¿Por qué el antivirus tradicional no puede detener los ataques de ransomware de día cero y sin archivos?

Respuesta breve: Las herramientas de seguridad basadas en firmas dependen del reconocimiento de patrones de ataque conocidos, pero los atacantes modernos prueban deliberadamente sus herramientas contra esas mismas defensas antes de implementarlas, y cada vez más evitan dejar archivos detectables por completo. Esta combinación de amenazas mutadas y no reconocidas junto con técnicas que operan únicamente en memoria ha hecho que los métodos de detección tradicionales sean mucho menos confiables.

El Problema de Depender de Firmas Conocidas

Los ataques de día cero son, por definición, lo suficientemente nuevos o alterados como para quedar fuera de lo que las herramientas de seguridad existentes ya reconocen. Los proveedores han prometido durante mucho tiempo mejoras para detectar estas amenazas, pero los atacantes tienen una ventaja inherente: pueden acceder a los mismos productos comerciales de seguridad que utilizan los defensores. Antes de lanzar una campaña, los atacantes suelen probar su malware contra herramientas de detección populares, refinándolo hasta que logra evadirlas. Esto convierte la detección en un objetivo en constante movimiento en lugar de una defensa fija.

Las Técnicas Sin Archivos Socavan las Listas Blancas

Los atacantes también han dejado de depender de colocar ejecutables maliciosos evidentes en un sistema. En cambio, secuestran aplicaciones legítimas y confiables ya aprobadas por las herramientas de listas blancas de aplicaciones, ejecutando actividad maliciosa a través de procesos que el software de seguridad asume que son seguros. Cuando este enfoque sin archivos se combina con código que muta rápidamente, los ataques pueden completarse en una ventana de

tiempo muy corta —a veces en apenas media hora— mucho antes de que un equipo humano de respuesta a incidentes pueda investigar de manera realista.

Los Atacantes Borran Sus Propias Huellas

En muchos casos, dado que el ataque reside en la memoria en lugar de en el disco, los atacantes eliminan registros, evidencia e incluso sensores de seguridad antes de finalizar su operación. Esto es similar a un ladrón que desactiva las cámaras de seguridad y las alarmas antes de cometer un delito: para cuando alguien busca evidencia, la visibilidad más útil ya ha sido destruida. Esta combinación de métodos de ataque impredecibles y evidencia autoeliminada es la razón por la que Cyber Crucible ha invertido un esfuerzo significativo en construir un enfoque automatizado y escalable, diseñado para capturar los datos críticos necesarios para tomar decisiones precisas antes de que los atacantes puedan borrar el rastro, en lugar de depender del reconocimiento de amenazas después de los hechos.

https://player.vimeo.com/video/1164197533?texttrack=es

Ver en Vimeo · Subtítulos: English, Français, Español, العربية

Revision #2
Created 2026-07-24 02:16:44 UTC by Dennis Underwood
Updated 2026-08-06 18:35:08 UTC by Dennis Underwood