Informe Código Dañino
CCN-CERT ID-12/22

Quantum ransomware

Diciembre 2022

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.12.14 10:29:50 +01'00'

Fecha de Edición: diciembre de 2022

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) del 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 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

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 ciber amenazas, 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. INFORMACIÓN DEL CÓDIGO DAÑINO

El presente documento recoge el análisis de una muestra de ransomware que pertenece a la familia Quantum.

Muestra	Hash SHA-1
Quantum	8D31D3E523D1E11631D05F01C410340CEF780BFC

"Quantum" es un código dañino del tipo ransomware. Este tipo de código dañino tiene las capacidades de cifrar los ficheros del sistema infectado, también conocido como Quantum Locker. Se observó su primera actividad en agosto de 2021 y funcionó como la versión 5.1 del ransomware MountLocker. Este ransomware aprovecha la táctica de doble extorsión al amenazar con publicar los datos extraídos de las víctimas si no se paga el rescate. Sus principales víctimas están ubicadas en Australia, Canadá, la Unión Europea (UE), el Reino Unido y los EE. UU., de las cuales obtuvo ingresos anuales superiores a los 100 millones de dólares. El 75 % de las víctimas de Quantum fueron medios de telecomunicaciones, entidades del sector público, industria, consumo y tecnología.

3. CARACTERÍSTICAS DEL CÓDIGO DAÑINO

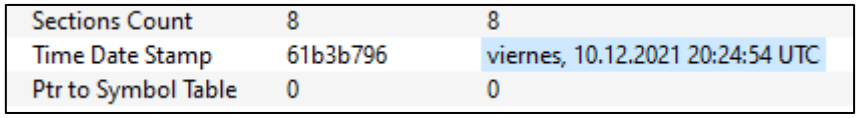
El código dañino examinado posee las siguientes características:

- Solo es compatible con sistemas Windows de 64 bits.
- Se puede propagar por la red interna.
- Utiliza técnicas para dificultar el análisis estático.
- Cifra ficheros utilizando algoritmos de cifrado simétrico y asimétrico.
- Crea un mensaje de rescate en el escritorio del usuario.
- No requiere de conexión a internet.
- Crea persistencia en el sistema.

4. DETALLES GENERALES

La muestra analizada es un fichero Portable Executable (PE) que se corresponde con un archivo de código ejecutable para sistemas operativos Windows. En este caso el código que contiene el fichero es de 64 bits, lo cual lo hace únicamente válido para sistemas Windows de 64 bits.

Tal y como se observa en la cabecera del fichero PE analizado, la fecha de compilación se corresponde con diciembre del año 2021.



Sections Count	8	8
Time Date Stamp	61b3b796	viernes, 10.12.2021 20:24:54 UTC
Ptr to Symbol Table	0	0

Figura 1. Información del código dañino Quantum.

Se debe tener en cuenta que esta cabecera puede ser manipulada por los autores del código dañino con la intención de dejar menos rastros y confundir a los investigadores.

5. CARACTERÍSTICAS TÉCNICAS

5.1 FUNCIONAMIENTO GENERAL

El código dañino acepta distintos argumentos por línea de comandos los cuales modifican ligeramente su comportamiento, permitiendo ajustar algunas variables al criterio del operador.

Alguno de estos argumentos no requiere de ningún valor adicional, como el argumento "/NOKILL", mientras que otros como el "/MAX=", requieren que se les especifique un valor, que en el caso de "/MAX=" es un número entero el cual indica el tamaño máximo de fichero a cifrar.

Si no se proporciona ningún argumento Quantum utiliza los valores por defecto que tiene.

A continuación, se listan los argumentos que acepta el código dañino.

Argumento	Requiere de valor adicional	Descripción
/LOGIN=	Sí	Nombre del usuario del servidor en el que se encuentran los recursos compartidos.
/PASSWORD=	Sí	Contraseña del servidor en el que se encuentran los recursos compartidos.
/CONSOLE	No	Imprimir resultado por la consola.
/NODEL	No	No borrar el ejecutable después del cifrado.
/NOKILL	No	No terminar algunos procesos y servicios determinados en la maquina infectada.
/NOLOG	No	No escribir un log con los resultados de la operación de cifrado.
/SHAREALL	No	Indica si se quiere intentar cifrar todos los recursos compartidos de un servidor.
/NETWORK=	Opcional	Si se especifica este campo, el ransomware intenta replicarse en la red. Acepta el parámetro "s" el cual intenta crear un servicio en la máquina remota, y el parámetro "w", el cual ejecuta el ransomware mediante WMI.

/TARGET=	Sí	Permite especificar una carpeta en concreto para ser cifrada, tanto local como un recurso compartido.
/FAST=	Sí	Indica el número de bytes a cifrar. Por defecto, este valor es el tamaño del fichero original a cifrar, en caso de que este sea menor a un 1MB. Sin embargo, con este campo se puede especificar un número más bajo de bytes a cifrar.
/MIN=	Sí	Tamaño mínimo que puede tener el fichero a cifrar. Si no se especifica el valor es que viene por defecto.
/MAX=	Sí	Tamaño máximo que puede tener el fichero a cifrar. Si no se especifica el valor es que viene por defecto.
/FULLPD	No	Saltarse los directorios "Program Files", "Program Files (x86)" y "ProgramData".
/MARKER=	Sí	Crea un fichero en el directorio root del disco cifrado, el cual indica que ya ha sido cifrado. El nombre de este fichero es el que se le pasa como argumento.
/NOLOCK=	Sí	Este argumento acepta uno o más de los siguientes valores "L", "N" y/o "S". Con este campo se indica el alcance de los ficheros a cifrar, por defecto intenta cifrar los ficheros locales (L), los de los recursos compartidos (S) así como las unidades de disco de red (N)

En la siguiente imagen se puede ver a grandes rasgos el flujo de ejecución del ransomware.

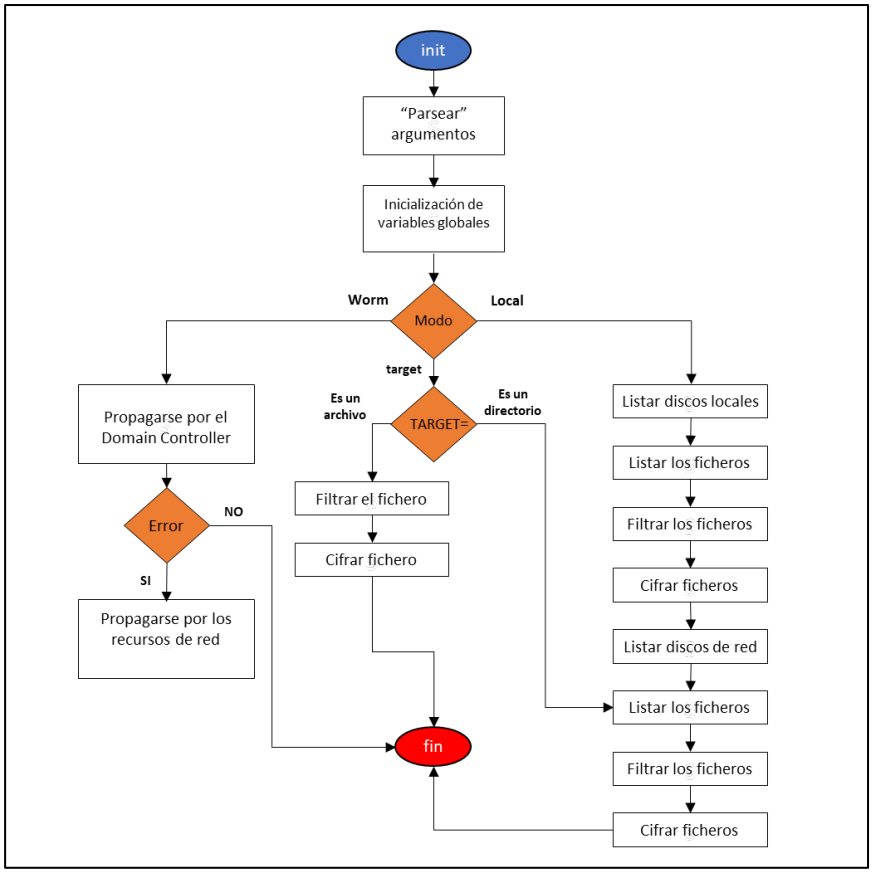


Figura 2. Flujo de ejecución

En la imagen anterior no se tienen en cuenta cada uno de los argumentos que acepta el programa con la idea de simplificar la imagen.

Todos los parámetros de la tabla anterior son ajustables a la hora de ejecutar el ransomware. Cabe destacar que tiene un componente de *worm* para poder expandirse por el dominio o servidores que estén en la misma red, para los que se puede especificar un nombre de usuario (/LOGIN=) y una contraseña (/PASSWORD=) para identificarse.

El código dañino comienza leyendo los argumentos que se le pasan por línea de comando ya que, como se ha explicado anteriormente, este tiene muchos parámetros que son ajustables desde la línea de comandos.

Quantum tiene tres modos distintos de ejecución: el modo por defecto, el modo target y el modo *worm*.

Modo por defecto. Este modo se llama internamente "default_lock" y su objetivo principal es cifrar las unidades de disco locales, así como las unidades de red.

```
__int64 default_lock_mode()
{
  log(3u, (int *)&unk_13F3AF620);
  if ( !ARG_NOLOCK_L )
    locker_work_start_local();
  if ( !ARG_NOLOCK_N || !ARG_NOLOCK_S )
    locker_work_start_network();
  return wait_for_threads();
}
```

Figura 3. Modo "default_lock".

Modo target. En este modo el código dañino se limita a cifrar únicamente la carpeta o el fichero que se le pasa por la línea de comandos en el argumento "/TARGET=". Este argumento no se limita solo a ficheros locales sino que también puede aplicarse a recursos compartidos, aunque estos requieran de autenticación. El código dañino puede obtener los parámetros para la autenticación en los argumentos "/LOGIN=" y "/PASSWORD=" en caso de ser indicados.

```
__int64 target_lock_mode()
{
  log(3u, (int *)&unk_13F3B14D0);
  locker_work_start_target();
  return wait_for_threads();
}
```

Figura 4. Modo "target_lock".

Modo worm. Si el código dañino es ejecutado en este modo, este intenta propagarse por la red haciendo copias de sí mismo en servidores y recursos compartidos de la red local y ejecutándolos, o bien por comandos WMI o creando un servicio en estas máquinas. Al igual que en el modo target, también se le pueden especificar los argumentos "/LOGIN=" y "/PASSWORD=" en caso de necesitar autenticación para acceder a estos servidores y/o recursos compartidos.

```
__int64 worm_mode()
{
  __int64 v0; // rax
  void *v1; // rbx
  DWORD v2; // eax
  __int64 result; // rax
  unsigned int v4; // edi

  v0 = sub_13F3A425C(8i64);
  v1 = (void *)v0;
  if ( v0 )
  {
    v4 = enum_pc_into_domain(v0);
    if ( !v4 )
      v4 = net_resources((__int64)v1);
    close_handles(v1);
    result = v4;
  }
  else
  {
    v2 = GetLastError();
    log((_DWORD)v1 + 3, (int *)&unk_13F3ADEA0, v2);
    result = 0i64;
  }
  return result;
}
```

Figura 5. Modo “worm”.

5.1.1 PROCESADO DE LOS FICHEROS.

Para el cifrado de los ficheros Quantum hace un filtrado de los mismos, para ello utiliza dos listas: una lista de directorios y una lista de extensiones de fichero.

Mientras recorre de forma recursiva todos los directorios, si se encuentra alguna carpeta que está en su lista de directorios, esta carpeta es ignorada. Al igual pasa con la lista de ficheros, antes de que estos sean cifrados se comprueba la extensión del fichero. Si la extensión está en la lista de extensiones del código dañino este fichero no es cifrado.

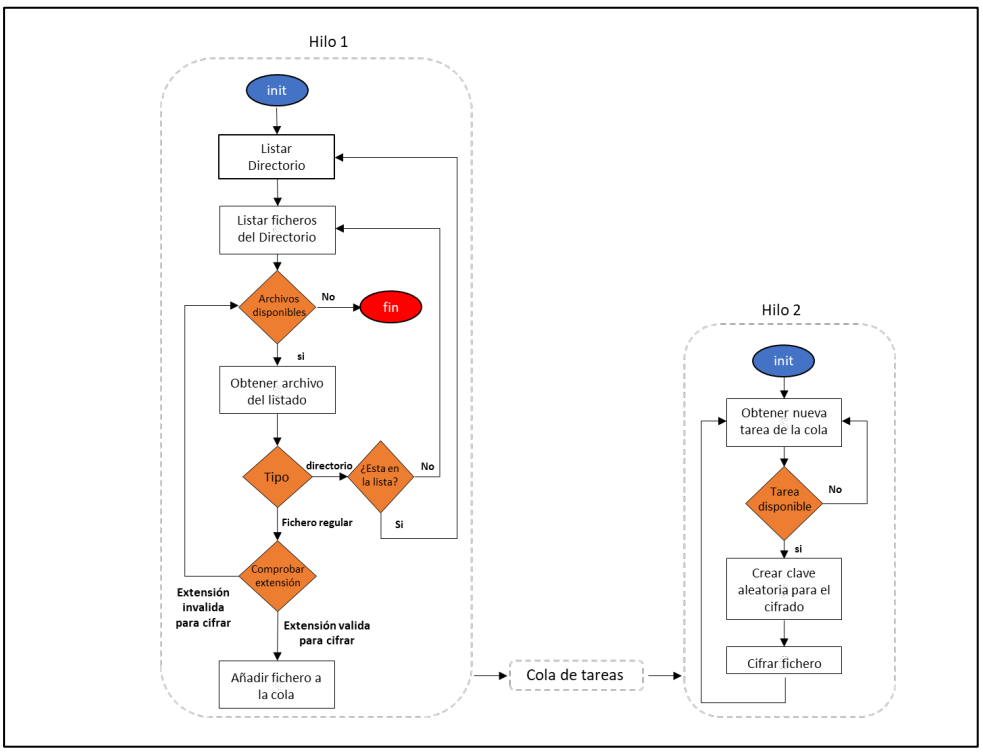


Figura 6. Flujo de filtrado y cifrado de los ficheros usando un sistema de colas.

Tanto la lista de directorios como la lista de extensiones se puede consultar en el ANEXO.

Para agilizar el proceso de cifrado, el código dañino crea dos hilos, uno de los hilos se encarga de recorrer los directorios y el otro del cifrado de los ficheros.

El primer hilo hace el filtrado que se ha explicado previamente. Cuando un fichero pasa todos los filtros el nombre del fichero es guardado en una cola que comparten ambos hilos.

Por otro lado, el segundo hilo, queda a la espera de que haya nuevas tareas en la cola que ambos hilos comparten. En cuanto hay un fichero nuevo en la cola empieza el proceso de cifrado usando los algoritmos que se explican en los siguientes apartados.

5.2 PERSISTENCIA

Una vez los ficheros son cifrados el ejecutable de quantum es borrado del sistema, por lo que no existe forma de que el propio ransomware se vuelva a ejecutar. Sin embargo, el código dañino crea una clave de registro para que cada vez que se intente abrir un fichero que ha sido cifrado se muestre el mensaje de rescate.

La clave de registro que crea es la siguiente, "HKLM\SOFTWARE\Classes\.quantum\shell\open\command". Esta clave de registro hace que cada vez que se ejecute un fichero con la extensión ".quantum" en el sistema, se muestre automáticamente el mensaje de rescate.

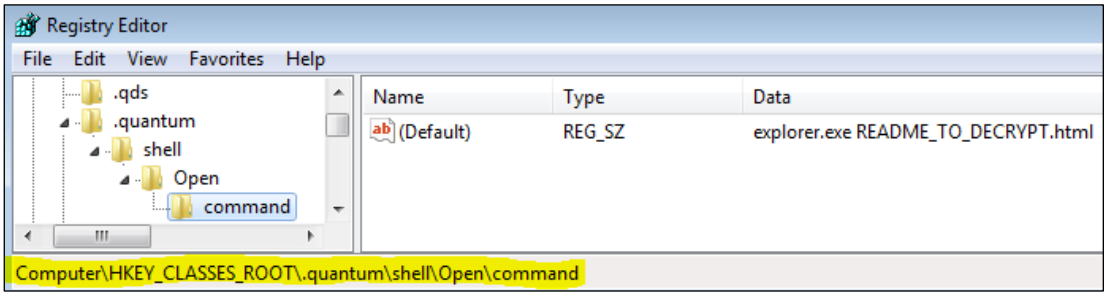


Figura 7. Clave de registro creada para mostrar el mensaje de rescate al iniciar el sistema.

Por otro lado, cuando Quantum es ejecutado en modo *worm*, podría crear un servicio en la maquina remota, tal y como se ve en la siguiente imagen.

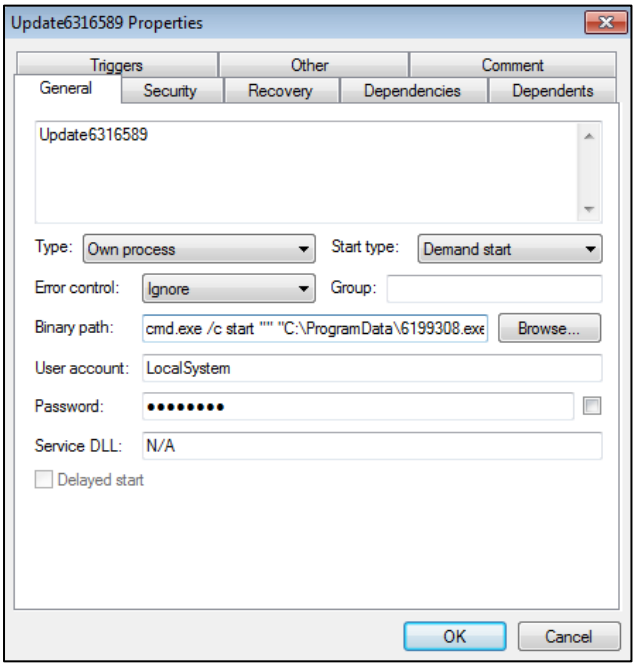


Figura 8. Servicio creado que ejecuta una copia del ransomware.

5.3 TÉCNICAS ANTIANÁLISIS

5.3.1 CIFRADO DE CADENAS

El código dañino mantiene cifradas las distintas cadenas que utiliza, como el mensaje de rescate, los argumentos que acepta y la lista de extensiones de ficheros a cifrar. Las cadenas se descifran en tiempo de ejecución.

En este caso el algoritmo de cifrado de las cadenas utiliza un simple XOR como se ve en la siguiente imagen.

```
1  char *__fastcall decrypt_string(EncData *enc_data, __int64 a2)
2  {
3    unsigned __int16 i; // [rsp+20h] [rbp-18h]
4    unsigned __int16 size; // [rsp+24h] [rbp-14h]
5    int v5; // [rsp+28h] [rbp-10h]
6    char *v6; // [rsp+40h] [rbp+8h]
7    char *dec_data; // [rsp+48h] [rbp+10h]
8
9    dec_data = (char *)a2;
10   v5 = enc_data->Key;
11   size = enc_data->EncStringSize ^ LOWORD(enc_data->Key);
12   v6 = &enc_data->EncString;
13   for ( i = 0; i < (signed int)size; ++i )
14   {
15     v5 = sub_13FA463C4(v5);
16     dec_data[i] = v5 ^ v6[i];
17   }
18   return dec_data;
19 }
```

Figura 9. Función utilizada para descifrar cadenas.

5.4 ESQUEMA DE CIFRADO

En este apartado se documenta el esquema de cifrado que utiliza el código dañino para cifrar los ficheros.

5.4.1 CIFRADO DE FICHEROS

Para el cifrado de los ficheros utiliza una combinación de cifrado asimétrico y cifrado simétrico, concretamente usa RSA para el cifrado asimétrico y el ChaCha20 para el cifrado simétrico.

Para cada fichero genera una clave aleatoria de 32 bytes. Esta clave es utilizada para cifrar el contenido del fichero.

La clave aleatoria generada es cifrada con una clave pública usando el algoritmo RSA. Esta clave pública esta embebida en el mismo código dañino. De esta forma solo quien tenga la clave privada podrá descifrar la clave simétrica y finalmente descifrar el contenido del fichero.

```
do
{
  random((__int64)&RANDOM_KEY_PLAINTEXT);
  Sleep(1u);
  --v3;
}
while ( v3 );
v5 = 32i64;
do
{
  v4[2].m128i_i8[0] = v4->m128i_i64[0];
  v4 = (__m128i *)((char *)v4 + 1);
  --v5;
}
while ( v5 );
rand();
if ( !encrypt_random_key_with_rsa_key((__int64)&RSA_KEY, (BYTE *)&RANDOM_KEY_ENCRYPTED) )
{
  v0 = GetLastError();
  v1 = (int *)&unk_13FA4E980;
  goto LABEL_3;
}
```

Figura 10. Función utilizada para cifrar la clave generada usando RSA.

Una vez los datos son cifrados, la clave simétrica que ha sido cifrada con la clave pública se escribe al final del fichero.

```
if ( v7 )
{
  random((__int64)GlobalStructure->RandomKey);
  v7 = write_key_at_the_end_of_file(GlobalStructure, a3, a4);
  if ( v7 )
  {
    v7 = encrypt_file_content((__int64)FileName, GlobalStructure, a3, a4);
    if ( v7 )
    {
      get_query_performance_counter(performance_counter);
```

```
  }
  while ( v5 );
  chacha((const __m128i *)v4->RandomKey, &buffer1_, 0x20ui64, &RANDOM_KEY_PLAINTEXT, a2, a3, &RANDOM_KEY_PLAINTEXT);
  return SetFilePointerEx(v4->hFile, 0i64, 0i64, 2u)
      && WriteFile(v4->hFile, &Buffer, 0x139u, &NumberOfBytesWritten, 0i64)
      && NumberOfBytesWritten == 0x139;
}
```

Figura 11. Función que escribe la clave cifrada al final del fichero.

5.5 MENSAJE DE RESCATE

En cada directorio el código dañino crea un mensaje de rescate. Concretamente, el mensaje de rescate está en formato HTML y su nombre es "README_TO_DECRYPT.html".

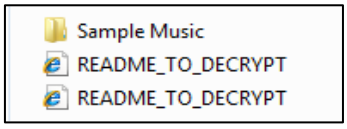
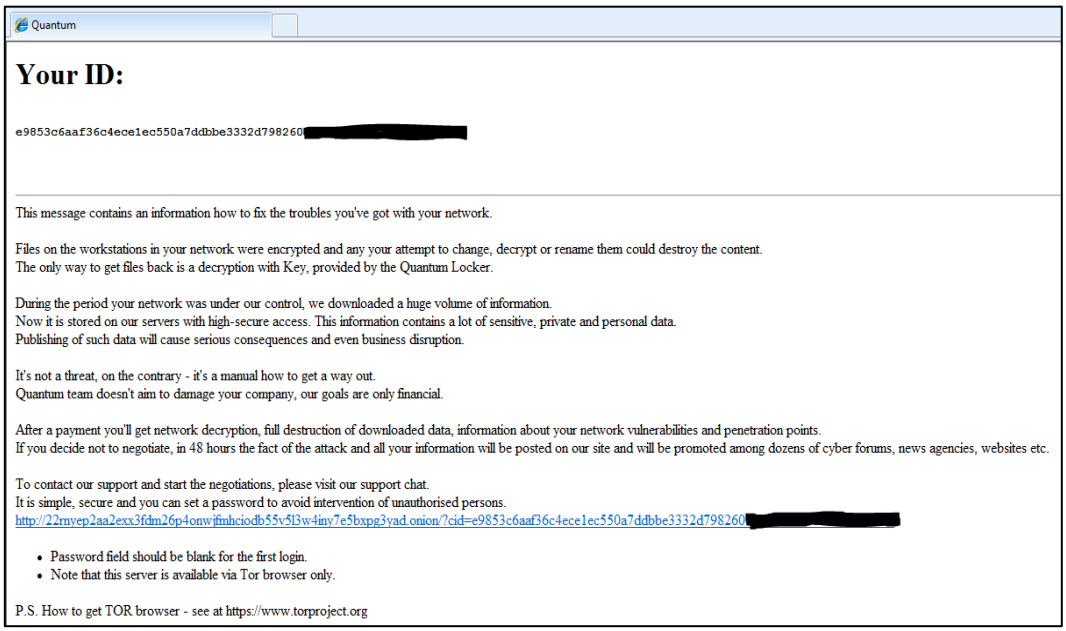


Figura 12. Mensaje de rescate creado por el código dañino.

En la siguiente imagen se puede ver el contenido del mismo mensaje. Este contenido se encuentra en el ANEXO del documento en formato de texto.


Quantum

Your ID:

e9853c6aaf36c4ece1ec550a7ddbbe3332d798260[redacted]

This message contains an information how to fix the troubles you've got with your network.

Files on the workstations in your network were encrypted and any your attempt to change, decrypt or rename them could destroy the content.
The only way to get files back is a decryption with Key, provided by the Quantum Locker.

During the period your network was under our control, we downloaded a huge volume of information.
Now it is stored on our servers with high-secure access. This information contains a lot of sensitive, private and personal data.
Publishing of such data will cause serious consequences and even business disruption.

It's not a threat, on the contrary - it's a manual how to get a way out.
Quantum team doesn't aim to damage your company, our goals are only financial.

After a payment you'll get network decryption, full destruction of downloaded data, information about your network vulnerabilities and penetration points.
If you decide not to negotiate, in 48 hours the fact of the attack and all your information will be posted on our site and will be promoted among dozens of cyber forums, news agencies, websites etc.

To contact our support and start the negotiations, please visit our support chat.
It is simple, secure and you can set a password to avoid intervention of unauthorised persons.
http://22rnyep2aa2exx3fdm26p4onwjfmhciodb55v5l3w4iny7e5bxpg3yad.onion/?cid=e9853c6aaf36c4ece1ec550a7ddbbe3332d798260[redacted]

- Password field should be blank for the first login.
- Note that this server is available via Tor browser only.

P.S. How to get TOR browser - see at https://www.torproject.org

Figura 13. Contenido del mensaje de rescate.

6. INDICADORES DE COMPROMISO

Quantum		
Tipo	**Descripción**	**Valor**
Sistema de ficheros	Extensión de los ficheros cifrados	".quantum"
Sistema de ficheros	Mensaje de rescate	README_TO_DECRYPT.html
Sistema de ficheros	Copia del código dañino cuando se propaga por la red	%PROGRAMDATA%\[0-9]{7}.exe
Servicio	Servicio que se crea en la máquina cuando el código dañino intenta propagarse en la red	**Nombre del servicio:** Update[0-9]{7} **Línea de comando a ejecutar por el servicio:** cmd.exe /c start "C:\ProgramData\[0-9]{7}.exe"
Clave de registro	Clave de registro creada para la persistencia	**Clave:** HKLM\SOFTWARE\Classes\.quantum\shell\open\command **Valor de Registro:** (Defecto) **Valor:** explorer.exe README_TO_DECRYPT.html

7. DESINFECCIÓN

Para los ficheros cifrados por el ransomware solo los operadores del ransomware son capaces de descifrar los ficheros.

Para evitar desencadenar subsecuentes ejecuciones del código dañino es conveniente revisar los posibles mecanismos que pueden relanzar la muestra.

En este caso, basta con borrar la clave de registro ya que el ransomware se borra a sí mismo una vez termina el cifrado de los ficheros. Así mismo, en caso de que existan mecanismo de persistencia, es necesario borrar tanto el servicio como el ejecutable al que apunta el servicio tal y como se indica en la tabla de los Indicadores de Compromiso.

8. MITIGACIÓN

Una buena estrategia para contener y reducir el impacto del ransomware es trabajar de forma paralela en el aislado de redes/VLAN que conforman la entidad afectada con el objetivo de contener los segmentos de red con equipos infectados y evitar su expansión.

Téngase en cuenta que estas medidas posiblemente interfieran con el correcto funcionamiento del dominio o redes afectadas y puedan causar diversos imprevistos como el reinicio de máquinas; no obstante, permitiría contener la amenaza de una manera resolutiva.

9. REGLAS DE DETECCIÓN

9.1 REGLAS YARA

```
rule Quantum_ransomware
{
        meta:
                author      = “Centro Criptológico Nacional (CCN)”
                date        = “2/12/2022”
                description = “Ransomware Quantum”
        strings:
                $s1 = { 81 F1 FE 93 00 00 8D 81 ?? ?? 00 00 D1 C0 2D A5 5A 00 00 D1 C8 F7 D0 2D 79 C7 01 00 C3 }
                $s2 = { 8B 4C ?? ?? E8 ?? ?? ?? ?? 89 44 ?? ?? 0F B7 ?? ?? ?? 48 8B ?? ?? ?? 0F B6 04 01 0F B6 ?? ?? ?? 33 C1
0F B7 ?? ?? ?? 48 8B ?? ?? ?? }

        condition:
                uint16(0) == 0x5A4D and
                uint32(uint32(0x3C)) == 0x00004550 and
        all of them
}
```

ANEXO

LISTA DE EXTENSIONES EXCLUIDAS DE SER CIFRADAS

exe	.icl
dll	.icns
sys	.ico
msi	.ics
mui	.idx
inf	.ldf
cat	.mod
bat	.mpa
cmd	.mp4
ps1	.mp3
vbs	.msc
ttf	.msp
fon	.msstyles
lnk	.msu
.386	.nls
.adv	.nomedia
.ani	.ocx
.bin	.prf
.cab	.rom
.com	.rtp
.cpl	.scr
.cur	.shs
.deskthemepack	.spl
.diagcab	.theme
.diagcfg	.themepack
.diagpkg	.wpx
.drv	.lock
.hlp	.key
	.hta

LISTA DE CARPETAS Y FICHEROS EXCLUIDOS DE SER CIFRADAS

:\Windows\	$\$WINDOWS.~BT\	\MicrosoftEdge\
:\System Volume Information\	$\Windows.old\	\Tor Browser\
:\$RECYCLE.BIN\	$\PerfLog\	\AppData\Local\Temp\
:\SYSTEM.SAV	$\PerfLogs\	\AppData
:\WINNT	$\Program Files\	\All Users
:\$WINDOWS.~BT\	$\Program Files (x86)\	\Boot
:\Windows.old\	$\Boot	\Google
:\PerfLog\	$\ProgramData\Microsoft\	\Mozilla
:\PerfLogs\	$\ProgramData\Packages\	\autorun.inf
:\Program Files\	$\EFI	\boot.ini
:\Program Files (x86)\	$\ProgramData	\bootfont.bin
:\Boot	\WindowsApps\	\bootsect.bak
:\ProgramData\Microsoft\	\Microsoft\Windows\	\bootmgr
:\ProgramData\Packages\	\Local\Packages\	\bootmgr.efi
:\EFI	\Windows Defender	\bootmgfw.efi
:\ProgramData	\microsoft shared\	\iconcache.db
$\Windows\	\Google\Chrome\	\desktop.ini
$\System Volume Information\	\Mozilla Firefox\	\ntldr
$\$RECYCLE.BIN\	\Mozilla\Firefox\	\ntuser.dat
$\SYSTEM.SAV	\Internet Explorer\	\ntuser.dat.log
	$\WINNT	\ntuser.ini
		\thumbs.db

MENSAJE DE RESCATE

```
<html>
	<head>
		<title>Quantum</title>
	</head>
	<body>
		<h1>Your ID:</h1>
		<b>
			<pre>

%CLIENT_ID%

			</pre>
		</b>
		<hr/>
This message contains an information how to fix the troubles you've got with your network.<br><br>

Files on the workstations in your network were encrypted and any your attempt to change, decrypt or rename them could destroy the content.<br>

The only way to get files back is a decryption with Key, provided by the Quantum Locker.<br><br>

During the period your network was under our control, we downloaded a huge volume of information.<br>

Now it is stored on our servers with high-secure access. This information contains a lot of sensitive, private and personal data.<br>

Publishing of such data will cause serious consequences and even business disruption.<br><br>

It's not a threat, on the contrary - it's a manual how to get a way out.<br>

Quantum team doesn't aim to damage your company, our goals are only financial.<br><br>

After a payment you'll get network decryption, full destruction of downloaded data, information about your network vulnerabilities and penetration points.<br>

If you decide not to negotiate, in 48 hours the fact of the attack and all your information will be posted on our site and will be promoted among dozens of cyber forums, news agencies, websites etc.<br><br>

To contact our support and start the negotiations, please visit our support chat.<br>

It is simple, secure and you can set a password to avoid intervention of unauthorised persons.<br>

<a href="http://22rnyep2aa2exx3fdm26p4onwjfmhciodb55v5l3w4iny7e5bxpg3yad.onion/?cid=%CLIENT_ID%
">http://22rnyep2aa2exx3fdm26p4onwjfmhciodb55v5l3w4iny7e5bxpg3yad.onion/?cid=%CLIENT_ID% </a>

<ul>
```

```
		<li>Password field should be blank for the first login.
		<li>Note that this server is available via Tor browser only.
</ul>

P.S. How to get TOR browser - see at https://www.torproject.org
		</body>
</html>
```

EJEMPLO DE FICHERO LOG

```
Ver 5.1 x64
========== SYS INFO ==========
CORE COUNT: 5
TOTAL MEM:  2047 MB
WIN VER:  6.1.7601 SP1
WIN ARCH: x64
USER NAME:  ccn-lab
PC NAME:  WIN-CCN-LAB
IN DOMAIN:  NO
IS ADMIN: YES
IN GROUPS:
  Mandatory WIN-CCN-LAB\None
  Mandatory \Everyone
  Mandatory BUILTIN\Administrators
  Mandatory BUILTIN\Users
  Mandatory NT AUTHORITY\INTERACTIVE
  Mandatory \CONSOLE LOGON
  Mandatory NT AUTHORITY\Authenticated Users
  Mandatory NT AUTHORITY\This Organization
  Mandatory \LOCAL
  Mandatory NT AUTHORITY\NTLM Authentication
  Integrity Mandatory Label\High Mandatory Level
CMDLINE:  quantum.exe  /CONSOLE

================================
       KILL SERVICE
================================

================================
       KILL PROCESS
================================
==========  DEFAULT LOCK ==========
[INFO] locker.work.start.local >
[INFO] locker.work.enum.local > name=\\?\c:\
[INFO] locker.work.start.network >
[INFO] locker.work.thread.local > path=\\?\c:\
[SKIP] locker.dir.check > black  list name=\\?\c:\$Recycle.Bin\
[SKIP] locker.dir.check > black  list name=\\?\c:\Boot\
[SKIP] locker.dir.check > target  visibled target=\??\C:\Users name=\\?\c:\Documents and Settings\
[SKIP] locker.dir.check > black  list name=\\?\c:\PerfLogs\
[SKIP] locker.dir.check > black  list name=\\?\c:\Program Files\
[SKIP] locker.dir.check > black  list name=\\?\c:\Program Files (x86)\
[SKIP] locker.dir.check > black  list name=\\?\c:\ProgramData\
[OK] locker.dir.check > name=\\?\c:\Recovery\
[INFO] locker.work.thread.network >
[INFO] locker.queue.worker > empty group=SLOW
[INFO] locker.queue.worker > empty group=FAST
[INFO] locker.queue.worker > empty group=SLOW
[OK] locker.dir.check > name=\\?\c:\Recovery\b5f5e224-2c00-11e8-a03e-9a65dd5e24a1\
[SKIP] locker.dir.check > black  list name=\\?\c:\System Volume Information\
[OK] locker.dir.check > name=\\?\c:\Users\
[SKIP] locker.dir.check > black  list name=\\?\c:\Users\All Users\
[OK] locker.dir.check > name=\\?\c:\Users\Default\
[SKIP] locker.dir.check > black  list name=\\?\c:\Users\Default\AppData\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default\AppData\Roaming name=\\?\c:\Users\Default\Application
Data\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default\AppData\Roaming\Microsoft\Windows\Cookies
name=\\?\c:\Users\Default\Cookies\
[OK] locker.dir.check > name=\\?\c:\Users\Default\Desktop\
[OK] locker.dir.check > name=\\?\c:\Users\Default\Documents\
[SKIP] locker.dir.check > target  visibled target=\??\C:\Users\Default\Music name=\\?\c:\Users\Default\Documents\My Music\
[SKIP] locker.dir.check > target  visibled target=\??\C:\Users\Default\Pictures name=\\?\c:\Users\Default\Documents\My Pictures\
[SKIP] locker.dir.check > target  visibled target=\??\C:\Users\Default\Videos name=\\?\c:\Users\Default\Documents\My Videos\
[OK] locker.dir.check > name=\\?\c:\Users\Default\Downloads\
[OK] locker.dir.check > name=\\?\c:\Users\Default\Favorites\
```

```
[OK] locker.dir.check > name=\\?\c:\Users\Default\Links\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default\AppData\Local name=\\?\c:\Users\Default\Local Settings\
[OK] locker.dir.check > name=\\?\c:\Users\Default\Music\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default\Documents name=\\?\c:\Users\Default\My Documents\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default\AppData\Roaming\Microsoft\Windows\Network Shortcuts name=\\?\c:\Users\Default\NetHood\
[OK] locker.dir.check > name=\\?\c:\Users\Default\Pictures\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default\AppData\Roaming\Microsoft\Windows\Printer Shortcuts name=\\?\c:\Users\Default\PrintHood\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default\AppData\Roaming\Microsoft\Windows\Recent name=\\?\c:\Users\Default\Recent\
[OK] locker.dir.check > name=\\?\c:\Users\Default\Saved Games\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default\AppData\Roaming\Microsoft\Windows\SendTo name=\\?\c:\Users\Default\SendTo\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu name=\\?\c:\Users\Default\Start Menu\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default\AppData\Roaming\Microsoft\Windows\Templates name=\\?\c:\Users\Default\Templates\
[OK] locker.dir.check > name=\\?\c:\Users\Default\Videos\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Default name=\\?\c:\Users\Default User\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\
[SKIP] locker.dir.check > black list name=\\?\c:\Users\ccn-lab\AppData\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\AppData\Roaming name=\\?\c:\Users\ccn-lab\Application Data\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Contacts\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\AppData\Roaming\Microsoft\Windows\Cookies name=\\?\c:\Users\ccn-lab\Cookies\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Desktop\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Desktop\HxD\
[OK] locker.file > time=0.087 size=0.008 MB speed=0.090 MB/s name=\\?\c:\BOOTSECT.BAK
[OK] locker.file > time=0.146 size=3.023 MB speed=20.655 MB/s name=\\?\c:\Recovery\b5f5e224-2c00-11e8-a03e-9a65dd5e24a1\boot.sdi
[OK] locker.file > time=0.113 size=0.250 MB speed=2.209 MB/s name=\\?\c:\Users\Default\NTUSER.DAT
[OK] locker.file > time=0.001 size=0.001 MB speed=1.833 MB/s name=\\?\c:\Users\Default\NTUSER.DAT.LOG
[OK] locker.file > time=0.029 size=0.181 MB speed=6.328 MB/s name=\\?\c:\Users\Default\NTUSER.DAT.LOG1
[OK] locker.file > time=0.001 size=0.063 MB speed=99.554 MB/s name=\\?\c:\Users\Default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
[OK] locker.file > time=0.298 size=0.500 MB speed=1.681 MB/s name=\\?\c:\Users\Default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
[OK] locker.file > time=0.033 size=0.500 MB speed=15.348 MB/s name=\\?\c:\Users\Default\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
[OK] locker.file > time=0.000 size=0.170 KB speed=0.482 MB/s name=\\?\c:\Users\desktop.ini
[OK] locker.file > time=0.029 size=0.402 KB speed=0.014 MB/s name=\\?\c:\Users\ccn-lab\Contacts\desktop.ini
[OK] locker.file > time=0.100 size=0.065 MB speed=0.649 MB/s name=\\?\c:\Users\ccn-lab\Contacts\ccn-lab.contact
[OK] locker.file > time=0.000 size=0.275 KB speed=0.973 MB/s name=\\?\c:\Users\ccn-lab\Desktop\desktop.ini
[INFO] locker.queue.worker > empty group=FAST
[INFO] locker.queue.worker > empty group=FAST
[OK] locker.file > time=2.593 size=161.375 MB speed=62.235 MB/s name=\\?\c:\Recovery\b5f5e224-2c00-11e8-a03e-9a65dd5e24a1\Winre.wim
[INFO] locker.queue.worker > empty group=SLOW
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Desktop\target\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Desktop\target\x64\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Desktop\target\x86\
[OK] locker.file > time=0.352 size=0.145 KB speed=0.000 MB/s name=\\?\c:\Users\ccn-lab\Desktop\target\kdpatch.reg
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Documents\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\Music name=\\?\c:\Users\ccn-lab\Documents\My Music\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\Pictures name=\\?\c:\Users\ccn-lab\Documents\My Pictures\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\Videos name=\\?\c:\Users\ccn-lab\Documents\My Videos\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Downloads\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Favorites\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Favorites\Links\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Favorites\Links for United States\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Favorites\Microsoft Websites\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Favorites\MSN Websites\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Favorites\Windows Live\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Links\
[OK] locker.file > time=1.074 size=0.651 MB speed=0.606 MB/s name=\\?\c:\Users\ccn-lab\Desktop\target\x64\kdbazis.pdb
[SKIP] locker.dir.check > target_visibled target=\??\C:\Users\ccn-lab\AppData\Local name=\\?\c:\Users\ccn-lab\Local Settings\
```

[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Music\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\Documents name=\\?\c:\Users\ccn-lab\My Documents\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\AppData\Roaming\Microsoft\Windows\Network Shortcuts name=\\?\c:\Users\ccn-lab\NetHood\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Pictures\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\AppData\Roaming\Microsoft\Windows\Printer Shortcuts name=\\?\c:\Users\ccn-lab\PrintHood\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\AppData\Roaming\Microsoft\Windows\Recent name=\\?\c:\Users\ccn-lab\Recent\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Saved Games\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Searches\
[OK] locker.file > time=1.116 size=1.159 MB speed=1.039 MB/s name=\\?\c:\Users\ccn-lab\Desktop\target\x64\kdpatch.pdb
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\AppData\Roaming\Microsoft\Windows\SendTo name=\\?\c:\Users\ccn-lab\SendTo\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\AppData\Roaming\Microsoft\Windows\Start Menu name=\\?\c:\Users\ccn-lab\Start Menu\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\ccn-lab\AppData\Roaming\Microsoft\Windows\Templates name=\\?\c:\Users\ccn-lab\Templates\
[OK] locker.dir.check > name=\\?\c:\Users\ccn-lab\Videos\
[OK] locker.dir.check > name=\\?\c:\Users\Public\
[OK] locker.dir.check > name=\\?\c:\Users\Public\Desktop\
[OK] locker.dir.check > name=\\?\c:\Users\Public\Documents\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Public\Music name=\\?\c:\Users\Public\Documents\My Music\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Public\Pictures name=\\?\c:\Users\Public\Documents\My Pictures\
[SKIP] locker.dir.check > target visibled target=\??\C:\Users\Public\Videos name=\\?\c:\Users\Public\Documents\My Videos\
[OK] locker.dir.check > name=\\?\c:\Users\Public\Downloads\
[OK] locker.dir.check > name=\\?\c:\Users\Public\Favorites\
[OK] locker.dir.check > name=\\?\c:\Users\Public\Libraries\
[OK] locker.file > time=2.267 size=0.644 MB speed=0.284 MB/s name=\\?\c:\Users\ccn-lab\Desktop\target\x86\kdbazis.pdb
[OK] locker.file > time=0.158 size=0.956 MB speed=6.058 MB/s name=\\?\c:\Users\ccn-lab\Desktop\target\x86\kdpatch.pdb
[OK] locker.file > time=0.001 size=0.393 KB speed=0.659 MB/s name=\\?\c:\Users\ccn-lab\Documents\desktop.ini
[OK] locker.file > time=0.000 size=0.275 KB speed=0.961 MB/s name=\\?\c:\Users\ccn-lab\Downloads\desktop.ini
[OK] locker.file > time=0.000 size=0.393 KB speed=1.354 MB/s name=\\?\c:\Users\ccn-lab\Favorites\desktop.ini
[OK] locker.file > time=0.000 size=0.078 KB speed=0.299 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Links\desktop.ini
[OK] locker.file > time=0.000 size=0.230 KB speed=0.921 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Links\Suggested Sites.url
[OK] locker.file > time=0.000 size=0.221 KB speed=0.486 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Links\Web Slice Gallery.url
[OK] locker.file > time=0.000 size=0.219 KB speed=0.592 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Links for United States\desktop.ini
[OK] locker.file > time=0.000 size=0.131 KB speed=0.317 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Links for United States\GobiernoUSA.gov.url
[OK] locker.file > time=0.000 size=0.131 KB speed=0.418 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Links for United States\USA.gov.url
[OK] locker.file > time=0.344 size=0.130 KB speed=0.000 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Microsoft Websites\IE Add-on site.url
[OK] locker.file > time=0.031 size=0.130 KB speed=0.004 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Microsoft Websites\IE site on Microsoft.com.url
[OK] locker.file > time=0.000 size=0.130 KB speed=1.047 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Microsoft Websites\Microsoft At Home.url
[OK] locker.file > time=0.136 size=0.130 KB speed=0.001 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Microsoft Websites\Microsoft At Work.url
[OK] locker.file > time=0.034 size=0.131 KB speed=0.004 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Microsoft Websites\Microsoft Store.url
[OK] locker.file > time=0.001 size=0.130 KB speed=0.192 MB/s name=\\?\c:\Users\ccn-lab\Favorites\MSN Websites\MSN Autos.url
[OK] locker.file > time=0.000 size=0.130 KB speed=0.322 MB/s name=\\?\c:\Users\ccn-lab\Favorites\MSN Websites\MSN Entertainment.url
[OK] locker.file > time=0.000 size=0.130 KB speed=0.430 MB/s name=\\?\c:\Users\ccn-lab\Favorites\MSN Websites\MSN Money.url
[OK] locker.file > time=0.001 size=0.130 KB speed=0.141 MB/s name=\\?\c:\Users\ccn-lab\Favorites\MSN Websites\MSN Sports.url
[OK] locker.file > time=0.112 size=0.130 KB speed=0.001 MB/s name=\\?\c:\Users\ccn-lab\Favorites\MSN Websites\MSN.url
[OK] locker.file > time=0.000 size=0.130 KB speed=0.414 MB/s name=\\?\c:\Users\ccn-lab\Favorites\MSN Websites\MSNBC News.url
[OK] locker.file > time=0.000 size=0.130 KB speed=0.370 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Windows Live\Get Windows Live.url
[OK] locker.file > time=0.000 size=0.130 KB speed=0.401 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Windows Live\Windows Live Gallery.url
[OK] locker.file > time=0.005 size=0.130 KB speed=0.027 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Windows Live\Windows Live Mail.url

```
[OK] locker.file > time=0.000 size=0.130 KB speed=0.428 MB/s name=\\?\c:\Users\ccn-lab\Favorites\Windows Live\Windows Live Spaces.url
[OK] locker.file > time=0.000 size=0.566 KB speed=1.944 MB/s name=\\?\c:\Users\ccn-lab\Links\desktop.ini
[OK] locker.file > time=0.000 size=0.492 KB speed=2.622 MB/s name=\\?\c:\Users\ccn-lab\Music\desktop.ini
[ERROR] locker.file > open gle=32 name=\\?\c:\Users\ccn-lab\NTUSER.DAT
[ERROR] locker.file > open gle=32 name=\\?\c:\Users\ccn-lab\ntuser.dat.LOG1
[ERROR] locker.file > open gle=32 name=\\?\c:\Users\ccn-lab\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TM.blf
[ERROR] locker.file > open gle=32 name=\\?\c:\Users\ccn-lab\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000001.regtrans-ms
[ERROR] locker.file > open gle=32 name=\\?\c:\Users\ccn-lab\NTUSER.DAT{016888bd-6c6f-11de-8d1d-001e0bcde3ec}.TMContainer00000000000000000002.regtrans-ms
[OK] locker.file > time=0.000 size=0.020 KB speed=0.086 MB/s name=\\?\c:\Users\ccn-lab\ntuser.ini
[OK] locker.file > time=0.000 size=0.492 KB speed=2.173 MB/s name=\\?\c:\Users\ccn-lab\Pictures\desktop.ini
[OK] locker.file > time=0.000 size=0.275 KB speed=1.487 MB/s name=\\?\c:\Users\ccn-lab\Saved Games\desktop.ini
[OK] locker.file > time=0.000 size=0.512 KB speed=2.864 MB/s name=\\?\c:\Users\ccn-lab\Searches\desktop.ini
[OK] locker.file > time=0.000 size=0.242 KB speed=0.950 MB/s name=\\?\c:\Users\ccn-lab\Searches\Everywhere.search-ms
[OK] locker.file > time=0.000 size=0.242 KB speed=1.151 MB/s name=\\?\c:\Users\ccn-lab\Searches\Indexed Locations.search-ms
[OK] locker.file > time=0.000 size=0.492 KB speed=2.725 MB/s name=\\?\c:\Users\ccn-lab\Videos\desktop.ini
[OK] locker.file > time=0.000 size=0.170 KB speed=0.712 MB/s name=\\?\c:\Users\Public\Desktop\desktop.ini
[OK] locker.file > time=0.000 size=0.170 KB speed=1.054 MB/s name=\\?\c:\Users\Public\desktop.ini
[OK] locker.file > time=0.000 size=0.271 KB speed=1.643 MB/s name=\\?\c:\Users\Public\Documents\desktop.ini
[OK] locker.file > time=0.000 size=0.170 KB speed=0.687 MB/s name=\\?\c:\Users\Public\Downloads\desktop.ini
[OK] locker.dir.check > name=\\?\c:\Users\Public\Music\
[OK] locker.dir.check > name=\\?\c:\Users\Public\Music\Sample Music\
[OK] locker.dir.check > name=\\?\c:\Users\Public\Pictures\
[OK] locker.dir.check > name=\\?\c:\Users\Public\Pictures\Sample Pictures\
[OK] locker.file > time=0.416 size=0.086 KB speed=0.000 MB/s name=\\?\c:\Users\Public\Libraries\desktop.ini
[OK] locker.file > time=0.006 size=0.855 KB speed=0.151 MB/s name=\\?\c:\Users\Public\Libraries\RecordedTV.library-ms
[OK] locker.file > time=0.000 size=0.371 KB speed=1.781 MB/s name=\\?\c:\Users\Public\Music\desktop.ini
[OK] locker.file > time=0.000 size=0.572 KB speed=1.851 MB/s name=\\?\c:\Users\Public\Music\Sample Music\desktop.ini
[OK] locker.dir.check > name=\\?\c:\Users\Public\Videos\
[OK] locker.dir.check > name=\\?\c:\Users\Public\Videos\Sample Videos\
[SKIP] locker.dir.check > black  list name=\\?\c:\Windows\
[INFO] locker.work.thread.local > enum finish path=\\?\c:\
[OK] locker.file > time=2.562 size=8.025 MB speed=3.132 MB/s name=\\?\c:\Users\Public\Music\Sample Music\Kalimba.mp3
[OK] locker.file > time=9.386 size=427.362 MB speed=27.274 MB/s name=\\?\c:\Users\ccn-lab\Desktop\ida77sp1.zip
[OK] locker.file > time=0.704 size=3.923 MB speed=5.575 MB/s name=\\?\c:\Users\Public\Music\Sample Music\Maid with the Flaxen Hair.mp3
[INFO] locker.work.thread.network > enum finish
[INFO] locker.thread.proxy > finish path=NONE
[OK] locker.file > time=1.721 size=4.618 MB speed=2.683 MB/s name=\\?\c:\Users\Public\Music\Sample Music\Sleep Away.mp3
[OK] locker.file > time=0.000 size=0.371 KB speed=2.052 MB/s name=\\?\c:\Users\Public\Pictures\desktop.ini
[OK] locker.file > time=0.264 size=0.839 MB speed=3.173 MB/s name=\\?\c:\Users\Public\Pictures\Sample Pictures\Chrysanthemum.jpg
[OK] locker.file > time=0.201 size=0.807 MB speed=4.014 MB/s name=\\?\c:\Users\Public\Pictures\Sample Pictures\Desert.jpg
[OK] locker.file > time=0.041 size=0.001 MB speed=0.026 MB/s name=\\?\c:\Users\Public\Pictures\Sample Pictures\desktop.ini
[OK] locker.file > time=0.358 size=0.568 MB speed=1.587 MB/s name=\\?\c:\Users\Public\Pictures\Sample Pictures\Hydrangeas.jpg
[OK] locker.file > time=0.031 size=0.740 MB speed=23.905 MB/s name=\\?\c:\Users\Public\Pictures\Sample Pictures\Jellyfish.jpg
[OK] locker.file > time=0.179 size=0.745 MB speed=4.155 MB/s name=\\?\c:\Users\Public\Pictures\Sample Pictures\Koala.jpg
[OK] locker.file > time=0.080 size=0.535 MB speed=6.721 MB/s name=\\?\c:\Users\Public\Pictures\Sample Pictures\Lighthouse.jpg
[OK] locker.file > time=3.282 size=25.030 MB speed=7.627 MB/s name=\\?\c:\Users\Public\Videos\Sample Videos\Wildlife.wmv
[INFO] locker.queue.worker > empty group=SLOW
[INFO] locker.queue.worker > empty group=SLOW
[OK] locker.file > time=0.302 size=0.742 MB speed=2.457 MB/s name=\\?\c:\Users\Public\Pictures\Sample Pictures\Penguins.jpg
[OK] locker.file > time=0.082 size=0.592 MB speed=7.259 MB/s name=\\?\c:\Users\Public\Pictures\Sample Pictures\Tulips.jpg
[OK] locker.file > time=0.000 size=0.371 KB speed=0.766 MB/s name=\\?\c:\Users\Public\Videos\desktop.ini
[OK] locker.file > time=0.000 size=0.318 KB speed=0.873 MB/s name=\\?\c:\Users\Public\Videos\Sample Videos\desktop.ini
[INFO] locker.queue.worker > empty group=FAST
[INFO] locker.thread.proxy > finish path=\\?\c:\
==[ STATS ]=======================
Total crypted:  0.462 GB
Crypt Avg:  29.546 MB/s
Files:   8.875 files/s
Time:   16 sec
==[ DIRS ]=======================
Total:   93
Skipped:  42
Error:   0
```

```
==[ FILES ]======================
Total:   142
Locked:  88
==[ FILES SKIPPED ]===============
Black:   46
Locked:  0
Manual:  0
Prog:  0
Size:  3
==[ FILE ERROR ]==================
Open:  5
Read:  0
Write:   0
Pos:   0
Rename:  0

[OK] locker > finished
```