¿Qué muestra la página de Creaciones de Procesos?

Es muy poco común, posiblemente nunca ocurra, que un atacante ejecute un ataque completo desde dentro de un solo proceso.

El hecho de que una herramienta de ataque o una biblioteca de Windows utilice múltiples procesos y programas de Windows a veces es invisible para los usuarios del malware (es decir, los delincuentes).

Los comportamientos de los procesos representan una fuente importante de variables durante la toma de decisiones de Cyber Crucible, la cual involucra indicadores de comportamiento provenientes de una variedad de fuentes.

En ocasiones, estos comportamientos de procesos pueden derivar finalmente en la suspensión de un proceso a causa del robo de datos o del cifrado por ransomware, y pueden rastrearse desde el punto de entrada del atacante en el sistema hasta la ejecución final del software de extorsión.

En otras ocasiones, el rastreo de procesos puede identificar acceso remoto no autorizado, fraude, amenazas internas o software inesperado, pero sin extorsión de datos. Por lo tanto, no se trata de algo que el software de prevención de extorsión de datos de Cyber Crucible suspenda automáticamente, pero sigue siendo algo que usted querrá conocer.

Ya sea que los datos del proceso formen parte de un ataque de extorsión de datos, de algo más digno de mención, o simplemente del comportamiento habitual de un programa, se pone a disposición la información de origen y destino de los programas, incluidos los argumentos del programa. Esto proporciona un rico conjunto de datos para rastrear a los atacantes, incluidos aquellos que aprovechan tácticas de “living off the land”.

A continuación se muestra una captura de pantalla del tipo de datos que se pueden recopilar a partir de las creaciones de procesos.

CC_process_creation_demo.mp4

Revision #1
Created 2026-07-24 01:34:23 UTC by Dennis Underwood
Updated 2026-07-24 01:34:23 UTC by Dennis Underwood