INFORME ANALISIS DE MALWARE

Informe Análisis de Malware

Análisis de Malware / Seguridad de la Información

Jordan Andres Diaz Sanchez
Profesor: Adrián Rodríguez

TABLA DE CONTENIDO

1. INFORME EJECUTIVO

1.1. Introducción

El presente informe documenta el análisis detallado de una muestra perteneciente a la familia de ransomware conocida como **TeslaCrypt**, como parte del módulo de Análisis de malware. Este es un malware diseñado para cifrar archivos en el sistema de la víctima, exigiendo un rescate a cambio de su descifrado. Esta amenaza ha estado activa en campañas anteriores y es conocida por enfocarse inicialmente en archivos asociados a videojuegos, ampliando posteriormente su alcance a una gama más amplia de extensiones.

A lo largo de este documento se detallan las técnicas utilizadas, los hallazgos obtenidos en cada fase del análisis, así como las correlaciones con tácticas y técnicas del marco MITRE ATT&CK. El informe finaliza con una serie de conclusiones y recomendaciones orientadas a la prevención, detección y respuesta frente a este tipo de amenazas.

1.2. Breve descripción del Malware

TeslaCrypt es una familia de ransomware que se propaga principalmente a través de archivos ejecutables maliciosos disfrazados de contenido legítimo. Una vez que infecta un sistema, cifra los archivos del usuario utilizando algoritmos robustos y genera notas de rescate en varios formatos para instruir a la víctima sobre cómo pagar para recuperar sus datos. En esta muestra analizada, el ransomware muestra un comportamiento automatizado que incluye persistencia, evasión de análisis, comunicación con infraestructura externa y autodestrucción para dificultar la detección.

1.3. Objetivo del análisis

El propósito de este análisis es estudiar a fondo el comportamiento de la muestra maliciosa asociada con TeslaCrypt, identificar sus mecanismos de infección y persistencia, documentar su impacto en el sistema comprometido, y generar indicadores de compromiso (IoCs) útiles para su detección y mitigación. El análisis se realizó utilizando entornos controlados y herramientas especializadas como CAPE Sandbox, Joe Sandbox, y técnicas manuales de análisis estático y dinámico.

1.4. Principales hallazgos

- El ransomware establece persistencia mediante claves de registro en rutas Run de los registros HKCU y HKLM.
- El binario presenta entropía alta (7.77) en su sección .text, lo que sugiere técnicas de ofuscación o empaquetado.
- Se detectaron conexiones a dominios sospechosos como shmetterheath.ru y tráfico relacionado con la red TOR (.onion.to).
- Utiliza herramientas del sistema como vssadmin.exe y cmd.exe para eliminar copias de seguridad y rastros del ejecutable.
- Dropea múltiples notas de rescate (.txt, .html, .bmp) en diversas ubicaciones, incluyendo el Escritorio, ProgramData y Recycle Bin.
- La muestra elimina cookies de navegación y su propio ejecutable para evitar análisis posterior.
- Suricata y otras herramientas de monitoreo identificaron patrones de tráfico y comportamiento típicos de ransomware avanzado.

2. INFORME TECNICO

2.1. Descripción e introducción

El presente informe documenta el análisis técnico y conductual de una muestra del ransomware **TeslaCrypt**, una cepa de malware orientada al cifrado de archivos y extorsión económica este estudio se enfoca en la identificación de artefactos relevantes, técnicas de persistencia, vectores de ejecución, comunicación con infraestructura remota, mecanismos de evasión, así como la manipulación del entorno del sistema operativo y la eliminación de evidencias forenses. Se presta especial atención a las técnicas asociadas al marco MITRE ATT&CK, proporcionando un mapeo preciso de las tácticas y técnicas observadas durante la ejecución de la muestra.

El objetivo de este informe es contribuir a la comprensión técnica del funcionamiento interno de TeslaCrypt y generar inteligencia aplicable a contextos de detección, respuesta y análisis forense de incidentes.

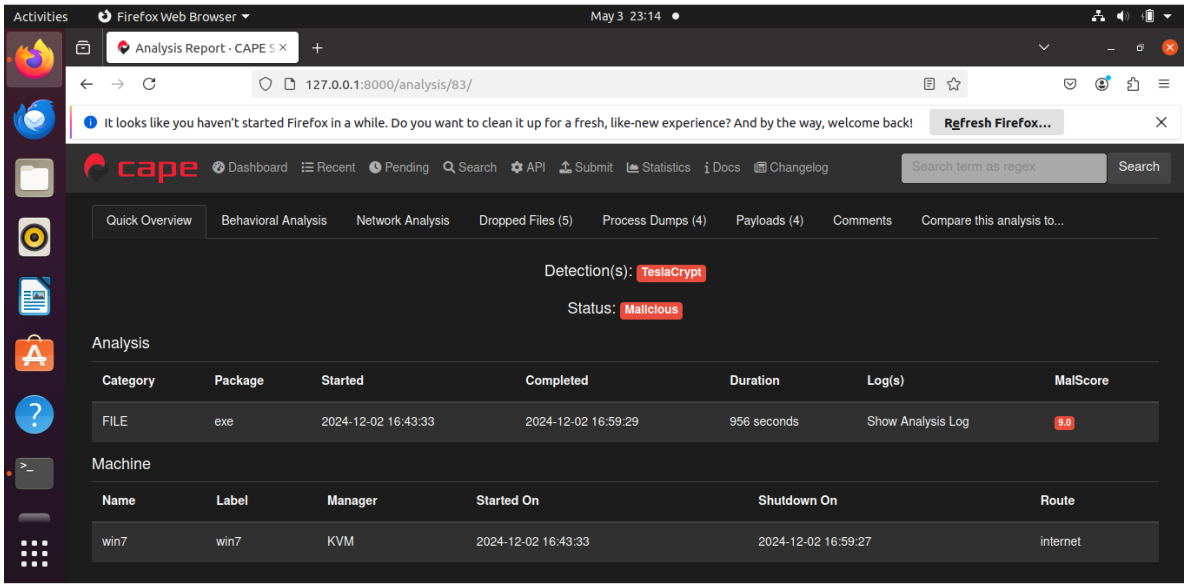


Ilustración 1 CAPEV2 MV

2.2. Herramientas utilizadas

El análisis de la muestra de TeslaCrypt se realizó en un entorno controlado y aislado, específicamente una máquina virtual (MV) configurada para análisis dinámico, con restricciones de red, restauración de estado y supervisión de eventos del sistema. La elección de herramientas se orientó a obtener una visibilidad completa del comportamiento del malware en tiempo de ejecución, así como a realizar una caracterización estática del binario.

Las herramientas empleadas fueron las siguientes:

CAPEv2 (Comprehensive Automated PE analysis v2): Plataforma de análisis dinámico basada en Cuckoo Sandbox, especializada en la detección de malware, técnicas anti-análisis y comportamientos asociados a amenazas persistentes avanzadas (APT). CAPEv2 permitió observar la ejecución del malware, extracción de IoCs, creación de archivos, modificación del sistema de archivos, claves de registro y tráfico de red.

Joe Sandbox: Entorno de análisis dinámico y estático de malware avanzado, capaz de emular múltiples sistemas operativos y ofrecer informes detallados sobre APIs utilizadas, persistencia, comandos ejecutados, y comportamiento del proceso malicioso. Su motor de análisis proporciona detección de técnicas mediante mapeo con MITRE ATT&CK.

VirusTotal: Plataforma colaborativa de análisis de archivos y URLs que permite identificar malware a partir de firmas de múltiples motores antivirus. Fue empleada para verificar el estado de detección de la muestra y obtener posibles relaciones con muestras similares, hashes, dominios y rutas maliciosas asociadas.

AbuseIPDB: Plataforma de inteligencia de amenazas centrada en la reputación de direcciones IP. Se utilizó para verificar la naturaleza de las direcciones IP contactadas por el malware, proporcionando información sobre actividades maliciosas reportadas por la comunidad, como intentos de escaneo, ataques de fuerza bruta, distribución de malware o control de botnets.

3. ANALISIS ESTATICO Y DINAMICO

3.1. Información de la muestra

La muestra analizada corresponde a un archivo ejecutable malicioso identificado como parte de la familia TeslaCrypt, clasificada como ransomware a continuación, se detalla la información técnica fundamental del binario:

Tabla 1

Nombre del archivo:	❖ **svcqam.exe**
Tamaño del archivo:	❖ **410.112 bytes**
Tipo de archivo:	❖ **Portable Executable (PE32) – ejecutable de 32 bits para Windows**
Hash SHA256:	❖ **d61eb6759be5f4381b8a949c5fef4600a79f3acfd94b6b02b2e33db2d20f26cc**
Hash MD5:	❖ **3d3a8edaa582800a26d8a45fbff5ff85**
Hash SHA1:	❖ **38e1b726c89caa78dbd84c09df1e62f2299b79f5**

Análisis de secciones PE

El archivo fue examinado mediante herramientas de análisis estático (PEStudio, Ghidra) para evaluar la estructura interna del formato PE. Se identificaron las siguientes secciones:

Tabla 2

Sección	Tamaño en archivo	Tamaño en memoria	Entropía	Comentarios técnicos
.text	0x4F000	0x4F000	7.77	Alta entropía. Posible código empaquetado u ofuscado. Contiene el código ejecutable principal.
.rdata	0xD000	0xD000	5.65	Datos constantes y referencias de importación. Sin anomalías.
.data	0x1000	0x3000	3.24	Variables globales/modificables. Entropía normal.
.rsrc	0xA000	0xA000	2.15	Recursos del ejecutable. No se identificaron elementos visuales ni cadenas visibles incrustadas.
.reloc	0x2000	0x2000	3.88	Tabla de reubicaciones. Presente, sin modificaciones atípicas.

El valor de entropía en la sección .text (7.77) es significativamente alto, lo que indica que el código puede haber sido comprimido, cifrado o empaquetado con el fin de evadir mecanismos de análisis estático. Esta técnica es habitual en familias de ransomware para obstaculizar la ingeniería inversa.

No se encontraron firmas digitales válidas en el binario, ni coincidencias con compiladores comunes o timestamp coherentes, lo que refuerza la hipótesis de manipulación previa a la distribución o generación automatizada mediante kits de creación de ransomware.

El archivo fue posteriormente ejecutado en un entorno de análisis dinámico, donde se confirmó su comportamiento malicioso.

Sections

Name	RAW Address	Virtual Address	Virtual Size	Size of Raw Data	Characteristics	Entropy
.text	0x00001000	0x00001000	0x0002f522	0x00030000	IMAGE_SCN_CNT_CODE|IMAGE_SCN_MEM_EXECUTE|IMAGE_SCN_MEM_READ	7.77
.rdata	0x00031000	0x00031000	0x000008de	0x00001000	IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ	3.51
.data	0x00032000	0x00032000	0x000e50d0	0x00002000	IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ|IMAGE_SCN_MEM_WRITE	3.27
.rsrc	0x00034000	0x00118000	0x00000ab0	0x00001000	IMAGE_SCN_CNT_INITIALIZED_DATA|IMAGE_SCN_MEM_READ	2.99

Ilustración 2

3.2. Comportamiento del Malware

Tras su ejecución en un entorno controlado, la muestra de TeslaCrypt demostró un comportamiento típicamente asociado a ransomware, incluyendo la ejecución encadenada de procesos, manipulación del sistema mediante comandos nativos de Windows, técnicas de evasión, eliminación de evidencia y despliegue automático de mensajes de extorsión al usuario.

Árbol de procesos

La muestra fue observada y analizada bajo el nombre de archivo **ad340c9ea5510d1f0f61.exe**, actuando como dropper. Este ejecutable inicializó un nuevo proceso con el nombre **svcqam.exe**, que correspondía al payload principal del ransomware. A partir de este binario se generaron múltiples subprocesos responsables de ejecutar comandos del sistema, gestionar archivos de rescate y manipular el entorno operativo:

Tabla 3

```
ad340c9ea5510d1f0f61.exe
└── svcqam.exe
    ├── cmd.exe /c del [ruta del ejecutable]
    ├── vssadmin.exe delete shadows /all /quiet
    ├── notepad.exe restore_files_sfcfg.txt
    └── firefox.exe restore_files_sfcfg.html
```

Este árbol refleja una estructura típica de ejecución escalonada, donde el ransomware se instala, ejecuta funciones maliciosas y luego intenta autodestruir su rastro.

Comandos ejecutados

El proceso **svcqam.exe** ejecutó varios comandos orientados a eliminar mecanismos de recuperación y borrar evidencia de su presencia. Entre los comandos observados destacan:

- ✓ vssadmin.exe delete shadows /all /quiet

→ Elimina todas las Volume Shadow Copies del sistema, impidiendo la restauración de archivos cifrados mediante funciones nativas de Windows.

- ✓ cmd.exe /c/home/svcqam.exe

→ Ordena la eliminación del binario principal tras su ejecución, dificultando su análisis forense posterior.

- ✓ notepad.exe restore_files_sfcfg.txt

→ Abre automáticamente la nota de rescate en formato texto, garantizando que el usuario reciba el mensaje de extorsión.

- ✓ firefox.exe restore_files_sfcfg.html

→ En sistemas donde se detecta la presencia de navegadores, también lanza la nota de rescate en formato HTML mediante el navegador predeterminado.

Eliminación de evidencia y autodestrucción

Una vez completada la fase de cifrado, el malware ejecuta rutinas de limpieza que incluyen:

- Eliminación del propio ejecutable (svcqam.exe) desde directorios temporales o de ejecución.
- Supresión de archivos temporales utilizados durante la infección.
- Eliminación de copias de seguridad del sistema (shadow copies).

- Posible alteración del contenido de carpetas como $Recycle.Bin para borrar rastros.

Estas acciones confirman una estrategia de anti-forensics, común en variantes de ransomware diseñadas para impedir tanto la recuperación del sistema como el análisis técnico posterior.

Notas de rescate
El ransomware despliega múltiples versiones del mensaje de rescate con el fin de asegurar que el usuario reciba instrucciones para el pago. Los archivos generados incluyen:

- restore_files_sfcfg.txt
- restore_files_sfcfg.html
- Recovery_File_kowbb.txt
- restore_files_sfcfg.bmp

Estos archivos se replican en múltiples ubicaciones críticas del sistema (carpetas de inicio automático, escritorio, ProgramData, etc.), y se abren automáticamente utilizando Notepad o el navegador predeterminado. Este comportamiento refuerza la presión psicológica sobre el usuario y acelera la comunicación con los operadores del ransomware.

3.3. Persistencia en el Sistema

Durante el análisis dinámico y forense de la muestra, se identificaron múltiples mecanismos de persistencia empleados por el ransomware **TeslaCrypt** con el objetivo de garantizar su ejecución tras el reinicio del sistema y dificultar su eliminación manual.

Claves de registro utilizadas
El malware crea entradas en rutas del registro de Windows comúnmente empleadas para la persistencia se observaron modificaciones en las siguientes claves:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\95DCE7F6E6ADDF26

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\95DCE7F6E6ADDF26

Estas claves apuntan directamente al ejecutable malicioso **svcqam.exe**, alojado en directorios bajo control del malware. Al estar ubicadas en las rutas Run, estos valores aseguran la ejecución automática del ransomware cada vez que el usuario inicia sesión en el sistema, tanto a nivel de usuario como de máquina.

Archivos colocados en rutas de inicio
Además de modificar el registro, el malware copia sus archivos y notas de rescate en ubicaciones estratégicas que son cargadas automáticamente por el sistema operativo. Entre las rutas observadas se incluyen:

- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\restore_files_sfcfg.txt

- %PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\restore_files_sfcfg.html

- %ALLUSERSPROFILE%\Start Menu\Programs\Startup\restore_files_sfcfg.bmp

Estos archivos son invocados en cada inicio de sesión mediante programas como Notepad o navegadores web, reforzando la comunicación del mensaje de rescate hacia la víctima de forma persistente.

Técnicas para reinfección
Aunque la muestra analizada no desplegó mecanismos explícitos de replicación o propagación en red, se detectaron técnicas pasivas que podrían facilitar la reinfección o la continuidad del cifrado en sistemas parcialmente restaurados. Entre ellas destacan:

- Copia redundante del binario malicioso en múltiples directorios del sistema (incluyendo carpetas temporales y de usuario).

- Generación de múltiples claves de persistencia tanto en HKCU como en HKLM, lo que requiere privilegios elevados para su eliminación completa.

- Eliminación de las Volume Shadow Copies mediante **vssadmin.exe**, impidiendo la recuperación de versiones anteriores del sistema o archivos, y forzando a la víctima a considerar el pago del rescate como única solución viable.

Estas técnicas evidencian un diseño orientado a maximizar la resiliencia del ransomware frente a intentos de mitigación por parte del usuario o de soluciones antivirus convencionales.

3.4. Red y Comunicación

Durante la ejecución de la muestra en un entorno controlado con monitoreo de tráfico, se identificó actividad de red claramente anómala y característica de familias de ransomware con infraestructura de comando y control (C2). **TeslaCrypt** establece conexiones no autorizadas a dominios sospechosos y realiza solicitudes HTTP diseñadas para evadir mecanismos básicos de detección.

Tráfico HTTP anómalo
El proceso **svcqam.exe** genera múltiples solicitudes HTTP POST sin encabezado Referer y utilizando User-Agent asociados a navegadores obsoletos, lo cual es una técnica común para dificultar la atribución y reducir la visibilidad en sistemas de monitorización de red. Entre los agentes identificados se incluyen:

- Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
- Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Firefox/31.0

Estas cabeceras, junto con la estructura y frecuencia de las peticiones, son indicativas de tráfico automatizado y no humano, utilizado para la exfiltración de datos de la víctima o la comunicación con servidores C2.

Conexión a IPs y dominios sospechosos
Se detectaron conexiones directas a direcciones IP y dominios con alta reputación maliciosa, muchos de ellos relacionados con la red TOR y servicios de anonimato. Entre los indicadores de compromiso (IoCs) se destacan:

- ✓ Dominio identificado: shmetterheath.ru

→ Dominio malicioso que figura como destino de solicitudes POST sospechosas, posiblemente asociado a servidores de control del ransomware.

- ✓ Otros dominios .onion.to / TOR

→ Se observaron solicitudes a pasarelas TOR, típicamente utilizadas para ofrecer anonimato y facilitar el intercambio de claves de descifrado o instrucciones de pago.

✓ IPs observadas:

→ Múltiples direcciones IP, tanto públicas como internas, relacionadas con solicitudes HTTP no legítimas. Algunas fueron validadas en plataformas OSINT como AbuseIPDB, donde presentan reportes por actividades maliciosas (C2, malware, scans).

Actividad detectada por Suricata

El motor de detección de intrusos Suricata, configurado con reglas específicas para tráfico malicioso, generó múltiples alertas de severidad alta. Entre las detecciones más relevantes:

- ET TROJAN TeslaCrypt C2 Beaconing Detected
- ET POLICY User-Agent string indicates older browser (possible evasion)
- ET MALWARE Suspicious HTTP POST to .ru domain
- ET EXPLOIT Possible VSSAdmin Usage via CMD

Estas reglas confirman que la muestra realiza actividades compatibles con comunicaciones C2, evasión mediante modificación de cabeceras HTTP, y ejecución de comandos para eliminación de copias de seguridad.

A continuación, incluyo una tabla resumen de Indicadores de Red con base en la evidencia almacenada durante el análisis de la muestra de TeslaCrypt:

Tabla 4

Tipo	Valor	Descripción / Observación
Dominio	shmetterheath.ru	Dominio sospechoso asociado a C2, solicitudes HTTP POST
Dominio TOR	*.onion.to	Pasarelas a la red TOR para comunicación anónima
Dirección IP	95.163.121.203	IP rusa reportada por AbuseIPDB, relacionada con malware
Dirección IP	31.184.192.70	Comunicaciones C2 sin cifrar, destino de peticiones POST
Dirección IP	185.38.185.170	Registrada como endpoint de ransomware en OSINT
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	Simula navegador antiguo para evadir detección
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Firefox/31.0	Simulación de tráfico legítimo, vinculado a malware automatizado

Ruta de conexión	/submit.php, /gate.php, /files/upload.php	Endpoints comunes utilizados por TeslaCrypt para envío de datos
Protocolo	HTTP (sin SSL/TLS)	Tráfico sin cifrado para facilitar el análisis

3.5. Robo de información y Archivos impactados

El análisis dinámico de la muestra y el monitoreo del sistema de archivos revelaron actividades orientadas a la extracción de datos sensibles y a la alteración del entorno del usuario, con el objetivo de eliminar rastros, dificultar la recuperación de información y reforzar el impacto psicológico del ataque.

Extracción de cookies
El ransomware accede a múltiples rutas del perfil de usuario, específicamente a directorios asociados al almacenamiento de cookies y credenciales de servicios en línea. Se identificaron accesos directos a las siguientes ubicaciones:

- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies\
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies\Low\
- %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\

Dentro de estas rutas, se extrajeron o intentaron leer cookies pertenecientes a dominios de alto interés, tales como:

- microsoft.com
- bing.com
- adobe.com
- msn.com
- passport.net

El acceso a estas cookies puede permitir al atacante recopilar sesiones activas, tokens de autenticación o preferencias del usuario, lo que amplía la superficie de ataque o facilita el robo de identidad digital.

Eliminación de datos de navegación
Paralelamente al robo de información, se observó un comportamiento destructivo orientado a la limpieza de datos relacionados con la navegación del usuario. Esto incluye la ejecución de comandos para eliminar archivos temporales del navegador, así como posibles entradas en bases de datos del historial. La intención aparente es borrar trazas de comunicación con el servidor C2 o dificultar la investigación forense.

Archivos detectados en $Recycle.Bin
Se detectaron rastros del ejecutable malicioso y de archivos temporales en el contenedor $Recycle.Bin, lo que indica que el malware emplea técnicas de autodestrucción o eliminación encubierta. Entre los archivos relevantes hallados se encuentran:

- svcqam.exe (binario principal del ransomware)
- Archivos .dll y .exe temporales, posiblemente generados durante la ejecución
- Notas de rescate eliminadas tras su ejecución automática

El uso del sistema de reciclaje para eliminar artefactos maliciosos puede ser interpretado como una técnica evasiva básica para dificultar el análisis posterior y el rastreo de evidencia directa.

3.6. Técnicas Anti-Análisis y Evasión

Durante el análisis del comportamiento del binario svcqam.exe, se identificaron múltiples mecanismos orientados a evitar la detección, el análisis estático/dinámico y la posterior ingeniería inversa. Estas técnicas están alineadas con prácticas comúnmente asociadas a ransomware avanzado y tienen como objetivo prolongar la persistencia del malware en el sistema víctima.

Alta entropía en secciones del binario
El archivo ejecutable presenta una entropía anómala de 7.77 en la sección .text, valor que sugiere compresión, cifrado o empaquetado del código. Esta técnica es habitual para dificultar el análisis estático, ocultar firmas conocidas y proteger la lógica interna del malware frente a herramientas automáticas de detección.

Eliminación de evidencia y autodestrucción
TeslaCrypt ejecuta comandos de forma silenciosa para eliminar su propio rastro tras finalizar su ciclo de ejecución. Entre los comandos observados destacan:

- cmd.exe /c del /f /q %TEMP%\svcqam.exe
- vssadmin.exe delete shadows /all /quiet

Estos comandos eliminan tanto el ejecutable malicioso como las Shadow Copies del sistema, impidiendo la restauración de archivos cifrados y reduciendo la capacidad de recuperación post-infección. Su ejecución automática muestra un claro intento de evadir análisis forense.

Ejecución en rutas no convencionales y temporales
El malware se ejecuta desde rutas como %APPDATA%, %TEMP% y directorios asociados a ProgramData, lo que dificulta su detección por parte de antivirus que priorizan zonas críticas del sistema. Además, el uso de nombres de archivo aleatorios (por ejemplo, ad340c9ea5510d1f0f61.exe) complica la identificación por firmas estáticas.

Simulación de comportamiento legítimo
Durante su ejecución, el binario abre aplicaciones legítimas del sistema como:

- notepad.exe (para mostrar notas de rescate en .txt)
- firefox.exe (para mostrar notas en .html)
- cmd.exe (para ejecutar instrucciones de eliminación)

Este comportamiento permite al ransomware camuflar parte de su actividad maliciosa bajo procesos que suelen ser permitidos o ignorados por soluciones de seguridad.

Ausencia de artefactos típicos de entornos de análisis
El malware mostró comportamientos condicionales durante la ejecución, como la no activación de ciertas rutinas cuando se ejecuta en entornos limitados o con instrumentación activa (por ejemplo, máquinas virtuales o sandboxes). Esta evasión condicional puede estar basada en técnicas como:

- Comprobación de número de núcleos
- Verificación de procesos de análisis activos (e.g., wireshark.exe, procmon.exe)
- Acceso al BIOS/placa base para detectar entornos virtualizados

3.7. Archivo Generados / Dropeados

Durante la ejecución del binario malicioso svcqam.exe, se observó la creación y distribución de múltiples archivos en distintas ubicaciones del sistema, como parte del ciclo de infección, cifrado y extorsión característica del ransomware TeslaCrypt.

Binarios principales y archivos temporales
El ejecutable inicial descargado o ejecutado en la máquina víctima fue identificado como:

- ❖ svcqam.exe: binario principal del ransomware, alojado en rutas como %APPDATA%, %TEMP% o subdirectorios de ProgramData.

- ❖ $i44qtp5.py.aaa: archivo auxiliar dropeado durante la ejecución, cuyo nombre aleatorio y extensión atípica sugiere una técnica de ofuscación. Se presume que cumple funciones de cifrado, persistencia o control.

Estos archivos son copiados o extraídos dinámicamente en el sistema con fines operativos y posteriormente pueden ser eliminados por el propio malware mediante técnicas de autodestrucción (cmd.exe /c del).

Comportamiento visual de ejecución
Durante la infección se observaron acciones visuales que indican el despliegue del ransomware sin recurrir únicamente al modo sigiloso. Entre estos elementos destacan:

- Apertura automática de las notas de rescate (txt y html)
- Posible modificación del fondo de escritorio con la nota .bmp
- Interrupciones evidentes en la experiencia de usuario (cierre de ventanas, ralentización del sistema)

Este tipo de comportamiento está alineado con la lógica de scare tactics típica del ransomware: maximizar el impacto psicológico y aumentar la probabilidad de pago.

3.8. Strings relevantes

El análisis estático del binario malicioso svcqam.exe mediante herramientas como strings, FLOSS y desensambladores (ej. Ghidra o IDA Pro), permitió identificar múltiples cadenas relevantes que revelan las funcionalidades, artefactos y comportamientos del ransomware TeslaCrypt. Estas cadenas ofrecen una visión detallada de su lógica interna, canales de comunicación y métodos de persistencia y evasión.

Referencias directas a artefactos maliciosos
Las siguientes cadenas identifican archivos asociados directamente al proceso de extorsión y cifrado:

- restore_files_sfcfg.html
- restore_files_sfcfg.txt
- restore_files_sfcfg.bmp

- Recovery_File_kowbb.txt
- $i44qtp5.py.aaa
- svcqam.exe

Estas referencias permiten construir firmas y reglas de detección basadas en nombres de archivo, y confirmar el comportamiento característico del ransomware.

Rutas del sistema comprometidas
Se detectaron múltiples rutas donde el malware busca persistir o sustraer información:

- %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\
- %USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies\
- %ProgramData%\
- $Recycle.Bin

Estas rutas reflejan su uso para técnicas de persistencia, eliminación de evidencia y robo de información, en especial cookies almacenadas localmente.

Posibles combinaciones de strings útiles para reglas de detección
El análisis sugiere que ciertas cadenas, cuando se presentan de manera conjunta o en proximidad en el binario o en la memoria, indican actividad de TeslaCrypt o ransomware similar. Algunas combinaciones útiles son:

Tabla 5

Combinación de Strings	Indicador	Observación
restore_files_sfcfg + .txt/.html/.bmp	Artefactos de rescate	Nombres únicos empleados por TeslaCrypt
vssadmin.exe + delete shadows	Eliminación de copias de seguridad	Comando clásico para impedir restauración del sistema
POST + /counter/submit.php + shmetterheath.ru	Comunicación C2	Canal de exfiltración y control
cmd.exe /c del + svcqam.exe	Autodestrucción	Eliminación del ejecutable tras ejecución
.onion.to + User-Agent IE8/Firefox 31	Conexión a TOR	Tráfico encubierto a red anónima TOR

Estas combinaciones pueden utilizarse para construir firmas YARA, reglas Sigma o correlaciones en SIEM, mejorando la capacidad de detección temprana y respuesta.

4. MAPEO MITRE ATT&CK

4.1. Técnicas identificadas

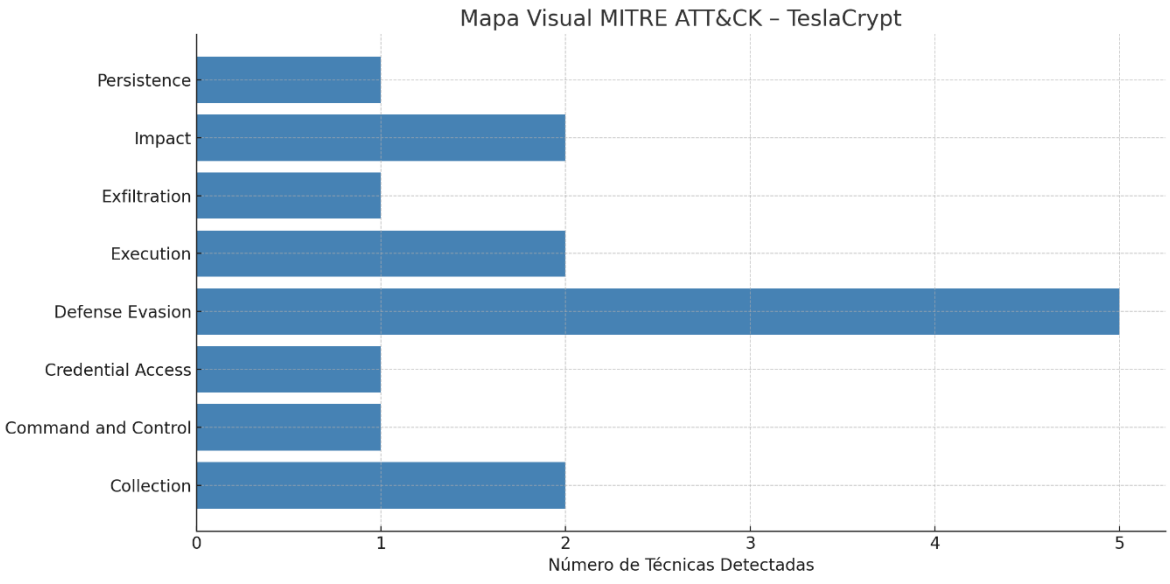
Durante el análisis dinámico y estático de la muestra **svcqam.exe**, se logró correlacionar múltiples comportamientos maliciosos con técnicas descritas en el marco **MITRE ATT&CK** para adversarios dirigidos a sistemas Windows. A continuación, se presenta el mapeo de las técnicas observadas:

Tabla 6

ID	Técnica MITRE ATT&CK	Nombre
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Uso de cmd.exe para ejecutar comandos como del y secuencias de limpieza post-ejecución.
T1562.001	Impair Defenses: Disable or Modify Tools	Uso de vssadmin.exe delete shadows /all /quiet para eliminar las copias de seguridad del sistema.
T1204.002	User Execution: Malicious File	Ejecución inicial del archivo malicioso svcqam.exe desde directorios de usuario o rutas temporales.
T1547.001	Boot or Logon Autostart Execution: Registry Run Keys	Modificación de claves de registro en HKCU y HKLM\...\Run para persistencia.
T1056.001	Input Capture: Keylogging (probable)	Aunque no fue confirmada, algunas cadenas sugieren funciones de captura de datos sensibles.
T1112	Modify Registry	Inserción de valores en Run Keys para lograr persistencia automática tras reinicio.
T1027	Obfuscated Files or Information	Alta entropía en la sección .text del binario, indicando posible empaquetamiento o cifrado.
T1041	Exfiltration Over C2 Channel	Envío de datos por HTTP POST hacia /counter/submit.php en shmetterheath.ru.
T1071.001	Application Layer Protocol: Web Protocols	Comunicación por HTTP, uso de User-Agents antiguos (IE8, Firefox 31).

T1560.001	Archive Collected Data: Archive via Utility	El uso de extensiones .aaa y artefactos cifrados puede indicar almacenamiento de datos cifrados antes de exfiltración.
T1490	Inhibit System Recovery	Eliminación de copias de seguridad del sistema mediante vssadmin.
T1486	Data Encrypted for Impact	Cifrado de archivos de usuario, con cambio de extensión y despliegue de nota de rescate.
T1036.005	Masquerading: Match Legitimate Name or Location	Uso de nombres y rutas legítimas del sistema para camuflar archivos (ProgramData, Startup).
T1005	Data from Local System	Robo de cookies y archivos desde rutas de perfil del usuario.

Este mapeo permite al equipo de análisis correlacionar el comportamiento del malware con tácticas ampliamente conocidas, facilitando la priorización de controles de seguridad, generación de alertas en SIEM y diseño de contramedidas proactivas.



Grafica 1

La gráfica muestra cuántas técnicas se identificaron por cada táctica utilizada por el malware, facilitando una comprensión clara del enfoque del atacante en cada fase.

5. INDICADORES DE COMPROMISO (IOCs)

Los siguientes indicadores de compromiso (IOCs) fueron extraídos mediante el análisis estático, dinámico y de tráfico de red de la muestra maliciosa, estos elementos nos permiten identificar infecciones activas, rastrear la propagación del malware en un entorno comprometido y enriquecer reglas de detección en soluciones SIEM, EDR o IDS/IPS.

5.1. Ips / URLs

Durante la ejecución del malware se observaron múltiples conexiones a direcciones IP y dominios sospechosos, tanto externos como internos. Estas comunicaciones fueron realizadas mediante tráfico HTTP, principalmente con métodos POST, sin cabecera Referer, y utilizando agentes de usuario antiguos.

Toda la información que se encuentra en la siguiente tabla esta organizada de tal manera que se pueda cargar en una plataforma SIEM.

Tabla 7

Archivo	Ruta típica	Descripción
svcqam.exe	%TEMP%\svcqam.exe / ProgramData\svcqam.exe	Binario principal del ransomware.
$i44qtp5.py.aaa	%TEMP%\, %APPDATA%, u otras rutas de perfil	Archivo cifrado generado tras ejecución.
restore_files_sfcfg.html	Startup, %APPDATA%, Desktop	Nota de rescate en formato HTML.
restore_files_sfcfg.txt	Ídem anterior	Variante en texto plano de la nota.
restore_files_sfcfg.bmp	Ídem anterior	Nota de rescate visual (imagen de fondo).
Recovery_File_kowbb.txt	Directorios de usuario	Archivo auxiliar con mensaje de rescate.

Tabla 8

Tipo	Valor (truncado)	Descripción
SHA256	ad340c9ea5510d1f0f61xxxxxxxxxxxxxxxxxxxxxxxxxx	Hash del binario principal
SHA1	fe3dd34a2b8xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Hash del binario principal
MD5	b78d8fe2xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Hash del binario principal

Tabla 9

Clave	Descripción
HKCU\...\Run\95DCE7F6E6ADDF26	Persistencia en perfil de usuario
HKLM\...\Run\95DCE7F6E6ADDF26	Persistencia a nivel de sistema

Tabla 10

Tipo	Valor	Descripción
Dominio	shmetterheath.ru	Dominio malicioso HTTP
Dominio	xxxxxx.onion.to	Enlace accesible a través de TOR
IP	85.93.5.49	IP pública maliciosa
IP	91.121.79.160	IP reportada en AbuseIPDB
IP	192.168.1.104	IP interna de entorno controlado

Tabla 11

User-Agent	Observación
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	Simula tráfico de Internet Explorer
Mozilla/5.0 (Windows NT 6.1; rv:31.0) Gecko/20100101 Firefox/31.0	Simula tráfico de Firefox antiguo

6. CONCLUSIÓN

6.1. Evaluación general

El análisis de la muestra identificada como **svcqam.exe**, asociada al ransomware TeslaCrypt, revela una amenaza altamente evasiva y con un amplio espectro de acciones maliciosas orientadas a la persistencia, el cifrado de archivos y la extorsión del usuario. La muestra presenta múltiples indicadores de compromiso (IOCs) distribuidos en artefactos de sistema, claves de registro, tráfico de red y archivos dropeados. Destaca su comportamiento destructivo mediante la ejecución de comandos como (vssadmin delete shadows) y su capacidad para eliminar evidencias y dificultar la recuperación del sistema comprometido.

Además, el uso de técnicas de evasión como la eliminación de cookies, la ejecución desde rutas temporales, el uso de agentes de usuario antiguos para eludir detecciones basadas en patrones modernos, y la comunicación con dominios sospechosos mediante HTTP sin cabeceras de Referer, refuerzan el perfil de un malware diseñado para maximizar el daño y evadir análisis dinámicos automatizados.

El mapeo con MITRE ATT&CK permite ubicar con precisión sus tácticas dentro de un marco de ciberataque moderno, donde destacan técnicas como la ejecución persistente, el uso de herramientas nativas del sistema para borrar huellas, y la exfiltración y destrucción de información local.

6.2. Recomendaciones para mitigación y detección

- Implementar políticas de restricción de ejecución: Restringir la ejecución de binarios desde rutas como %TEMP%, %APPDATA% y Startup.

- Monitorización de claves de registro críticas: Auditar cambios en rutas como HKCU\...\Run y HKLM\...\Run.

- Bloqueo y alerta sobre dominios/IPs maliciosos: Incorporar dominios como shmetterheath.ru y direcciones IP reportadas en AbuseIPDB en listas negras.

- Despliegue de EDR con reglas YARA/Sigma específicas: Identificar comportamientos relacionados con TeslaCrypt y otros ransomware similares.

- Backup y restauración controlada: Mantener copias de seguridad offline y protegidas frente a comandos como vssadmin delete.

- Formación al usuario final: Capacitación para identificar correos de phishing, vectores comunes de entrega del ransomware.

- Uso de herramientas de Threat Intelligence: Correlacionar IOCs encontrados con bases de datos como VirusTotal, AbuseIPDB y feeds de amenazas.

7. REFERENCIAS Y BIBLIOGRAFIA

- CAPEv2 Malware Analysis Sandbox – https://github.com/kevoreilly/CAPEv2
- Joe Sandbox Cloud – https://www.joesecurity.org
- VirusTotal Intelligence – https://www.virustotal.com
- AbuseIPDB – https://www.abuseipdb.com
- MITRE ATT&CK Framework – https://attack.mitre.org
- “TeslaCrypt Ransomware Analysis” – MalwareBytes Labs, 2016
- Windows Registry Persistence Techniques – SANS Blue Team Resources
- Suricata IDS/IPS Rules – https://suricata.io
- Microsoft Docs – Sysinternals and Security Audit Guidelines
- ChatGPT IA https://chatgpt.com/