18-11-2022

Análisis y propuestas de mejoras de ciberseguridad para LEXCORP

Analista de Ciberseguridad: Galvalisi Elvis
elvisgbvgd505@gmail.com

Situación:

El día 27 de Abril del 2022, la empresa LexCorp sufrió un ataque de un malware, el cual afectó tanto al servidor como a los equipos clientes de la red (equipos de los usuarios) que forman parte de su infraestructura. Una vez identificados los equipos alcanzados por el personal técnico de la empresa, se tomaron las siguientes medidas:

a) Guardaron una muestra del malware para analizar.
b) Apagaron la totalidad de los equipos.
c) Analizaron el alcance del malware sobre los equipos (determinando que fueron afectados los backups también).
d) Reinstalaron la totalidad de los equipos (servidores y terminales).
e) Se solicitó un informe de análisis completo sobre el ataque de malware para sentar un precedente sobre el daño sufrido y evitar a futuro pasar por lo mismo o por lo menos minimizar los daños.

1) Acciones llevadas a cabo:

	Acción/Medida	Procedimiento	Justificación
1	Guardaron una muestra del Malware.	Correcto	Guardar una muestra, permite hacer un análisis más profundo sobre el malware, su alcance y posibles medidas a tomar.
2	Apagaron la totalidad de los equipos.	Incorrecto	Al apagar las máquinas, el registro de eventos de los equipos se vio afectado perdiendo información importante a la hora de realizar un análisis forense.
3	Analizaron el alcance del malware sobre los equipos (determinando que fueron afectados los backups también)	Correcto	Al realizar un control general sirvió para determinar el alcance y las medidas a tomar.
4	Reinstalaron la totalidad de los equipos (servidores y terminales)	Correcto	Al ser afectados la totalidad de los equipos, fue la medida adecuada.
5	Se solicitó un informe completo sobre el ataque del malware para sentar un precedente sobre el daño sufrido y evitar a futuro pasar por lo mismo o minimizar los daños.	Correcto	La empresa no contaba con personal para afrontar e investigar este tipo de incidentes, por lo que se recurrió a un consultor externo para llevar a cabo la tarea.

2) Informe de Análisis de Malware

a) 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 *phishing* (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.

b) 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
Link de informe detallado: https://app.any.run/tasks/02c74be4-4ba6-4494-bb52-a77cedc589fe/

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

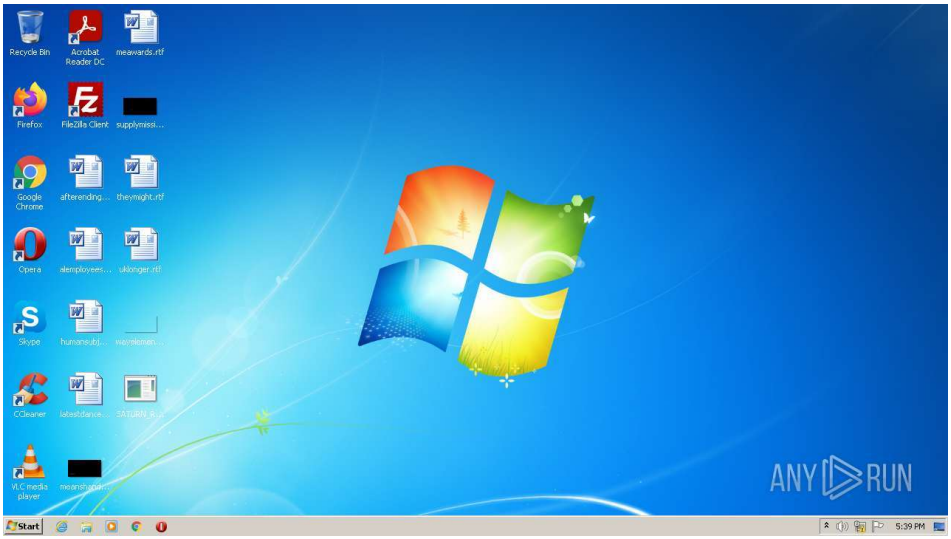
SubsystemVersion: 6

Subsystem: Windows GUI

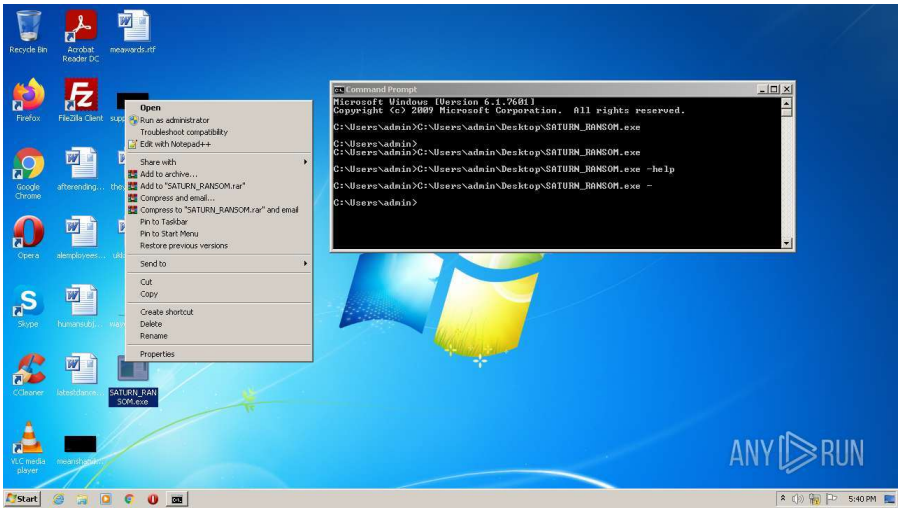
Screenshots del comportamiento:

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:

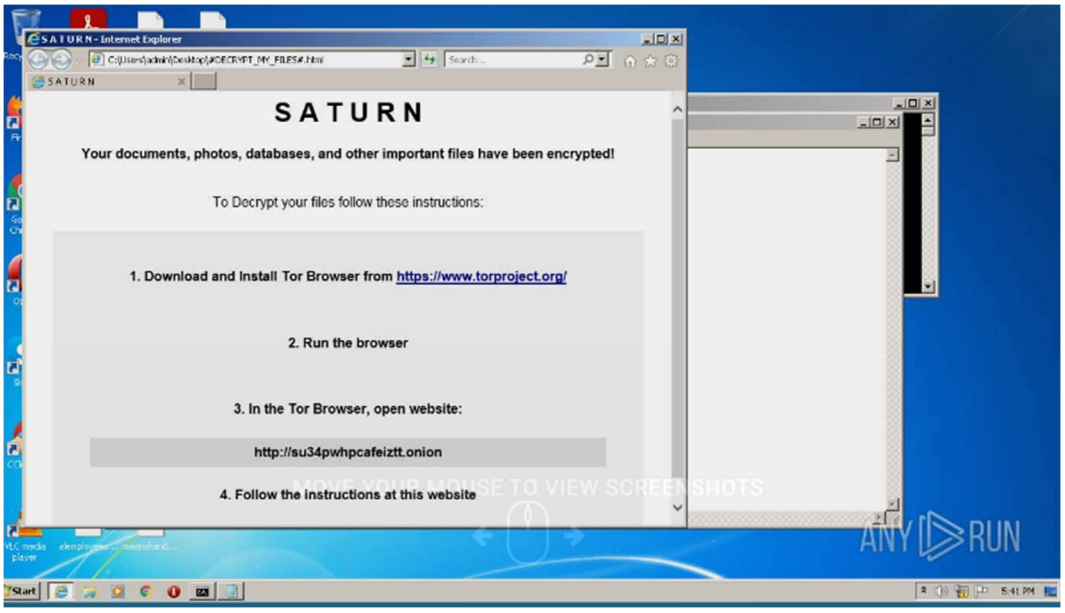
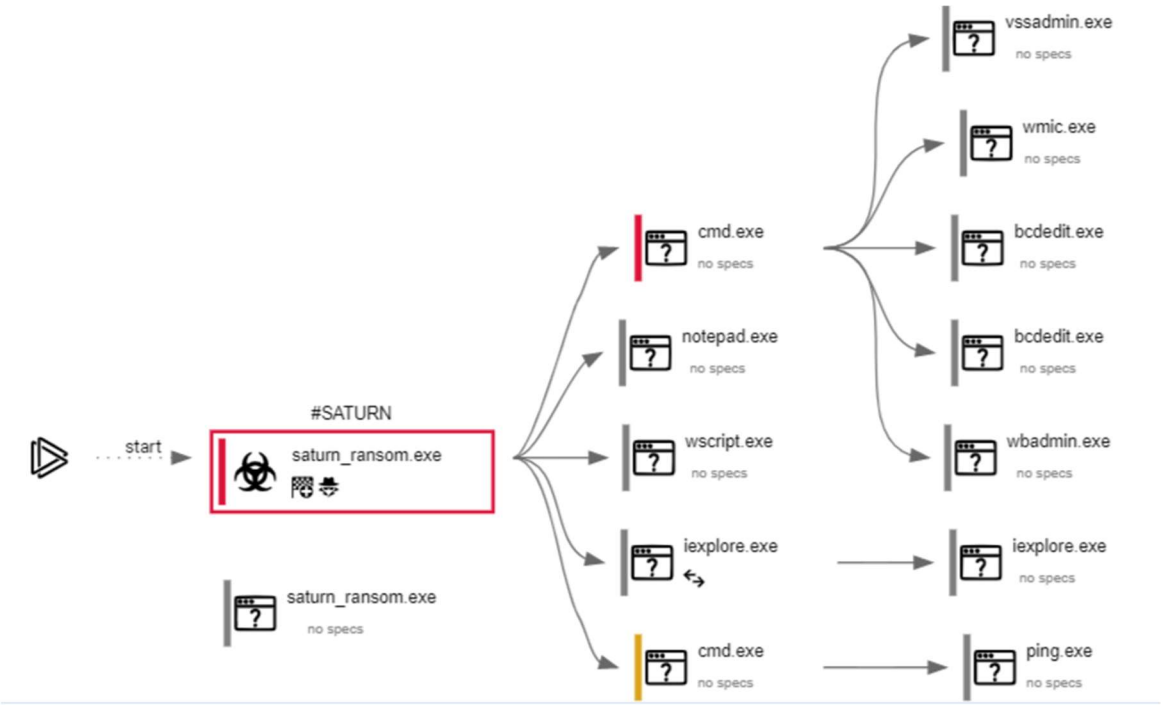


Diagrama de Proceso de Comportamiento:

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

c) **Conclusión del informe**:

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.

3) Posibles Acciones del atacante – paciente cero y origen del ataque

Como se planteó en la hipótesis del punto 2, no se puede determinar el origen y/o el ingreso del malware, por lo que se sospecha que el usuario de la computadora infectada en la cual se detectó el ataque puede haber sido víctima de *phishing*, facilitando el acceso del atacante a la red de la empresa, donde pudo obtener datos de accesos, preparando 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, destruyendo previamente los archivos de respaldo, para luego solicitar el rescate de la información encriptada.

4) Propuesta de Mejora de Ciberseguridad

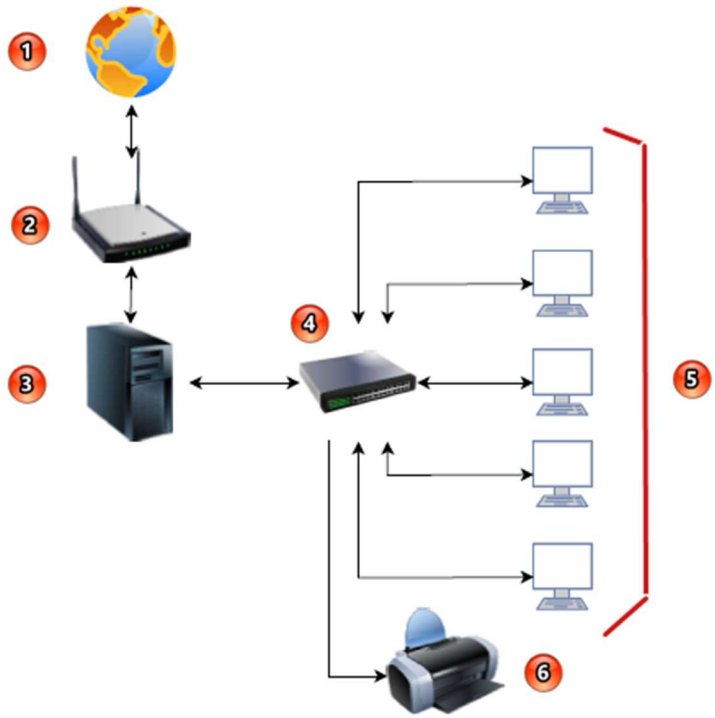
El día 27 de abril de 2022, la empresa LexCorp sufrió un ataque de un malware, el cual afectó a la totalidad de los equipos, cifrando todos los datos que contenían estos.

A raíz de ese incidente, se había solicitado un informe sobre el ataque para determinar origen y daños causados. Posterior a esto, se solicita una propuesta de mejora para evitar sufrir nuevamente este tipo de ataques.

Como primer tarea, se realiza es una investigación de la estructura de red, los usuarios finales y eventuales, obteniendo los siguientes datos:

Esquema de red:

Diagrama de Red Actual



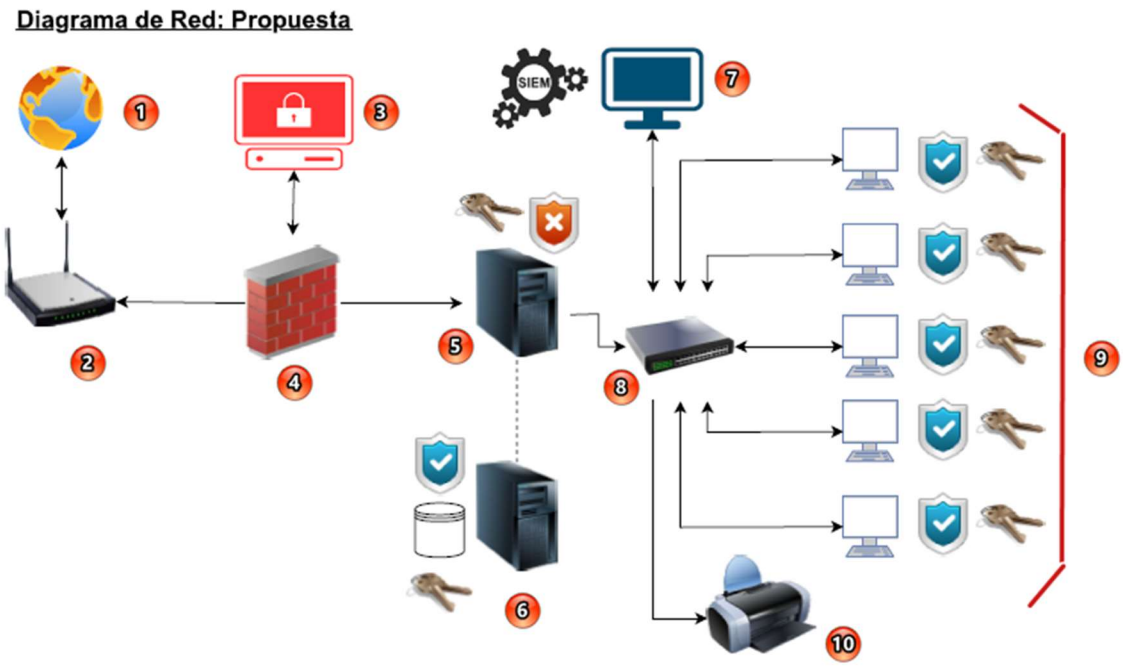
Referencias:

1) Internet
2) Router (ethernet + wifi)
3) Servidor
4) Switch
5) Terminales
6) Impresora

Posterior a esto, se indaga sobre la red y accesos a la misma. Determinando que la red es simple, sin restricciones y con muchas vulnerabilidades teniendo en cuenta que los usuarios finales y permanentes son cinco (5), mientras que los usuarios eventuales son tres (3); y en donde todos los mencionados, aparte de conectarse a la red en sus terminales, también lo hacen con sus dispositivos móviles o notebook personales.

En conclusión, las vulnerabilidades son altas y requieren una acción inmediata en el corto plazo.

A continuación, se expone la propuesta de mejoras en forma gráfica:



Referencias:

1- Internet
2- Router (ethernet + wifi)
3- EDR (Plataforma de Protección de detección y respuesta)
4- Firewall
5- Servidor Principal
6- Servidor Backup
7- SIEM
8- Switch
9- Terminales
10- Impresora

Detalle de propuesta para control de Perímetro:

Como primera medida, se recomienda implementar una barrera firewall (4) desde la conexión a internet externas a la red interna de la empresa administrado por un equipo con un sistema protección y respuesta en tiempo real a las amenazas (EDR), y se sugiere implementar la herramienta "Palo Alto Networks Cortex XDR" que recibe información en tiempo real de todos los equipos de la red. En base a esto, la configuración para el servidor (5) que se debería implementar es la siguiente:

- Sistema Operativo con Licencia (Windows Server 2012 – o superiores).
- Sistema de Gestión Unificada de Amenazas (UTM), para administrar el control de ingresos no autorizados y prevención de ingresos no autorizados (IDS/IPS). Sofware sugerido: "Trend Micro Apex One"
- Administración de credenciales de usuarios aplicando políticas de grupo para acceder a determinados directorios y aplicaciones (IAM).
- Servicio de RDP para las conexiones permitidas en el controlador de dominio.
- Limitar y administrar el tiempo de conexión/desconexión de usuarios internos y externos.
- Bloquear la instalación de programas en todas las terminales.
- Administrar y limitar el acceso a internet generando un repositorio de webs visitadas con frecuencia para configurar como excepciones para determinados usuarios.
- Monitoreo de archivos adjuntos recibidos, permitiendo la descarga previo análisis de agente.
- Bloqueo de puertos USB de todas las terminales.
- Bloqueo y/o retiro de lectoras de CD (si las hubiere).
- Administración y monitoreo de dispositivos externos que pueden conectarse a la red, ya sea de manera física (ethernet) o por wifi. Configurar una red invitados para este tipo de casos.

Por otro lado, se recomienda configurar un equipo (7) exclusivamente para el monitoreo del tráfico de datos e interacciones en la red mediante un software del tipo SIEM (Seguridad de la información y gestión de Eventos) con el software libre recomendado "AlienVault OSSIM". El mencionado equipo por medio del switch estará interconectado con todos los equipos de la red.

Otra medida para tener en cuenta es la implementación de un servidor de backup (6), el cual NO va a estar conectado de manera directa a la red, sino que, de acuerdo a una frecuencia a definir, se conectará y se correrá una rutina de copiado de la información total del servidor siempre y cuando no existan alarmas o eventos captados por el SIEM. Otra opción a contemplar a futuro es la contratación de un servicio de backup en la nube.

Para el resto de los equipos (9), se requiere una configuración de doble factor de autentificación al servicio RDP del servidor. Y como complemento muy importante, se requiere una capacitación para todos los usuarios finales en el uso responsable y seguro de las computadoras y la información de la empresa (confidencialidad).

Todas las propuestas mencionadas son escalables, por lo que se pueden planificar a corto/mediano plazo en este orden de prioridades:

Corto Plazo:

1) Capacitación en ciberseguridad y buenas prácticas para todo el personal.
2) Configurar un firewall implementando un software EDR para protección de las entradas y salidas de internet.
3) Antivirus en todas las terminales y servidor (agentes del EDR).
4) Configurar un Controlador de Dominio con reglas de acceso y permisos adaptables al negocio.
5) Bloqueo de puertos USB y/o cualquier medio físico de entrada.
6) Configuración de red invitados y restricción de conexión de dispositivos externos.

Mediano Plazo:

1) Implementación de un equipo con SIEM, IPS/IDS.
2) Servidor de Backup.

CONCLUSIÓN:

La implementación de las medidas de ciberseguridad planteadas, le van a permitir a la empresa ir mejorando su postura y protegerse de posibles nuevos ataques. La mitigación de estos radica en capacitaciones y en la realización de campañas internas para la prevención de phishing, incluyendo a todo el personal perteneciente a la empresa, ya que fomentando las buenas prácticas en todos los niveles la empresa puede realizar sus operatorias habituales con mayor seguridad.