Informe de Análisis de Malware

1) **Hipótesis**:

No se puede determinar el origen y/o el ingreso del malware, por lo que se presenta la siguiente hipótesis al respecto:

El usuario de la computadora infectada puede haber sido víctima de *pishing* (técnica de ingeniería social que utilizan los ciberdelincuentes para la suplantación de identidad) lo cual le facilitó el acceso de su computadora al atacante. Éste último mencionado, posterior a obtener los accesos, preparó el equipo con los programas necesarios dentro del menú de Inicio y el CMD (consola de Windows) para ejecutar el ataque utilizando las credenciales antes obtenidas y de esta manera poder ejecutar el malware logrando encriptar todos los archivos de la pc y de la red a la que se encontraba conectado, destruyendo previamente los archivos de respaldo.

2) Muestra analizada con la herramienta**:** Any.run
   Nombre de la muestra: SATURN_RANSOM.exe
   Fecha: 27 de Abril del 2022 a las 13:39:05
   OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
   MD5: BBD4C2D2C72648C8F871B36261BE23FD

   Comportamiento: MALICIOSO

Path:"C:\Usuarios\admin\Escritorio\SATURN_RANSOM.exe".

El archivo ejecutable SATURN_RAMSOM.exe primero escribe en un archivo del Menú de Inicio, elimina instantáneas (backups) utilizando el comando *wmic.exe shadowcopy delete*, inicia el BCEDIT.exe para deshabilitar

la recuperación, abre un bloc de notas con las instrucciones del rescate y luego suelta el archivo ejecutable una vez que se inicia.

Las acciones parecen robo de datos personales, en donde el archivo soltado contiene instrucciones de ramsomware. Se roban las credenciales de navegadores web y se ejecuta PING.exe para la simulación del retraso.

Información estática:

De acuerdo a lo recolectado de información estática y analizando las extensiones, podemos determinar que los archivos ejecutables (.exe) y las librerías (.dll) estaban preparadas para correr en un Sistema Operativo Windows, ampliando el ataque con versiones para las dos arquitecturas posibles (32x y 64x). Debajo se exponen los tipos de extensión y sus propiedades:

TRiD
.exe | Win64 Executable (generic) (64.6)
.dll | Win32 Dynamic Link Library (generic) (15.4)
.exe | Win32 Executable (generic) (10.5)
.exe | Generic Win/DOS Executable (4.6)
.exe | DOS Executable Generic (4.6)

En la siguiente columna se determina el tipo de máquina (microprocesador) donde podría correr el ejecutable malicioso.

EXIF
EXE
MachineType: Intel 386 or later, and compatibles
TimeStamp: 2018:02:14 20:19:14+01:00
PEType: PE32
LinkerVersion: 14.11

CodeSize: 211968

InitializedDataSize: 137728

UninitializedDataSize: 0

EntryPoint: 0x151bc

OSVersion:6

ImageVersion: 0

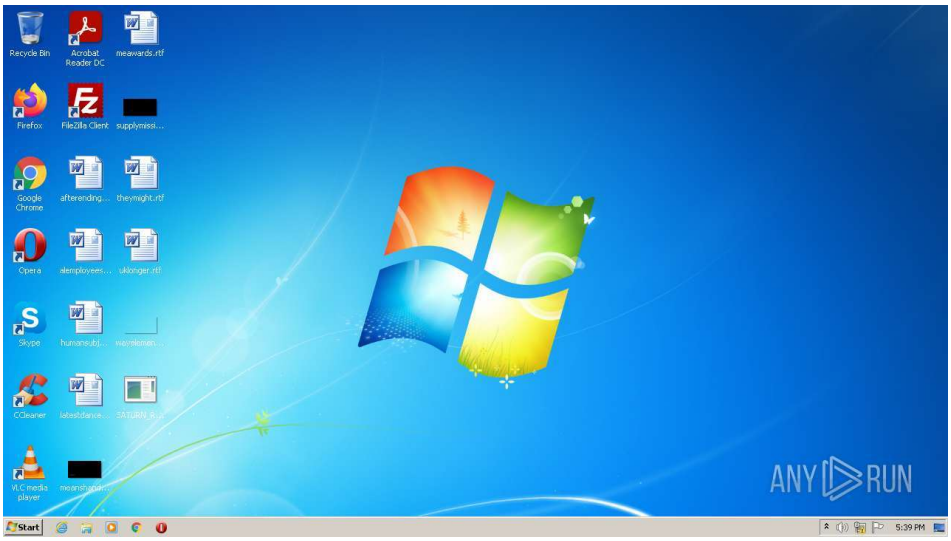
SubsystemVersion: 6

Subsystem: Windows GUI

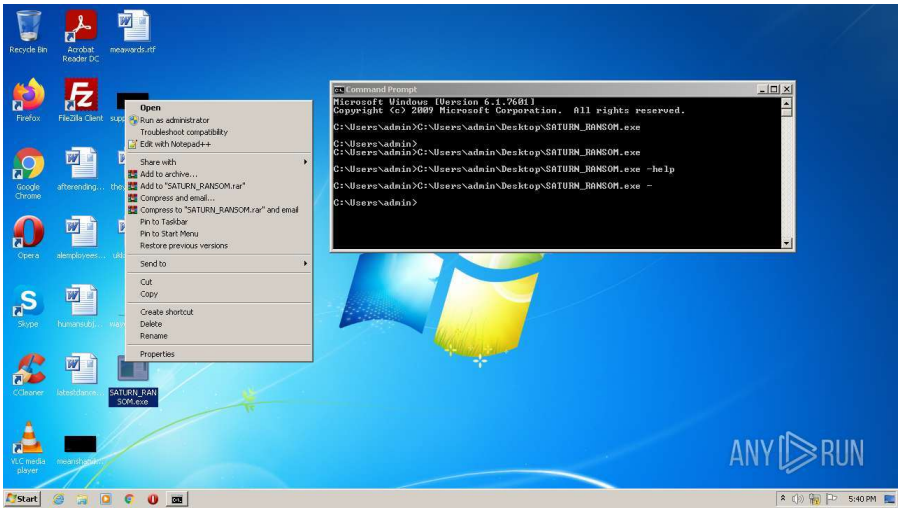
Screenshots del comportamiento:

A continuación, se presentan 3 capturas sobre el comportamiento antes, durante y después de haberse ejecutado el ataque, donde se muestra el mensaje donde se solicita el rescate de los datos cifrados.

Antes:



Durante:



Después:

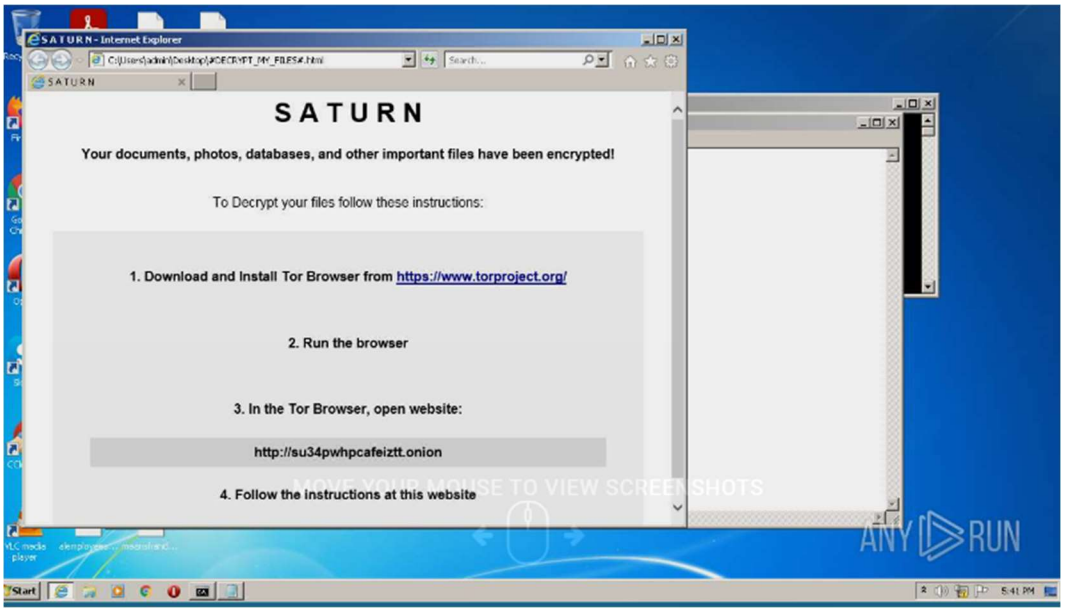
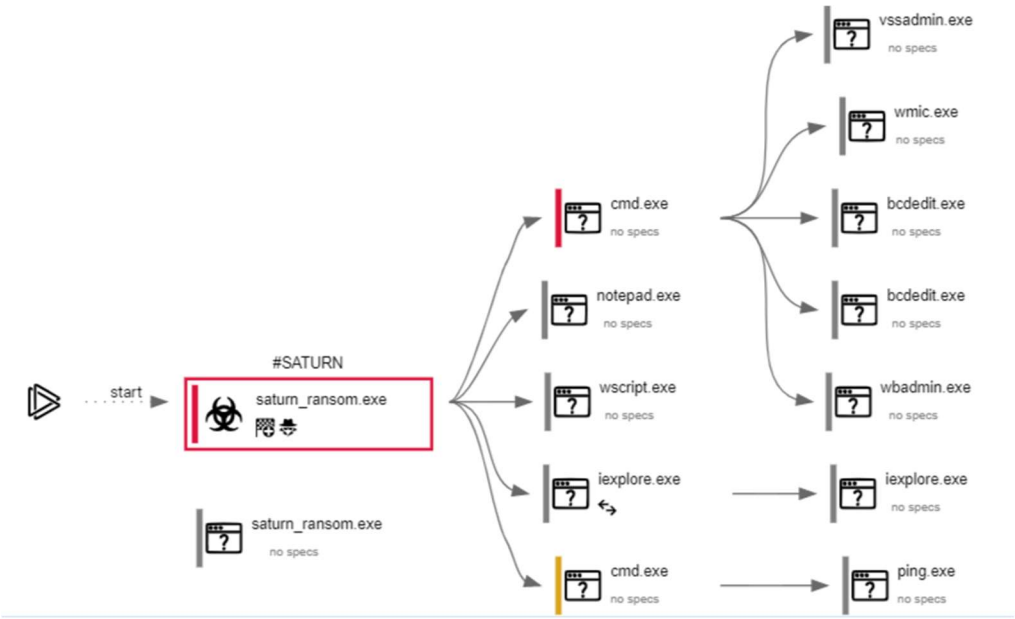


Diagrama de Proceso de Comportamiento:

En el siguiente diagrama de tipo grafo, puede verse de forma gráfica como el archivo malicioso ejecuta sus tareas, servicios y los programas que necesitó para propagarse en la red.



En siguiente cuadro, se muestran algunos de los eventos que se pudieron recolectar del visor de eventos de Windows.

Como puede verse, se ejecutaron un total de 25.502, donde 24.359 fueron lectura de archivos, 636 de escritura y 507 fueron borrados.

Total events	Read events	Write events	Delete events
25 502	24 359	636	507

Modification events

(PID) Process:	(3132) SATURN_RANSOM.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	ProxyBypass
Value:	1		
(PID) Process:	(3132) SATURN_RANSOM.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	IntranetName
Value:	1		
(PID) Process:	(3132) SATURN_RANSOM.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	UNCAsIntranet
Value:	1		
(PID) Process:	(3132) SATURN_RANSOM.exe	Key:	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
Operation:	write	Name:	AutoDetect
Value:	0		
(PID) Process:	(3320) WINWORD.EXE	Key:	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems
Operation:	write	Name:	,o!
Value:	2C6F2100F80C000001000000000000000000000		

Las conexiones que se fueron realizando y se muestran gráficamente en el siguiente cuadro, estuvieron geolocalizadas en nodos ubicados en las ciudades/países que se mencionan a continuación:

- Amsterdam, North Holland, Netherlands.
- Redmond, Washington, United States.
- San Jose, California, United States.
- Frankfurt am Main, Hesse, Germany
- Culver City, California, United States
- Ashburn, Virginia, United States

Fuente de búsqueda: https://ipinfo.io/

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
4048	opera.exe	185.26.182.93:443	certs.opera.com	Opera Software AS	–	suspicious
4048	opera.exe	185.26.182.109:80	redir.opera.com	Opera Software AS	–	unknown
1828	iexplore.exe	13.107.22.200:443	www.bing.com	Microsoft Corporation	US	whitelisted
1828	iexplore.exe	8.252.189.126:80	ctldl.windowsupdate.com	Level 3 Communications, Inc.	US	unknown
1828	iexplore.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
4048	opera.exe	185.26.182.94:443	certs.opera.com	Opera Software AS	–	malicious
1828	iexplore.exe	152.199.19.161:443	r20swj13mr.microsoft.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
4048	opera.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
–	–	185.26.182.93:443	certs.opera.com	Opera Software AS	–	suspicious
4048	opera.exe	142.250.185.174:80	clients1.google.com	Google Inc.	US	whitelisted

En el siguiente cuadro, se muestran las solicitudes de HTTP realizadas a los servidores web. Se puede visualizar el método utilizado (GET) y las URLs que se ejecutaron.

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1828	iexplore.exe	GET	200	8.252.189.126:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?ed8446c2897ba05c	US	compressed	4.70 Kb	whitelisted
1828	iexplore.exe	GET	200	8.252.189.126:80	http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?d5e84181f228487d	US	compressed	4.70 Kb	whitelisted
4048	opera.exe	GET	200	185.26.182.109:80	http://redir.opera.com/favicons/google/favicon.ico	unknown	image	5.30 Kb	whitelisted
4048	opera.exe	GET	200	142.250.185.174:80	http://clients1.google.com/complete/search?q=su34pwhpcafeiztt&client=opera-suggest-search&hl=de	US	text	43 b	whitelisted
4048	opera.exe	GET	200	93.184.220.29:80	http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl	US	der	592 b	whitelisted
1828	iexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8gIGmZT9XHrHiJQeI%3D	US	der	1.47 Kb	whitelisted
1828	iexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	US	der	471 b	whitelisted

En el siguiente cuadro, se pueden observar las peticiones realizadas al servidor de nombres de dominio que llevó a cabo el malware durante su ejecución.

DNS requests

Domain	IP	Reputation
api.bing.com	13.107.5.80	whitelisted
www.bing.com	131.253.33.200 13.107.22.200	whitelisted
ctldl.windowsupdate.com	8.252.189.126 67.26.163.254 8.252.188.126 8.250.188.126 67.26.161.254	whitelisted
ocsp.digicert.com	93.184.220.29	whitelisted
certs.opera.com	185.26.182.94 185.26.182.93	whitelisted
r20swj13mr.microsoft.com	152.199.19.161	whitelisted
iecvlist.microsoft.com	152.199.19.161	whitelisted
su34pwhpcafeiztt.onion	–	unknown
clients1.google.com	142.250.185.174	whitelisted
redir.opera.com	185.26.182.109 185.26.182.110	whitelisted

Las amenazas detectadas y expuestas en el siguiente cuadro, hacen referencia a las redes TOR (The Onion Router) por la extensión .onion detectada.

Dicha red de cebolla, es posiblemente la principal y más conocida Darknet de Internet. El objetivo de este proyecto es el de crear una red de comunicaciones distribuida y superpuesta al Internet convencional. Las Dark Webs que puedes encontrar en la Darknet de TOR se diferencian por tener el dominio .onion.

amenazas

PID	Proceso	Clase	Mensaje
–	–	Posible violación de la privacidad corporativa	POLÍTICA ET Consulta de DNS para dominio oculto TOR .onion accesible a través de TOR
–	–	Posible violación de la privacidad corporativa	AV POLICY Consulta de DNS para el dominio .onion a través de TOR, no Google

3) **Conclusiones**:

Comportamiento del malware: CIFRADO DE DATOS sin posibilidad de recuperación.

Nombre del Malware: SATURN

Origen del Nombre: La han bautizado con el nombre de Saturn, ya que añade esta extensión a todos aquellos archivos del sistema que se ven afectados por su cifrado.

Tipo de Malware: Ramsomware.

Información del Malware:

Su descubrimiento fue en el año 2018, donde el mismo ataca a equipos de particulares como de empresas.

Por el momento no está del todo claro cuál es su método de difusión, pero se pide extremar las precauciones con esta amenaza ya que su accionar deja irrecuperables los archivos sino se tiene una copia de seguridad reciente.

Un dato más, es que la amenaza una vez instalada en el sistema, realiza una serie de comprobaciones para cerciorarse del entorno. Otras realizan esto antes de instalarse en el sistema para evitar dejar pistas del funcionamiento.

Fecha: 01/10/2022

Analista de Ciberseguridad: Galvalisi Elvis