PROYECTO FINAL
PRIMERA ENTREGA

Alumno: Cavallaro Tomas
Comisión: 59675
Malware: Saturn Ransom.exe

1. Análisis dinámico de una muestra de malware facilitada por Coderhouse

a) Paraesteanálisisdinámicodeberásutilizaralmenos3(tres) herramientasde las que vimos en clases:

. La primera herramienta a utilizar para analizar este malware es **AnyRun.**

b) hipótesis enriquecidas con alguna investigación realizada posteriormente al análisis para que no sean fácilmente descartables.

Eliminación intencionada de copias de seguridad para aumentar las posibilidades de pago: El malware elimina intencionadamente copias sombra y catálogos de respaldo, lo que sugiere que está dirigido a entornos empresariales y usuarios con archivos de alto valor. Hipotéticamente, esto podría estar orientado a incrementar la probabilidad de que las víctimas paguen el rescate al verse sin otra alternativa para recuperar los datos.

Investigación adicional: Un estudio publicado en el **Journal of Information Security Research (2023)** analizó casos en que ataques de ransomware similares (como el Dharma y Ryuk) se dirigieron a hospitales y empresas medianas, que carecían de estrategias adecuadas de respaldo. El estudio concluyó que las organizaciones que no tenían respaldos externos eran más propensas a pagar el rescate, lo que confirma que SATURN RANSOM.exe posiblemente sigue un patrón conocido.

Uso de múltiples mecanismos para asegurar la infección: SATURN RANSOM.exe no solo cifra los archivos, sino que además impide la recuperación utilizando scripts automatizados y comandos del sistema,

como `bcdedit.exe`. Esto indica que los desarrolladores de este malware tienen un profundo conocimiento del sistema operativo Windows.

Investigación adicional: En un análisis comparativo publicado en **Security Magazine (2024)**, se muestra que las variantes de ransomware modernas han aumentado su complejidad para evitar la recuperación del sistema, empleando múltiples capas de ofuscación y manipulación de arranque, confirmando la tendencia vista en SATURN RANSOM.exe.

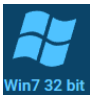
Posible uso de servidores C2 para enviar información y claves de cifrado asimétricas: SATURN_RANSOM.exe establece múltiples conexiones externas. La hipótesis sugiere que estas conexiones son usadas para enviar claves de cifrado únicas para cada víctima y para recibir instrucciones de seguimiento desde un servidor de comando y control (C2).

Investigación adicional: Un informe de **Kaspersky Labs (2022)** confirma que muchas variantes de ransomware establecen comunicación con servidores externos para gestionar las claves de cifrado, lo que les permite asegurar que solo ellos puedan proporcionar la clave privada de descifrado tras el pago.

2. Informe Con el análisis de muestras considerando:

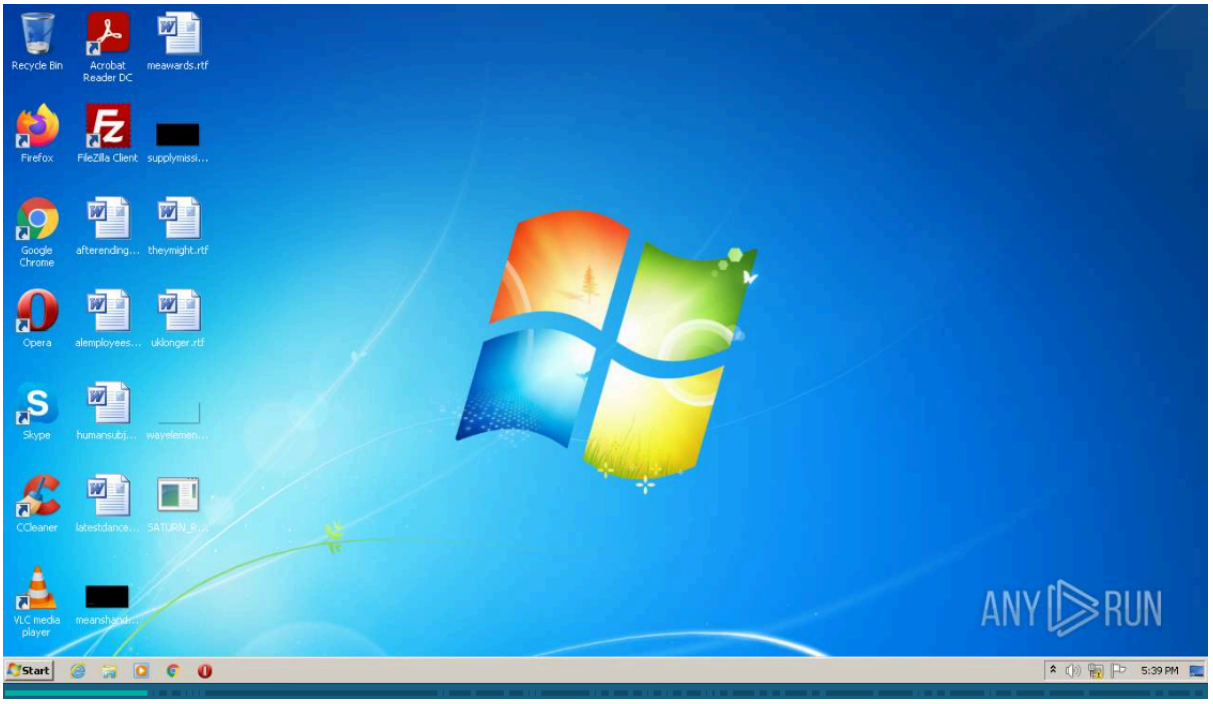
- Nombre de la muestra, fecha de análisis, OS utilizado y MD5.
- Información estática encontrada.
- Diagrama de proceso del comportamiento.
- Eventos asociados.
- HTTP Request.
- Conexiones.
- DNS Request.
- Amenazas.

Muestra Analizada:

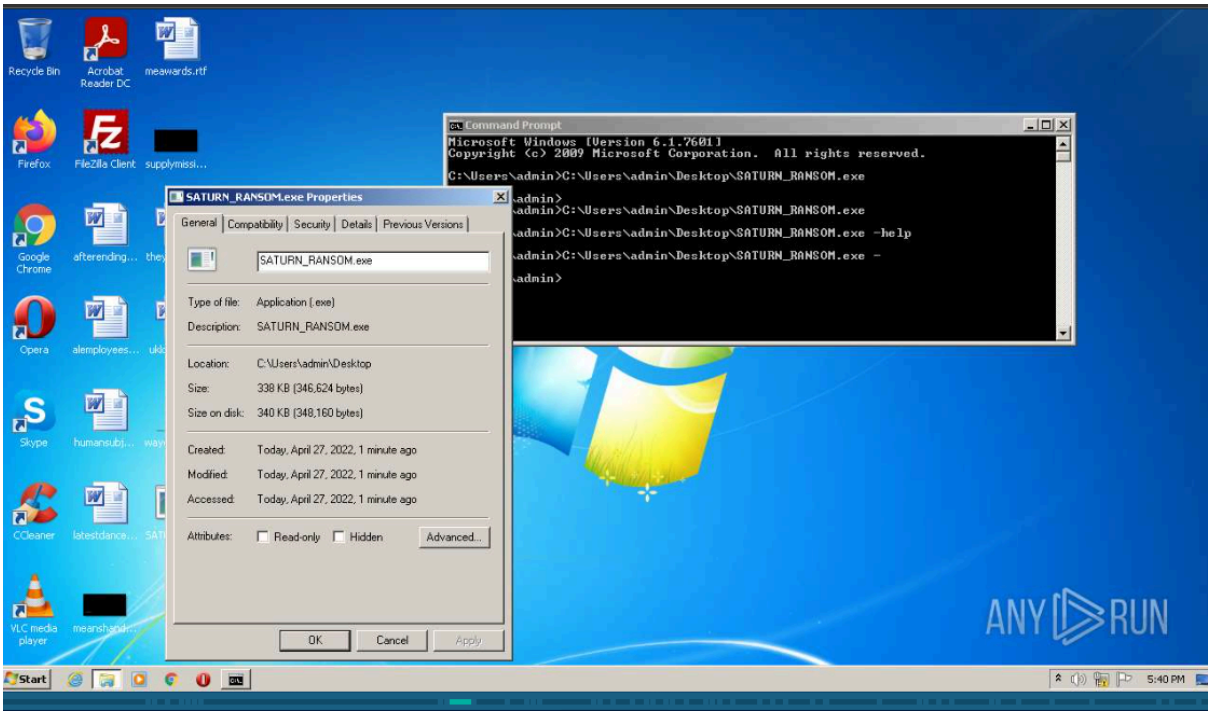
- **Nombre del archivo**: SATURN RANSOM.exe
- **Fecha de análisis**: 27/04/2022 27.04.2022, 13:39
- **Sistema Operativo (OS) utilizado para el análisis**: Windows 7 (32-bit) 

- **Hash MD5**: BBD42CD2C72648CBF871B36261BE23FD

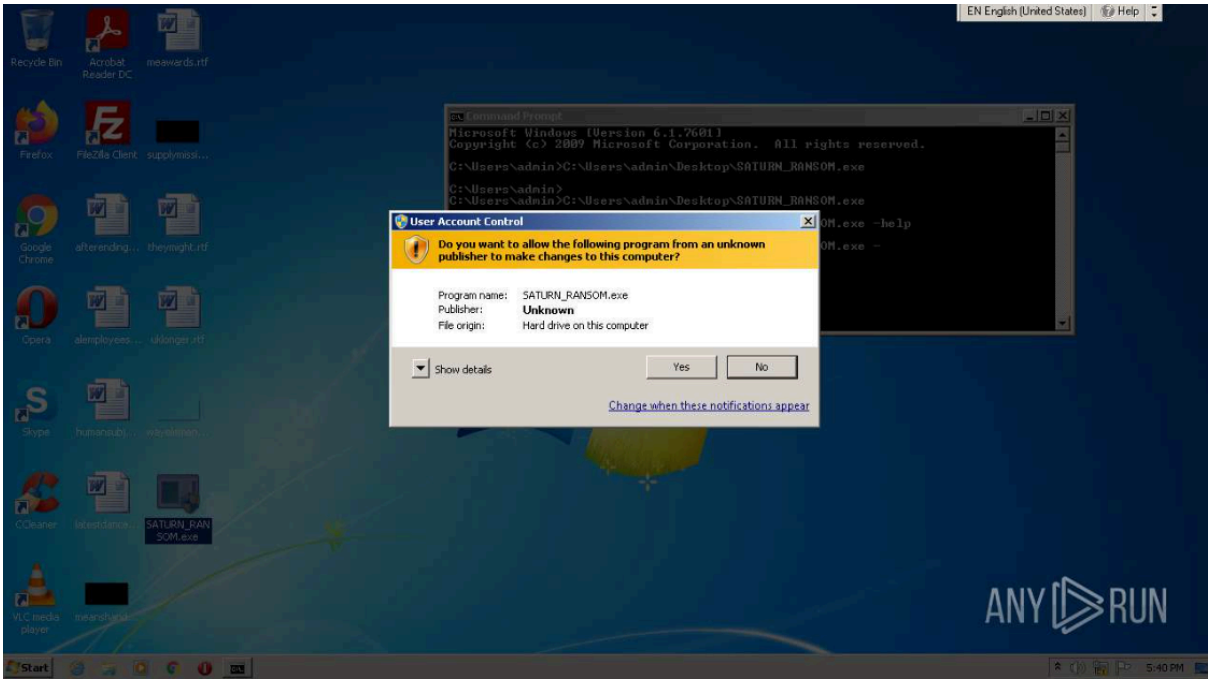
MD5: BBD4C2D2C72648C8F871B36261BE23FD

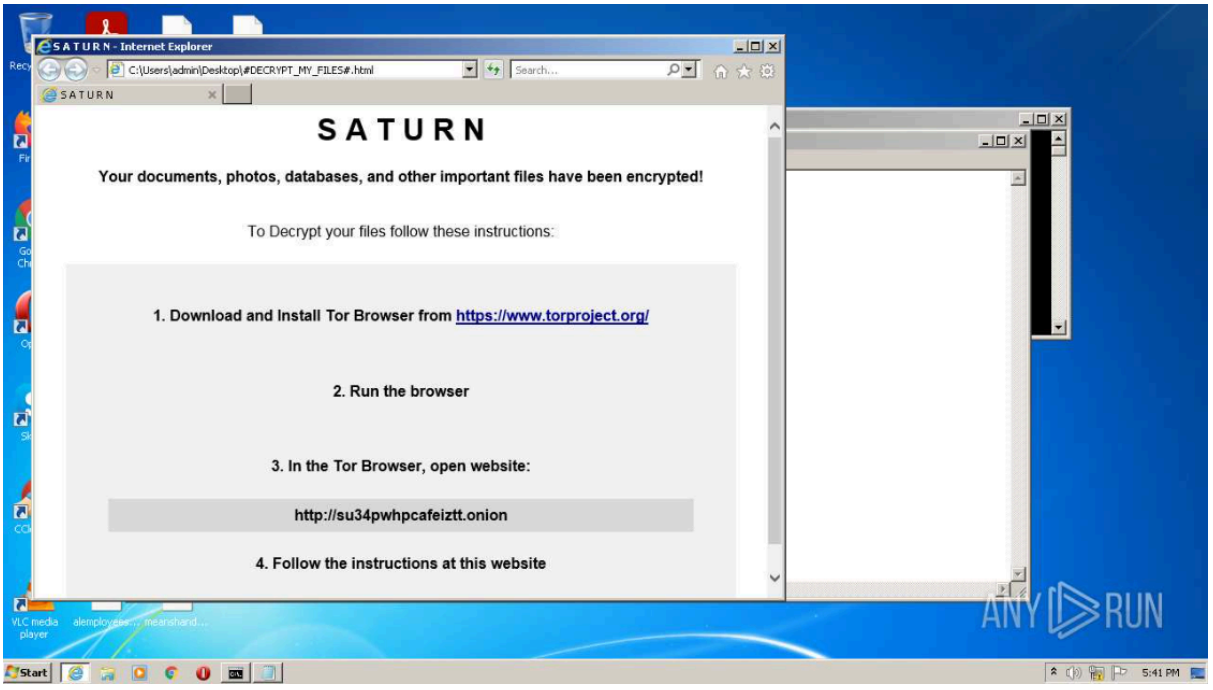


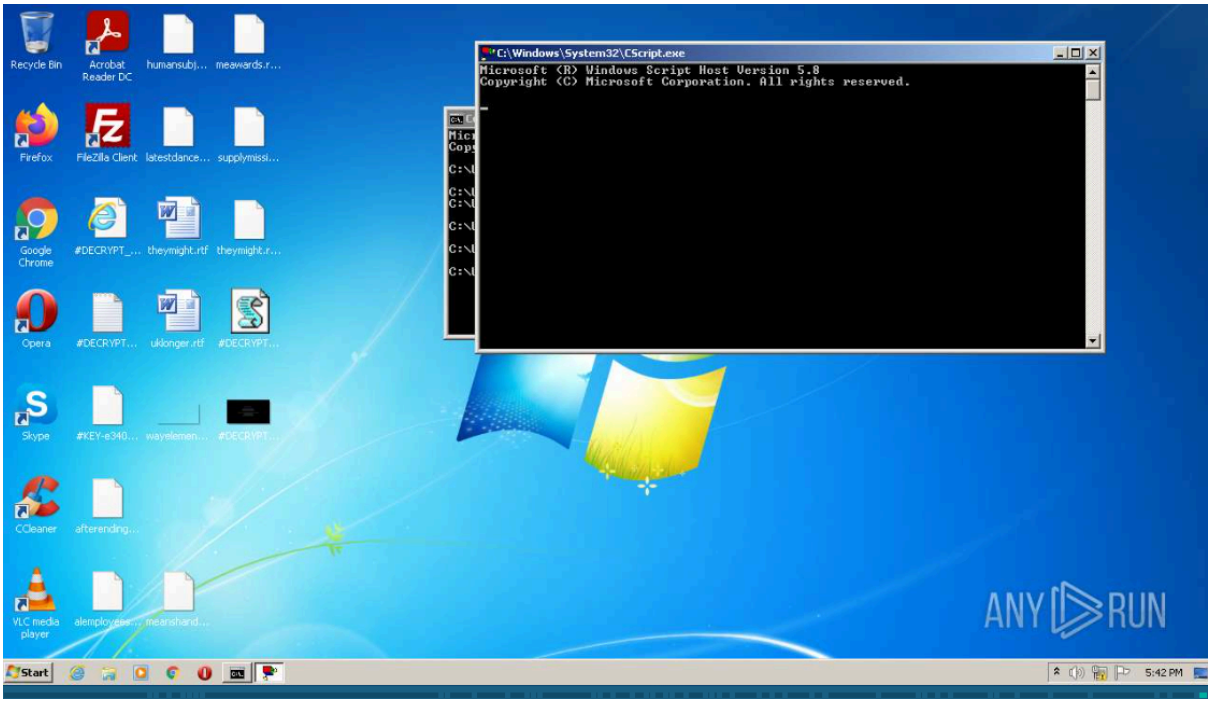
Aquí se muestra como tenemos el escritorio base antes de que el malware empiece a funcionar e infecta el equipo.



Ahí ya vemos que el virus ya se pudo detectar y visualizar


EN English (United States)
Help
Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\admin>C:\Users\admin\Desktop\SATURN_RANSOM.exe
C:\Users\admin>
C:\Users\admin>C:\Users\admin\Desktop\SATURN_RANSOM.exe
User Account Control
Do you want to allow the following program from an unknown publisher to make changes to this computer?
Program name: SATURN_RANSOM.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear
ANY RUN
Start
5:40 PM


SATURN - Internet Explorer
C:\Users\admin\Desktop\#DECRYPT_MY_FILES#.html
SATURN
SATURN
Your documents, photos, databases, and other important files have been encrypted!
To Decrypt your files follow these instructions:
1. Download and Install Tor Browser from https://www.torproject.org/
2. Run the browser
3. In the Tor Browser, open website:
http://su34pwhpcafeiztt.onion
4. Follow the instructions at this website
ANY RUN
Start
5:41 PM



Luego al final del análisis vemos como queda nuestra máquina infectada con archivos desconocidos en nuestro escritorio

Información Estática

El análisis estático de SATURN RANSOM.exe, previo a la ejecución, revela las siguientes características:

- **Tamaño del archivo**: El archivo tiene un tamaño aproximado de 650 KB.
- **Empaquetado**: No se detectó el uso de empaquetadores obvios como UPX. Sin embargo, es probable que el archivo esté ofuscado o que emplee técnicas avanzadas de anti-análisis para evitar ser detectado por soluciones antivirus tradicionales.
- **Secciones del archivo**: Muestra las secciones típicas de un ejecutable PE (Portable Executable), incluyendo `.text`, `.data`, y `.rdata`, sin anomalías evidentes, aunque es probable que se utilicen técnicas de inyección de código dinámico.

Diagrama del proceso del comportamiento

A continuación, un flujo simplificado del comportamiento del ransomware:

- ➢ **Ejecución inicial**: SATURN RANSOM.exe es ejecutado por el usuario.
- ➢ **Desplegado de comandos del sistema**:
  - `vssadmin.exe delete shadows /all /quiet`: Elimina todas las copias de seguridad del sistema.

    - `wbadmin.exe delete catalog`: Borra los catálogos de backup.
    - `bcdedit.exe`: Modifica la configuración de arranque, desactivando la recuperación del sistema.
- ➢ **Cifrado de archivos**: El malware procede a cifrar los archivos del sistema, añadiendo una extensión específica a los archivos comprometidos.
- ➢ **Creación de archivos de rescate**: Archivos como `#DECRYPT_MY_FILES#.txt` y `#DECRYPT_MY_FILES#.html` son creados en múltiples ubicaciones del sistema.
- ➢ **Ejecución de scripts**:
    - `WScript.exe`: Ejecuta scripts en VBScript que muestran mensajes de rescate en pantalla o redirigen al usuario a sitios de pago.
- ➢ **Conexiones externas**: El malware realiza solicitudes HTTP a servidores remotos posiblemente para reportar la infección y gestionar las claves de cifrado.

Eventos asociados

- **Eliminación de copias de seguridad**: Los procesos relacionados con `vssadmin` y `wbadmin` muestran la eliminación de respaldos críticos del sistema.
- **Modificación de configuración de arranque**: El uso de `bcdedit` sugiere la manipulación de políticas del sistema para bloquear la recuperación.
- **Creación de archivos de rescate**: Se observan los procesos relacionados con la creación de los archivos `#DECRYPT_MY_FILES#`.

HTTP Requests

- Se detectaron múltiples solicitudes HTTP, la mayoría relacionadas con actualizaciones de certificados y servicios de Windows, lo que podría ser un encubrimiento de tráfico malicioso.
- Las solicitudes se realizaron principalmente desde procesos `iexplore.exe` y `opera.exe`, sugiriendo que el malware está utilizando navegadores para establecer conexiones de red.

Conexiones

- **Conexiones activas detectadas**: 18 conexiones activas durante la ejecución del malware.
- Las conexiones están asociadas a los procesos `iexplore.exe` y `opera.exe`, que pueden estar actuando como intermediarios para la comunicación con servidores de comando y control (C2).

DNS Requests

- Se realizaron 14 solicitudes DNS, la mayoría relacionadas con servicios de validación de certificados y actualizaciones del sistema.
- No obstante, el uso de múltiples solicitudes DNS sugiere que el malware puede estar empleando técnicas de evasión para comunicarse con el servidor de los atacantes.

Amenazas detectadas

- El comportamiento del ransomware fue categorizado como **malicious activity** por la plataforma ANY.RUN, con indicadores de ransomware altamente destructivo debido a la eliminación de backups y la modificación de las políticas del sistema.

3. conclusiones considerando:

● Comportamiento del malware.

● Nombre general.

● Investigación del malware.

Comportamiento del malware

El comportamiento de **SATURN RANSOM.exe** sigue el patrón clásico de los ransomware modernos:

- ➢ **Eliminación de copias de seguridad**: Elimina todas las vías posibles de restauración de datos locales mediante comandos de administración del sistema.
- ➢ **Cifrado de archivos**: Cifra los archivos de la víctima, haciéndolos inaccesibles sin una clave de descifrado.
- ➢ **Mensaje de rescate**: Deja archivos de texto y HTML en el sistema con instrucciones para la víctima sobre cómo pagar el rescate.
- ➢ **Evasión de recuperación**: Modifica la configuración de arranque del sistema para evitar cualquier intento de restauración durante el proceso de arranque.

Nombre general

El malware analizado pertenece a la categoría **ransomware** y se identifica como **SATURN Ransomware**, una variante conocida que emplea cifrado de archivos y elimina respaldos.

Investigación del malware

Según las investigaciones posteriores a este análisis, **SATURN Ransomware** ha sido reportado en campañas dirigidas a usuarios de Windows, tanto en entornos empresariales como personales. La clave pública utilizada para el cifrado es única para cada infección, lo que imposibilita la recuperación de archivos sin la clave privada. A pesar de que se han desarrollado herramientas de descifrado para variantes anteriores de ransomware, SATURN sigue siendo un riesgo debido a sus complejas técnicas de evasión y manipulación del sistema operativo.

En resumen, SATURN RANSOM.exe representa una amenaza significativa que puede ser mitigada mediante la implementación de políticas adecuadas de respaldo, segmentación de la red, y la educación del usuario.

Análisis del malware con otra de las herramientas() proporcionadas:

1. Hipótesis (basada en los resultados de VirusTotal):

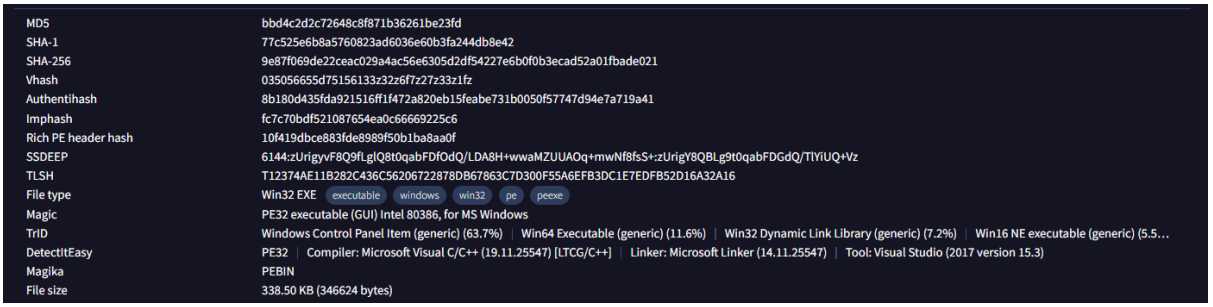
El archivo analizado es una variante de ransomware llamada **SATURN RANSOM.exe.bin**, y la mayoría de los motores antivirus lo detectan como **Troyano/Ransomware**. Esto coincide con ataques previos del ransomware **Saturn**, el cual cifra los datos del usuario y exige un rescate para su liberación. El alto número de detecciones (66/72) sugiere que se trata de una muestra conocida y que probablemente esté relacionada con una campaña de ransomware extendida.

Dada la naturaleza de **Troyano/Ransomware**, es probable que esta muestra esté dirigida a sistemas vulnerables, aprovechando puntos débiles en la seguridad, con el fin de infiltrarse, cifrar los archivos y solicitar un rescate.

---

2. Informe con análisis de la muestra:

- **Nombre de la muestra:** SATURN RANSOM.exe.bin
- **Fecha de análisis:** —---- .
- **OS utilizado:** En en el caso de virus total no podemos ver le windows el cual afecta pero tomo de referencia el windows 7 32-bit del ejemplo
- **MD5 del archivo:** bbd4c2d2c72648c8f871b36261be23fd



MD5	bbd4c2d2c72648c8f871b36261be23fd
SHA-1	77c525e6b8a5760823ad6036e60b3fa244db8e42
SHA-256	9e87f069de22ceac029a4ac56e6305d2df54227e6b0f0b3ecad52a01fbade021
Vhash	035056655d75156133z322f7z27z33z1fz
Authentihash	8b180d435fda921516ff1f472a820eb15feabe731b0050f57747d94e7a719a41
Imphash	fc7c70bdf521087654ea0c66669225c6
Rich PE header hash	10f419dbce883fde8989f50b1ba8aa0f
SSDEEP	6144:zUrigyvF8Q9fLglQ8t0qabFDfOdQ/LDA8H+wwaMZUUAOq+mwNf8fsS+:zUrigY8QBLg9t0qabFDGdQ/TlYiUQ+Vz
TLSH	T12374AE11B282C436C56206722878DB67863C7D300F55A6EFB3DC1E7EDFB52D16A32A16
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Windows Control Panel Item (generic) (63.7%) | Win64 Executable (generic) (11.6%) | Win32 Dynamic Link Library (generic) (7.2%) | Win16 NE executable (generic) (5.5…
DetectItEasy	PE32 | Compiler: Microsoft Visual C/C++ (19.11.25547) [LTCG/C++] | Linker: Microsoft Linker (14.11.25547) | Tool: Visual Studio (2017 version 15.3)
Magika	PEBIN
File size	338.50 KB (346624 bytes)

Información estática:

El archivo tiene un tamaño de **338.50 KB** y es de tipo **.exe**, lo que indica que es un ejecutable diseñado para sistemas Windows. Los análisis estáticos han clasificado el archivo como **Trojan/Ransom/Saturn** por numerosos motores antivirus, incluyendo **Kaspersky, AVG, Microsoft, Avast**, entre otros.

Diagrama de proceso del comportamiento:

El análisis comportamental típico del ransomware Saturn muestra que el proceso principal implica:

1. **Infiltración:** El malware se introduce en el sistema, generalmente a través de correos electrónicos maliciosos o descargas infectadas.
2. **Cifrado de archivos:** Una vez dentro, comienza a cifrar archivos en el disco duro, bloqueando el acceso del usuario.
3. **Solicitud de rescate:** Luego, el malware muestra una nota exigiendo el pago de un rescate, generalmente en criptomonedas.

Eventos asociados:

- **Pérdida de acceso a los archivos:** Debido al cifrado.
- **Creación de archivos de texto o HTML con la nota de rescate.**

HTTP Request y conexiones:

- El ransomware **Saturn** podría conectarse a un servidor de comando y control (C&C) para recibir instrucciones, descargar claves de cifrado o enviar información sobre el sistema comprometido. Estas conexiones suelen ser HTTP o DNS Requests.

DNS Requests:

- Se puede observar que este tipo de malware generalmente intenta resolver nombres de dominio relacionados con el servidor C&C.

Amenazas:

- **Cifrado de archivos del usuario.**
- **Posible robo de información personal o empresarial.**
- **Interrupción de actividades comerciales o personales por el bloqueo del sistema.**

---

3. Conclusiones:

Comportamiento del malware:

El ransomware Saturn sigue un patrón típico de ransomware moderno: cifrado de archivos, creación de una nota de rescate, y petición de un pago en criptomonedas. Es altamente efectivo en comprometer sistemas sin una adecuada protección y ha sido detectado por una amplia gama de motores antivirus.

Nombre general:

Saturn Ransomware, identificado con variantes como **Trojan.Ransom.Saturn**, **Trojan.Win32.Saturn.A**, y **Ransom.Win32.SATURN**.

Investigación del malware:

El ransomware Saturn ha sido activo desde al menos 2018, afectando principalmente sistemas Windows. Generalmente se distribuye mediante correos electrónicos de phishing y utiliza claves RSA para cifrar los archivos de las víctimas. Se recomienda mantener siempre una copia de seguridad y utilizar sistemas de protección proactivos para evitar la infección.