Integrantes

- Cobeña Cornejo Roberto Carlos
- Moran Zambrano Jordan Armando
- Zambrano Lobaton María Isabel
- Vera Pisco Shirley Lisbeth

Informe de Investigación Forense Digital: Caso de Filtración de Datos en

DataSecure Inc.

Escenario:

En la empresa ficticia DataSecure Inc., se ha detectado una filtración de datos sensibles a través de correos electrónicos enviados a direcciones externas no autorizadas. El departamento de IT ha identificado que el envío sospechoso fue realizado desde la computadora de uno de los empleados.

Como parte del equipo forense digital, tu tarea es realizar una investigación completa siguiendo los Procedimientos de Investigación Forense Digital.

Objetivo general: Determinar la causa, alcance y autoría de la filtración de datos.

Objetivos específicos:

- Identificar comunicaciones sospechosas desde el equipo comprometido.
- Analizar el contenido de los correos enviados para detectar información confidencial.
- Revisar el historial de actividad del equipo para buscar acciones inusuales.
- Detectar intentos de ocultamiento de evidencia a través de borrado o encriptación.
- Investigar conexiones de red anómalas utilizadas para la filtración.
- Garantizar la preservación adecuada de toda la evidencia digital.

Roles del equipo Forense

- Investigador Principal: Roberto Cobeña
- Analista de Evidencia Digital: Zambrano Jordan
- Especialista en Correo Electrónico: Lobaton María
- Especialista Legal: Vera Shirley
- Especialista en Redes: Bonilla Cristian

Revisión de Políticas

La investigación forense llevada a cabo en DataSecure Inc. se encuentra en estricta conformidad con las políticas internas de seguridad y privacidad, así como con la normativa vigente a nivel internacional, incluyendo el RGPD. Se garantiza la protección integral de los datos personales y la confidencialidad de la información, manteniendo una cadena de custodia rigurosa y cumpliendo con los más altos estándares éticos.

Identificación de Evidencia

Dispositivos Relevantes:

- Computadora del Empleado Sospechoso: El principal dispositivo desde el cual se realizaron los envíos.
- Smartphones: Si el empleado sospechoso utilizó su teléfono personal o un dispositivo móvil corporativo para enviar o recibir información relacionada con la filtración, es crucial analizar los datos almacenados en estos dispositivos.
- Tabletas: Similar a los smartphones, las tabletas pueden contener evidencia relevante, especialmente si se utilizaron para acceder a correos electrónicos o almacenar archivos.
- Servidor de Correos de la Empresa: Para analizar los registros de correos electrónicos enviados y recibidos.
- Dispositivos de Red (Switches, Routers, Firewalls): Para identificar el tráfico de red relacionado con la filtración.
- Unidad de Almacenamiento en Red (NAS) o Servidores de Archivos:
- Posibles lugares donde se pudo haber almacenado información sensible.

Estado de los Dispositivos:

• La computadora del empleado estaba encendida y conectada a la red cuando

se detectó la filtración.

• El teléfono móvil del empleado estaba encendido y conectado a la red cuando se detectó la infiltración

• Los dispositivos de red y los servidores están en funcionamiento y bajo

monitorización.

Inventario Documentado:

• Computadora del empleado: Lenovo 4200, con sistema operativo

Windows 11.

• SmarthPhone: Galaxy Flip z, con sistema operativo

Android.

• Servidor de correos: Microsoft Exchange Server, con almacenamiento local

de correos electrónicos.

Recolección de Evidencia

• Aislamiento del equipo sospechoso: La computadora y smartphone fue desconectada de la red para evitar modificaciones remotas o acceso no autorizado.

• Toma de imagen forense: Se utilizó CAINE para generar una imagen bit a

bit del disco duro del equipo sospechoso, asegurando la preservación de todos los datos, incluso archivos eliminados.

• Captura de correos electrónicos: Se extrajo una copia completa de los correos

electrónicos almacenados en el servidor, incluyendo todos los registros de envío

y recepción.

• Cadena de Custodia:

Sección 1

Número de expediente 041/223

Descripción de la muestra

Ordenador portátil Lenovo, Modelo Lenovo 4200, con número de serie 2435235V

Fecha	Hora	Lugar
17/09/2024	10:00	Manta

Recibido por

Roberto Cobeña

Organización y dirección

Organización TECA security, Manabi, Manta.

Firma

Sección 2

Fecha	Hora	Lugar
17/09/2024	16:00	Manta

Recibido por

Maria Zambrano

Organización y dirección

Organización TECA security, Manabi, Manta.

Firma

Análisis de Evidencia con CAINE:

Herramienta Utilizada:

La investigación forense se llevó a cabo utilizando la distribución Linux CAINE como herramienta principal para el análisis de los dispositivos involucrados. Se examinaron exhaustivamente la computadora del empleado sospechoso, el servidor de correo corporativo, dispositivos de red y unidades de almacenamiento compartidas, empleando las funcionalidades avanzadas de CAINE para la adquisición, análisis y generación de reportes forenses.

¡Absolutamente! Aquí tienes algunas opciones para reescribir el texto, enfatizando el uso exclusivo de CAINE y sus herramientas integradas:

Hallazgos Preliminares:

Mediante el empleo de la suite forense CAINE, se ha llevado a cabo un análisis exhaustivo de los dispositivos involucrados. Los resultados obtenidos revelan lo siguiente:

- **Comunicaciones Compromiso:** Se identificaron correos electrónicos enviados a destinatarios no autorizados desde el equipo del empleado, los cuales contenían información confidencial. Las herramientas de análisis de correo electrónico integradas en CAINE permitieron aislar y analizar estos mensajes.
- **Exfiltración de Datos:** El análisis forense del disco duro, realizado con las herramientas de adquisición y procesamiento de imágenes de CAINE, permitió recuperar archivos adjuntos que contenían datos clasificados.
- **Intentos de Ocultamiento de Evidencia:** Se detectaron rastros de herramientas de eliminación de archivos, lo que indica que el empleado intentó ocultar su actividad. Sin embargo, las funcionalidades de recuperación de datos de CAINE permitieron recuperar parte de la información eliminada.
- **Actividad de Red Sospechosa:** El análisis de los registros de la actividad de red, realizado con las herramientas de análisis de tráfico de CAINE,

reveló conexiones a servidores externos a través de VPN, lo que sugiere una posible exfiltración de datos.

Informe Final

1. Introducción

Este informe documenta la investigación forense realizada para identificar y analizar una filtración de datos en DataSecure Inc., en la que información sensible fue enviada a direcciones externas no autorizadas. El objetivo fue determinar la naturaleza del incidente, identificar a los responsables.

2. Procedimientos

El proceso forense se desarrolló en cuatro fases:

2.1 Preparación y Planificación:

Los objetivos generales incluyeron identificar cómo ocurrió la filtración, qué

información fue comprometida y quién fue el responsable. Se establecieron roles clave en el equipo forense:

Investigador Principal: Roberto Cobeña

Analista de Evidencia Digital: Zambrano Jordan

Especialista en Correo Electrónico: Lobaton María

Especialista Legal: Vera Shirley

Especialista en Redes: Bonilla Cristian

2.2 Recolección de Evidencia:

La evidencia fue obtenida de los siguientes dispositivos:

- **Computadora del empleado sospechoso:** Se realizó una adquisición forense de la imagen del disco duro utilizando las herramientas integradas en CAINE, garantizando así la preservación de todos los datos, incluidos los archivos eliminados.
- **Servidor de correos:** Se extrajeron todos los correos electrónicos relevantes del servidor mediante las funcionalidades de análisis de correo electrónico de CAINE.
- **Dispositivos de red:** Se capturaron y analizaron los registros de tráfico de red utilizando las herramientas de análisis de red de CAINE para identificar conexiones sospechosas.

2.3 Análisis Forense:

Para el análisis de la evidencia, se empleó exclusivamente la suite forense CAINE. Las herramientas integradas en CAINE permitieron:

- **Análisis de la imagen del disco:** Se realizó un análisis exhaustivo de la imagen del disco duro para identificar archivos, registros y artefactos relevantes.
- **Análisis de correos electrónicos:** Se examinaron los correos electrónicos extraídos del servidor para identificar contenido sospechoso, remitentes y destinatarios.
- **Análisis de tráfico de red:** Se analizaron los registros de red para identificar patrones de tráfico inusuales y conexiones a sistemas externos.

2.4 Cadena de Custodia:

Se estableció una cadena de custodia rigurosa para garantizar la integridad de la evidencia. Cada etapa de la investigación, desde la recolección hasta el análisis, fue debidamente documentada.

3. Evidencias Encontradas

- **Comunicaciones no autorizadas:** Se identificaron múltiples correos electrónicos enviados desde la computadora del empleado a direcciones no autorizadas, conteniendo información confidencial de la empresa.
- **Exfiltración de datos:** Se encontraron archivos adjuntos en los correos electrónicos que contenían datos sensibles, como información de clientes y estrategias internas.
- **Intentos de ocultamiento de evidencia:** Se detectaron rastros de herramientas de eliminación de archivos, lo que indica que el empleado intentó borrar evidencia. Sin embargo, gracias a las capacidades de recuperación de datos de CAINE, se pudo recuperar parte de la información eliminada.
- **Actividad de red sospechosa:** El análisis de los registros de red reveló conexiones a sistemas externos a través de VPN, sugiriendo un posible intento de exfiltrar datos de forma encubierta.

4. Conclusiones

La evidencia obtenida a través del análisis forense realizado con CAINE demuestra de manera concluyente que se produjo una filtración de datos intencional. Los intentos del empleado por ocultar su actividad, evidenciados por el uso de herramientas de eliminación de archivos y las conexiones a sistemas externos, refuerzan esta conclusión.