Informe Código Dañino
CCN-CERT ID-10/22

Cuba Ransomware

Octubre 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
2022.10.07 13:07:52 +02'00'

© Centro Criptológico Nacional, 2019

Fecha de Edición: octubre 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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE CCN-CERT, 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 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 Cuba**, identificada por la firma SHA256 0a3517d8d382a0a45334009f71e48114d395a22483b01f171f2c3d4a9cfdbfbf.

Las primeras muestras de Cuba ransomware emergieron en diciembre de 2019 y en noviembre de 2021 se le atribuían al menos 49 entidades comprometidas a lo largo de cinco sectores relacionados con infraestructura crítica, de acuerdo al siguiente informe del Federal Bureau of Investigation (FBI):

- https://www.ic3.gov/Media/News/2021/211203-2.pdf

El objetivo del código dañino es cifrar los ficheros de los sistemas que infecta para, posteriormente, negociar el pago de un rescate a cambio de la herramienta de descifrado. Mientras que su implementación es relativamente simple en cuanto a funcionalidad, el esquema de cifrado es robusto y cumple con su cometido.

Los actores que utilizan Cuba ransomware en sus operaciones siguen el modelo de "Big Game Hunting" (BGH) en que, una vez obtienen acceso ilícito a la red interna de una empresa y se mueven de forma lateral, generalmente para colonizar el controlador de dominio, realizan el despliegue masivo de la herramienta de cifrado en tantos sistemas como puedan alcanzar. El despliegue del ransomware suele ser la etapa final en la cadena de postexplotación, que puede haber sido precedida por exfiltración de información (por medios ajenos al ransomware).

En los siguientes apartados se entra en detalles técnicos sobre las características de **Cuba ransomware**, su esquema de cifrado y se adjunta una regla YARA para su identificación.

3. DETALLES GENERALES

El binario objeto de análisis es un *Portable Executable* (PE) para sistemas de 32-bit que también es compatible con sistemas de 64-bit. Su fecha de compilación data del 19.06.1992 22:22:17 UTC y se identifica con la firma SHA256 recogida en la siguiente tabla.

Fichero	SHA256
Cuba packed	0a3517d8d382a0a45334009f71e48114d395a22483b01f171f2c3d4a9cfdbfbf

Su funcionalidad se encuentra protegida por un *packer* desarrollado en Delphi (de ahí la fecha de compilación de 1992). Para proceder al análisis es necesario un proceso

de *unpacking* para obtener el *payload* final. Su fecha de compilación data del 06.03.2022 16:40:09 UTC y se identifica con la firma SHA256 recogida en la siguiente tabla.

Fichero	SHA256
Cuba unpacked	5fc815fede67245eff6d657960c045eae4d7e37d7e1e525e8ca4dffb070c764a

Buscando referencias al hash del binario, se ha encontrado que la primera fecha de la que se tiene constancia es el 17 de mayo de 2022.

4. PROCESO DE INFECCIÓN

4.1 PUNTO DE ENTRADA

El primer paso del código dañino es obtener el idioma del teclado a través de la llamada GetKeyboardLayoutList. Si el último byte del código del teclado es 0x19, la ejecución finaliza sin mayor afectación y el ejecutable se autoelimina.

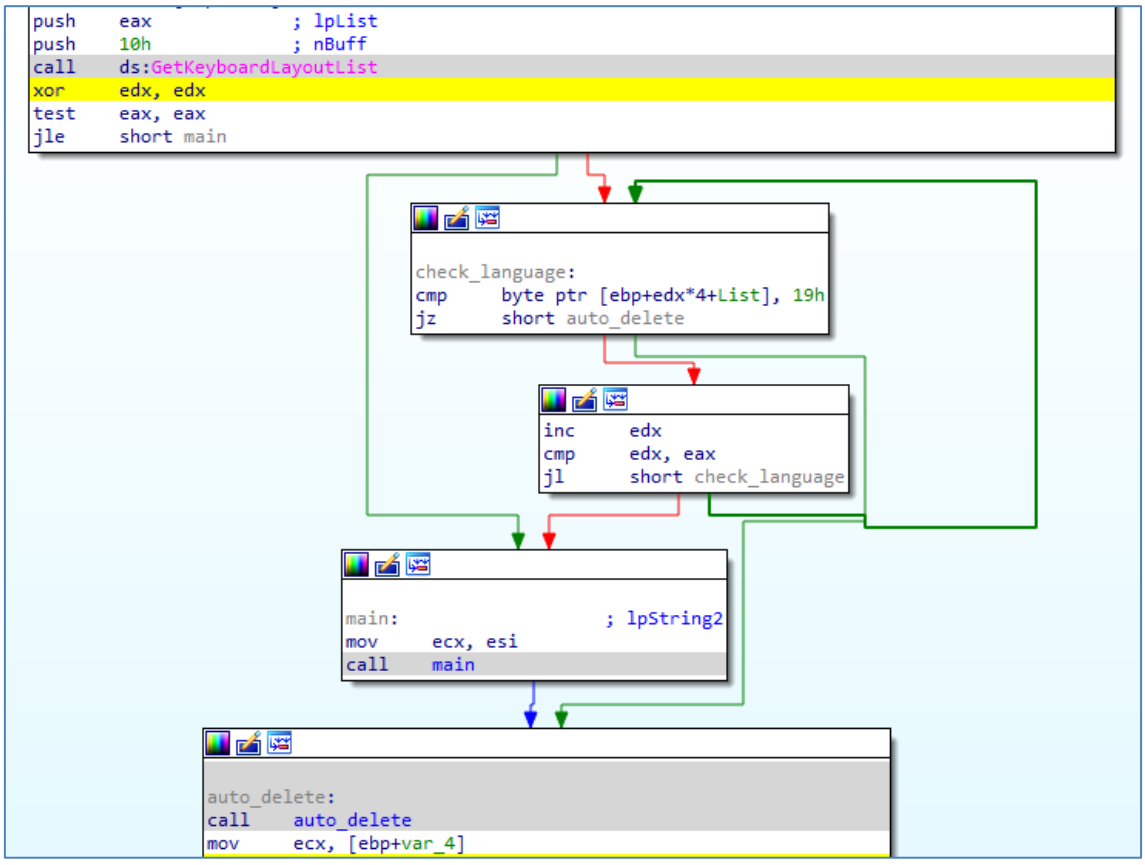

Figura 1. Punto de entrada del código dañino

Las dos opciones de teclado que satisfacen esa comprobación son el ruso y el ruso – Moldavia.

Locale	Language code	LCID string	LCID Decimal	LCID Hexadecimal	Codepage
Russian	ru	ru	1049	419	1251
Russian - Moldova	ru	ru-mo	2073	819	

Figura 2. Idiomas protegidos

Si uno de esos dos códigos es detectado, el código dañino procede a su autoeliminación. Si de forma contraria la infección continúa, cuando el proceso de cifrado concluye, el flujo de ejecución desemboca en la misma función de autoeliminado. Esta función se basa en la creación de un proceso con la siguiente línea de comandos.

```
C:\Windows\system32\cmd.exe /c del C:\Users\User\Desktop\cuba.exe >> NUL
```

La muestra de Cuba ransomware analizada no incluye ningún otro chequeo para prevenir la infección ni mecanismos para el control de instancias como “mutex”.

4.2 ARGUMENTOS

Si el sistema es susceptible de ser cifrado, es decir, si no incluye ninguno de los idiomas protegidos, la siguiente función es la encargada de decidir el flujo de ejecución en base a los argumentos de entrada que se faciliten por línea de comandos al proceso del código dañino.

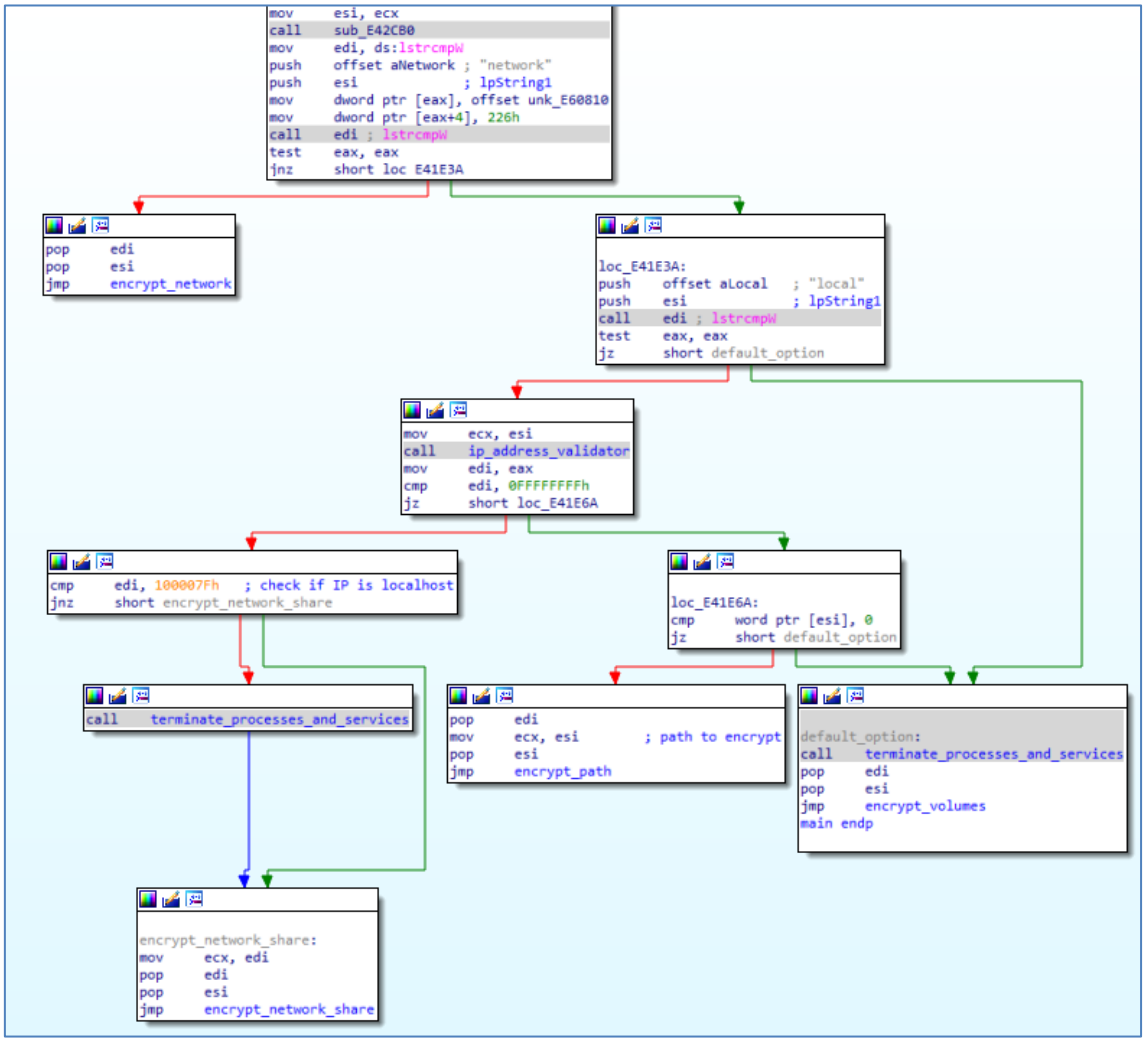

Figura 3. Flujo de ejecución controlado por argumentos

El proceso acepta un total de cuatro argumentos por línea de comandos.

Argumento	Comentarios
network	Utiliza las funciones GetIpNetTable y NetShareEnum para cifrar otras máquinas en la red así como recursos compartidos
local (opción por defecto)	Itera por los volúmenes del sistema cifrando ficheros
<dirección IP>	Cifra los contenidos de un recurso compartido de determinado servidor
<ruta a directorio>	Únicamente cifra el contenido de un directorio en la máquina local

Además, cuando el cifrado se efectúa en la máquina local, el código dañino trata de terminar una serie de procesos y servicios que potencialmente puedan bloquear algún fichero de interés para el proceso de cifrado y así maximizar el daño causado.

La siguiente tabla recoge los procesos que el código dañino trata de finalizar.

Procesos a finalizar	
Microsoft.Exchange.Store.Worker.exe	sqlceip.exe
msdtc.exe	sqlservr.exe
outlook.exe	sqlwriter.exe
sqlagent.exe	vmsp.exe
sqlbrowser.exe	vmwp.exe

La siguiente tabla recoge los servicios que el código dañino trata de finalizar.

Servicios a finalizar			
MSDTC	MSExchangeAntispamUpdate	MSExchangeCompliance	MSExchangeDagMgmt
MSExchangeDelivery	MSExchangeDiagnostics	MSExchangeEdgeSync	MSExchangeFastSearch
MSExchangeFrontEndTransport	MSExchangeHM	MSExchangeHMRecovery	MSExchangeImap4
MSExchangeIMAP4BE	MSExchangeIS	MSExchangeMailboxAssistants	MSExchangeMailboxReplication
MSExchangeNotificationsBroker	MSExchangePop3	MSExchangePOP3BE	MSExchangeRepl
MSExchangeRPC	MSExchangeServiceHost	MSExchangeSubmission	MSExchangeThrottling
MSExchangeTransport	MSExchangeTransportLogSearch	MSExchangeUM	MSExchangeUMCR
MSSQLSERVER	MySQL	MySQL80	SQLBrowser
SQLSERVERAGENT	SQLTELEMETRY	SQLWriter	vmcompute
vmms			

4.3 ESQUEMA DE CIFRADO

El código dañino implementa un simple esquema de cifrado que, a la vez, ofrece la robustez necesaria para garantizar que solo quien posea la clave privada del par maestro RSA pueda proceder al descifrado.

Antes de proceder al cifrado de un fichero, se realizan una serie de comprobaciones para decidir si continuar con la operación. En primer lugar, los ficheros con las siguientes extensiones no son cifrados:

Extensiones	
.cuba	.dll
.exe	.ini
.lnk	.sys
.vbm	

También se filtran los ficheros bajo el nombre "!! READ ME !!.txt", debido a que este es el título de la nota de rescate. Además de las extensiones mencionadas, los ficheros en los siguientes directorios se encuentran exentos del cifrado.

Directorios exentos del cifrado	
\\$recycle.bin\\	\\boot\\
\\google\\	\\inetcache\\
\\msocache\\	\\program files (x86)\\avs\\
\\program files (x86)\\microsoft office	\\program files\\avs\\
\\program files\\microsoft office\\	\\recovery\\
\\system volume information\\	\\temp\\
\\users\\all users\\	\\users\\default user\\
\\users\\default\\	\\windows\\

El esquema de criptografía elegido se basa en clave simétrica para los ficheros y clave asimétrica para proteger las claves generadas de forma aleatoria. Para cada fichero se genera una clave de 32 bytes y un *nonce* de 12 bytes mediante la función *CryptGenRandom*. Ese par de artefactos se emplean para cifrar bajo ChaCha20 RFC-7539 el contenido del fichero para posteriormente ser cifrados ellos mismos bajo RSA.

En un intento de acelerar el proceso de cifrado, Cuba ransomware deja fragmentos en texto claro si el fichero supera los 2 Mb. En tal caso se cifran bloques de 1 Mb y se intercalan bloques sin cifrar que varían en función del tamaño del fichero. La siguiente tabla resume el resultado en función del tamaño del fichero a cifrar.

Tamaño del fichero (bytes)	Tamaño del fichero (Megabytes/Gigabytes)	Fragmentos cifrados (Megabytes)	Fragmentos sin cifrar (Megabytes)
Tamaño <= 0x200000	Tamaño <= 2 Mb	El fichero se cifra al completo	-
0x200000 < Tamaño <= 0xA00000	2 Mb < Tamaño <= 10 Mb	1 Mb	4 Mb
0xA00000 < Tamaño <= 0x3200000	10 Mb < Tamaño <= 50 Mb	1 Mb	8 Mb
0x3200000 < Tamaño <= 0xC800000	50 Mb < Tamaño <= 200 Mb	1 Mb	16 Mb
0xC800000 < Tamaño <= 0x280000000	200 Mb < Tamaño <= 10 Gb	1 Mb	200 Mb
0x280000000 < Tamaño	10Gb < Tamaño	1 Mb	500 Mb

Finalmente, a cada fichero cifrado se le añade una cabecera de 1024 bytes que contiene la siguiente información y se le concatena la extensión "**.cuba"**:

- Marca de cifrado "FIDEL.CA" (0x100 bytes)
- Clave y *nonce* cifrados con RSA (0x200 bytes)
- Bloque nulo (0x100 bytes)

Para ofrecer una representación más visual, el siguiente esquema muestra el resultado de cifrar un fichero de menos de 2 Mb (izquierda) y uno de un tamaño superior (derecha).

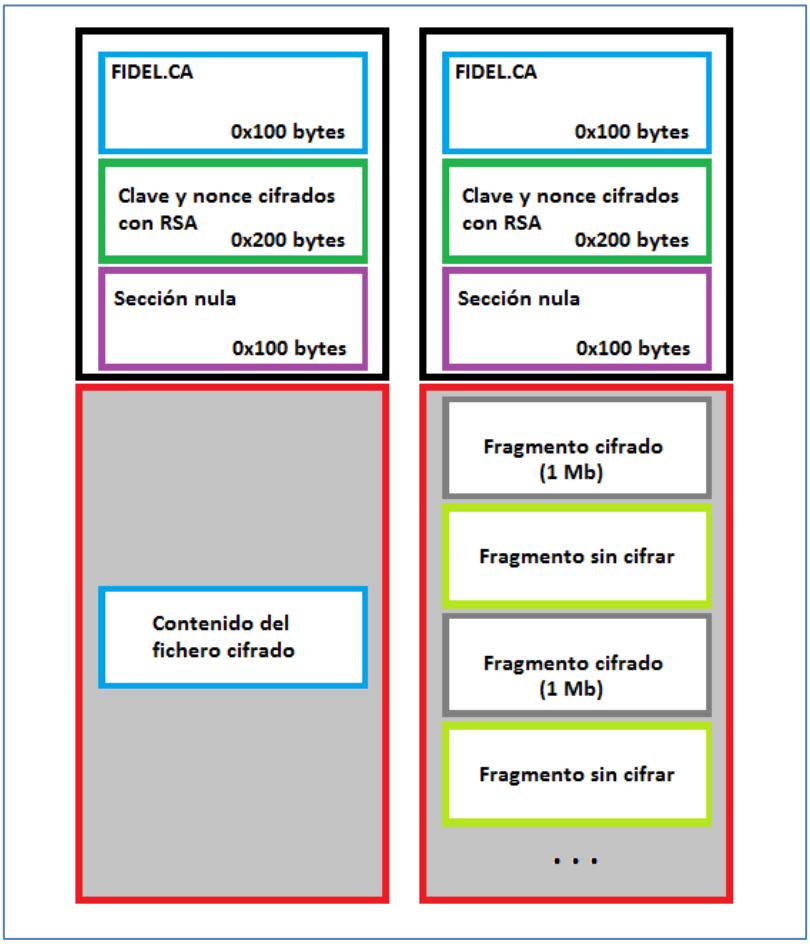

Figura 4. Esquema de un fichero cifrado

5. RESCATE

En cada carpeta con ficheros cifrados, la nota de rescate bajo el nombre "!! READ ME !!.txt" facilita los datos de contacto de los operadores de Cuba Ransomware. En la nota se incluye el identificador para la aplicación de mensajería instantánea qTox y un correo electrónico como método de contacto alternativo. En caso de no cumplirse las condiciones del rescate, también se incluye el portal de *leaks* donde se publicarían los datos sensibles sustraídos de la red de la compañía afectada.

El contenido completo de la nota de rescate se muestra a continuación.

> Greetings! Unfortunately we have to report you that your company were compromised. All your files were encrypted and you can't restore them without our private key. Trying to restore it without our help may cause complete loss of your data. Also we researched whole your corporate network and downloaded all your sensitive data to our servers. If we will not get any contact from you in 3 next days we will public it in our news site.
>
> You can find it there (http://cuba4ikm4jakjgmkezytyawtdgr2xymvy6nvzgw5cglswg3si76icnqd.onion/)
>
> Tor Browser is needed (https://www.torproject.org/download/)
>
> Also we respect your work and time and we are open for communication. In that case we are ready to discuss recovering your files and work. We can grant absolute privacy and compliance with agreements by our side.
>
> Also we can provide all necessary evidence to confirm performance of our products and statements.

```
Feel free to contact us with quTox ( https://tox.chat/download.html)

Our ToxID: 37790E2D198DFD20C9D2887D4EF7C3E2951BB84248D192689B64DCCA3C8BD808A1895676B271

Alternative method is email: inbox@mail.supports24.net

Mark your messages with your personal ID: GA6GD342D0
```

6. DESINFECCIÓN

El esquema de criptografía empleado garantiza que solo los operadores de Cuba ransomware puedan proceder al descifrado de los ficheros afectados por el ransomware.

Debido a que el código dañino se autoelimina al finalizar su ejecución, no se precisa de un proceso de desinfección para los sistemas afectados por esta variante.

7. REGLAS DE DETECCIÓN

7.1 REGLA YARA

```
rule cuba
{
   meta:
      author = "CCN-CERT"
      date = "2022-10-06"
      description = "Cuba Ransomware"

   strings:
      $encryption_0 = "expand 32-byte k" ascii
      $encryption_1 = "expand 16-byte k" ascii

      $cmdline_0 = "network" wide
      $cmdline_1 = "local" wide

      $api_0 = "OpenSCManagerW" ascii
      $api_1 = "OpenServiceW" ascii
      $api_2 = "EnumProcesses" ascii
      $api_3 = "OpenProcess" ascii
      $api_4 = "TerminateProcess" ascii
```

```
        $file_size_check_0 = {3D 00 00 20 00} // cmp eax, 200000h
        $file_size_check_1 = {3D 00 00 A0 00} // cmp eax, 0A00000h
        $file_size_check_2 = {3D 00 00 20 03} // cmp eax, 3200000h
        $file_size_check_3 = {3D 00 00 80 0C} // cmp eax, 0C800000h
        $file_size_check_4 = {3D 00 00 00 80} // cmp eax, 80000000h
    condition:
        (uint16(0) == 0x5A4D and
        all of them)
}
```

8. INDICADORES DE COMPROMISO (IOCs)

Cuba ransomware SHA256
0a3517d8d382a0a45334009f71e48114d395a22483b01f171f2c3d4a9cfdbfbf

Extensión
.cuba

Nota de rescate
!! READ ME !!.txt

E-mail de contacto
inbox@mail.supports24.net

E-mail de contacto
inbox@mail.supports24.net