¿Cómo puedo investigar la causa raíz de un evento?

- Análisis de Memoria
- Análisis de Inyección de Procesos
- Análisis de Creación de Procesos
- Uniéndolo todo: una investigación de extremo a extremo
  - ¿Por qué elegimos mostrar este ejemplo?

Existen tres bloques fundamentales de análisis a su disposición al investigar una alerta.

Actualmente, es más probable que un atacante realice una variedad de actividades en un sistema, utilizando una combinación de técnicas en memoria y secuestro de procesos (inyección o hollowing), que ejecutar un programa "hacker.exe" evidente.

Análisis de Memoria

El primer bloque fundamental se encuentra en la propia página de Respuesta o Incidente. Los análisis de memoria rastrean los comportamientos del proceso en memoria durante la inspección continua de posibles comportamientos de extorsión de datos (robo o cifrado).

Un estado de memoria que indica una probable manipulación suele ser indicativo de un problema.

No siempre es malicioso en sí mismo, ya que las malas prácticas de programación o los errores de software también pueden hacer que el estado de memoria de un programa en ejecución se vea alterado.

63504385.png?width=680
Aquí vemos un caso en el que un proceso de Adobe Acrobat exhibe posibles comportamientos de extorsión de datos después de abrir un PDF descargado, y vemos que la memoria del proceso Acrobat había sido modificada. El proceso Acrobat.exe en el disco no se vio afectado de ninguna manera.

El análisis forense de la memoria involucrada con el Acrobat.exe suspendido probablemente indicará un problema de preocupación, posiblemente un exploit en uso, si no una inyección de

proceso o un hollowing de proceso.

Para las respuestas de extorsión con un valor de Memoria Modificada de True (Verdadero), hay un ícono de descarga en la columna de Análisis de Causa Raíz para descargar el archivo de Diferencia de Memoria (Memory Diff) de la respuesta:

63602693.png?width=680
El archivo de Diferencia de Memoria (Memory Diff File) es el código fuente compilado de lo que se inyectó en el programa. Probablemente contenga malware y/o código de exploit, para que un analista de malware o de seguridad lo examine. Tenga en cuenta que este archivo no contiene el programa completo, solo la parte que fue alterada mediante un exploit o una técnica de ataque como la inyección de procesos. Obtenga más información sobre este archivo aquí.

Análisis de Inyección de Procesos

El primer indicador de que puede haber un evento de inyección de procesos relevante para una respuesta automatizada es la columna de Subprocesos Remotos No Confiables (Untrusted Remote Threads) de un Incidente/Respuesta. Esto indica que el análisis de comportamiento a nivel de kernel reveló un subproceso remoto no confiable observado con el proceso que realiza robo de datos o un comportamiento similar al ransomware.

63471635.png?width=680
Se puede realizar una investigación adicional en la página de Inyección de Procesos. Que el valor de Subprocesos Remotos No Confiables sea True (Verdadero) es un buen indicador de si se debe acudir allí.

La columna de Análisis de Causa Raíz también tiene un ícono para redirigirlo automáticamente a la página de Inyecciones, para mostrar solo las inyecciones de procesos relacionadas con la respuesta.

63602703.png?width=680
Después de hacer clic en el ícono de inyecciones, será dirigido a la página de Inyecciones de Procesos, donde verá solo las inyecciones de procesos relacionadas con la respuesta:

63569930.png?width=680
Aquí, en la página de Eventos de Inyección de Procesos, vemos la ruta y los argumentos del proceso inyector, y la ruta y los argumentos del proceso inyectado. Por lo general, los argumentos desempeñan un papel muy importante en los análisis de memoria, o indican, por ejemplo, qué comandos de PowerShell ejecutar. Los ID de proceso también están presentes, para ayudar a rastrear las inyecciones iterativas realizadas cuando un atacante salta de proceso en proceso, o para buscar el análisis de causa raíz en la página de Creación de Procesos.

63438879.png?width=680
¿Cómo supimos que rundll32.exe era en realidad un proveedor de antivirus? ¡Sigan leyendo!

Análisis de Creación de Procesos

Es muy poco común que un atacante utilice un solo proceso durante su ataque. Puede que ni siquiera sepa que las herramientas que está utilizando están generando nuevos procesos y utilizando varias herramientas administrativas en el sistema infectado.

La página de Creación de Procesos rastrea todos los procesos que abren otros procesos (o el mismo proceso), los argumentos utilizados y los ID de proceso, o Pids, para cada origen y destino.

Esto se realiza a nivel de kernel, lo que significa que no se pasa por alto nada.

Nota: la telemetría de Microsoft cuenta con parte de estos datos, pero no con todos. Optamos por no utilizar esa fuente de datos, ya que hemos observado que dicha fuente de telemetría tiende a pasar por alto eventos importantes, o los atacantes la desactivan durante un ataque.

¿Qué tan buena es nuestra visibilidad?

Uniéndolo todo: una investigación de extremo a extremo

¿Qué tan buena es nuestra visibilidad y con qué rapidez puede realizar un Análisis de Causa Raíz? Vea este ejemplo: se observó que un antivirus, que posiblemente cuenta con algunos de los permisos más altos en un sistema, intentaba inyectar código en nuestro software Cyber Crucible. Esperamos que haya sido para investigar nuestro software, pero de todos modos entramos en modo de autoprotección (por lo tanto, esto hizo que nuestro software rechazara la manipulación del antivirus... no existen puertas traseras que permitan el acceso para editar o utilizar nuestro software por parte de terceros externos).

Entonces, empecemos por aquí, con una respuesta automatizada:

63569937.png?width=680

Obviamente, Cyber Crucible no es ransomware. Aquí vemos que hubo un intento de inyección de procesos que implicaba un comportamiento sospechoso de subprocesos remotos, junto con comportamientos similares a la extorsión de datos.

De acuerdo, veamos qué está sucediendo en Eventos de Inyección de Procesos haciendo clic en el ícono de inyecciones. 5 segundos después, ¡tenemos nuestra respuesta!

63471644.png?width=56463438879.png?width=680

Pero espere, ¿rundll? Eso no es un hacker, ¿verdad? Seguramente, eso no es un programa hacker.exe. Hagamos algo de filtrado para obtener nuestra respuesta en la página de Creación de Procesos. No tenemos una captura de pantalla aquí, pero los ID de proceso están disponibles para todas las respuestas e inyecciones de procesos. Volvamos a la página de respuestas y hagamos clic en el ícono de creaciones de procesos para ir a la página de Creaciones de Procesos y filtrar automáticamente la cuadrícula para mostrar las creaciones de procesos relacionadas con esta respuesta.

63537184.png63438886.png?width=680

De forma rápida y sencilla, ahora vemos que la "raíz" (sin juego de palabras) fue WebRoot, un proveedor de antivirus, que generó un proceso rundll32.exe para cargar una de las DLL de WebRoot, la cual luego intentó hacer *algo* con el software de Cyber Crucible, para forzarlo a recorrer archivos como una herramienta de robo de datos.

¿Por qué elegimos mostrar este ejemplo?

Contamos con numerosos ejemplos de las técnicas de los atacantes, con distintos niveles de competencia por parte de estos. Los antivirus alcanzan un nivel de permisos en un sistema que requiere un nivel muy alto de habilidad, tecnología y preparación por parte de los atacantes. Que Cyber Crucible detecte comportamientos "similares a los de un hacker" provenientes de una herramienta de seguridad convencional, y luego los detenga automáticamente, demuestra algunos de los niveles más altos de ingeniería y excelencia en seguridad de nuestra parte, sin perdernos en exploits individuales o técnicas específicas de los atacantes.

Revision #1
Created 2026-07-24 01:34:00 UTC by Dennis Underwood
Updated 2026-07-24 01:34:00 UTC by Dennis Underwood