange.pop3.exe	rpctest.exe	thirdpips.exe
aspnet_state.exe	microsoft.notes.exe	rrmsvr.exe	tnslsnr.exe
autodown.exe	microsoft.photos.exe	rsync.exe	toad.exe
axurerp8.exe	microsoftedge.exe	ruby.exe	tomcat7.exe
axurerp9.exe	microsoftedgecp.exe	sacmonitor.exe	tomcat7w.exe
baidupinyin.exe	microsoftpdfreader.exe	sacsrv.exe	tomcat8.exe
bash.exe	mjastickynotes.exe	sangforpromoteservice.exe	tortoisemerge.exe
bcclipboard.exe	mongod.exe	scanningprocess.exe	totalcmd64.exe
bcompare.exe	msdtssrvr.exe	scriptedsandbox64.exe	trustedinstaller.exe

Procesos a finalizar			
bddlsvc.exe	msexchangeadtopologyservice.exe	searchui.exe	tschelp.exe
bds.exe	msexchangedagmgmt.exe	sec.plug.request.exe	tsservice.exe
bestsyncsvc.exe	msexchangedelivery.exe	secbizsrv.exe	tvnserver.exe
blnsvr.exe	msexchangefds.exe	securecrt.exe	typora.exe
bsqlserver.exe	msexchangefrontendtransport.exe	sendonlineservicemail.exe	uedit32.exe
cajshost.exe	msexchangehmhost.exe	serv-u-tray.exe	ultracti.exe
calculator.exe	msexchangehmworker.exe	serv-u.exe	ultralnk.exe
cclibrary.exe	msexchangemailboxassistants.exe	servercmdatasync.exe	ultramci.exe
ccservice.exe	msexchangemailboxreplication.exe	service.exe	umservice.exe
ccxprocess.exe	msexchangemailsubmission.exe	servicehub.datawarehousehost.exe	umworkerprocess.exe
cherrytree.exe	msexchangerepl.exe	servicehub.host.clr.x86.exe	uniclient.exe
cloud.exe	msexchangesubmission.exe	servicehub.host.node.x86.exe	updateservice.exe
cloudtester.exe	msexchangethrottling.exe	servicehub.identityhost.exe	vcddaemon.exe
clussvc.exe	msexchangetransport.exe	servicehub.settingshost.exe	vcpkgsrv.exe
cmbcu.exe	msexchangetransportlogsearch.exe	servicehub.vsdetouredhost.exe	vdagent.exe
code.exe	msftefd.exe	servicemonitor.exe	vdassignserver.exe
codehelper.exe	msftesql.exe	sftracing.exe	vdinternet.exe
codemanager.exe	msmdsrv.exe	sgtool.exe	vdservice.exe
coresync.exe	msosync.exe	sh.exe	video.ui.exe
cosmostools.exe	mspdbsrv.exe	shellexperiencehost.exe	visio.exe
cryptoserver.exe	mssecsvc.exe	skypeapp.exe	visualsvnserver.exe
csdispatcher.exe	msvsmon.exe	skypebackgroundhost.exe	vmacthlp.exe
csliveviewer.exe	mwicbcukeytoolu.exe	smgspider.exe	vmtoolsd.exe

Procesos a finalizar			
cygrunsrv.exe	mwicbcukeyui.exe	smtpforwarder.exe	vmware-authd.exe
dbghost.exe	mysql.exe	snagit32.exe	vmware-hostd.exe
dbus-daemon.exe	mysqld-nt.exe	snagiteditor.exe	vmware-tray.exe
dcrotatelogs.exe	mysqld.exe	snagpriv.exe	vmware-unity-helper.exe
dcshelper.exe	mysqlinstallerconsole.exe	snipaste.exe	vmware-usbarbitrator.exe
dcusbsummary.exe	mysqlnotifier.exe	sogoucloud.exe	vmware-usbarbitrator64.exe
devenv.exe	mysqlworkbench.exe	soundman.exe	vmware-vmx.exe
dhmachinesvc.exe	navicat.exe	splwow64.exe	vmware.exe
dhpluginmgr.exe	netbeans64.exe	sqlagent.exe	vncserver.exe
distrib.exe	nmesrvc.exe	sqlagent90.exe	vncviewer.exe
dotnet.exe	node.exe	sqlbrowser.exe	vprintproxy.exe
dtshellhlp.exe	noderunner.exe	sqlceip.exe	vstest.console.exe
dualmonitor.exe	notepad++.exe	sqldbxu.exe	wbox.exe
eclipse.exe	notepadstarter.exe	sqliteexpertpers.exe	wbrowser.exe
edb.exe	nscaagent.exe	sqlplus.exe	wdplogin.exe
editplus.exe	nscauth.exe	sqlservr.exe	webanalyticsservice.exe
emagent.exe	nscauthservice.exe	sqlwriter.exe	webstorm64.exe
enginehost.exe	nsclient++.exe	sqlyog.exe	weip.exe
epenvupdate.exe	nsdvigil.exe	ssereg.exe	weipconsole.exe
epmd.exe	nsdvigilserver.exe	sshd.exe	wifiopenmonitor2.exe
erl.exe	occlient.exe	ssms.exe	wim.exe
erlsrv.exe	occlientmonitor.exe	ssudt.exe	win32sysinfo.exe
everything.exe	oclistener.exe	standardcollector.service.exe	wind.3c.voip.stpush.exe
excel.exe	oconsole3.exe	startmenuexperiencehost.exe	wind.adm.service.exe
extjob.exe	ocontrol3.exe	starwindmanagementconsole.exe	wind.aegis.basesystem.rms.exe

Procesos a finalizar			
falcon-agent.exe	ocrobert.exe	starwindservice.exe	wind.aegis.commonservice.exe
fdhost.exe	officeclicktorun.exe	store.exe	wind.aegis.comsystem.config.exe
fdlauncher.exe	oguard3.exe	studio.exe	wind.aegis.comsystem.log.exe
fetionbox.exe	ois.exe	studio.vshost.exe	wind.aegis.comsystem.org.exe
fh_shell.exe	omailrpt.exe	sublime_text.exe	wind.aegis.crmindexadmin.exe
fiddler.exe	omtsreco.exe	svnpermissionservice.exe	wind.aegis.crmservice.exe
filezilla.exe	onedrive.exe	syhttpd.exe	wind.aegis.crmservice.vshost.exe
flux.exe	onenote.exe	sypns.exe	wind.aegis.crmsyncserver.exe
fms.exe	onenotem.exe	systemsettings.exe	wind.aegis.dashboardservice.exe
foxit reader.exe	oracle.exe	taobaoprotect.exe	wind.aegis.financeservice.exe
foxitprotect.exe	oravssw.exe	tapaccept_cust.exe	wind.aegis.hrmserver.exe
fscapture.exe	oserver3.exe	tapaccept_opt.exe	wind.aegis.indexadmin.exe
fsnotifier64.exe	osppsvc.exe	tapaccept_qh.exe	wind.aegis.ipdservice.exe
gm3000gfamon.exe	ouc.exe	tapaccept_rzrqstock.exe	wind.aegis.lbs.exe
groove.exe	outlook.exe	tapaccept_stock.exe	wind.aegis.level2report.exe
gsfwzx.exe	packetbeat.exe	tapadmin.exe	windbg.exe
haozipsvc.exe	packetserverhost.exe	tapatm.exe	windserver.exe
helppane.exe	pcas.exe	tapchecker.exe	winpty-agent.exe
hiditf.exe	pdfsaver3.exe	tapcustomermanager.exe	winrar.exe
hprsnap8.exe	peopleexperiencehost.exe	tapdaemon.exe	winserv.exe
hpwucli.exe	perfwatson2.exe	tapemailservice.exe	winstore.app.exe
hpwuschd2.exe	perl.exe	taperror2eagle.exe	winword.exe

Procesos a finalizar			
hqrecv_cf2_n.exe	pic_2345svc.exe	tapfuture.exe	wmain.exe
hqrecv_cf_n.exe	picpick.exe	tapfutureatm.exe	wps.exe
hqrecv_file.exe	pingan_certd.exe	taphkstock.exe	wpscenter.exe
hqrecv_hk2_n.exe	plsqldev.exe	tapmain.exe	wrapper.exe
hqrecv_l1_n.exe	plugin_host.exe	tapmargintrading.exe	writage.exe
hqrecv_l1_op.exe	pmsagentserver.exe	tapoptionatm.exe	wscheduler.exe
hqrecv_l1_pt.exe	portmap.exe	tapoptionindex.exe	wservice.exe
hqrecv_l1_uo.exe	postgres.exe	tapoptionstock.exe	wslogon.exe
hqrecv_l1_wp.exe	powerpnt.exe	tapproxyserver.exe	xendpriv.exe
hqrecv_l2_n.exe	presentationfontcache.exe	tapserverconfig.exe	xftp.exe
hqrecv_sh2_n.exe	printserverwinservice.exe	tapsimumatch.exe	xmind.exe
hqrecv_sz2_n.exe	prunsrv64.exe	tapstock.exe	xshell.exe
hqsend_all.exe	pwsearch.exe	taptestquorecv.exe	xshellcore.exe
hqsend_l1.exe	pycharm64.exe	tbsecsvc.exe	youdaodict.exe
hqsend_l1_n.exe	python.exe	tdbserver2_l1.exe	youdaoeh.exe
hqsend_l2_n.exe	pythonservice.exe	tdbserver2_l2.exe	youdaoocr.exe
httpd.exe	qemu-ga.exe	tdbserver_hk.exe	youdaowsh.exe
hxaccounts.exe	qiyiservice.exe	tdbserver_l1.exe	yourphone.exe
hxoutlook.exe	qtwebengineprocess.exe	tdbserver_l2.exe	yqzszxzx.exe
hxtsr.exe	raautoinstsrv.exe	tdcserver_l1_new.exe	zdserv.exe
inet_gethost.exe	rcp.exe	tdcserver_l2_new.exe	

11. Anexo C. SERVICIOS A FINALIZAR.

Servicios a finalizar			
AcronisAgent	McShield	MySQL57ntrtscan	SQLAgent$TPS
AcrSch2Svc	McTaskManager	MySQL80	SQLAgent$TPSAMA
Antivirus	mfefire	NetMsmqActivator	SQLBrowser
ARSMbedbg	mfemms	ntrtscan	SQLSERVERAGENT
avast! Antivirus	mfevtp	PDVFSService	SQLTELEMETRY
bedbg	MMS	POP3Svc	SQLWriter
DCAgent	mozyprobackup	Postgresql	SstpSvc
EhttpSrv	MsDtsServer	postgresql-9.0	svcGenericHost
ekrn	MsDtsServer100	ReportServer	swi_filter
EPUpdateService	MsDtsServer110	ReportServer$TPS	swi_service
EraserSvc11710	MSExchangeES	RESvc	swi_update_64
EsgShKernel	MSExchangeIS	sacsvrsacsvr	swi_update
ESHASRV	MSExchangeMGMT	SamSs	TmCCSF
ESHASRVAVPAVP	MSExchangeMTA	SAVAdminService	tmlisten
FA_Scheduler	MSExchangeSA	SAVService	TrueKey
IISAdmin	MSExchangeSRS	SCCommService	TrueKeyScheduler
IMAP4Svc	msftesql$PROD	SDRSVC	UI0Detect
KAVFS	MSOLAP$SQL_2008	SepMasterService	VeeamBackupSvc
KAVFSGT	MSOLAP$TPS	ShMonitor	VeeamBrokerSvc
kavfsslp	MSOLAP$TPSAMA	Smcinst	VeeamCatalogSvc
klactprx	MSSQL$BKUPEXEC	SmcService	VeeamCloudSvc
kladminserver	MSSQL$ECWDB2	SMTPSvc	VeeamDeploySvc
klnagent	MSSQL$PROD	SNAC	VeeamMountSvc
klwebsrv	MSSQL$SHAREPOINT	SntpService	VeeamNFSSvc

Servicios a finalizar			
ksnproxy	MSSQL$SOPHOS	Sophos Agent	VeeamRESTSvc
macmnsvc	MSSQL$SQL_2008	Sophos Heartbeat	W3Svc
masvc	MSSQL$SQLEXPRESS	Sophos MCS Agent	wampapache
mbaeSvc	MSSQL$SYSTEM_BGC	sophossps	wampapache64
MBAMProtector	MSSQL$TPS	SQL Backups	wbengine
MBAMScheduler	MSSQL$TPSAMA	SQLAgent$CXDB	WinDefend
MBAMService	MSSQLFDLauncher	SQLAgent$ECWDB2	WRSVC
MBEndpointAgent	MSSQLSERVER	SQLAgent$PROD	Zoolz 2 Service
McAfeeFramework	MySQL57	SQLAgent$SOPHOS	