Proyecto Final Primera Entrega

Dato fuente de información

Para elaborar este informe, fueron analizadas las siguientes fuentes de información:

• Informe de estatus de situación actual.

• Muestra de informe entregado por el equipo de soporte técnico de Corporación Acme.

Análisis del malware

El presente informe responde a la necesidad de conocer el alcance del incidente de seguridad provocado por el cifrado masivo de archivos (ransomware) en la infraestructura de LexCorp, identificado del 20 al 23 de junio de 2021. Con base en las actuaciones de respuesta, los técnicos de Corporación Acme tomaron las medidas de contención que consideraron necesarias y llevaron a cabo la restauración de los sistemas afectados por el ataque. Como resultado del análisis de malware, se ha identificado lo siguiente:

Muestra analizada con Any.Run

Nombre de la muestra	SATURN_RAMSOM.exe
Fecha del análisis	28/9/22, 22:04:49
OS utilizado para análisis	Windows 7 Professional Service Pack 1 (build 7601, 32 bits)
MD5	**BBD4C2D2C72648C8F871B36261BE23FD**

Comportamiento:

MALICIOUS

Writes to a start menu file
- SATURN_RANSOM.exe (PID: 3132)

Deletes shadow copies
- cmd.exe (PID: 2936)

Starts BCDEDIT.EXE to disable recovery
- cmd.exe (PID: 2936)

Saturn ransom note found
- SATURN_RANSOM.exe (PID: 3132)

Drops executable file immediately after starts
- SATURN_RANSOM.exe (PID: 3132)

Dropped file may contain instructions of ransomware
- SATURN_RANSOM.exe (PID: 3132)

Steals credentials from Web Browsers
- SATURN_RANSOM.exe (PID: 3132)

Actions looks like stealing of personal data
- SATURN_RANSOM.exe (PID: 3132)

Runs PING.EXE for delay simulation
- cmd.exe (PID: 2996)

SUSPICIOUS

Reads the computer name
- SATURN_RANSOM.exe (PID: 3132)
- WMIC.exe (PID: 3688)
- SATURN_RANSOM.exe (PID: 2468)
- SATURN_RANSOM.exe (PID: 3396)
- SATURN_RANSOM.exe (PID: 3472)
- SATURN_RANSOM.exe (PID: 2028)
- SATURN_RANSOM.exe (PID: 3432)
- SATURN_RANSOM.exe (PID: 2524)
- SATURN_RANSOM.exe (PID: 2104)
- SATURN_RANSOM.exe (PID: 2452)
- SATURN_RANSOM.exe (PID: 1724)
- WScript.exe (PID: 3524)
- WScript.exe (PID: 2084)
- WScript.exe (PID: 3136)
- CScript.exe (PID: 2460)

Checks supported languages
- SATURN_RANSOM.exe (PID: 3132)
- cmd.exe (PID: 2936)
- WMIC.exe (PID: 3688)
- SATURN_RANSOM.exe (PID: 3472)
- SATURN_RANSOM.exe (PID: 3396)
- SATURN_RANSOM.exe (PID: 2468)
- SATURN_RANSOM.exe (PID: 3432)
- cmd.exe (PID: 1996)
- SATURN_RANSOM.exe (PID: 2524)
- SATURN_RANSOM.exe (PID: 2028)
- SATURN_RANSOM.exe (PID: 2104)
- SATURN_RANSOM.exe (PID: 1724)
- SATURN_RANSOM.exe (PID: 2452)
- cmd.exe (PID: 2996)
- WScript.exe (PID: 3524)
- WScript.exe (PID: 3136)
- WScript.exe (PID: 2084)
- CScript.exe (PID: 2460)

INFO

Reads the computer name
- vssadmin.exe (PID: 3636)
- wbadmin.exe (PID: 2396)
- WINWORD.EXE (PID: 3320)
- WINWORD.EXE (PID: 2976)
- iexplore.exe (PID: 1828)
- PING.EXE (PID: 4048)
- iexplore.exe (PID: 2440)
- opera.exe (PID: 4048)

Checks supported languages
- vssadmin.exe (PID: 3636)
- bcdedit.exe (PID: 292)
- bcdedit.exe (PID: 1984)
- wbadmin.exe (PID: 2396)
- WINWORD.EXE (PID: 3320)
- rundll32.exe (PID: 1268)
- WINWORD.EXE (PID: 2976)
- iexplore.exe (PID: 1828)
- NOTEPAD.EXE (PID: 4056)
- PING.EXE (PID: 4048)
- iexplore.exe (PID: 2440)
- opera.exe (PID: 4048)

Manual execution by user
- SATURN_RANSOM.exe (PID: 3472)
- SATURN_RANSOM.exe (PID: 2468)
- SATURN_RANSOM.exe (PID: 3396)
- cmd.exe (PID: 1996)
- SATURN_RANSOM.exe (PID: 1724)
- SATURN_RANSOM.exe (PID: 3916)
- WINWORD.EXE (PID: 3320)
- SATURN_RANSOM.exe (PID: 3652)
- SATURN_RANSOM.exe (PID: 2452)
- rundll32.exe (PID: 1268)
- WINWORD.EXE (PID: 2976)
- opera.exe (PID: 4048)

Reads Windows Product ID
- SATURN_RANSOM.exe (PID: 3132)
- SATURN_RANSOM.exe (PID: 2468)
- SATURN_RANSOM.exe (PID: 3396)
- SATURN_RANSOM.exe (PID: 3472)
- SATURN_RANSOM.exe (PID: 2028)
- SATURN_RANSOM.exe (PID: 3432)
- SATURN_RANSOM.exe (PID: 2524)
- SATURN_RANSOM.exe (PID: 2104)
- SATURN_RANSOM.exe (PID: 1724)
- SATURN_RANSOM.exe (PID: 2452)

Reads the date of Windows installation
- SATURN_RANSOM.exe (PID: 3132)
- SATURN_RANSOM.exe (PID: 2468)
- SATURN_RANSOM.exe (PID: 3396)
- SATURN_RANSOM.exe (PID: 3472)
- SATURN_RANSOM.exe (PID: 3432)
- SATURN_RANSOM.exe (PID: 2524)
- SATURN_RANSOM.exe (PID: 2028)
- SATURN_RANSOM.exe (PID: 2104)
- SATURN_RANSOM.exe (PID: 1724)
- SATURN_RANSOM.exe (PID: 2452)

Starts CMD.EXE for commands execution
- SATURN_RANSOM.exe (PID: 3132)

Drops a file with a compile date too recent
- SATURN_RANSOM.exe (PID: 3132)

Creates files in the user directory
- SATURN_RANSOM.exe (PID: 3132)
- WScript.exe (PID: 3524)

Reads the cookies of Mozilla Firefox
- SATURN_RANSOM.exe (PID: 3132)

Creates files in the program directory
- SATURN_RANSOM.exe (PID: 3132)

- WScript.exe (PID: 3136)
- CScript.exe (PID: 2460)
- WScript.exe (PID: 2084)

Dropped object may contain TOR URL's
- SATURN_RANSOM.exe (PID: 3132)

Creates files in the user directory
- WINWORD.EXE (PID: 3320)
- WINWORD.EXE (PID: 2976)
- iexplore.exe (PID: 1828)
- opera.exe (PID: 4048)

Checks Windows Trust Settings
- WScript.exe (PID: 3524)
- iexplore.exe (PID: 1828)
- WScript.exe (PID: 3136)
- WScript.exe (PID: 2084)
- CScript.exe (PID: 2460)

Changes internet zones settings
- iexplore.exe (PID: 1828)

Application launched itself
- iexplore.exe (PID: 1828)

Reads Microsoft Office registry keys
- WINWORD.EXE (PID: 3320)
- WINWORD.EXE (PID: 2976)

Reads settings of System Certificates
- iexplore.exe (PID: 1828)

Check for Java to be installed
- opera.exe (PID: 4048)

Reads internet explorer settings
- iexplore.exe (PID: 2440)

Dropped object may contain Bitcoin addresses
- opera.exe (PID: 4048)

Creates files like Ransomware instruction
- SATURN_RANSOM.exe (PID: 3132)

Executes scripts
- SATURN_RANSOM.exe (PID: 3132)

Starts CMD.EXE for self-deleting
- SATURN_RANSOM.exe (PID: 3132)

Starts Internet Explorer
- SATURN_RANSOM.exe (PID: 3132)

Reads Microsoft Outlook installation path
- iexplore.exe (PID: 2440)

Reads the date of Windows installation
- iexplore.exe (PID: 1828)
- opera.exe (PID: 4048)

Información Estática encontrada:

.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)

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:
null

EntryPoint:
0x151BC

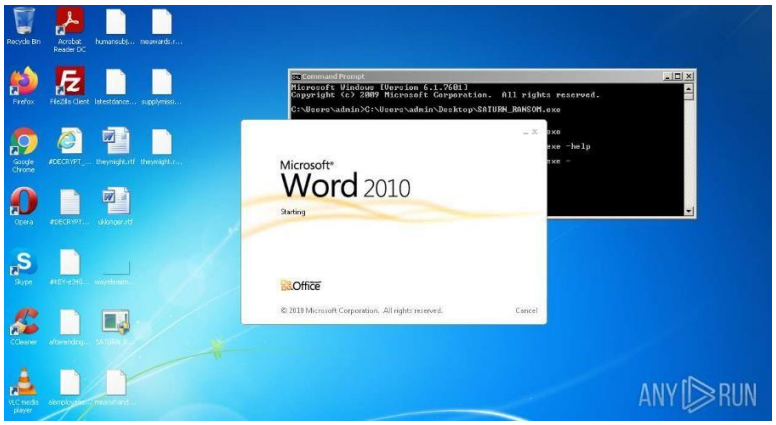
OSVersion:
6

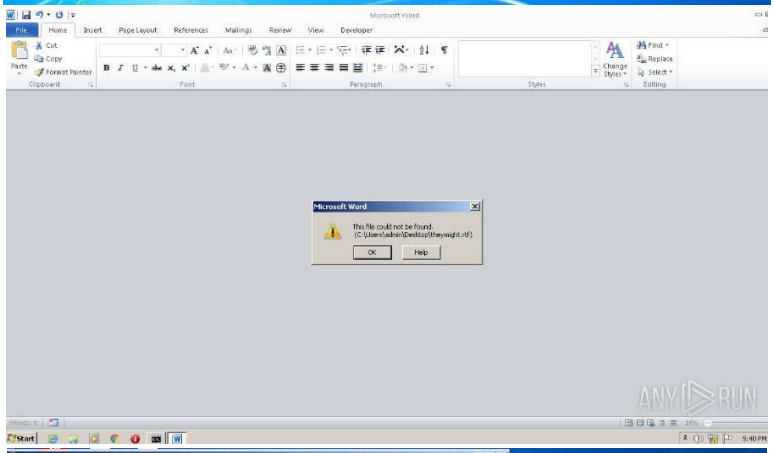
ImageVersion:
null

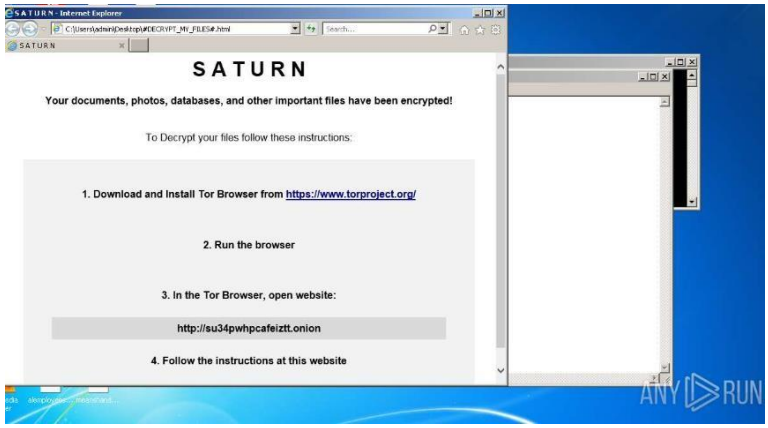
SubsystemVersion:
6

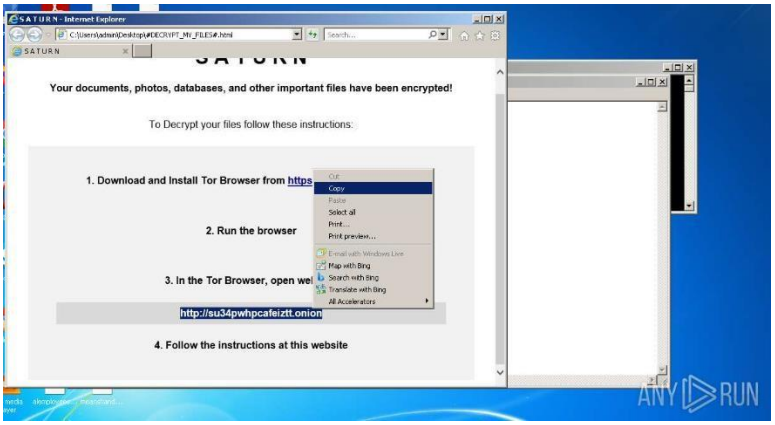
Subsystem:
Windows GUI

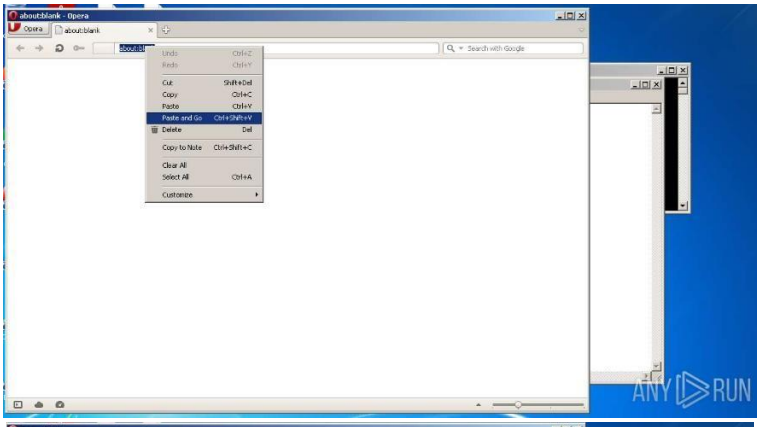
Screenshots de la simulación:

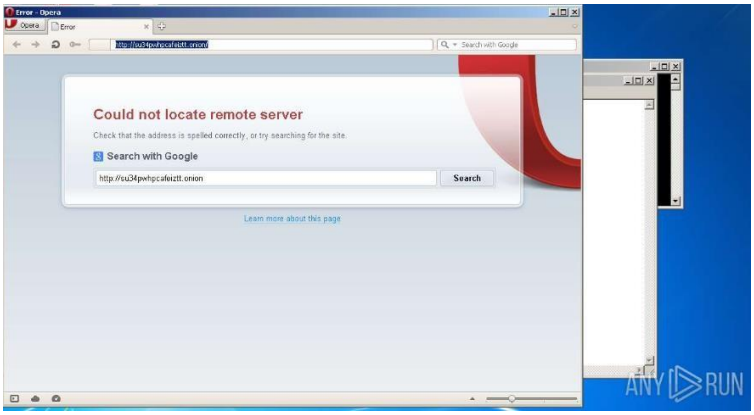

Microsoft Word 2010
Starting
Office
© 2010 Microsoft Corporation. All rights reserved.
Cancel
ANY RUN

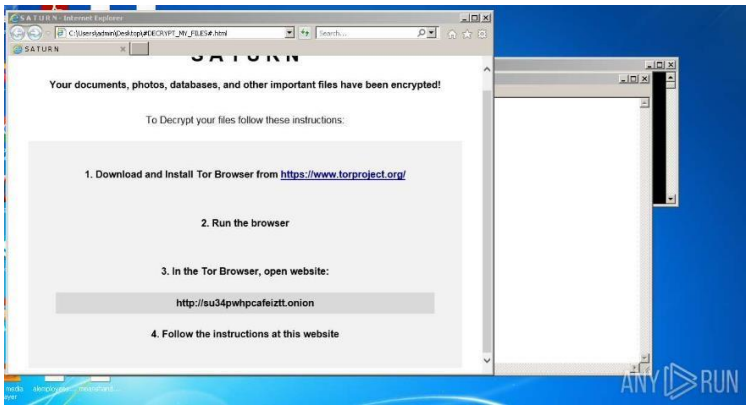

Microsoft Word
This file could not be found.
(C:\Users\admin\Desktop\theymight.rtf)
OK
Help
ANY RUN


SATURN - Internet Explorer
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


SATURN - Internet Explorer
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
2. Run the browser
3. In the Tor Browser, open wel
http://su34pwhpcafeiztt.onion
4. Follow the instructions at this website
Copy
Select all
Print...
Print preview...
ANY RUN


aboutblank - Opera
Opera
aboutblank
Undo Ctrl+Z
Redo Ctrl+Y
Cut Shift+Del
Copy Ctrl+C
Paste Ctrl+V
Paste and Go Ctrl+Shift+V
Delete Del
Copy to Note Ctrl+Shift+C
Clear All
Select All Ctrl+A
Customize
Search with Google
ANY RUN


Error - Opera
Opera
Error
Search with Google
Could not locate remote server
Check that the address is spelled correctly, or try searching for the site.
Search with Google
http://su34pwhpcafeiztt.onion
Search
Learn more about this page
ANY RUN


SATURN - Internet Explorer
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

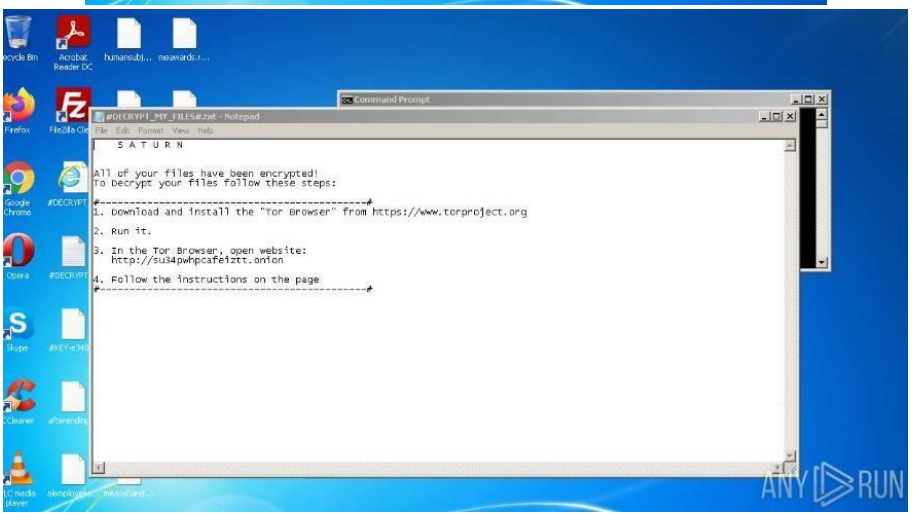
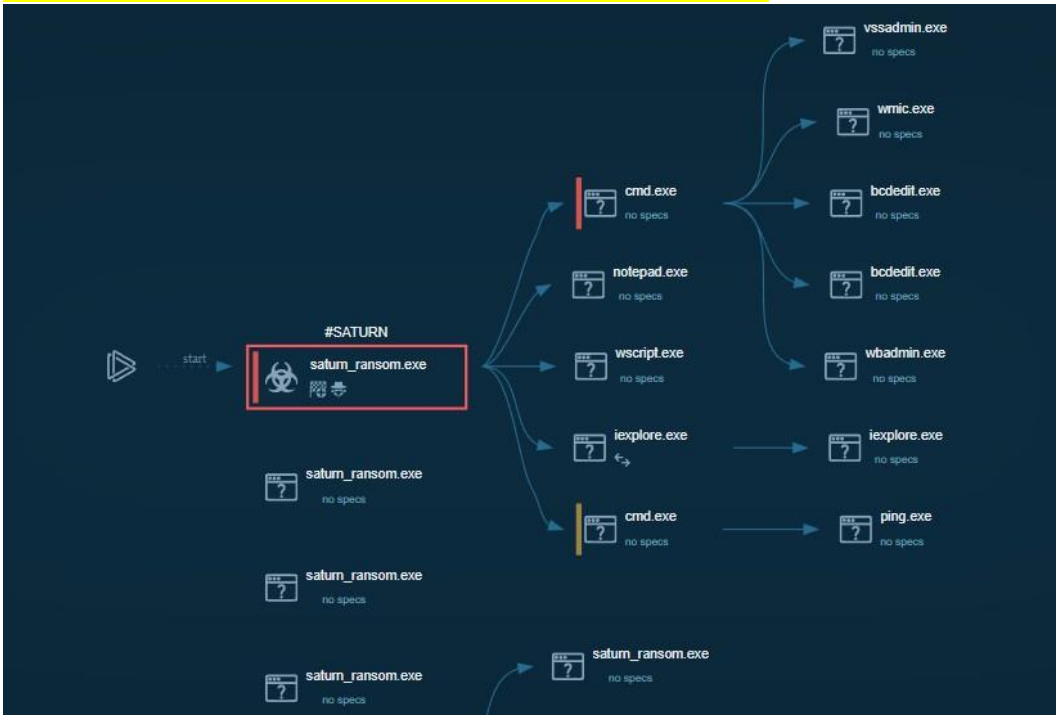
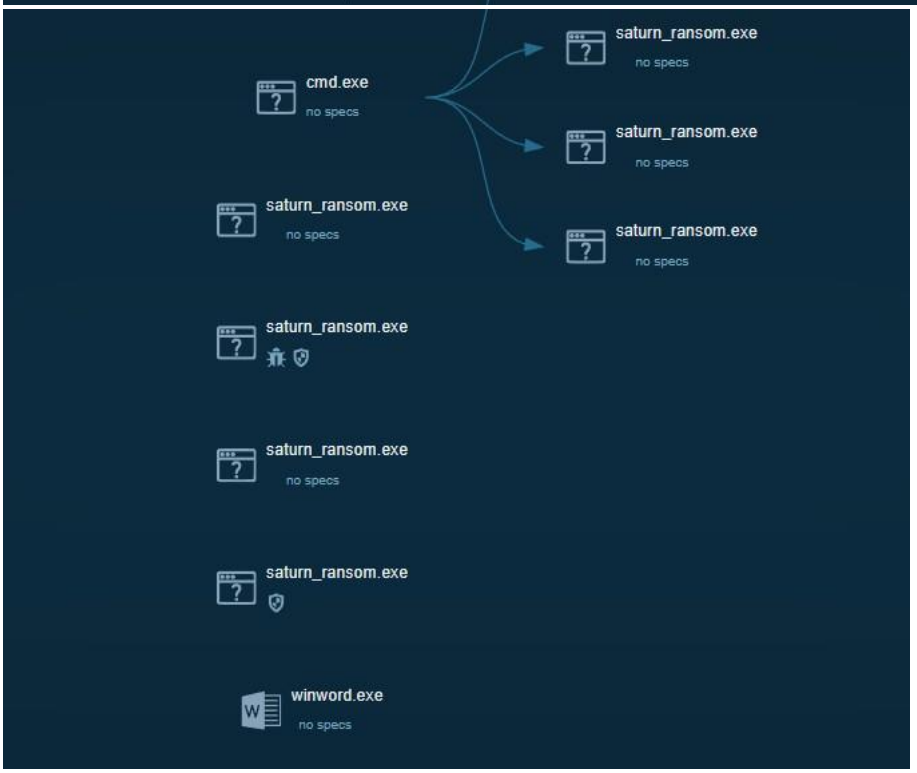

Command Prompt
#DECRYPT_MY_FILES#.txt - Notepad
File Edit Format View Help
S A T U R N
All of your files have been encrypted!
To Decrypt your files follow these steps:
#---#
1. Download and Install the "Tor Browser" from https://www.torproject.org
2. Run it.
3. In the Tor Browser, open website:
http://su34pwhpcafeiztt.onion
4. Follow the instructions on the page
#---#
ANY RUN

Diagrama de procesos de comportamiento:





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:	2C6F2100F80C0000010000000000000000000000		
(PID) Process:	(3320) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1033
Value:	Off		
(PID) Process:	(3320) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1041
Value:	Off		
(PID) Process:	(3320) WINWORD.EXE	**Key:**	HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages
Operation:	write	**Name:**	1046
Value:	Off		

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
1828	iexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Ull8glGmZT9XHrHiJQel%3D	US	der	1.47 Kb	whitelisted
1828	iexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	US	der	471 b	whitelisted
4048	opera.exe	GET	200	142.250.185.174:80	http://clients1.google.com/complete/search?q=su34pwhpcafeizzt&client=opera-suggest-search&hl=de	US	text	43 b	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	93.184.220.29:80	http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl	US	der	592 b	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
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
—	—	185.26.182.93:443	certs.opera.com	Opera Software AS	—	suspicious
4048	opera.exe	185.26.182.93:443	certs.opera.com	Opera Software AS	—	suspicious
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	142.250.185.174:80	clients1.google.com	Google Inc.	US	whitelisted
4048	opera.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
4048	opera.exe	185.26.182.109:80	redir.opera.com	Opera Software AS	—	unknown

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	–	malicious
clients1.google.com	142.250.185.174	whitelisted
redir.opera.com	185.26.182.109 185.26.182.110	whitelisted

Conclusiones:

Comportamiento del Malware:

Saturn es un virus encriptador y secuestrador de equipos que, una vez dentro, cifra los archivos almacenados y pide un rescate.

Nombre general:

Saturn

Investigación del malware:

SATURN_RANSOM.exe

Tipo de malware:

Ransomware

Información sobre Saturn:

Este ransomware fue descubierto por primera vez por MalwareHunterTeam, simula un encriptado de archivos del usuario una vez se ejecuta el programa.
El mismo muestra los archivos que se encriptan mientras completa una serie de pasos que el usuario puede seguir.

Hipótesis:

Como ya se ha mencionado, saturn fue descubierto por primera vez por MalwareHunterTeam, es un virus encriptador y secuestrador de equipos que, una vez dentro, cifra los archivos almacenados y pide un rescate. Durante la encriptación, Saturn añade la extensión “. saturn" a los nombres de archivo (por ejemplo, "**sample.jpg**" pasaría a llamarse "**sample.jpg.saturn**"). A partir de ese momento, los archivos se vuelven inutilizables. Una vez se ha completado la encriptación, Saturn crea cinco archivos ("**#DECRYPT_MY_FILES#.vbs", "#DECRYPT_MY_FILES.BMP**" [configurado como fondo de escritorio],

"**#DECRYPT_MY_FILES#.txt", "#DECRYPT_MY_FILES#.html**" y "**#KEY-dea23dbdbbfeba538e0c3aac3751331d.KEY**") y los coloca en el escritorio. Los archivos BMP, TXT y HTML contienen el texto donde se pide una recompensa.

Hay que mencionar que Saturn está disponible como servicio generador de cibersecuestros RaaS - 'Ransomware as a Service'. Asimismo, este software malicioso es gratuito y anima a los ciberlincuentes a descargarlo en su sitio web en la internet oscura. Normalmente, los proveedores de RaaS exigen un pago determinado por adelantado. Los desarrolladores de Saturn ofrecen a los distribuidores (aspirantes a ciberdelincuentes) propagar el software malicioso y recibir un 70 % de los pagos recibidos a cambio. El resto (30%) va a los desarrolladores de Saturn. Este modelo de negocio es muy atractivo para los desarrolladores, puesto que el esfuerzo vertido en la distribución es mínimo; otras personas hacen el trabajo por ellos. Los desarrolladores se limitan a compartir los pagos recibidos.

Los nuevos archivos contienen mensajes que informan a las víctimas del cifrado y les instan a pagar una recompensa a cambio de descifrar los archivos. Aunque no se sabe actualmente si Saturn usa criptografía simétrica o asimétrica, se requiere en el descifrado una clave única para cada víctima. Esas claves son almacenadas en un servidor remoto controlado por los ciberdelincuentes de Saturn y las víctimas deben pegar un rescate para recibirlas. El coste del descifrado es $300 en Bitcoins; sin embargo, el pago debe realizarse en 7 días; de lo contrario, el coste se duplicará. En un mes, los archivos se habrán destruido de forma permanente. A pesar de las amenazas y exigencias, le recomendamos encarecidamente hacer caso omiso a esas peticiones de pago. Los estudios ponen de manifiesto que los ciberdelincuentes ignoran a las víctimas una vez que se ha realizado el pago del rescate. Con otras palabras, no conseguirá probablemente nada con pagar y será estafado. Le recomendamos que no contacte con esa gente ni realice ningún pago. Por desgracia, no hay herramientas capaces de restaurar los archivos encriptados por Saturn. La única solución es restaurarlo todo desde una copia de respaldo.

En cuanto a la incógnita de ¿Cómo llego el virus a mi red? La respuesta puede ser bastante simple, los virus de tipo criptográfico se propagan de distintas formas; sin embargo, las más comunes son: correos basura, fuentes de descarga de terceros, herramientas de actualización de software fraudulentas y troyanos. Algunos mensajes de correo basura contienen adjuntos maliciosos (p. ej. documentos MS Office, archivos JavaScript, etc.) que cuando se abren, descargan e instalan malware. Fuentes de descarga no oficiales (redes P2P, portales de alojamiento de archivos y otras fuentes de descarga no oficiales) propagan el software malicioso a través de ejecutables maliciosos como software legítimo. Se engaña a los usuarios para que descarguen e instalen software malicioso. Las herramientas de actualización de software falso infectan el sistema aprovechándose de errores en versiones de software antiguas o instalando malware en vez de la aplicación seleccionada.

Para evitar infectar la red con este virus las recomendaciones son tener mucho cuidado al navegar por internet, no abrir nunca adjuntos recibidos de direcciones de email sospechosas; eliminar estos emails sin leerlos, descargar sus aplicaciones de fuentes fiables a través de un enlace de descarga directo, mantener actualizado el software instalado y usar una solución antivirus o antiespía fiable.