Microsoft anunció una nueva iniciativa de uso gratuito destinada a descubrir evidencia forense de sabotaje en sistemas Linux, incluidos rootkits y malware intrusivo que de otra forma, podrían pasar desapercibidos.

Se trata de Project Freta, un mecanismo forense de memoria basado en instantáneas que tiene como objetivo proporcionar una inspección de memoria volátil de sistema completo automatizada de snapshots de máquinas virtuales, con capacidades para detectar software malicioso, rootkits de kernel y otras técnicas de malware sigiloso como el proceso de ocultación.

El proyecto lleva el nombre de la calle Freta, de Varsovia, lugar de nacimiento de Marie Curie, famosa científica franco-polaca que trajo imágenes médicas de rayos X al campo de batalla durante la Primera Guerra Mundial.

> *«El malware moderno es complejo, sofisticado y está diseñado con la no capacidad de descubrimiento como principio básico. Project Freta tiene la intención de utomatizar y democratizar el análisis forense de VM hasta el punto en que cada usuario y cada empresa puedan barrer la memoria volátil en busca de malware desconocido con solo presionar un botón, sin necesidad de configuración»,* dijo Mike Walker, director senior de New Security Ventures en Microsoft.

El objetivo de este proyecto es evitar la presencia de malware desde la memoria, al mismo tiempo de ganar ventaja en la lucha contra los actores de amenazas que implementan y reutilizan malware sigiloso en los sistemas objetivo por motivos ulteriores, que hacen que la evasión sea inviable y aumentan el desarrollo y costo de malware en la nube no detectable.

El *«sistema de detección confiable»* funciona al abordar cuatro aspectos distintos que harían que los sistemas sean inmunes a los ataques en primer lugar al evitar que cualquier programa realice lo siguiente:

- Detectar la presencia de un sensor de seguridad antes de instalarse

- Residir en un área que está fuera de la vista del sensor
- Detectando la operación del sensor y, en consecuencia, borrándose o modificándose para escapar de la detección
- Alterar las funciones del sensor para causar sabotaje

> *«Cuando los atacantes y los defensores comparten una microarquitectura, cada movimiento de detección que hace un defensor perturba el medio ambiente de una forma que eventualmente puede ser descubierta por un atacante investido en secreto. La única forma de descubrir a esos atacantes es eliminar su visión de la defensa»,* dijo Walker.

Project Freta está abierto a cualquier persona con una cuenta de Microsoft (MSA), o una cuenta de Azure Active Directory (AAD), y permite a los usuarios enviar imágenes de memoria (.vmrs, .lime, .core o .raw), a través de un portal en línea o una API, publicar que genera un informe detallado que profundiza en diferentes secciones (módulos del núcleo, archivos en memoria, posibles rootkits, procesos y más), que pueden exportarse a través del formato JSON.

Microsoft informó que se centró en Linux debido a la necesidad de tomar sistemas de huellas digitales en la nube de una forma independiente de la plataforma a partir de una imagen de memoria codificada. También citó la mayor complejidad del proyecto, dada la gran cantidad de núcleos disponibles públicamente para Linux.

Esta versión de lanzamiento inicial de Project Fetra es compatible con más de 4000 núcleos de Linux, con soporte de Windows en proceso.

También está el proceso de agregar una capacidad de sensor que permite a los usuarios migrar la memoria volátil de máquinas virtuales en vivo a un entorno fuera de línea para un análisis posterior y más herramientas para toma de decisiones basadas en inteligencia artificial para la detección de amenazas.

> *«El objetivo de este esfuerzo de democratización es aumentar el costo de desarrollo de malware en la nube no detectable hacia su máximo teórico. Los productores de malware sigiloso quedarían encerrados en un ciclo costoso de reinvención completa, convirtiendo a esa nube en un lugar inadecuado para los ataques cibernéticos»,* dijo Walker.

Para más información, se puede acceder al portal de análisis en línea.