¿En qué se diferencia el Análisis de Comportamiento de Memoria de CC del escaneo de memoria?

¿Qué es el escaneo de memoria?

El escaneo de memoria es la práctica de tomar un bloque de memoria, normalmente copiándolo a una ubicación diferente en el sistema para su análisis, y escanearlo para su análisis.

Fotografía vs. acción en vivo

Esto no es un escaneo en vivo del programa mientras se comporta, sino una instantánea en el tiempo del programa. Piense en ello como una fotografía, en comparación con una transmisión en vivo. El estado del programa puede ser drásticamente diferente de un momento a otro, por lo que es más útil como ejercicio forense en un entorno controlado. Es menos útil en un entorno no controlado, como el entorno de un cliente. Cuanto más ocupada esté la máquina, o cuanto más esté haciendo un programa, más difícil es tener una imagen precisa del estado actual de un programa.

Cyber Crucible comenzó con un uso intensivo del escaneo de memoria, tratando de tomar muchas “fotografías” de los estados de memoria de los programas. A medida que nos volvimos más rápidos, encontramos múltiples cuellos de botella en cuanto a la rapidez con la que se podían tomar instantáneas de memoria, y a través de múltiples programas.

Preocupaciones sobre el consumo de recursos de CPU o GPU

Este escaneo de memoria puede ser extremadamente intensivo en recursos, y puede tomar algo de tiempo para programas grandes. Cuando Cyber Crucible utilizaba el escaneo de memoria, en

lugar del monitoreo inteligente del comportamiento de la memoria, se dedicaba un núcleo completo de CPU al escaneo.

Intel tiene una tecnología innovadora llamada Intel TDT AMS, que está disponible en arquitecturas específicas basadas en Intel con una GPU Intel integrada.

Escanea la memoria de un programa cuando se inicia por primera vez, utilizando la GPU para ayudar a no sobrecargar la CPU. Además, la GPU tiene un mejor rendimiento para el tipo de escaneo que se realiza (más sobre esto más adelante).

Metodología de escaneo

El escaneo de memoria se realiza para buscar códigos o “cadenas” específicas. Estas suelen ser las mismas piezas de datos que las herramientas de antivirus/EDR buscan en archivos potencialmente maliciosos.

El escaneo de memoria específicamente es más limitado que algunas de las búsquedas complejas que se pueden realizar contra un archivo.

Por lo tanto, el escaneo, por defecto, busca elementos ya conocidos, como malware antiguo, pero su capacidad para hacerlo es limitada.

Cyber Crucible solía escanear segmentos de memoria en busca de material criptográfico, pero resultó demasiado limitado para los entornos modernos, y desarrollamos un método diferente para observar comportamientos, utilizando lógica basada en el kernel.

Metodologías basadas en comportamiento vs. escaneo

Cyber Crucible migró de una metodología basada en escaneo a una basada en comportamiento por un par de razones.

Desventajas del escaneo

La primera es que se necesitaba usar una imagen en vivo en todos los programas. Las instantáneas dificultaban enormemente completar incluso un análisis limitado antes de que se necesitara otra. Se estaba perdiendo demasiada actividad del programa, casi como tener una cámara de video funcionando a una velocidad de fotogramas demasiado baja. Esto se agravaba

con la necesidad de monitorear todos los programas simultáneamente. Los servidores o estaciones de trabajo con mucha actividad, posiblemente las computadoras que más necesitaban monitoreo y que eran las más importantes, terminaban con el menor porcentaje de vigilancia realizada. Independientemente de la empresa o el producto, las limitaciones tecnológicas eran evidentes e inviables.

La segunda es que, más allá del consumo de recursos, el escaneo requiere, por defecto, buscar **algo conocido**. Por lo tanto, el escaneo de memoria debe basarse en firmas. Además, el escaneo de firmas debe ser un subconjunto limitado del escaneo de firmas más completo que se encuentra en el escaneo de antivirus basado en archivos. Los atacantes ya han eludido las defensas basadas en firmas de archivos durante años; hay muy pocas probabilidades de que los atacantes sean descubiertos por un sistema basado en firmas menos capaz.

Ventajas del análisis de comportamiento

El monitoreo de memoria basado en comportamiento de Cyber Crucible no requiere firmas, y aprovecha el acceso a la memoria del kernel para rastrear los comportamientos de todos los programas simultáneamente. Vamos a desglosar esto.

Primero, el monitoreo de comportamiento significa que el malware nuevo, o el malware que ha sido editado por atacantes para parecer nuevo, puede descubrirse fácilmente en tiempo real. El escaneo basado en firmas, ya sea de memoria o de archivos, depende de haber visto antes esa pieza específica de malware. Los atacantes han estado eludiendo las defensas basadas en firmas durante años, a pesar de contar con un conjunto completo de técnicas de escaneo contra archivos. Las técnicas de escaneo disponibles contra la memoria son un subconjunto de eso, y son incluso menos efectivas.

Segundo, el novedoso monitoreo del comportamiento de memoria de Cyber Crucible puede mantenerse en tiempo real en todos los programas simultáneamente, durante toda la ejecución de los programas. El escaneo de memoria sufre de graves cuellos de botella en los recursos que solo empeoran a medida que se ejecutan más programas. Los atacantes normalmente ejecutan docenas de muestras de malware a la vez, ahogando el análisis de escaneo de memoria debido a la velocidad y cantidad de programas a examinar a la vez, sin importar si se trata de un día cero o malware antiguo.

Revision #1
Created 2026-07-24 01:48:18 UTC by Dennis Underwood
Updated 2026-07-24 01:48:18 UTC by Dennis Underwood