



# INFORME DE CIBERSEGURIDAD

AÑO 2023

## LEXCORP COMPANY

ALUMNO: SEBASTIAN A.  
RUBILAR

# CONTEXTO

La noche del 20 al 23 de junio de 2021, LexCorp fue víctima de un malware (ataque) que afectó a sus servidores (Windows Server 2003/2012) y equipos de usuario (Windows 7/Windows 10) de toda la infraestructura.

## ACCIONES TOMADAS POR EL PERSONAL

Tras identificar todos los dispositivos infectados, el área de soporte técnico tomó las siguientes acciones:

Guardaron una muestra del malware.

Apagaron, el mismo día 23 de septiembre, las máquinas que se habían identificado como afectadas durante el incidente.

En las máquinas que disponían de copia de seguridad (back-up), restauraron al estado correspondiente al día 19 de septiembre (fecha de último backup disponible previo al ataque). Solo un 10% del Parque contaba con backup.

El 24 de septiembre, LexCorp solicita los servicios de un analista de ciberseguridad para analizar una muestra y emitir recomendaciones para su infraestructura de red y mejorar su postura de ciberseguridad.

LexCorp solicita la elaboración de un informe de análisis del ataque, que tipo de malware es y el vector de ataque para aportar más detalles sobre el incidente y el nivel de compromiso derivado del mismo.



# OBJETIVOS

- 01** Identificar qué acciones llevadas por el área de soporte técnico son correctas o incorrectas.
- 02** Identificar la muestra de malware, comportamiento y posibles vectores de ataque.
- 03** Identificar las posibles acciones que realizó el atacante en los sistemas.
- 04** Diseñar una solución para evitar este tipo de incidente y mejorar la postura de ciberseguridad de LexCorp.

# ACCIONES REALIZADAS POR LOS MIEMBROS DE LEXCORP

## LAS ACCIONES CORRECTAMENTE REALIZADAS FUERON:

Guardar una muestra del malware: ya que permitirá hacer el análisis forense del malware

Reinstalar el sistema operativo en algunas máquinas: Si cuenta con una copia de seguridad de archivo, en el mejor de los casos es mejor restaurar

Corporación Acme solicitó un informe de análisis del ataque: Lo mejor es solicitar servicios de análisis y sugerencias para mejorarlo.

## LAS ACCIONES INCORRECTAMENTE REALIZADAS FUERON:

Apagar todas las máquinas: Al apagar las máquinas la información útil se pierde llegando a perder información importante para un análisis forense

Al otro día encendieron las máquinas y corrieron un antivirus: Las máquinas infectadas deberían de ser desconectadas de la red antes de encenderlas

# ANALISIS DE MALWARE

## Informe de análisis

- NOMBRE DE LA MUESTRA: dovidka.chm
- FECHA DE ANÁLISIS: 27/04/2022,  
16:34:45
- OS UTILIZADO PARA ANÁLISIS: Windows 7  
Professional Service Pack 1 (build 7601,  
32 bit)
- TIPO DE MALWARE IDENTIFICADO:  
Troyano



# POSIBLES ACCIONES - PACIENTE CERO Y ORIGEN DEL ATAQUE

**NO SE HA PODIDO DETERMINAR LA VÍA DE ENTRADA DEL ATAQUE DEBIDO A LA AUSENCIA DE FUENTES DE DATOS CLAVE QUE PERMITAN CONOCER EL ALCANCE COMPLETO DEL INCIDENTE.**  
**NO OBSTANTE, PLANTEO LAS SIGUIENTES HIPÓTESIS EN BASE A LAS FUENTES DE INFORMACIÓN ANALIZADAS:**

## POSIBLE CAUSA

Un empleado abrió un mail que consideró de fuente confiable e hizo click a un mail con link malicioso que descargó la muestra del malware.

## POSIBLE CAUSA

Un empleado descargó un archivo, ejecutó el .zip explotando el archivo que de inmediato desempaquetó y ejecutó una carga útil de MicroBackdoor, brindando al adversario acceso remoto al equipo.

## POSIBLE CAUSA

Un empleado insertó un dispositivo USB infectado a su ordenador.

# IMPLEMENTACIÓN DE SOLUCIÓN

Usar la plataforma “Palo Alto Networks Cortex XDR” ya que es capaz de detener los ataques hechos a mano, con un aprendizaje automático sólido y un monitoreo del comportamiento hasta la red y la nube.

## REVISIÓN DE PERÍMETRO

- Usar el firewall de última generación (NGFW) “Fortinet FortiGate”, el cual ofrece protección completa contra amenazas cibernéticas, incluyendo virus, malware, spam y ataques de phishing.
- Usar un Sistema de Prevención y Detección de Intrusos (IPS)(IDS) como la herramienta “Snort” para detectar y prevenir ataques cibernéticos en tiempo real. Funciona escuchando el tráfico de red y comparando el contenido de los paquetes con un conjunto de reglas predefinidas.
- Instalar un software de seguridad en todos los dispositivos de la empresa, como “McAfee”, para protegerlos de malware y otros tipos de software malicioso.
- Usar la VPN “NordVPN” que permite a los usuarios conectarse a Internet de manera segura y privada a través de una conexión cifrada.
- No hacer click en enlaces sospechosos de correos electrónicos o mensajes de texto.

# PROPUESTA DE MEJORA





# PROPUESTA DE MEJORA

## IMPLEMENTACIÓN DE PROGRAMA

Implementar PhishMe, plataforma de simulación de phishing y capacitación que permite a las organizaciones evaluar el riesgo de sus empleados y capacitarlos en la identificación y prevención de estos ataques.

Se recomienda usarla de manera regular para evaluar la capacidad de los empleados para detectar y evitar este tipo de amenazas.

## EJECUCIÓN DE PROGRAMA

Ejecutar de manera cuatrimestral los servicios de pentesting de "Cobalt" para poder cubrir todas las necesidades que tiene LexCorp en cuanto a seguridad, desde identificar vulnerabilidades en sistemas y aplicaciones hasta cumplir con regulaciones y estándares de seguridad.

Estos servicios incluyen pruebas de penetración externas e internas, pruebas de cumplimiento, evaluaciones de seguridad de aplicaciones, y investigaciones de amenazas.

