La empresa de ciberseguridad CrowdStrike atribuyó a un problema en su sistema de validación la causa del bloqueo de millones de dispositivos con Windows, lo que provocó una interrupción generalizada a finales de la semana pasada.

> *«El viernes 19 de julio de 2024 a las 04:09 UTC, como parte de las operaciones regulares, CrowdStrike lanzó una actualización de configuración de contenido para el sensor de Windows con el fin de recopilar telemetría sobre posibles nuevas técnicas de amenaza»*, dijo la compañía en su Revisión Preliminar Posterior al Incidente (PIR).
>
> *«Estas actualizaciones son una parte regular de los mecanismos de protección dinámica de la plataforma Falcon. La actualización problemática de configuración de contenido de Respuesta Rápida resultó en un bloqueo del sistema Windows».*

El incidente afectó a los hosts de Windows que ejecutaban la versión 7.11 del sensor y superiores, que estaban en línea entre el 19 de julio de 2024 a las 04:09 UTC y las 05:27 UTC y recibieron la actualización. Los sistemas Apple macOS y Linux no se vieron afectados.

CrowdStrike explicó que entrega actualizaciones de configuración de contenido de seguridad de dos maneras: una a través del Contenido del Sensor que se envía con Falcon Sensor y otra a través del Contenido de Respuesta Rápida, que le permite identificar nuevas amenazas utilizando diversas técnicas de coincidencia de patrones de comportamiento.

Se informó que el bloqueo fue el resultado de una actualización de Contenido de Respuesta Rápida que contenía un error previamente no detectado. Cabe destacar que tales actualizaciones se entregan en forma de Instancias de Plantilla correspondientes a comportamientos específicos, que se asignan a Tipos de Plantilla específicos, para habilitar nueva telemetría y detección.

Las Instancias de Plantilla, a su vez, se crean utilizando un Sistema de Configuración de

Contenido, después del cual se despliegan en el sensor a través de la nube mediante un mecanismo denominado Archivos de Canal, que finalmente se escriben en el disco en la máquina Windows. El sistema también incluye un componente Validador de Contenido que realiza comprobaciones de validación en el contenido antes de que se publique.

> *«El Contenido de Respuesta Rápida proporciona visibilidad y detecciones en el sensor sin requerir cambios en el código del sensor»,* explicó la compañía.
>
> *«Esta capacidad es utilizada por los ingenieros de detección de amenazas para recopilar telemetría, identificar indicadores de comportamiento adversario y realizar detecciones y prevenciones. El Contenido de Respuesta Rápida son heurísticas de comportamiento, separadas y distintas de las capacidades de prevención y detección de IA en el sensor de CrowdStrike».*

Estas actualizaciones son luego analizadas por el Intérprete de Contenido del sensor Falcon, que facilita al Motor de Detección del Sensor para detectar o prevenir actividades maliciosas.

Aunque cada nuevo Tipo de Plantilla se somete a pruebas de estrés para diferentes parámetros, como la utilización de recursos y el impacto en el rendimiento, la causa raíz del problema, según CrowdStrike, se remonta al despliegue del Tipo de Plantilla de Comunicación Interproceso (IPC) el 28 de febrero de 2024, que se introdujo para identificar ataques a tuberías nombradas.

La línea de tiempo de los eventos es la siguiente:

- 28 de febrero de 2024: CrowdStrike lanza el sensor 7.11 a los clientes con el nuevo Tipo de Plantilla IPC
- 5 de marzo de 2024: El Tipo de Plantilla IPC pasa la prueba de estrés y se valida para su uso
- 5 de marzo de 2024: La Instancia de Plantilla IPC se lanza a producción a través del

Archivo de Canal 291

- 8-24 de abril de 2024: Se despliegan tres más Instancias de Plantilla IPC en producción
- 19 de julio de 2024: Se despliegan dos instancias adicionales de Plantilla IPC, una de las cuales pasa la validación a pesar de tener datos de contenido problemáticos

> *«Basado en las pruebas realizadas antes del despliegue inicial del Tipo de Plantilla (el 5 de marzo de 2024), la confianza en las verificaciones realizadas en el Validador de Contenido y los despliegues anteriores exitosos de Instancias de Plantilla IPC, estas instancias se desplegaron en producción»*, dijo CrowdStrike.
>
> *«Cuando el sensor recibió y cargó el contenido problemático en el Intérprete de Contenido, el contenido problemático en el Archivo de Canal 291 resultó en una lectura de memoria fuera de límites que desencadenó una excepción. Esta excepción inesperada no pudo ser manejada adecuadamente, resultando en un bloqueo del sistema operativo Windows (BSoD)».*

En respuesta a las interrupciones generalizadas causadas por el bloqueo y para evitar que vuelvan a ocurrir, la compañía con sede en Texas dijo que ha mejorado sus procesos de prueba y ha reforzado su mecanismo de manejo de errores en el Intérprete de Contenido. También planea implementar una estrategia de despliegue escalonado para el Contenido de Respuesta Rápida.