Reporte de Análisis Forense

Tarea:	Análisis Forense Consolidado
Fecha:	12/11/2025 23:00:24
Herramienta:	AutoForense v1.0
Sistema:	Windows

Resumen Ejecutivo

Resumen Corto: El análisis forense revela un sistema con serios problemas de estabilidad y corrupción, en lugar de una infección maliciosa activa. Se ha identificado un reinicio inesperado del sistema, múltiples fallos en la instalación de actualizaciones de Windows y errores en el inicio de servicios. Los procesos sin firma detectados parecen estar relacionados con estos fallos de actualización. La recomendación principal es ejecutar herramientas de reparación del sistema para restaurar la integridad de los archivos. JSON Estructurado: ```json

Análisis General

El sistema presenta una inestabilidad significativa evidenciada por un apagado inesperado, errores críticos de arranque y fallos generalizados en actualizaciones y servicios. Aunque se detectaron procesos sin firma, la evidencia correlacionada sugiere que son síntomas de corrupción del sistema o actualizaciones fallidas, no de un compromiso malicioso directo. Se requiere acción para reparar la integridad del sistema operativo.

Hallazgos Detectados

Hallazgo 1: Inestabilidad Crítica del Sistema y Apagado Inesperado

Nivel de Riesgo: MEDIUM

Confianza: HIGH

Descripción: Se ha detectado un evento crítico (ID 41) que indica que el sistema se reinició sin un apagado limpio, corroborado por un evento de error (ID 6008) que registra un cierre inesperado del sistema dos días antes. Esto, junto con un error de inicio rápido (ID 29), apunta a problemas graves de

estabilidad que podrían ser causados por fallos de hardware, conflictos de controladores o corrupción del sistema de archivos.

Evidencia: EventID 41 (Crítico, Reinicio inesperado), EventID 6008 (Error, Cierre anterior inesperado), EventID 29 (Error, Fallo en inicio rápido)

Hallazgo 2: Fallos Múltiples en Actualizaciones y Servicios del Sistema

Nivel de Riesgo: MEDIUM

Confianza: HIGH

Descripción: El visor de eventos muestra repetidos fallos en la instalación de actualizaciones de Windows (EventID 20) para componentes clave como la Tienda de Windows y CrossDevice. Esto se correlaciona con errores de inicio de servicios de terceros (Steam, Google Update) y errores de registro DCOM (ID 10010), indicando un problema sistémico que impide el correcto funcionamiento y actualización de las aplicaciones, lo que representa un riesgo de seguridad a largo plazo.

Evidencia: EventID 20 (Error instalación de actualizaciones: 9NTXGKQ8P7N0-MicrosoftWindows.CrossDevice, 9MSSGKG348SP-MicrosoftWindows.Client.WebExperience), EventID 7000, 7009 (Error inicio de servicios: Steam, gupdate), EventID 10010 (Error DCOM)

Hallazgo 3: Procesos de Componentes de Windows Sin Firma Digital

Nivel de Riesgo: LOW

Confianza: MEDIUM

Descripción: Se identificaron dos procesos sin firma: 'EdgeGameAssist.exe' y 'WidgetService.exe'. Aunque un proceso sin firma es una anomalía, ambos se ejecutan desde el directorio protegido 'C:\Program Files\WindowsApps', que es la ubicación legítima para aplicaciones de la Tienda de Microsoft. Dada la existencia de fallos de actualización para componentes de la tienda (hallazgo F2), es probable que la falta de firma sea una consecuencia de una instalación o actualización corrupta, en lugar de ser software malicioso.

Evidencia: Proceso: EdgeGameAssist.exe, Ruta: C:\Program Files\WindowsApps\... | Proceso: WidgetService.exe, Ruta: C:\Program Files\WindowsApps\...

Recomendaciones

1. URGENTE: Ejecutar un análisis de integridad de archivos del sistema. Abrir un Símbolo del sistema como Administrador y ejecutar 'sfc /scannow' seguido de 'DISM /Online /Cleanup-Image /RestoreHealth'.

2. Investigar la causa del apagado inesperado: revisar si hay actualizaciones recientes de controladores, realizar pruebas de diagnóstico de memoria (memtest) y verificar la salud del disco duro

(CHKDSK).

3. Ejecutar el Solucionador de problemas de Windows Update para intentar reparar los componentes de actualización.

4. Asegurarse de que todos los controladores del sistema, especialmente los del chipset y la BIOS/UEFI, estén actualizados desde el sitio web del fabricante (ASUS).

5. Una vez estabilizado el sistema, intentar reinstalar las aplicaciones que fallan (Steam, Google Chrome) y reparar las aplicaciones de la Tienda de Microsoft desde 'Configuración -> Aplicaciones'.

Declaración Legal

AutoForense se proporciona "tal cual", sin garantías de ningún tipo. Su uso es bajo su exclusiva responsabilidad. Ni el autor ni los distribuidores serán responsables por daños directos, indirectos, incidentales, consecuentes o de cualquier otra índole derivados del uso o mal uso del software. AutoForense no sustituye asesoría profesional forense ni legal; el usuario debe verificar el cumplimiento de todas las leyes y regulaciones aplicables.

Este reporte fue generado automáticamente por AutoForense y debe ser revisado por un profesional calificado antes de tomar cualquier acción basada en sus hallazgos.