Caso de seguridad en la empresa **ShopNow**

ShopNow es una compañía emergente en el sector del comercio electrónico que ha experimentado un crecimiento acelerado en los últimos años. Sus ingresos superaron los 20 millones de dólares en el último período fiscal, consolidándose como un competidor fuerte dentro de su industria. Este éxito también ha despertado el interés de actores maliciosos, quienes en varias ocasiones han intentado comprometer los sistemas tecnológicos que soportan la operación de la empresa.

Hace pocos días, ShopNow enfrentó un incidente grave de ciberseguridad. El ataque comenzó con una estrategia de ingeniería social: un atacante logró establecer contacto con el área de recepción, responsable de gestionar un registro electrónico con los datos de visitantes, incluyendo nombres, documentos de identidad y correos electrónicos. Dicho archivo debía estar protegido y accesible únicamente para personal autorizado.

El adversario utilizó esta cercanía para ejecutar un ataque de fuerza bruta sobre las credenciales del encargado de recepción. Tras obtener acceso a su cuenta, comenzó a explorar la red interna y a identificar los servicios críticos de la organización. Con esta información, el atacante localizó vulnerabilidades en el servidor web corporativo y lanzó un ataque exitoso contra dicho sistema.

Como parte de sus acciones posteriores, el intruso desplegó un ransomware en el equipo de la recepción, lo que ocasionó el cifrado completo de los archivos allí almacenados. Posteriormente, apareció un mensaje exigiendo un pago de 1.500 dólares en criptomonedas a cambio de la clave para restaurar la información comprometida.

La dirección de ShopNow ha solicitado tu apoyo como analista de seguridad, con el fin de estudiar el ataque, evaluar los errores que permitieron la intrusión y recomendar medidas de mitigación para fortalecer la infraestructura tecnológica y evitar que se repitan incidentes similares.

Plantilla de Informe de Análisis de Incidente de Seguridad

1. Portada

- Título del informe

- Nombre del estudiante

- Fecha de entrega

2. Resumen Ejecutivo (máximo un párrafo)

- Descripción breve del incidente

3. Descripción del Incidente

- Qué ocurrió

El servidor web de la empresa ShopNow fue objeto de intentos de acceso anómalos. Inicialmente, se observó tráfico legítimo hacia el portal de login de la aplicación bWAPP, pero poco después se registraron múltiples solicitudes malformadas que devolvieron errores HTTP 400, lo que sugiere un intento de explotación o escaneo automatizado.

- Cómo fue detectado

La detección se dio por el mensaje emergente del ransomware en la estación de trabajo afectada. Posteriormente, se revisaron los logs del servidor web para descartar compromiso de otros activos.

- Qué activos fueron afectados

- PC Recepción
- Archivos PC recepción: Base de datos de ingreso
- El servidor web mostró intentos de exploración, pero no evidencia de intrusión exitosa.

4. Análisis de Evidencia Digital

- Descripción de al menos tres eventos relevantes extraídos del log

- Explicación del significado de cada evento

Eventos relevantes del log:

1. **[21/Jul/2021:16:25:44]**
   - Evento: múltiples solicitudes GET legítimas a /bWAPP/login.php y archivos CSS/JS/Imágenes.
   - Significado: acceso normal a la página de login, posiblemente un usuario real cargando la aplicación.
2. **[21/Jul/2021:16:26:05 – 16:26:09]**
   - Evento: varias solicitudes GET /?xxx HTTP/1.1 devolviendo error 400.
   - Significado: tráfico anómalo, posiblemente un escaneo automatizado o intento de fuzzing para descubrir vulnerabilidades en parámetros.
3. **Cambio de agente de usuario (User-Agent):**
   - Primeras solicitudes → Firefox 78.0 en Linux.
   - Solicitudes sospechosas → Chrome 53 en Mac OS.
   - Significado: podría indicar que el atacante está cambiando de herramientas o simulando diferentes navegadores para evadir detecciones.

5. Aplicación del Ciclo de Respuesta a Incidentes

Detección:
- Incidente identificado por el mensaje de ransomware en el equipo de recepción.

Contención:
- Desconectar el equipo de recepción de la red para evitar propagación.
- Bloquear la IP sospechosa (`192.168.110.139`) en el firewall como medida preventiva.

Erradicación:
- Formateo del equipo de recepción y reinstalación del sistema operativo.
- Eliminación del ransomware detectado.

Recuperación:
- Restauración de archivos a partir de copias de seguridad (si disponibles).
- Reincorporación del equipo a la red con medidas reforzadas de seguridad.

6. Hallazgos Clave

- El incidente principal fue un ransomware en el equipo de recepción.
- El servidor web recibió intentos de exploración maliciosa, pero sin explotación confirmada.
- La detección no fue proactiva, sino reactiva (mensaje de ransomware).
- La falta de controles de seguridad (copias de respaldo y MFA) facilitó el impacto.

7. Recomendaciones

- Implementar copias de seguridad regulares y pruebas de restauración.
- Desplegar un antimalware actualizado en equipos finales.
- Configurar un sistema de monitoreo de logs (SIEM) para detección temprana.

- Restringir acceso al servidor de pruebas (bWAPP) solo a entornos de laboratorio.
- Aplicar autenticación multifactor en cuentas críticas.
- Capacitar al personal en identificación de intentos de ingeniería social.

8. Anexos (Opcional)

- Capturas de pantalla, tablas, resumen de logs, etc.