

Informe de Análisis de Ataque y Propuesta de Mejora de Ciberseguridad para LexCorp

Análisis y estrategias para la protección de la infraestructura digital.

Autor: Emanuel Sanchez.

Índice

Introducción.....	5
<ul style="list-style-type: none">• Descripción general del incidente• Objetivo del informe	
Descripción del Incidente.....	5
<ul style="list-style-type: none">• Cronología del ataque (20-23 de junio de 2021)• Resumen de los eventos previos, durante y posteriores al ataque	
Análisis y Datos Técnicos de la Amenaza.....	5
<ul style="list-style-type: none">• Identificación del ransomware 'Saturn'• Características y capacidades de Saturn• Detalles del ransomware Saturn• Información técnica relevante (MD5, sistema operativo, tipo de malware)	
Posibles Causas de Infección.....	5
<ul style="list-style-type: none">• Hipótesis de vectores de entrada del malware• Análisis del hash y propagación en redes compartidas	
Comportamiento del Ransomware.....	6
<ul style="list-style-type: none">• Actividad sospechosa observada• Análisis estático de la amenaza	
Simulación de la Amenaza.....	8
<ul style="list-style-type: none">• Capturas de pantalla antes, durante y después de la ejecución del malware• Diagrama de comportamiento• Eventos Asociados• Actividad de Archivos• Conexiones de la Amenaza	
Conclusiones Finales.....	13
<ul style="list-style-type: none">• Resumen de las características de Saturn• Impacto y comportamiento general del ransomware• Listado de métodos de propagación identificados	

Acciones Incorrectas Tomadas en el Suceso.....	14
<ul style="list-style-type: none"> • Errores y su justificación • Recomendaciones para prevenir errores similares en el futuro 	
Acciones Correctas Tomadas en el Suceso.....	15
<ul style="list-style-type: none"> • Buenas prácticas y su justificación • Recomendaciones de mejora 	
Recomendaciones Generales para la Seguridad.....	16
<ul style="list-style-type: none"> • Implementación de software y protocolos preventivos • Políticas de gestión de archivos y credenciales 	
Propuesta de Mejora para la Seguridad de LexCorp.....	17
<ul style="list-style-type: none"> • Planificación de la respuesta a incidentes • Protección de endpoints • Creación del rol de Digital Awareness Officer (DAO) • Seguridad perimetral de la red 	
Presupuesto	22
<ul style="list-style-type: none"> • Valores de tecnologías utilizadas para la propuesta de mejora de seguridad 	

INFORME CIBERSEGURIDAD

LexCorp

En el presente informe se documenta el análisis del incidente de seguridad sufrido por LexCorp entre el 20 y el 23 de junio de 2021. El informe incluye una descripción detallada de los eventos previos, durante, y posteriores al ataque, así como las posibles causas del mismo, junto con otra información relevante.

Análisis de la amenaza

La amenaza que generalizó el ataque a la infraestructura de LexCorp fue identificada como 'Saturn', un ransomware conocido por su capacidad para cifrar archivos y exigir un rescate, mostrando gran resistencia frente a las barreras de seguridad convencionales, como algunos antivirus.

Datos técnicos de la amenaza

- Nombre: Saturn
- Fecha de análisis: 24 de junio de 2021.
- OS utilizado: Windows 7/10.
- MD5: BBD4C2D2C72648C8F871B36261BE23FD
- Tipo de malware: Ransomware

Posibles causas de infección

Aunque el análisis permite intuir cuál fue el vector de ataque, no se pudo determinar con certeza debido a la falta de información concluyente. Sin embargo, nuestro equipo ha desarrollado varias hipótesis sobre los posibles puntos de entrada de la amenaza en el sistema de LexCorp.

Durante nuestra investigación exhaustiva y el análisis del hash del ransomware, utilizando la herramienta VirusTotal, identificamos que este malware puede llegar a ingresar por un troyano. Esto sugiere que una posible causa del ataque fue la entrada del ransomware en el equipo infectado como un troyano, lo que permitió su rápida propagación lateral a través de redes compartidas. Esta hipótesis explicaría la velocidad con la que se infectó la infraestructura de LexCorp.

Comportamiento del ransomware

MALICIOUS

Saturn ransom note found

- SATURN_RANSOM.exe (PID: 3132)

Writes to a start menu file

- SATURN_RANSOM.exe (PID: 3132)

Starts BCDEDIT.EXE to disable recovery

- cmd.exe (PID: 2936)

Deletes shadow copies

- cmd.exe (PID: 2936)

Drops executable file immediately after starts

- SATURN_RANSOM.exe (PID: 3132)

Actions looks like stealing of personal data

- 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)

Runs PING.EXE for delay simulation

- cmd.exe (PID: 2996)

SUSPICIOUS

Reads the date of Windows installation

- SATURN_RANSOM.exe (PID: 3132)

- SATURN_RANSOM.exe (PID: 3472)

- SATURN_RANSOM.exe (PID: 2468)

- SATURN_RANSOM.exe (PID: 3396)

- 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)

Checks supported languages

- WMIC.exe (PID: 3688)

- cmd.exe (PID: 2936)

- SATURN_RANSOM.exe (PID: 3132)

- SATURN_RANSOM.exe (PID: 3396)

- SATURN_RANSOM.exe (PID: 2468)

- SATURN_RANSOM.exe (PID: 3472)

- cmd.exe (PID: 1996)

- SATURN_RANSOM.exe (PID: 3432)

- SATURN_RANSOM.exe (PID: 2028)

- SATURN_RANSOM.exe (PID: 2524)

- SATURN_RANSOM.exe (PID: 2104)

- SATURN_RANSOM.exe (PID: 1724)

- SATURN_RANSOM.exe (PID: 2452)

- WScript.exe (PID: 3524)

- cmd.exe (PID: 2996)

- WScript.exe (PID: 2084)

- CScript.exe (PID: 2460)

- WScript.exe (PID: 3136)

INFO

Checks supported languages

- bcdedit.exe (PID: 292)

- bcdedit.exe (PID: 1984)

- vssadmin.exe (PID: 3636)

- 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)

Reads the computer name

- wbadmin.exe (PID: 2396)

- vssadmin.exe (PID: 3636)

- WINWORD.EXE (PID: 3320)

- WINWORD.EXE (PID: 2976)

- PING.EXE (PID: 4048)

- iexplore.exe (PID: 1828)

- iexplore.exe (PID: 2440)

- opera.exe (PID: 4048)

Manual execution by user

- SATURN_RANSOM.exe (PID: 2468)

- SATURN_RANSOM.exe (PID: 3396)

- SATURN_RANSOM.exe (PID: 3472)

- cmd.exe (PID: 1996)

- SATURN_RANSOM.exe (PID: 3916)

- SATURN_RANSOM.exe (PID: 1724)

- SATURN_RANSOM.exe (PID: 2452)

Dentro del comportamiento de la amenaza se pueden encontrar una gran cantidad de actividad sospechosa, esto es un ejemplo.

Información estática de la amenaza

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:	-
EntryPoint:	0x151bc
OSVersion:	6
ImageVersion:	-
SubsystemVersion:	6
Subsystem:	Windows GUI

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)

Screenshots de la simulación

Foto previa a la ejecución del malware.

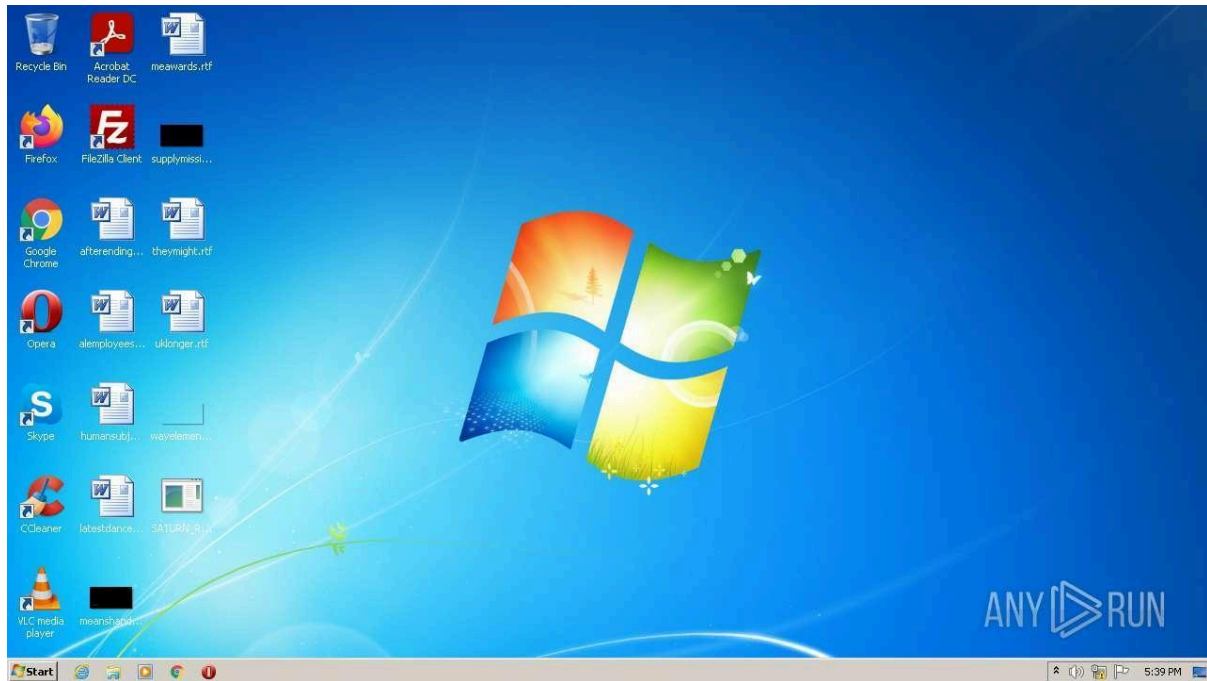


Foto ejecutando el malware.

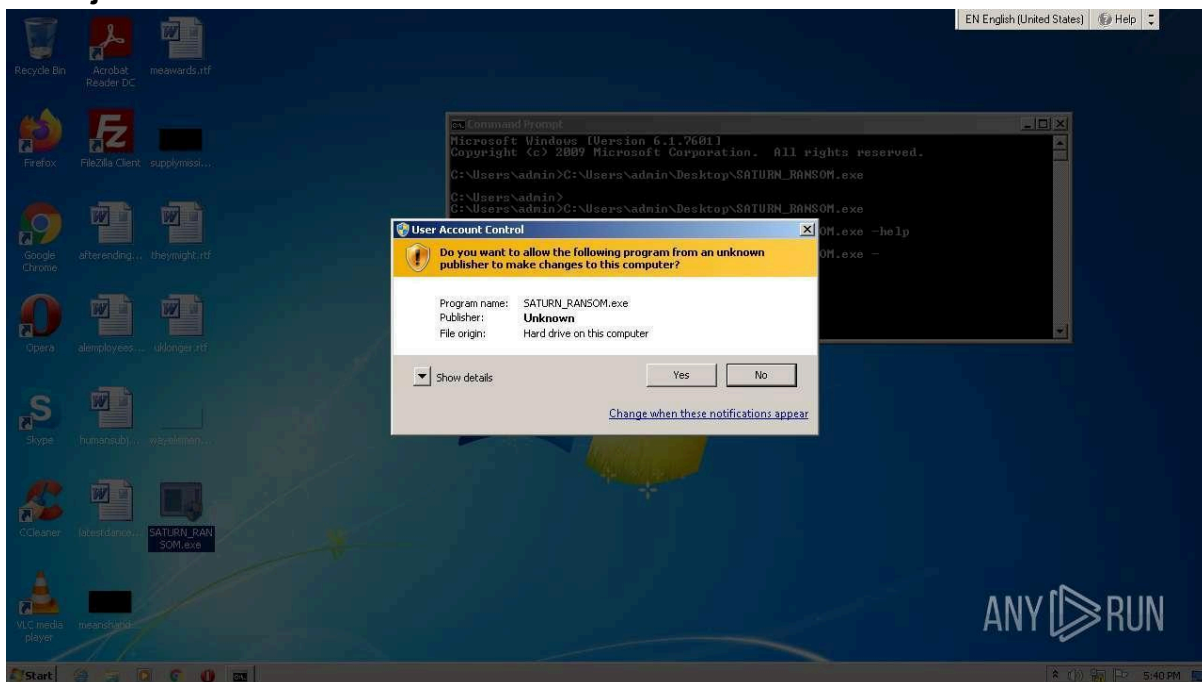


Foto que muestra el pedido de rescate tras la ejecución del malware.

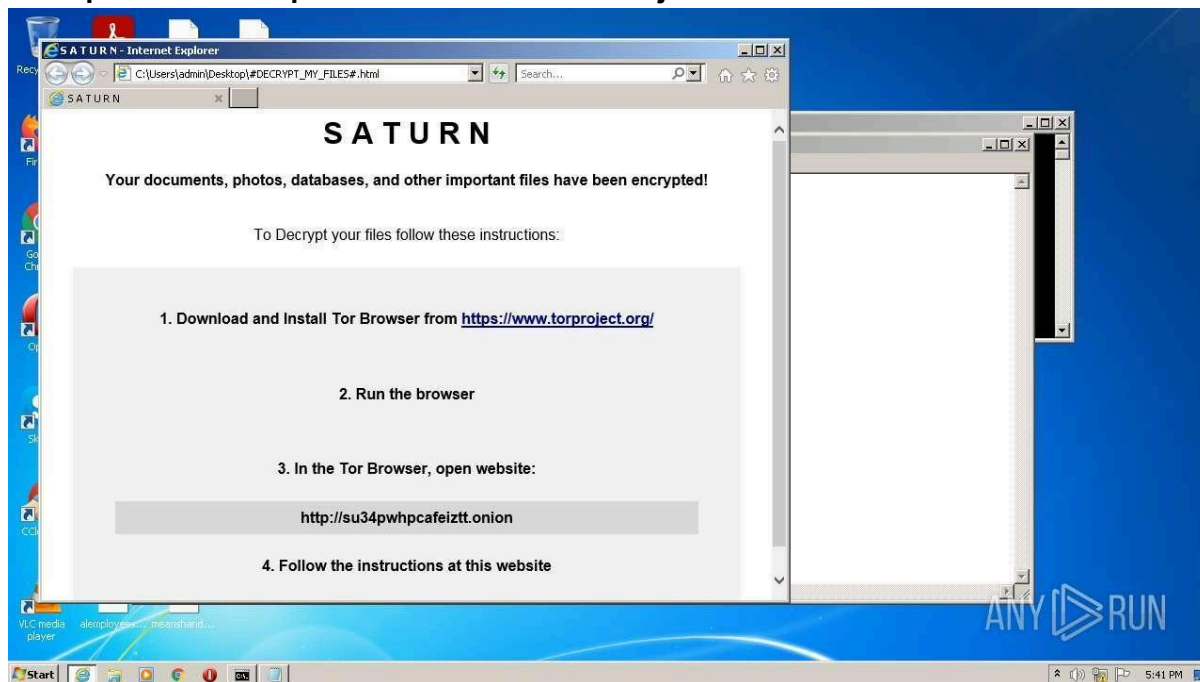
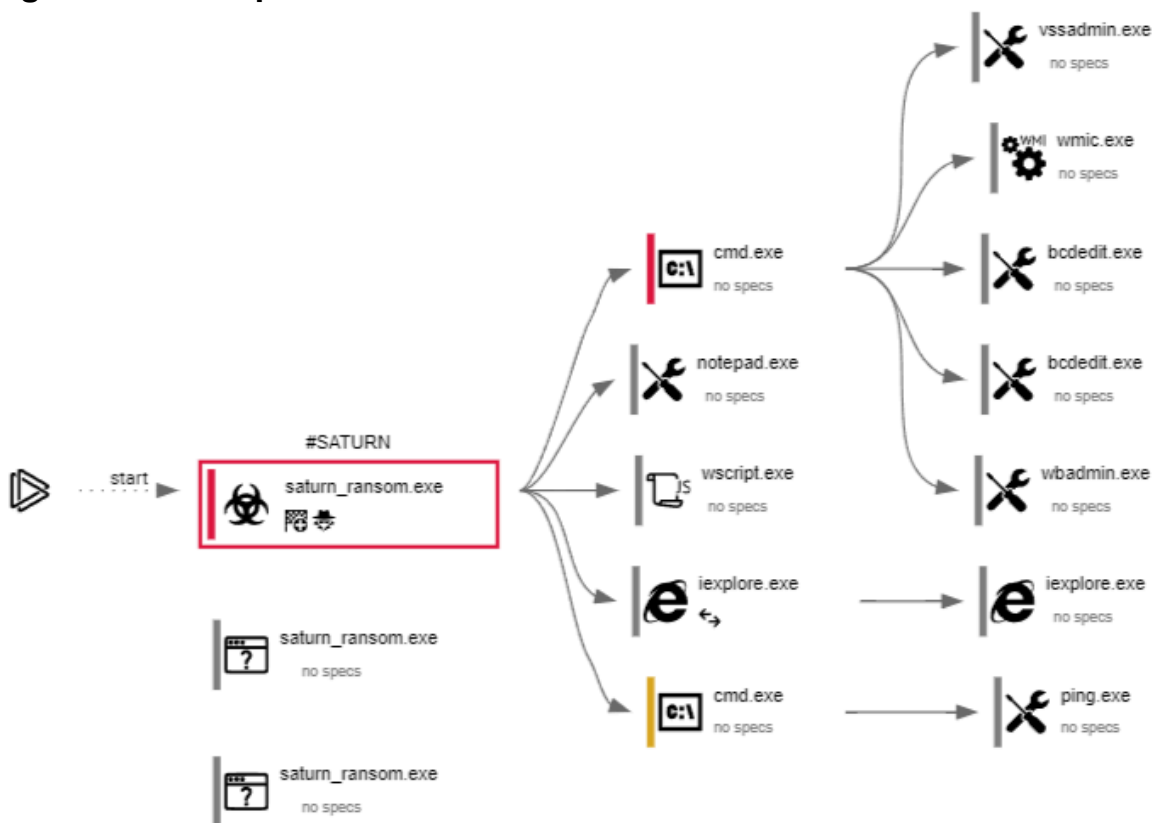


Diagrama de comportamiento de la amenaza



Eventos asociados

Registro de actividad

Eventos totales del sistema: 25502

Eventos de lectura: 24359

Eventos de escritura: 636

Eventos de eliminación: 507

Ejemplos de eventos de modificación:

(PID) Process: (3132) SATURN_RANSOM.exe Operation: write Value: 1	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Name: ProxyBypass
(PID) Process: (3132) SATURN_RANSOM.exe Operation: write Value: 1	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Name: IntranetName
(PID) Process: (3132) SATURN_RANSOM.exe Operation: write Value: 1	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Name: UNCAsIntranet
(PID) Process: (3132) SATURN_RANSOM.exe Operation: write Value: 0	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap Name: AutoDetect
(PID) Process: (3320) WINWORD.EXE Operation: write Value: 2C6F2100F80C00000100000000000000000000000000	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\StartupItems Name: ,o!
(PID) Process: (3320) WINWORD.EXE Operation: write Value: Off	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages Name: 1033
(PID) Process: (3320) WINWORD.EXE Operation: write Value: Off	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages Name: 1041
(PID) Process: (3320) WINWORD.EXE Operation: write Value: Off	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages Name: 1046
(PID) Process: (3320) WINWORD.EXE Operation: write Value: Off	Key: HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Common\LanguageResources\EnabledLanguages Name: 1036

Actividad de archivos

Archivos ejecutables: 0

Archivos sospechosos: 1758

Archivos de texto: 480

Archivos desconocidos: 31

Ejemplo de actividad de archivos en el sistema:

PID	Process	Filename	Type
3132	SATURN_RANSOM.exe	C:\MSOCache\All Users\{90140000-0015-0407-0000-0000000FF1CE}-C\Setup.xml.saturn MD5: 6357010684574AD3E6A1B0784DC20C40 SHA256: 4BD00B1505B9F423028CECE358029F33EB1A00DDB2CF7A41C1EA56424AAACB33	binary
3132	SATURN_RANSOM.exe	C:\MSOCache\All Users\{90140000-0015-0407-0000-0000000FF1CE}-C\AccessMUI.xml MD5: F15AB75E6E64B92AB449B36B35BC0A73 SHA256: A4C0A700A9815BCCF889DA68F63FB27CA3B1B03F3B38CE255F13ADFF5AA848D8	binary
3132	SATURN_RANSOM.exe	C:\MSOCache\All Users\{90140000-0015-040C-0000-0000000FF1CE}-C\AccessMUI.xml MD5: 0C9BE58D93432B6F7830AACB0069BA86 SHA256: D4599B57711AFAD279DD0278A76856250B30900B8B5FE0143EDACA9A86CCA809	binary
3132	SATURN_RANSOM.exe	C:\MSOCache\All Users\{90140000-0015-0407-0000-0000000FF1CE}-C\branding.xml MD5: 8BCAD13471FE29AD5129B39ED112FB84 SHA256: 2B8E923D40321AE12ABD43FB6C490E80A674C8B1CB3F996EA2EFF50AC57EED8	binary
3132	SATURN_RANSOM.exe	C:\MSOCache\All Users\{90140000-0015-0407-0000-0000000FF1CE}-C\Setup.xml.XYWs MD5: 28743E37F6B7EDBF328E0DF087F86891 SHA256: 2E4766151FA28874B2C6577EFD93666EF81B41B00149CFA1131915C44344A974	binary
3132	SATURN_RANSOM.exe	C:\MSOCache\All Users\{90140000-0015-040C-0000-0000000FF1CE}-C\#KEY-e340015603cf0fc144de5d2be9ca6d09.KEY MD5: FDEC72840D186E0A17A6DBAA9B770A1B SHA256: B1DED9FC52425ADE6EA5FFAF664E9A65A15EFF611337D5139A04380AABE8329E	binary
3132	SATURN_RANSOM.exe	C:\MSOCache\All Users\{90140000-0015-0407-0000-0000000FF1CE}-C\#KEY-e340015603cf0fc144de5d2be9ca6d09.KEY MD5: 628C95D16CAC4A317BF1355D47959F3E SHA256: FF2A99A0356E7F1DC72FF2B71079D50C79ECEA1F928AEBB0C8AB2DAEA79AA0C3	binary
3132	SATURN_RANSOM.exe	C:\MSOCache\All Users\{90140000-0015-0407-0000-0000000FF1CE}-C\AccessMUI.xml.saturn MD5: F15AB75E6E64B92AB449B36B35BC0A73 SHA256: A4C0A700A9815BCCF889DA68F63FB27CA3B1B03F3B38CE255F13ADFF5AA848D8	binary
3132	SATURN_RANSOM.exe	C:\MSOCache\All Users\{90140000-0015-0407-0000-0000000FF1CE}-C\branding.xml.saturn MD5: 8BCAD13471FE29AD5129B39ED112FB84 SHA256: 2B8E923D40321AE12ABD43FB6C490E80A674C8B1CB3F996EA2EFF50AC57EED8	binary
3132	SATURN_RANSOM.exe	C:\MSOCache\All Users\{90140000-0015-0407-0000-0000000FF1CE}-C\Setup.xml MD5: 6357010684574AD3E6A1B0784DC20C40 SHA256: 4BD00B1505B9F423028CECE358029F33EB1A00DDB2CF7A41C1EA56424AAACB33	binary

Conexiones

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

DNS request

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

HTTP request

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1828	iexplore.exe	GET	200	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPIGxvDI7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	US	der	471 b	whitelisted
4048	opera.exe	GET	200	93.184.220.29:80	http://crl3.digicert.com/DigiCertHighAssuranceEVRootCA.crl	US	der	592 b	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	185.26.182.109:80	http://redir.opera.com/favicons/google/favicon.ico	unknown	image	5.30 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	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	93.184.220.29:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMys%2BghUNoZ7OrUETfACEA8Uil8glGmZT9XHrHiJQel%3D	US	der	1.47 Kb	whitelisted

Amenazas

PID	Process	Class	Message
-	-	Potential Corporate Privacy Violation	ET POLICY DNS Query for TOR Hidden Domain .onion Accessible Via TOR
-	-	Potential Corporate Privacy Violation	AV POLICY DNS Query for .onion Domain Via TOR - Not Google

Conclusiones finales

Nombre de la amenaza: Saturn.

Comportamiento del malware: Encriptamiento.

Tipo de malware: Ransomware.

Información sobre Saturn:

Saturn es un ransomware de tipo cifrado (encryption ransomware) que se caracteriza

por su rápida propagación y su capacidad para comprometer redes compartidas. Su principal objetivo es cifrar archivos críticos en los dispositivos infectados, añadiendo extensiones específicas, como '.saturn'. Además de cifrar los archivos, puede exfiltrar datos sensibles. Una vez que los archivos han sido comprometidos, Saturn deja una nota de rescate exigiendo un pago en criptomonedas, generalmente Bitcoin, a cambio de la clave de descifrado que permite recuperar la información afectada. Su comportamiento incluye la propagación lateral dentro de redes y la persistencia en el sistema, lo que le permite causar un daño considerable en un corto período de tiempo.

Posibles métodos de propagación del malware

- Phishing masivo dentro de la organización.
- Propagación lateral a través de redes compartidas.
- Explotación de credenciales comprometidas.
- Conexiones VPN y acceso remoto inseguro.
- Uso de dispositivos USB infectados.

Acciones incorrectas tomadas en el suceso

1. Descubrimiento y acción ante malware

- **Justificación:** El incidente de malware fue detectado entre el 20 y el 23 de junio de 2021, pero tomó 3 días en tomarse acción. Este tiempo de respuesta es excesivo para un ciberataque. Una respuesta rápida es crucial para limitar el daño y contener el ataque, especialmente frente a malware que puede propagarse rápidamente o causar daños irreversibles en la red y los sistemas.
- **Recomendación:** Se recomienda implementar un sistema de monitoreo continuo de seguridad que permita la detección casi inmediata de ataques y contar con procedimientos de respuesta a incidentes más ágiles para reducir el tiempo de reacción.

2. Apagado de PCs y preservación de evidencia

- **Justificación:** Apagar máquinas infectadas sin preservar la memoria volátil (RAM) representa un error crítico en la investigación forense y análisis de incidentes. La RAM puede contener datos esenciales sobre el malware, como

patrones de comportamiento, procesos activos y posibles comunicaciones con servidores de comando y control (C&C). Al no realizar una imagen forense de la memoria antes de apagar las máquinas, se pierde información clave que podría haber ayudado a comprender mejor el ataque.

- **Recomendación:** Antes de apagar una máquina infectada, es fundamental capturar la memoria volátil (RAM) y realizar imágenes forenses completas de los discos duros para preservar la evidencia y permitir un análisis exhaustivo del incidente.

3. Copias de seguridad (backups)

- **Justificación:** El hecho de que solo un 10% de los dispositivos contara con copias de seguridad representa una grave vulnerabilidad. Las copias de seguridad son cruciales para restaurar los sistemas sin pérdida de datos críticos en caso de un ataque. Sin un respaldo adecuado en la mayoría de los dispositivos, LexCorp experimentó pérdidas de información y tiempo valioso al intentar recuperar los sistemas afectados.
- **Recomendación:** Es esencial establecer una política de respaldo robusta que garantice que todos los dispositivos y servidores críticos estén respaldados de manera regular. Las copias de seguridad deben almacenarse en ubicaciones seguras externas y verificarse periódicamente para asegurar su integridad.

Acciones correctas tomadas en el suceso

1. Guardar una muestra del malware

- **Justificación:** La preservación de una muestra del malware fue una decisión correcta y necesaria para un análisis forense detallado. Esta muestra permite identificar el tipo exacto de malware, comprender su comportamiento, los sistemas a los que afecta y su método de propagación. Además, podría ser útil compartirla con proveedores de seguridad y autoridades externas en caso de ser necesario.
- **Recomendación:** Es fundamental mantener siempre una muestra intacta del malware en un entorno seguro para el análisis. Esta medida es clave para entender el vector de ataque y las implicaciones de la vulnerabilidad.

2. Apagar las máquinas infectadas

- **Justificación:** Aunque apagar las máquinas sin preservar la memoria RAM es una mala práctica (como se explicó previamente), desconectar los sistemas afectados en sí mismo fue una acción correcta. Al aislar los sistemas infectados de la red, se contuvo la propagación del malware y se mitigó el alcance del ataque, evitando que se extendiera a otros dispositivos y servidores.
- **Recomendación:** Aunque la contención mediante el apagado fue adecuada, en el futuro se recomienda realizar esta acción de manera más controlada, asegurando primero la preservación de la evidencia disponible en la memoria volátil.

3. Restauración desde copias de seguridad en el 10% de los dispositivos

- **Justificación:** A pesar de que solo el 10% de los dispositivos contaba con respaldo, la restauración desde copias de seguridad en los sistemas afectados fue una medida adecuada. Esta acción permitió a LexCorp recuperar parte de su infraestructura de manera rápida, especialmente en los dispositivos con backups recientes.
- **Recomendación:** Si bien esta fue una medida positiva, LexCorp debe mejorar su política de backups para que todos los sistemas críticos estén protegidos regularmente. Las copias de seguridad son esenciales en la recuperación ante malware y otros desastres.

4. Análisis externo por parte de un experto en ciberseguridad.

- Fue positivo que LexCorp solicitara a un experto en ciberseguridad que realizara un análisis de posibles mejoras en la seguridad de la empresa. Esta evaluación externa permitió identificar áreas clave donde la infraestructura de seguridad podría fortalecerse para proteger mejor los datos y la continuidad de las operaciones. Basándose en la arquitectura de red actual, que comprende 20 equipos remotos conectados mediante VPN y 60 equipos conectados a la red local (LAN), se han propuesto las siguientes recomendaciones para mejorar la protección de los endpoints, el control de acceso y la segmentación de la red.

Recomendaciones generales

Dada la extensión del daño en la infraestructura de LexCorp, se recomienda implementar las siguientes medidas para prevenir futuros ataques informáticos.

- Se sugiere la implementación de programas como Autoruns en todos los equipos de la empresa para monitorear y prevenir la ejecución de software no autorizado.
- Se sugiere la implementación de programas como Kaspersky y Fortigate en todos los equipos de la organización para la protección del perímetro y protección de endpoints.
- Se recomienda la instalación de un equipo central que cuente con herramientas como Wireshark, a través del cual se monitoricen los datos y archivos utilizados en los dispositivos de la empresa. Esto permitirá detectar conexiones ilegítimas y archivos maliciosos de manera efectiva.
- Se propone la creación de un protocolo para la gestión de archivos externos en la organización, que permita a un grupo selecto de empleados descargar y manipular información. Este protocolo deberá incluir el uso de herramientas preventivas como VirusTotal u otras similares para garantizar la seguridad de la información
- Creación de un protocolo específico para la manipulación de credenciales y datos críticos o sensibles de la organización.
- Durante nuestro análisis, observamos que la organización LexCorp contaba con respaldos (backups) únicamente en un 10% de sus equipos. Aumentar significativamente esta proporción reduciría considerablemente las pérdidas de información valiosa, así como de activos críticos para la empresa.

Propuesta de Mejora para la Seguridad de LexCorp

Dada la arquitectura de red corporativa, que incluye 20 equipos remotos conectados a la red interna de la empresa mediante VPN y 60 equipos conectados directamente a la LAN (red local), se ha desarrollado una propuesta

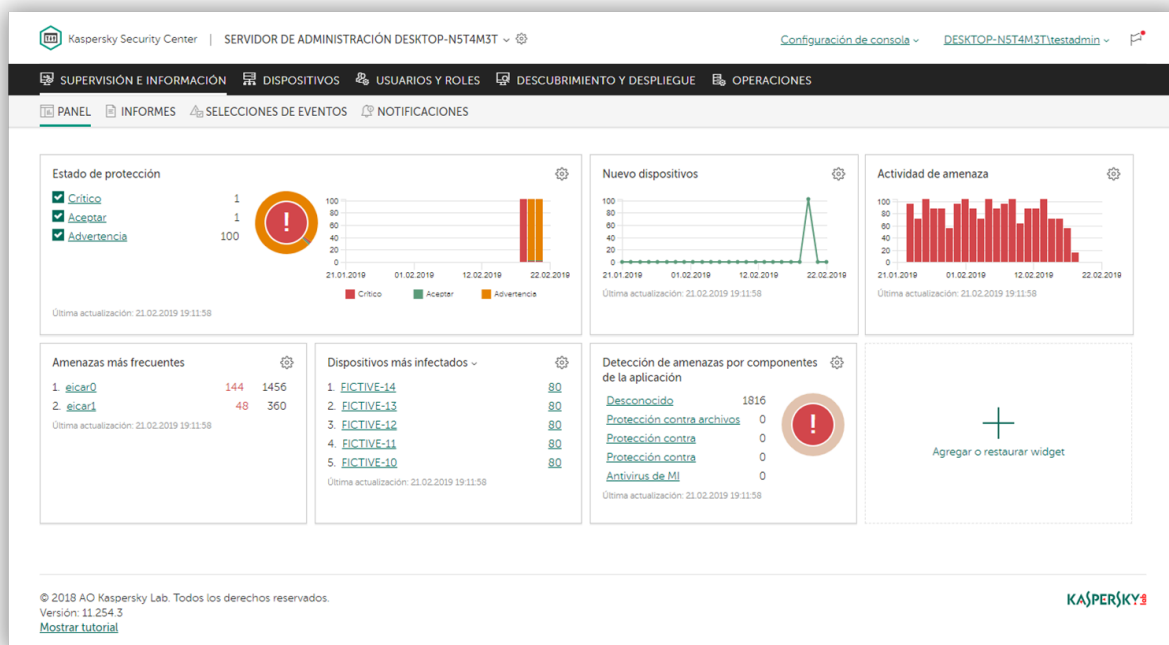
de mejora enfocada en la protección de endpoints, el control de acceso y la segmentación de la red. La propuesta incluye las siguientes recomendaciones:

1. Planificación de la Respuesta a Incidentes

- **Definición de un plan de respuesta:** Crear un plan claro de respuesta ante incidentes, que incluya herramientas para detección temprana y gestión de logs.
- **Procedimiento formal para gestión de incidentes:** Establecer protocolos específicos de manejo de incidentes de seguridad.
- **Implementación de herramientas de monitoreo:** Integrar sistemas de monitoreo y análisis de eventos como SIEM para centralizar y analizar logs de seguridad.
- **Capacitación del personal:** Entrenar a los empleados en identificación y respuesta ante incidentes de ciberseguridad.

2. Protección de Endpoints

- **Uso de EDR y EPP:** Implementar herramientas de protección de endpoints, como EDR y EPP:
 - **EPP (Endpoint Protection Platform):** Utiliza antivirus y antimalware para prevenir ataques conocidos, bloqueando amenazas antes de que ocurran.
 - **EDR (Endpoint Detection and Response):** Detecta, investiga y responde a amenazas avanzadas y desconocidas, permitiendo monitoreo continuo y análisis de comportamiento para detectar actividades sospechosas.



● **Programa de testeo de vulnerabilidad:** Usar herramientas como RanSim para evaluar la seguridad de los endpoints de manera iterativa. ● **Buenas prácticas:**

- **Pentesting:** Realizar pruebas de penetración para detectar y corregir vulnerabilidades.
- **Control de puertos:** Usar herramientas como Nmap para monitorear puertos abiertos y reducir vectores de ataque.
- **Aplicación de parches y actualizaciones:** Mantener actualizados todos los dispositivos de seguridad perimetral y asegurarse de que firewalls y filtros estén configurados para permitir solo el tráfico autorizado.

3. Creación del Rol de Digital Awareness Officer (DAO)

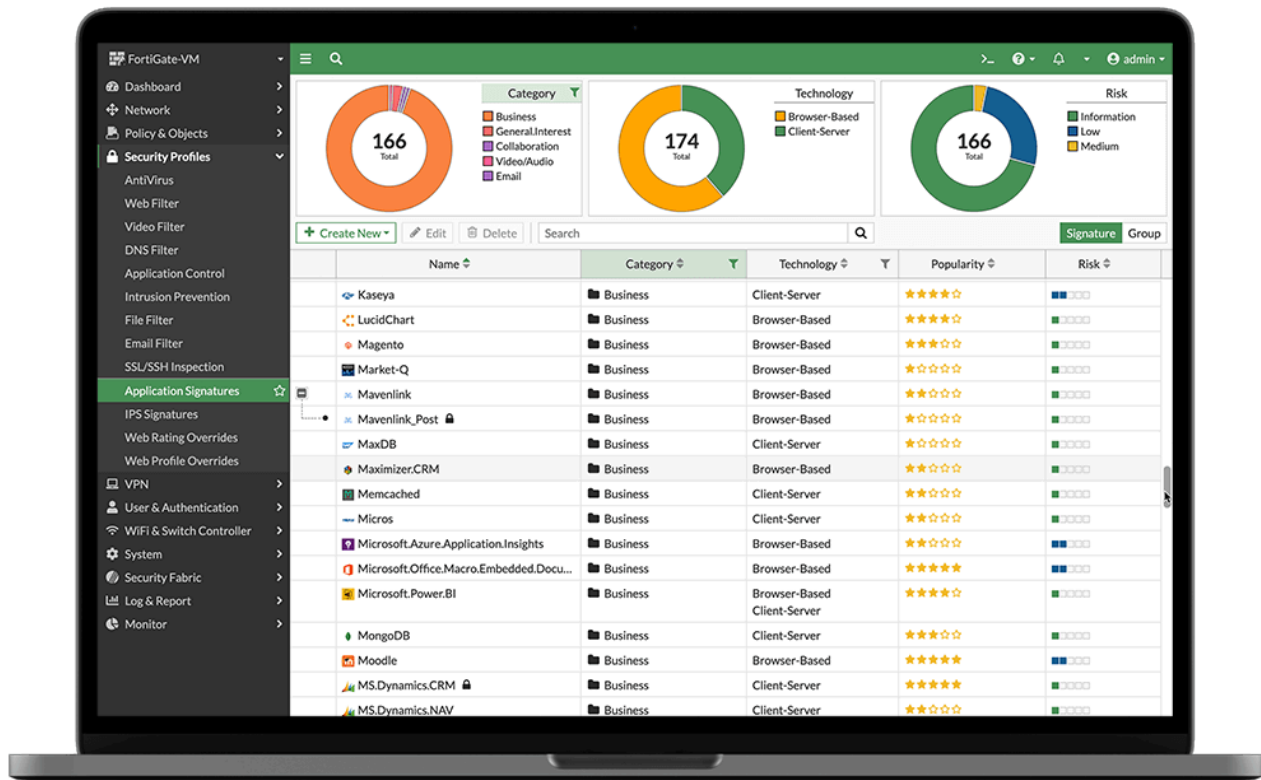
- **Responsabilidades:** El DAO debe evaluar el cumplimiento de las políticas de seguridad, fomentar la concienciación en ciberseguridad y capacitar al personal de manera continua. Su objetivo es integrar la ciberseguridad en la cultura organizacional.

- **Actividades de capacitación:** Implementar programas educativos como "Phishing Quiz" de Google para enseñar al personal a detectar ataques de phishing, analizar URLs y comprender prácticas seguras para el manejo de credenciales e información sensible.

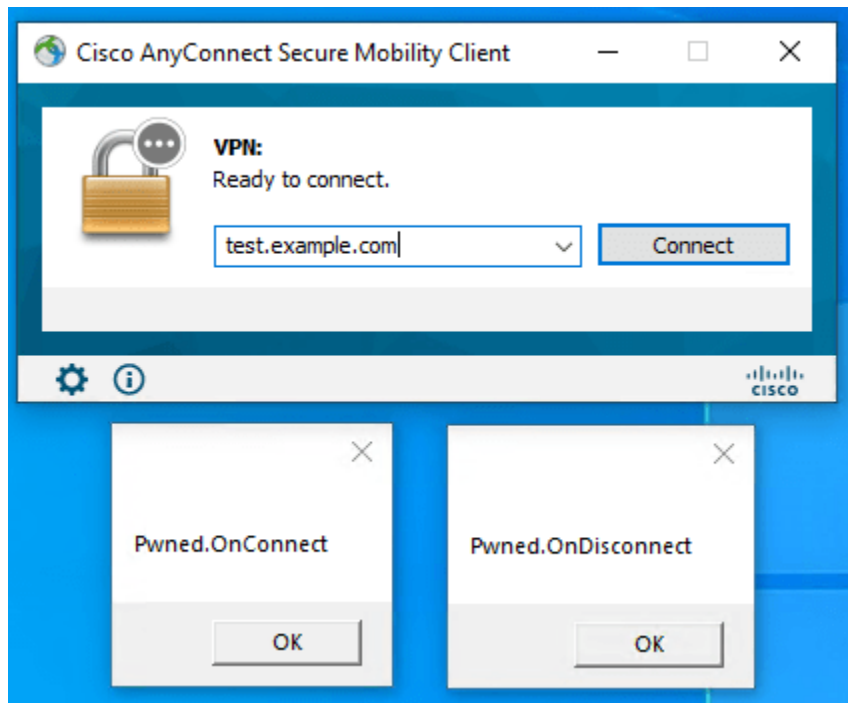
Importancia del rol: Aunque el DAO no necesariamente es un experto técnico, su enfoque en educación y concienciación es clave para reducir incidentes causados por ingeniería social, responsable de hasta un 94% de los ataques de malware.

4. Seguridad Perimetral de la Red

- **Implementación de UTM (Unified Threat Management):** Usar soluciones UTM como Fortinet FortiGate que integran IDS, IPS, firewall, antivirus y VPN para proteger la red. Estas soluciones filtran el tráfico no deseado y protegen contra malware, piratería y otras amenazas.



- **VPN de acceso remoto para equipos externos:** Reemplazar las VPN de acceso personal con una VPN de acceso remoto empresarial como Cisco AnyConnect, diseñada específicamente para conexiones LAN seguras y escalables.



Buenas prácticas en seguridad perimetral:

- **Monitoreo continuo:** Vigilar el tráfico de red y detectar intrusiones de manera proactiva.
- **Revisión periódica de configuraciones:** Mantener actualizadas las configuraciones de seguridad en los dispositivos perimetrales, ajustándolas según las mejores prácticas y amenazas emergentes.

Presupuesto

- **Kaspersky Costo anual:** \$3.500 USD por un año.
- **Cisco AnyConnect:** \$150 - \$200 USD por equipo, anualmente.

- **Fortinet FortiGate 100F:** Compra única \$2.500 USD (para 100 dispositivos).
- **Suscripción FortiGate (actualizaciones y licencias):** \$1.350 - \$1.750 USD anuales, con opción de combo de compra (por única vez) y suscripción \$3.250 USD.

Total: \$10.785 USD primer año.
\$8.885 segundo año.