Detección, Análisis y Eliminación de Malware en Codearts Solutions

---

🔹 Fase 1: Identificación y detección del malware

Se identificaron procesos sospechosos tanto en Linux como en Windows utilizando herramientas estándar. Se analizaron los registros del sistema y se escanearon los equipos con ClamAV y Malwarebytes, detectando varias amenazas potenciales. También se detectó tráfico de red anómalo asociado a conexiones persistentes con IPs externas no autorizadas.

Errores comunes:

- **Falsos positivos del antivirus:** puede marcar como sospechoso software legítimo.
  Solución: confirmar los hashes en VirusTotal antes de actuar.

- **No ejecutar el análisis con privilegios suficientes:** puede omitir archivos importantes.
  Solución: usar sudo o “Ejecutar como administrador”.

🔹 Fase 2: Análisis del malware y evaluación del impacto

Se analizaron los archivos maliciosos detectados para determinar su tipo (ransomware y spyware). Se extrajeron sus hashes para análisis en VirusTotal y se investigaron patrones de comportamiento utilizando herramientas como strings y editores hexadecimales. También se evaluó la extensión del daño a archivos críticos.

Errores comunes:

- **Eliminar archivos sin analizarlos previamente:** puede perderse evidencia útil.
  Solución: hacer copia forense antes de intervenir.

- **No distinguir entre malware y herramientas administrativas personalizadas.**
  Solución: verificar el contexto del archivo y su origen.

🔹 Fase 3: Eliminación del malware y recuperación del sistema

Los procesos maliciosos fueron detenidos y sus archivos eliminados de forma segura. Se restauraron archivos críticos desde copias de seguridad verificadas. Se revisaron logs del sistema para asegurar que el sistema quedó limpio y sin persistencia maliciosa.

Errores comunes:

- **Restaurar archivos desde una copia también infectada.**
  Solución: validar integridad antes de restaurar.

- **No reiniciar servicios después de limpiar procesos.**
  Solución: revisar y reiniciar servicios manualmente si es necesario.

🔹 Fase 4: Implementación de medidas de protección

Se activaron soluciones antivirus permanentes, listas blancas de ejecución y se reforzaron los firewalls para bloquear comunicaciones salientes no autorizadas. Se aplicó autenticación de múltiples factores y se endurecieron las políticas de acceso para prevenir nuevas infecciones.

Errores comunes:

- **No actualizar el antivirus después de instalarlo.**
  Solución: programar actualizaciones automáticas.

- **Aplicar reglas demasiado restrictivas en el firewall.**
  Solución: probar en entorno de pruebas antes de producción.