Informe Código Dañino
CCN-CERT ID-13/21

EKING

Octubre 2021

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Fecha de Edición: octubre de 2021

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 **EKING**, identificada por la firma SHA256 bb1e8e2dcc7b03cad837602c067a2d688ef1675b8552613f584d345917aaa52a.

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.

EKING es una variante de **Phobos**, familia de ransomware que apareció a principios de 2019. Debido a las diferentes extensiones que este ransomware ha utilizado (opción posiblemente personalizable en el *builder*), es frecuente encontrar referencias a este código dañino basadas únicamente en la extensión que añade a los ficheros cifrados. Tanto la nota de rescate como la nomenclatura de los documentos que han sufrido modificaciones recuerdan al ransomware Dharma, familia que evoluciona del ransomware Crysis y que surgió en 2016.

Estas variantes han estado relacionadas, históricamente, con accesos hacia las redes internas de compañías aprovechando servicios RDP expuestos a Internet. Sin embargo, hoy en día son tan numerosos los actores involucrados en ransomware, que es difícil relacionar una variante en concreto con un vector de entrada. Los grupos cibercriminales aprovecharán cualquier vector que les garantice el acceso ilícito a la red local.

En los siguientes apartados se entra en detalles técnicos sobre las características de la variante **EKING**, se propone una vacuna que evitaría infecciones de la muestra analizada y se adjunta una regla YARA para su identificación.

3. DETALLES GENERALES

El binario objeto de análisis, ejecutable para sistemas de 32-bit, se identifica con la firma SHA256 recogida en la tabla a continuación.

Fichero	SHA256
eKING.exe	bb1e8e2dcc7b03cad837602c067a2d688ef1675b8552613f584d345917aaa52a

El payload no se encuentra protegido por un packer que oculte su funcionalidad, por tanto, debido a la popularidad de Phobos, 56 de 70 antivirus catalogan la muestra como dañina.

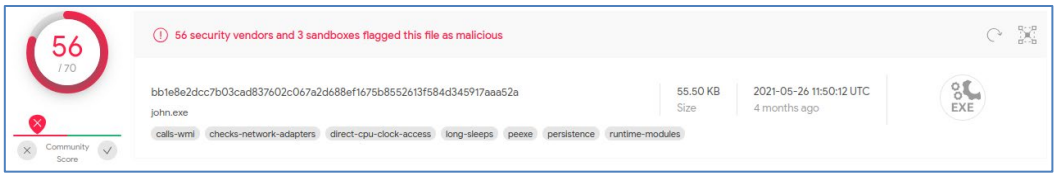

Figura 1. Ransomware EKING

4. PROCESO DE INFECCIÓN

El proceso de ejecución de EKING se divide tres grandes apartados.

1. El código dañino decide si el sistema cuenta con un lenguaje protegido y procede al control de instancias.
2. Se establece la persistencia en el equipo y se monitorizan los procesos susceptibles de ser finalizados.
3. Se lleva a cabo el cifrado de ficheros y se muestran las instrucciones para el rescate.

Una de las primeras comprobaciones que se efectúan para decidir si continuar o finalizar la ejecución es consultar el idioma por defecto a través de la función **GetLocaleInfoW**. En concreto, el código dañino comprueba el noveno bit de la información retornada por la llamada a esa función, para identificar si el sistema usa el alfabeto cirílico. De ser así, el proceso finaliza sin mayor afectación.

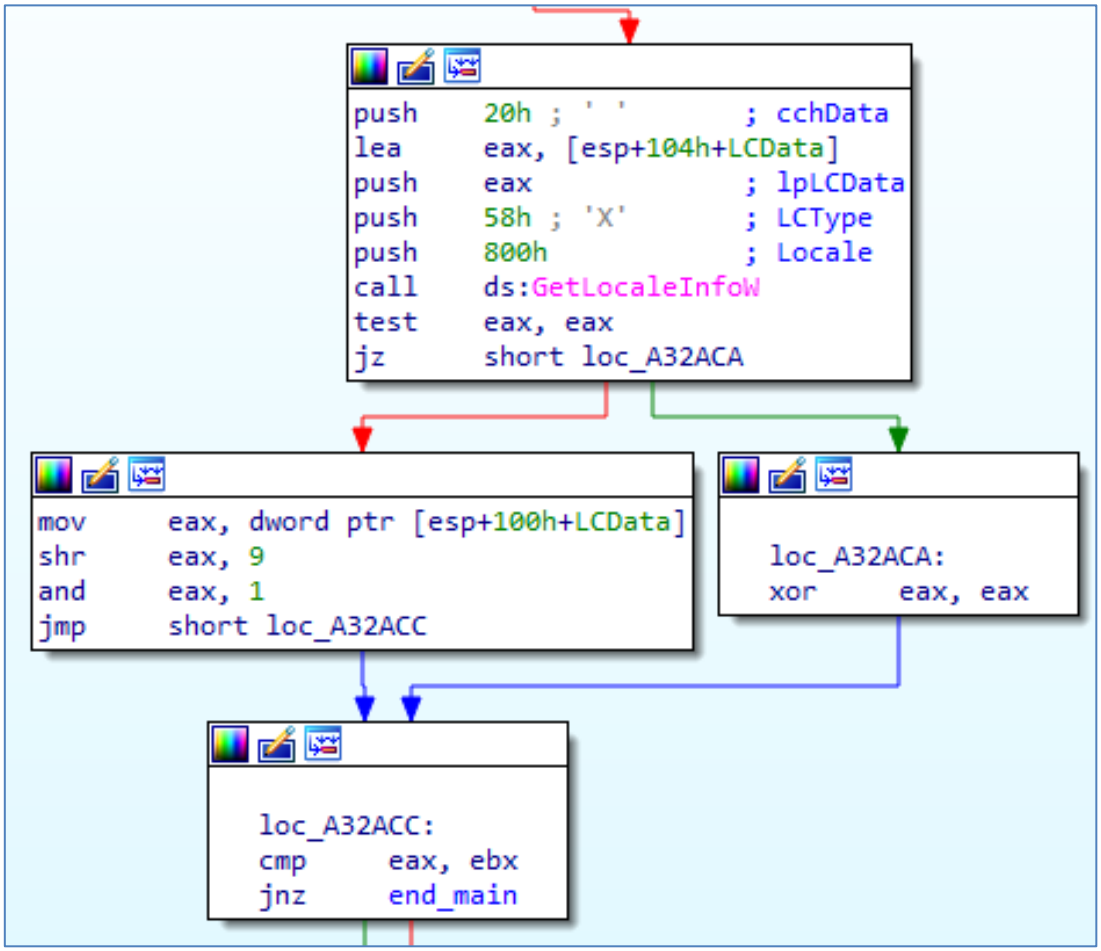

Figura 2. Chequeo del idioma por defecto

5. MUTEX

Otra de las comprobaciones efectuadas a continuación, se corresponde con el control de instancias.

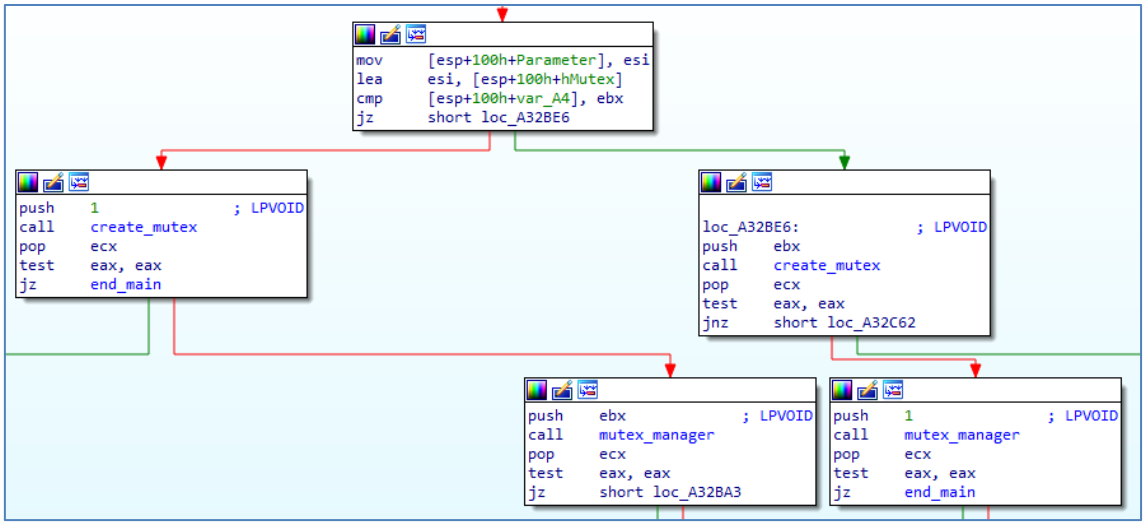

Figura 3. Control de instancias mediante mutexes

Con este propósito, EKING genera varios mutex a partir de la siguiente plantilla.

Global\<<BID>><<ID>><<ELVL>>

Los valores que completan el nombre del mutex se descomponen en la tabla a continuación.

Valor	Descripción
<<BID>>	Parece que este valor no se modifica
<<ID>>	ID de la víctima que toma el valor del VolumeSerialNumber de la unidad C:/ (8 bytes)
<<ELVL>>	Relacionado con el nivel de privilegios del proceso (8 bytes)

Para el control de estancias, el código dañino genera varios mutex, de los que nos interesan los siguientes dos ejemplos:

Global\<<BID>>XXXXXXXX00000000

Global\<<BID>>XXXXXXXX00000001

Donde **XXXXXXXX**, en el ejemplo, sería el valor del **VolumeSerialNumber** de la unidad "**C:/**". EKING toma este último valor a través de la función **GetVolumeInformationW**, que se puede consultar por línea de comandos mediante la instrucción "**vol C:**". Tomando el valor del **VolumeSerialNumber** para cada equipo y añadiendo las terminaciones 00000000 y 00000001 para completar la plantilla, se podrían generar los mutex que impedirían la ejecución de la muestra evitando el cifrado de ficheros.

6. PERSISTENCIA

Con el objetivo de ejecutarse en cada inicio del sistema y cifrar los nuevos documentos que hayan podido crearse, EKING establece hasta 4 tipos diferentes de mecanismos para lograr persistencia en el equipo. Si el proceso **no** cuenta con privilegios elevados, se establecen sólo 2 medidas para alcanzar la persistencia.

Método	Ruta
Clave de registro CurrentVersion\Run	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Copia del código dañino en StartUp	C:\Users\[User]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

Sin embargo, si el proceso cuenta con privilegios elevados, además de los métodos mencionados en la tabla anterior, también se establecen los definidos en la siguiente tabla.

Método	Ruta
Clave de registro CurrentVersion\Run	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Copia del código dañino en StartUp	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

Para la elevación, el código dañino simplemente muestra al usuario el menú del *User Account Control* (UAC) para autorizar la ejecución con los nuevos permisos. La imagen a continuación muestra la persistencia lograda por una muestra ejecutada con privilegios.

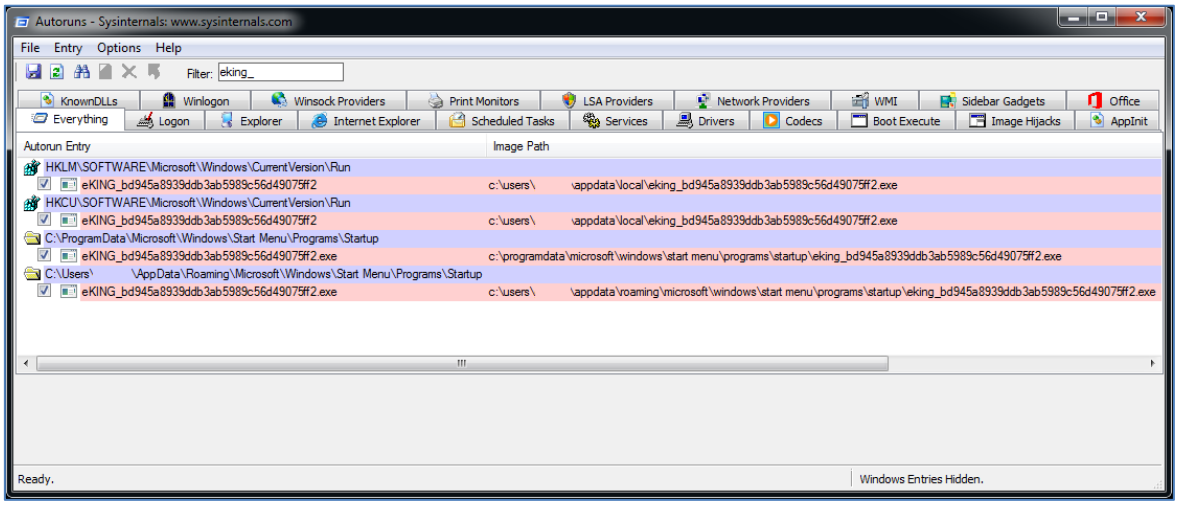

Figura 4. Persistencia en el equipo

7. FINALIZACIÓN DE PROCESOS

Antes de empezar con el proceso de cifrado, una de las medidas que EKING implementa para garantizar la máxima afectación posible, es la creación de un hilo encargado de finalizar procesos susceptibles de manejar información de valor. Al finalizar los procesos de esta manera, los ficheros abiertos por esas aplicaciones dejan de estar bloqueados y su modificación (mediante el cifrado de su contenido) es factible.

La muestra incluye un total de 38 procesos a finalizar, que se incluyen en la tabla siguiente.

Procesos a finalizar			
agntsvc.exe	dbeng50.exe	dbsnmp.exe	encsvc.exe
excel.exe	firefoxconfig.exe	infopath.exe	isqlplussvc.exe
msaccess.exe	msftesql.exe	mspub.exe	mydesktopqos.exe
mydesktopservice.exe	mysqld-nt.exe	mysqld-opt.exe	mysqld.exe
ocautoupds.exe	ocomm.exe	ocssd.exe	onenote.exe
oracle.exe	outlook.exe	powerpnt.exe	sqbcoreservice.exe
sqlagent.exe	sqlbrowser.exe	sqlservr.exe	sqlwriter.exe
steam.exe	synctime.exe	tbirdconfig.exe	thebat.exe
thebat64.exe	thunderbird.exe	visio.exe	winword.exe
wordpad.exe	xfssvccon.exe		

8. ESQUEMA DE CIFRADO

Para el cifrado de la información, se emplea un modelo de criptografía simétrica para el contenido del fichero y asimétrica para proteger la clave simétrica. EKING embebe una clave RSA de 128-bytes y genera por cada infección una única clave AES de 256-bit. Esa clave AES es cifrada con la RSA y el blob resultante se anexa al final de cada fichero cifrado. El modo de AES empleado es CBC (*Cipher Block Chaining*) y para cada fichero se utiliza un vector de inicialización aleatorio de 128-bit.

Una vez iniciado el proceso de cifrado, EKING genera múltiples hilos de ejecución con la intención de mejorar la eficiencia y cifrar la información en el menor tiempo posible. Además, el código dañino prioriza el cifrado de documentos relativos a bases de datos suponiendo que serán de mayor valor para el usuario. Las extensiones cuyo cifrado se prioriza se encuentran en el **anexo A**.

Si bien es frecuente que el ransomware incluya un listado de ciertas extensiones que se encontrarían exentas del cifrado, EKING sólo hace referencia a versiones

anteriores del código dañino. De esta manera, extensiones como **eking** o **phobos** se encuentran exentas del cifrado pero, ficheros .exe o .dll se cifran a no ser que se encuentren en directorios críticos del sistema como el directorio Windows. Las extensiones que se encuentran exentas del cifrado se encuentran en el **anexo B**.

La clave AES de 256-bit que se genera de forma aleatoria se usa para cifrar todos los ficheros en una misma ejecución en un mismo equipo. Sin embargo, por cada fichero, se genera un vector de inicialización de 128-bit. Este vector se añade en claro (remarcado en verde) en el bloque de información que se anexa a cada fichero para hacer posible el descifrado. La clave AES de 256-bit se cifra con la parte pública del par RSA y el resultado (marcado en azul) también se añade al final del fichero cifrado.

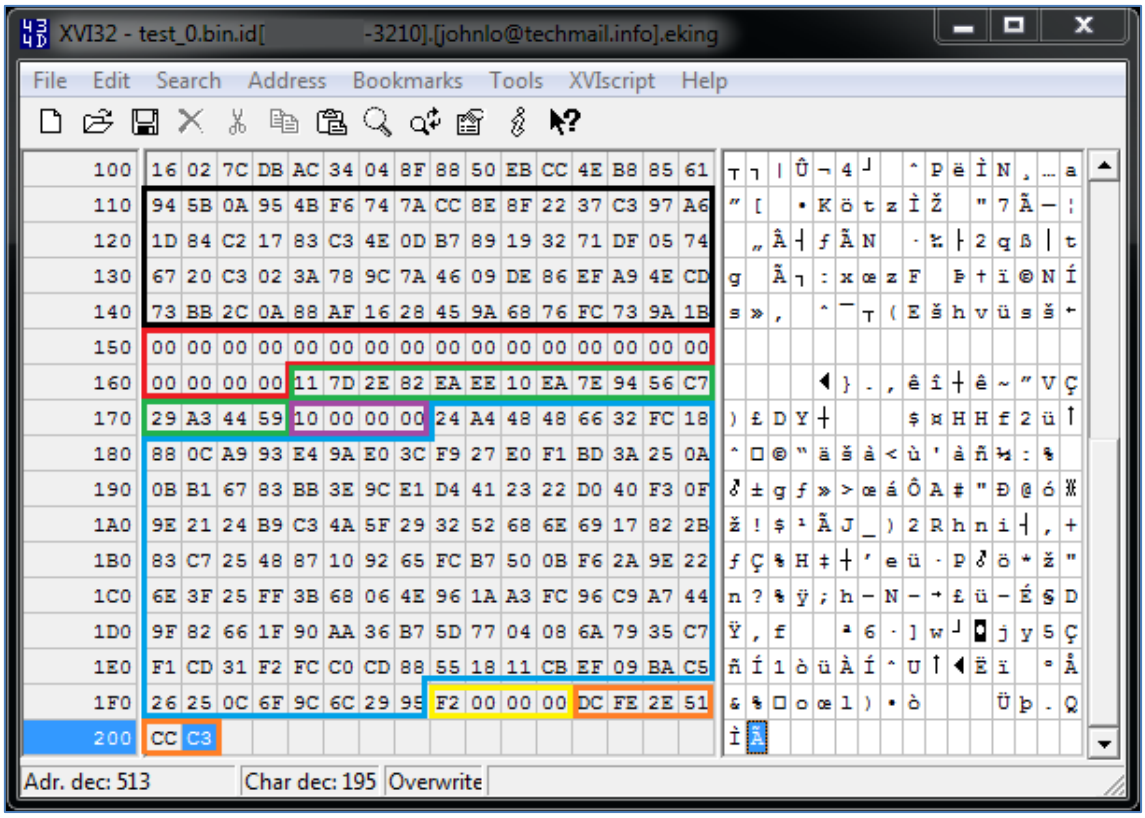

Figura 5. Esquema de cifrado

Además del vector de inicialización y la clave AES, el bloque de información contiene más elementos. Remarcado en negro y justo a continuación del contenido cifrado, se añade, también bajo una capa de cifrado, cierta información del fichero original como, por ejemplo, el nombre del documento. En rojo, una cadena de 20 valores nulos que podrían servir como delimitador. En morado, 4 bytes que indican cuanto relleno se ha añadido al contenido cifrado. En amarillo, se indica el tamaño total del bloque de información anexado al contenido cifrado. Finalmente, en naranja, un marcador que esta muestra en particular añade al final del bloque.

Al nombre del fichero original se le añade el identificador de usuario infectado, formado por el valor del **VolumeSerialNumber** mencionado anteriormente y los

dígitos **3210**. Es posible que este último valor identifique al cliente del proveedor de ransomware.

test.bin.id[XXXXXXXX-3210].[johnlo@techmail.info].eking

A continuación del identificador de usuario, uno de los e-mails de los actores y la extensión específica de la variante completa el nombre del fichero cifrado.

Finalmente, cabe destacar que EKING no sólo intenta cifrar los ficheros del equipo puesto que, si es posible acceder a recursos compartidos en la red, también implementa la funcionalidad para cifrar estos recursos.

9. COMUNICACIÓN

Esta variante de Phobos incorpora la funcionalidad necesaria para realizar una petición POST a un posible servidor controlado por el atacante.

```
v11 = 0;
v4 = WinHttpOpen(&pszAgentW, 1u, 0, 0, 0);
v9 = v4;
if ( v4 )
{
  v5 = WinHttpConnect(v4, pswzServerName, 0, 0);
  hInternet = v5;
  if ( v5 )
  {
    v6 = WinHttpOpenRequest(v5, L"POST", pwszObjectName, 0, 0, 0, 0);
    v7 = v6;
    if ( v6 )
    {
      if ( WinHttpSendRequest(v6, 0, 0, lpOptional, dwOptionalLength, dwOptionalLength, 0) )
        v11 = WinHttpReceiveResponse(v7, 0);
      WinHttpCloseHandle(v7);
    }
    WinHttpCloseHandle(hInternet);
  }
  WinHttpCloseHandle(v9);
}
return v11;
```

Figura 6. Código para realizar peticiones POST

Sin embargo, en la muestra analizada no se incluye ningún servidor de mando y control y no se completa ninguna estructura que enviar como cuerpo de la petición POST. Este fragmento de código no llega a ser ejecutado por el código dañino.

10. RESCATE

La nota de rescate **info.txt** facilita dos direcciones de e-mail para iniciar el contacto y negociar el precio de la herramienta de descifrado. A continuación, el total del contenido de la nota se muestra en el fragmento.

!!!All of your files are encrypted!!!

To decrypt them send e-mail to this address: johnlo@techmail.info.

If we don't answer in 24h., send e-mail to this address: johnlo@keemail.me

Además del fichero de texto anterior, el código dañino también escribe en disco y lanza un fichero HTA (HTML Application) con instrucciones extendidas. En este nuevo artefacto, **info.hta**, se indica el identificador de usuario afectado y se adelanta que el rescate se cobra en Bitcoin. El diseño de las instrucciones en la aplicación HTA recuerda al usado por el ransomware Dharma.

Figura 7. Nota de rescate en formato HTA

11. DESINFECCIÓN

Para evitar desencadenar siguientes ejecuciones del código dañino, es conveniente eliminar el ejecutable de las rutas donde se instala para asegurar la persistencia.

Para las claves de registro **CurrentVersion/Run**, la localización del ejecutable es la misma tanto para **HKLM** como para **HKCU** (ver figura 4).

```
C:\Users\[User]\AppData\Local\
```

La localización de las muestras a eliminar cuando ésta se copia en las carpetas **StartUp**, se podrá encontrar en hasta dos directorios distintos, dependiendo de los privilegios otorgados al proceso de infección.

```
C:\Users\[User]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\
```

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

12. REGLA DE DETECCIÓN YARA

```
rule EKING_phobos
{
   meta:
      author = "CCN-CERT"
      date = "2021-10-19"
      description = "Detects EKING/Phobos ransomware"

   strings:
      $decoding_routine = { 33 D0             // xor     edx, eax
                            81 E2 FF 00 00 00    // and     edx, 0FFh
                            C1 E8 08           // shr     eax, 8
                            33 04 95 ?? ?? ?? ?? // xor     eax, dword_A3B000[edx*4]
                            41                 // inc     ecx
                          }
      $elevation_level = "ELVL" wide
      $unc = "\\\\?\\UNC\\\\\\e-" wide

   condition:
      (uint16(0) == 0x5A4D and
      all of them)
}
```

13. INDICADORES DE COMPROMISO

Ransomware EKING – SHA256
bb1e8e2dcc7b03cad837602c067a2d688ef1675b8552613f584d345917aaa52a

ota de rescate
info.hta
info.txt

ANEXO A - EXTENSIONES PRIORITARIAS PARA EL CIFRADO

Extensiones prioritarias para el cifrado			
4dd	4dl	abs	abx
accdb	accdc	accde	adb
adf	ckp	db	db-journal
db-shm	db-wal	db2	Db3
dbc	dbf	dbs	dbt
dbv	dcb	dp1	eco
edb	epim	fcd	fdb
gdb	ldf	mdb	mdf
myd	ndf	nwdb	nyf
sql	sqlite	sqlite3	sqlitedb

ANEXO B - EXTENSIONES DE VARIANTES ANTERIORES

Extensiones de variantes anteriores			
actin	Acton	actor	Acuff
Acuna	acute	adage	Adair
Adame	banhu	banjo	Banks
Banta	Barak	bbc	blend
bqux	Caleb	Cales	Caley
calix	Calle	Calum	Calvo
CAPITAL	com	DDoS	deuce
Dever	devil	Devoe	Devon
Devos	dewar	eight	eject
eking	Elbie	elbow	elder
help	KARLOS	karma	mamba
phobos	phoenix	PLUT	WALLET