

# 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_RAMDOM.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	<b>BBD4C2D2C72648C8F871B36261BE23FD</b>

# Comportamiento:

MALICIOUS	SUSPICIOUS	INFO
<p><b>Writes to a start menu file</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Deletes shadow copies</b></p> <ul style="list-style-type: none"><li>• cmd.exe (PID: 2936)</li></ul> <p><b>Starts BCDEDIT.EXE to disable recovery</b></p> <ul style="list-style-type: none"><li>• cmd.exe (PID: 2936)</li></ul> <p><b>Saturn ransom note found</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Drops executable file immediately after starts</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Dropped file may contain instructions of ransomware</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Steals credentials from Web Browsers</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Actions looks like stealing of personal data</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Runs PING.EXE for delay simulation</b></p> <ul style="list-style-type: none"><li>• cmd.exe (PID: 2996)</li></ul>	<p><b>Reads the computer name</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li><li>• WMIC.exe (PID: 3688)</li><li>• SATURN_RANSOM.exe (PID: 2468)</li><li>• SATURN_RANSOM.exe (PID: 3396)</li><li>• SATURN_RANSOM.exe (PID: 3472)</li><li>• SATURN_RANSOM.exe (PID: 2028)</li><li>• SATURN_RANSOM.exe (PID: 3432)</li><li>• SATURN_RANSOM.exe (PID: 2524)</li><li>• SATURN_RANSOM.exe (PID: 2104)</li><li>• SATURN_RANSOM.exe (PID: 2452)</li><li>• SATURN_RANSOM.exe (PID: 1724)</li><li>• WScript.exe (PID: 3524)</li><li>• WScript.exe (PID: 2084)</li><li>• WScript.exe (PID: 3136)</li><li>• CScript.exe (PID: 2460)</li></ul> <p><b>Checks supported languages</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li><li>• cmd.exe (PID: 2936)</li><li>• WMIC.exe (PID: 3688)</li><li>• SATURN_RANSOM.exe (PID: 3472)</li><li>• SATURN_RANSOM.exe (PID: 3396)</li><li>• SATURN_RANSOM.exe (PID: 2468)</li><li>• SATURN_RANSOM.exe (PID: 3432)</li><li>• cmd.exe (PID: 1996)</li><li>• SATURN_RANSOM.exe (PID: 2524)</li><li>• SATURN_RANSOM.exe (PID: 2028)</li><li>• SATURN_RANSOM.exe (PID: 2104)</li><li>• SATURN_RANSOM.exe (PID: 1724)</li><li>• SATURN_RANSOM.exe (PID: 2452)</li><li>• cmd.exe (PID: 2996)</li><li>• WScript.exe (PID: 3524)</li><li>• WScript.exe (PID: 3136)</li><li>• WScript.exe (PID: 2084)</li><li>• CScript.exe (PID: 2460)</li></ul> <p><b>Reads Windows Product ID</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li><li>• SATURN_RANSOM.exe (PID: 2468)</li><li>• SATURN_RANSOM.exe (PID: 3396)</li><li>• SATURN_RANSOM.exe (PID: 3472)</li><li>• SATURN_RANSOM.exe (PID: 2028)</li><li>• SATURN_RANSOM.exe (PID: 3432)</li><li>• SATURN_RANSOM.exe (PID: 2524)</li><li>• SATURN_RANSOM.exe (PID: 2104)</li><li>• SATURN_RANSOM.exe (PID: 1724)</li><li>• SATURN_RANSOM.exe (PID: 2452)</li></ul> <p><b>Reads the date of Windows installation</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li><li>• SATURN_RANSOM.exe (PID: 2468)</li><li>• SATURN_RANSOM.exe (PID: 3396)</li><li>• SATURN_RANSOM.exe (PID: 3472)</li><li>• SATURN_RANSOM.exe (PID: 3432)</li><li>• SATURN_RANSOM.exe (PID: 2524)</li><li>• SATURN_RANSOM.exe (PID: 2028)</li><li>• SATURN_RANSOM.exe (PID: 2104)</li><li>• SATURN_RANSOM.exe (PID: 1724)</li><li>• SATURN_RANSOM.exe (PID: 2452)</li></ul> <p><b>Starts CMD.EXE for commands execution</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Drops a file with a compile date too recent</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Creates files in the user directory</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li><li>• WScript.exe (PID: 3524)</li></ul> <p><b>Reads the cookies of Mozilla Firefox</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Creates files in the program directory</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Creates files like Ransomware instruction</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Executes scripts</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Starts CMD.EXE for self-deleting</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Starts Internet Explorer</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Reads Microsoft Outlook installation path</b></p> <ul style="list-style-type: none"><li>• iexplore.exe (PID: 2440)</li></ul>	<p><b>Reads the computer name</b></p> <ul style="list-style-type: none"><li>• vssadmin.exe (PID: 3636)</li><li>• wbadmin.exe (PID: 2396)</li><li>• WINWORD.EXE (PID: 3320)</li><li>• WINWORD.EXE (PID: 2976)</li><li>• iexplore.exe (PID: 1828)</li><li>• PING.EXE (PID: 4048)</li><li>• iexplore.exe (PID: 2440)</li><li>• opera.exe (PID: 4048)</li></ul> <p><b>Checks supported languages</b></p> <ul style="list-style-type: none"><li>• vssadmin.exe (PID: 3636)</li><li>• bcdedit.exe (PID: 292)</li><li>• bcdedit.exe (PID: 1984)</li><li>• wbadmin.exe (PID: 2396)</li><li>• WINWORD.EXE (PID: 3320)</li><li>• rundll32.exe (PID: 1268)</li><li>• WINWORD.EXE (PID: 2976)</li><li>• iexplore.exe (PID: 1828)</li><li>• NOTEPAD.EXE (PID: 4056)</li><li>• PING.EXE (PID: 4048)</li><li>• iexplore.exe (PID: 2440)</li><li>• opera.exe (PID: 4048)</li></ul> <p><b>Manual execution by user</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3472)</li><li>• SATURN_RANSOM.exe (PID: 2468)</li><li>• SATURN_RANSOM.exe (PID: 3396)</li><li>• cmd.exe (PID: 1996)</li><li>• SATURN_RANSOM.exe (PID: 1724)</li><li>• SATURN_RANSOM.exe (PID: 3916)</li><li>• WINWORD.EXE (PID: 3320)</li><li>• SATURN_RANSOM.exe (PID: 3652)</li><li>• SATURN_RANSOM.exe (PID: 2452)</li><li>• rundll32.exe (PID: 1268)</li><li>• WINWORD.EXE (PID: 2976)</li><li>• opera.exe (PID: 4048)</li></ul> <p><b>Reads the date of Windows installation</b></p> <ul style="list-style-type: none"><li>• WScript.exe (PID: 3136)</li><li>• CScript.exe (PID: 2460)</li><li>• WScript.exe (PID: 2084)</li></ul> <p><b>Dropped object may contain TOR URL's</b></p> <ul style="list-style-type: none"><li>• SATURN_RANSOM.exe (PID: 3132)</li></ul> <p><b>Creates files in the user directory</b></p> <ul style="list-style-type: none"><li>• WINWORD.EXE (PID: 3320)</li><li>• WINWORD.EXE (PID: 2976)</li><li>• iexplore.exe (PID: 1828)</li><li>• opera.exe (PID: 4048)</li></ul> <p><b>Checks Windows Trust Settings</b></p> <ul style="list-style-type: none"><li>• WScript.exe (PID: 3524)</li><li>• iexplore.exe (PID: 1828)</li><li>• WScript.exe (PID: 3136)</li><li>• WScript.exe (PID: 2084)</li><li>• CScript.exe (PID: 2460)</li></ul> <p><b>Changes internet zones settings</b></p> <ul style="list-style-type: none"><li>• iexplore.exe (PID: 1828)</li></ul> <p><b>Application launched itself</b></p> <ul style="list-style-type: none"><li>• iexplore.exe (PID: 1828)</li></ul> <p><b>Reads Microsoft Office registry keys</b></p> <ul style="list-style-type: none"><li>• WINWORD.EXE (PID: 3320)</li><li>• WINWORD.EXE (PID: 2976)</li></ul> <p><b>Reads settings of System Certificates</b></p> <ul style="list-style-type: none"><li>• iexplore.exe (PID: 1828)</li></ul> <p><b>Check for Java to be installed</b></p> <ul style="list-style-type: none"><li>• opera.exe (PID: 4048)</li></ul> <p><b>Reads internet explorer settings</b></p> <ul style="list-style-type: none"><li>• iexplore.exe (PID: 2440)</li></ul> <p><b>Dropped object may contain Bitcoin addresses</b></p> <ul style="list-style-type: none"><li>• opera.exe (PID: 4048)</li></ul> <p><b>Reads the date of Windows installation</b></p> <ul style="list-style-type: none"><li>• iexplore.exe (PID: 1828)</li><li>• opera.exe (PID: 4048)</li></ul>

## 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

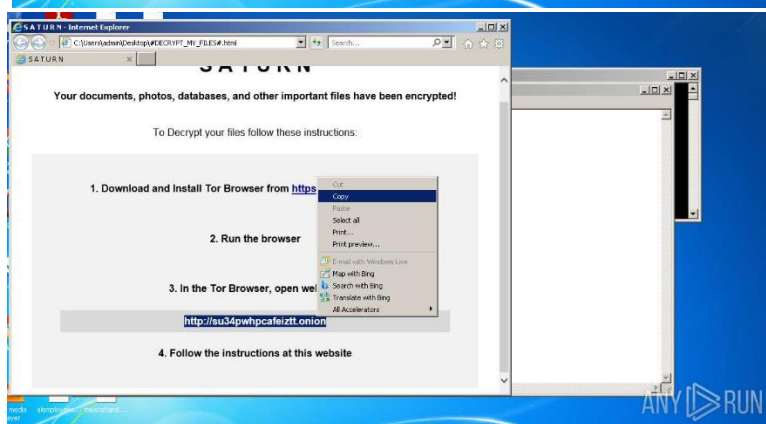
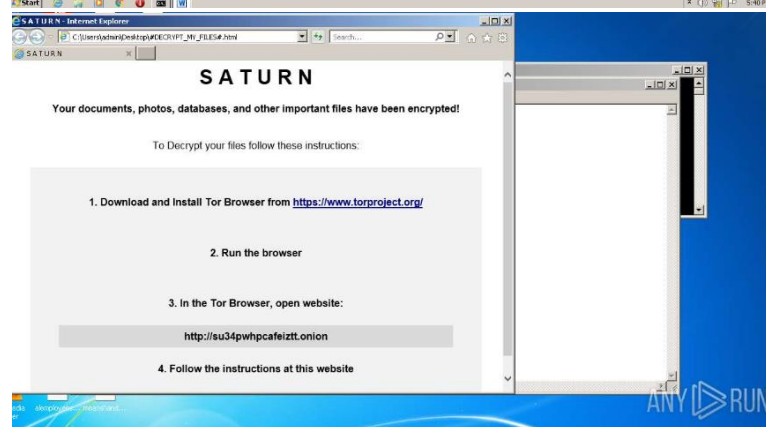
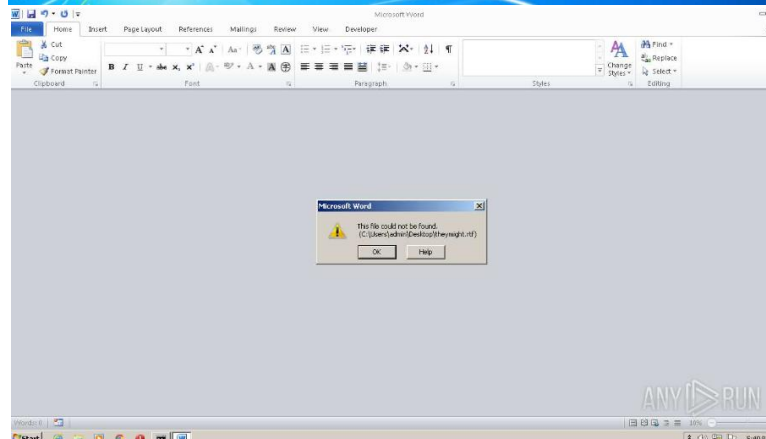
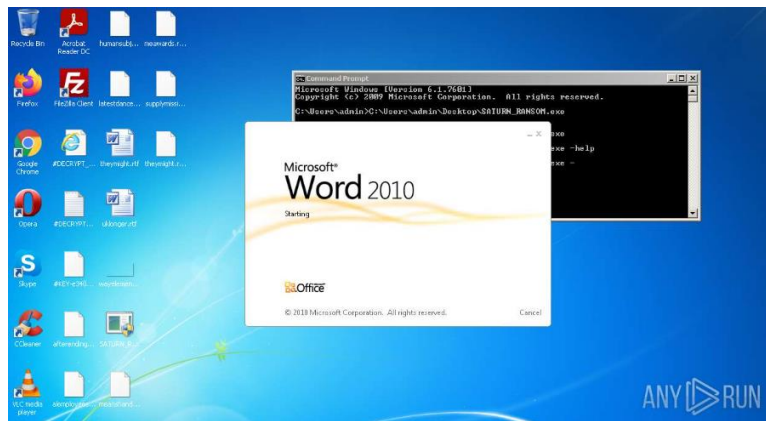
### SubsystemVersion:

6

### Subsystem:

Windows GUI

## Screenshots de la simulación:





## 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: .ol
Value: 2C6F2100F80C00000100	
(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	ieexplore.exe	GET	200	8.252.189.126:80	http://ctldl.windowsupdate.com/mdownload/update/v3/static/trusted/en/disallowedcertatl.cab?ed8446c2897ba05c	US	compressed	4.70 Kb	whitelisted
1828	ieexplore.exe	GET	200	8.252.189.126:80	http://ctldl.windowsupdate.com/mdownload/update/v3/static/trusted/en/disallowedcertatl.cab?d5e84181f228487d	US	compressed	4.70 Kb	whitelisted
1828	ieexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCgUABBTBL0V27RVZ7LBduom%2FnYB455PUewQU521ZMJJHWMys%2BghUNoZ70rUETfACEA8Ull8lgmZT9XHrHIJQel%3D	US	der	1.47 Kb	whitelisted
1828	ieexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCgUABBSAUQYBMq2awn1Rh6Doh%2F8YgFV7gQUA95QNVBRTLtm8KPIgXvDI7190VUCEAJ0LqoXyo4hxex7H%2Fz9DKA%3D	US	der	471 b	whitelisted
4048	opera.exe	GET	200	142.250.185.174:80	http://clients1.google.com/complete/search?q=su34pwhpcafeizt&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://orl3.digicert.com/DigiCertHighAssuranceEVRRootCA.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	<span>whitelisted</span>
1828	iexplore.exe	8.252.189.126:80	ctdl.windowsupdate.com	Level 3 Communications, Inc.	US	<span>unknown</span>
1828	iexplore.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	<span>whitelisted</span>
4048	opera.exe	185.26.182.94:443	certs.opera.com	Opera Software AS	—	<span>malicious</span>
—	—	185.26.182.93:443	certs.opera.com	Opera Software AS	—	<span>suspicious</span>
4048	opera.exe	185.26.182.93:443	certs.opera.com	Opera Software AS	—	<span>suspicious</span>
1828	iexplore.exe	152.199.19.161:443	r20sjw13mr.microsoft.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	<span>whitelisted</span>
4048	opera.exe	142.250.185.174:80	clients1.google.com	Google Inc.	US	<span>whitelisted</span>
4048	opera.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	<span>whitelisted</span>
4048	opera.exe	185.26.182.109:80	redir.opera.com	Opera Software AS	—	<span>unknown</span>

#### 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. 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-dea23dbdbbfba538e0c3aac3751331d.KEY") y los coloca en el escritorio. Los archivos BMP, TXT y HTML contienen el texto donde se pide una recompensa.

### 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.