Nro. Alerta:	EC-2022-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	14-febrero-2022	**Se detecta campaña de Ransomware Elbie (Ransomware Phobos) en Ecuador**	V 1.0

I. DATOS GENERALES:

Clase de alerta: Malware

Tipo de incidente: Ransomware

Nivel de riesgo: Medio

II. ALERTA

El 12 de febrero de 2022, una Institución de Ecuador, fue víctima de un ciberataque de tipo Ramsomware Elbie, también conocido como Phobos (similar a la familia de Ransomware Dharma).

Figura 1. Nota de rescate de información Ransomware Elbie **Fuente:** Help Ransomware

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	14-febrero-2022	**Se detecta campaña de Ransomware Elbie (Ransomware Phobos) en Ecuador**	V 1.0

III. INTRODUCCIÓN

Ransomware, es un tipo de malware (programa malicioso) que impide a usuarios, acceder a su sistema o, a sus archivos, ya sean empresariales o personales, exigiendo el pago de un rescate para poder acceder de nuevo a ellos. Durante los últimos años, los ciberataques de ransomware han ido evolucionando sus técnicas, lenguaje de programación y respectivo vector de ataque, con el objetivo de llegar a muchas más víctimas a nivel Global, ya sean ataques dirigidos, esporádicos, o arbitrarios, el ramsomware se ha convertido en un problema para muchos profesionales en Ciberseguridad tanto a nivel Nacional como Internacional, y, más aún, con el surgimiento del denominado Ransomware as a Service (RaaS), a través del cual, ciberdelincuentes venden sus desarrollos de Ransomware al mejor postor, con el objetivo de llegar a tantas víctimas como sea posible, y, generar ganancias a través de los rescates solicitados, las cuales son a través de la criptomonedas.

El ransomware Phobos apareció a principios de 2019. Se ha observado que esta nueva variedad de ransomware se basa en gran medida en la familia conocida anteriormente: Dharma (también conocida como CrySis), y probablemente distribuida por el mismo grupo que Dharma.

IV. VECTOR DE ATAQUE

Local, Red, Phishing

V. IMPACTO

El ransomware Elbie (Phobos), se propaga principalmente a través de campañas de spam, malware troyanos, canales de descarga no confiables, herramientas de activación ilegales ("cracks") y actualizadores falsas. Las campañas de spam se utilizan para enviar miles de correos electrónicos con archivos infectados adjuntos (o enlaces web que conducen a ellos).

Este correo engañoso generalmente se presenta como "oficial", "urgente", "importante", etc. Los archivos adjuntos vienen en varios formatos (por ejemplo, archivos de archivo y ejecutables, documentos PDF y de Microsoft Office, JavaScript, etc.) y, cuando se abren, se inicia el proceso de infección.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	14-febrero-2022	**Se detecta campaña de Ransomware Elbie (Ransomware Phobos) en Ecuador**	V 1.0

Elbie, es un ransomware desagradable que agrega la extensión ".[xxxxxxxx@privatemail.com].Elbie" a los nombres de los archivos después de cifrar los datos de las víctimas. La amenaza descargable, es el último desarrollo de los ciberdelincuentes detrás de Phobos Ransomware. Cuando este virus cifra los archivos, su nombre es cambiado de manera muy distintiva, siguiendo este patrón: el nombre original de su archivo seguido de la identificación única asignada a las víctimas y luego la dirección de correo electrónico de los ciberdelincuentes y, finalmente la extensión ".Elbie" . Por ejemplo, si un archivo llamado "1.jpg" se cifra, se cambiará a "1.jpg.id[C279F237-3182].[xxxxxx@privatemail.com].Elbie" .

Incluso después de que aparece la nota de rescate inicial, el malware aún se ejecuta en segundo plano y sigue cifrando los archivos recién creados. Todos los discos locales, así como los recursos compartidos de red, son atacados.

También se utilizan varios mecanismos de persistencia: se instala en %APPDATA% y en una carpeta de Inicio, agregando las claves de registro para iniciar automáticamente su proceso cuando se reinicia el sistema, podemos encontrar una lista de algunas palabras clave:

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

Ésta, es una lista de posibles extensiones utilizadas por este ransomware. Se utilizan (probablemente) para reconocer y omitir los archivos que ya han sido cifrados por un ransomware de esta familia. La extensión que se usará en la ronda de cifrado actual está codificada.

El ransomware, viene con una lista de procesos que elimina antes de implementar el cifrado. Al igual que otras cadenas, la lista completa se descifra a pedido:

```
msftesql.exe sqlagent.exe sqlbrowser.exe sqlservr.exe sqlwriter.exe
oracle.exe    ocssd.exe    dbsnmp.exe    synctime.exe    agntsvc.exe
mydesktopqos.exe
isqlplussvc.exe xfssvccon.exe mydesktopservice.exe
ocautoupds.exe agntsvc.exe agntsvc. exe agntsvc.exe encsvc.exe
firefoxconfig.exe  tbirdconfig.exe  ocomm.exe  mysqld.exe  mysqld-
```


Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	14-febrero-2022	**Se detecta campaña de Ransomware Elbie (Ransomware Phobos) en Ecuador**	V 1.0

```
nt.exe
mysqld-opt.exe     dbeng50.exe     sqbcoreservice.exe     excel.exe
infopath.exe
msaccess.exe    mspub.exe    onenote.exe    Outlook.exe    powerpnt.exe
steam.exe
thebat.exe thebat64.exe thunderbird.exe visio.exe winword.exe
wordpad.exe
```

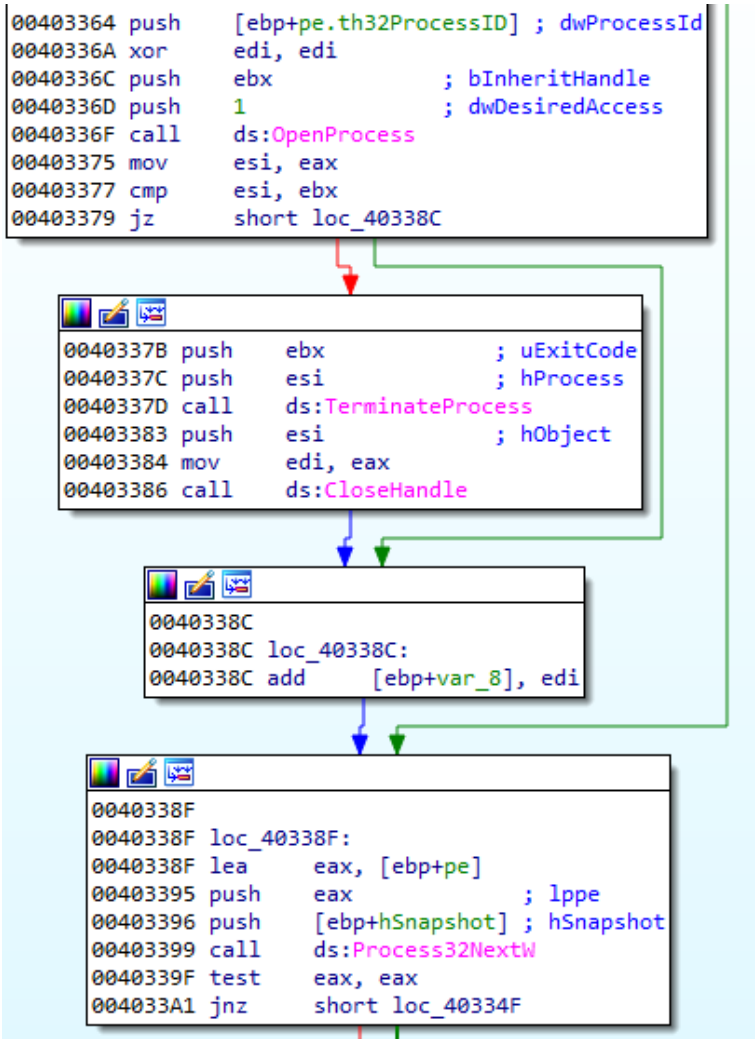

Figura 2. Fragmento de la función enumerando y terminando procesos **Fuente:** Malwarebytes

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	14-febrero-2022	**Se detecta campaña de Ransomware Elbie (Ransomware Phobos) en Ecuador**	V 1.0

Elbie, implementa varios comandos desde la línea de comandos. Se supone que esos comandos, evitan la recuperación de archivos cifrados de cualquier copia de seguridad existente.

Eliminación de las instantáneas:

```
vssadmin delete shadows /all /quiet
wmic shadowcopy delete
```

Cambiar las opciones de Bcdedit (evitar el arranque del sistema en modo de recuperación):

```
bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit /set {default} recoveryenabled no
```

Elimina el catálogo de respaldo en la computadora local:

```
wbadmin delete catalog -quiet
```

También desactiva el cortafuegos:

```
netsh advfirewall set currentprofile state off
netsh firewall set opmode mode=disable
exit
```

Podemos encontrar, por ejemplo, la lista negra (esos archivos se omitirán). Esos archivos están relacionados con el sistema operativo, más los archivos info.txt, info.hta son los nombres de las notas de rescate de Elbie(Phobos):

```
info.hta
info.txt
boot.ini
bootfont.bin
ntldr
ntdetect.com
io.sys
```

También, existe una lista de directorios para omitir; en el caso analizado, contiene solo un directorio:

```
C:\Windows.
```


Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	14-febrero-2022	**Se detecta campaña de Ransomware Elbie (Ransomware Phobos) en Ecuador**	V 1.0

Entre los archivos omitidos también se encuentran las extensiones que utilizan las variantes de Elbie:

```
1cd 3ds 3fr 3g2 3gp 7z accda accdb accdc accde accdt accdw adb adp
ai ai3 ai4 ai5 ai6 ai7 ai8 anim arw as asa asc ascx asm asmx asp
aspx asr asx avi avs backup bak bay bd bin bmp bz2 c cdr cer cf cfc
cfm cfml cfu chm cin class clx config cpp cr2 crt crw cs css csv
cub dae dat db dbf dbx dc3 dcm dcr der dib dic dif divx djvu dng
doc docm docx dot dotm dotx dpx dqy dsn dt dtd dwg dwt dx dxf edml
efd elf emf emz epf eps epsf epsp erf exr f4v fido flm flv frm fxg
geo gif grs gz h hdr hpp hta htc htm html icb ics iff inc indd ini
iqy j2c j2k java jp2 jpc jpe jpeg jpf jpg jpx js jsf json jsp kdc
kmz kwm lasso lbi lgf lgp log m1v m4a m4v max md mda mdb mde mdf
mdw mef mft mfw mht mhtml mka mkidx mkv mos mov mp3 mp4 mpeg mpg
mpv mrw msg mxl myd myi nef nrw obj odb odc odm odp ods oft one
onepkg onetoc2 opt oqy orf p12 p7b p7c pam pbm pct pcx pdd pdf pdp
pef pem pff pfm pfx pgm php php3 php4 php5 phtml pict pl pls pm png
pnm pot potm potx ppa ppam ppm pps ppsm ppt pptm pptx prn ps psb
psd pst ptx pub pwm pxr py qt r3d raf rar raw rdf rgbe rle rqy rss
rtf rw2 rwl safe sct sdpx shtm shtml slk sln sql sr2 srf srw ssi st
stm svg svgz swf tab tar tbb tbi tbk tdi tga thmx tif tiff tld
torrent tpl txt u3d udl uxdc vb vbs vcs vda vdr vdw vdx vrp vsd vss
vst vsw vsx vtm vtml vtx wb2 wav wbm wbmp wim wmf wml wmv wpd wps
x3f xl xla xlam xlk xlm xls xlsb xlsm xlsx xlt xltm xltx xlw xml
xps xsd xsf xsl xslt xsn xtp xtp2 xyze xz zip
```

VI. INDICADORES DE COMPROMISO

Resumen de Amenaza de Elbie	
Nombre	[XXXXXXXX-XXXX]**.exe** de archivo elbie
Extensión	[xxxxxxxxxxxxxxx@privatemail.com].elbie
Descripción	Secuestro de datos
Detección	Win32/Agent.NZW , Trojan-Ransom.Win32.Zerber.eqxc , Trojan:Win32/Occamy.C3C, Win32:Phobos-D [Ransom], Gen:Variant.Ransom.Phobos.62, W32/Generic.AP.34AB98!tr, entre otros
Breve descripción	El ransomware modifica los documentos en el dispositivo atacado a través del cifrado y solicita que la víctima pague el rescate supuestamente para recuperarlos.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	14-febrero-2022	**Se detecta campaña de Ransomware Elbie (Ransomware Phobos) en Ecuador**	V 1.0

Resumen de Amenaza de Elbie	
Síntomas	El virus de archivo encripta los datos agregando la extensión .elbie, generando también el identificador único. Tenga en cuenta que la **extensión [xxxxxxxxx@privatemail.com].elbie** se convierte en la secundaria.
Método de distribución	Spam, archivos adjuntos de correo electrónico, descargas legítimas comprometidas, ataques que explotan credenciales RDP débiles o robadas.

Propiedades Básicas	
MD5	9e79576cbd90a80fe04a8f4afa7cbece
SHA-1	3d51b94960c3bb966a8a886aacf75cbb6ff98556
SHA-256	9bd421c6f7f7d8278036944fcad3e04db408619678acf1b2024ef69d85c3932b
Vhash	054056655d655d70d8z447z37z13z25zd7z
Authentihash	fc280468ae6386853041e3db89ea41bac5117be9e3418bf95f5abdf31e55c444
Imphash	851a0ba8fbb71710075bdfe6dcef92eb
Rich PE header hash	256b60751602028612562b73ecdb163c
SSDEEP	1536:kNeRBl5PT/rx1mzwRMSTdLpJeB6EP4oKeRwBB4rk:kQRrmzwR5JGhQc
TLSH	T19F43B00A746984B2CD6645B1293A2F5F4FBE650140B844838F3D4DD63FE5076EB3A37A
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win64 Executable (generic) (32.2%)
TrID	Win32 Dynamic Link Library (generic) (20.1%)
TrID	Win16 NE executable (generic) (15.4%)
TrID	Win32 Executable (generic) (13.7%)
TrID	OS/2 Executable (generic) (6.2%)
Nombres de Archivo	software.exe
	file.exe
	ccm.exe
Sistemas Operativos afectados	Todas las versiones a nivel de Windows PC y Windows Server a partir de XP en adelante

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	14-febrero-2022	**Se detecta campaña de Ransomware Elbie (Ransomware Phobos) en Ecuador**	V 1.0

VII. RECOMENDACIONES

El EcuCERT, recomienda a su comunidad objetivo, tomar en consideración lo siguiente:

- En el caso de que la Organización/Institución se vea afectada por un ransomware, lo más importante es NO PAGAR el rescate.
- Realizar copias de respaldo de seguridad periódicas, de la información crítica para evitar la pérdida de la misma.
- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Otorgar privilegios de usuario al mínimo dependiendo del tipo de labor a realizar.
- Implementar técnicas de navegación segura en toda la Institución/Organización, como por ejemplo visita únicamente de sitios con certificados SSL, y, de origen no sospechoso.
- Bloquear el acceso de usuarios, a dispositivos de almacenamiento externo, ajenos a la Institución/Organización, a través de políticas de seguridad adecuadas.
- Implementar y monitorear, plataformas de seguridad perimetral para identificar posible tráfico malicioso tanto a nivel interno como externo a la infraestructura de red de la organización/Institución
- Descargar programas, archivos y actualizaciones, solamente desde fuentes oficiales y verificadas.
- Cerrar todo tipo de conexión/protocolo de acceso remoto a infraestructuras críticas en la Organización/Institución, en el caso de requerir su implementación, realizarlo bajo estrictas normas de seguridad apalancados en plataformas de seguridad perimetral y, uso de una VPN.
- Tener actualizado y utilizar, un software anti-virus
- Mantener actualizados, y, bajo licenciamiento, (ya sea a nivel de software libre o de paga, de ser el caso), todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura de IT y OT de la Institución, esto es, incluido a nivel de Firmware de todos los componentes.
- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.
- Implementar un plan de respuesta a emergencias de la Organización/Institución.
- En el caso de que la Organización/Institución se vea afectada por un ransomware, visita los siguientes enlaces; a fin de establecer un panorama de la situación: https://www.nomoreransom.org/es/decryption-tools.html#LockFile (herramientas de des

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-031	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	14-febrero-2022	**Se detecta campaña de Ransomware Elbie (Ransomware Phobos) en Ecuador**	V 1.0

encriptado en el caso de existir) / https://id-ransomware.malwarehunterteam.com/ (identificación de tipo de Ransomware y herramienta de des encriptado en el caso de existir una)

- En el caso de sufrir un ataque de proporciones mayores, contacte a las Autoridades competentes en base a la Normativa Legal Vigente a nivel Nacional.

VIII. REFERENCIAS:

Hasherezade. (16 de julio de 2021). MalwareBytes. Obtenido de https://blog.malwarebytes.com/threat-analysis/2019/07/a-deep-dive-into-phobos-ransomware/

Help Ransomware. (2021). Help Ransomware. Obtenido de https://helpransomware.com/es/ransomware-phobos/

Virus Total. (31 de enero de 2022). Virus Total. Obtenido de https://www.virustotal.com/gui/file/9bd421c6f7f7d8278036944fcad3e04db408619678acf1b2024ef69d85c3932b/detection

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec