

¿Cyber Crucible prueba de manera exhaustiva todo el ransomware posible?

Cyber Crucible opera a partir de un modelado conductual a nivel de kernel, para descubrir rápidamente comportamientos de robo de datos, robo de credenciales y cifrado de ransomware. Las decisiones conductuales se toman utilizando información del comportamiento de los procesos, comportamientos derivados de la memoria y ciertos tipos de comportamientos originados en archivos, para tomar una decisión justo antes de que ocurra la extorsión.

A pesar del gran número de muestras de software de ransomware y extorsión, estas pueden categorizarse conductualmente en un número relativamente pequeño de conjuntos.

Sin embargo, en la superficie, las defensas “superficiales” utilizadas por una variedad de herramientas de seguridad tienen que intentar contrarrestar un número muy grande de herramientas de extorsión. Es importante entender que nuestros análisis conductuales llegan mucho más a fondo en las herramientas y tácticas de los atacantes, reduciendo drásticamente la necesidad de algún tipo de prueba exhaustiva (imposible) de todo el malware posible en todo momento.

Los desarrolladores de Cyber Crucible categorizan el comportamiento a nivel de kernel de la memoria, los procesos y los archivos de una herramienta de extorsión, y luego se aseguran de que encaje en una de las capacidades defensivas conocidas. Ocasionalmente, de manera similar a una vacuna, la fórmula puede ajustarse ligeramente para producir una respuesta más precisa.

Muy rara vez aparece algo completamente nuevo.

El equipo de Cyber Crucible trabaja de manera exhaustiva para descubrir de forma preventiva técnicas novedosas que aún no se han observado en nuestra base de clientes ni en la inteligencia de amenazas.

¿El efecto?

1. La defensa de Cyber Crucible contra herramientas de extorsión es completa frente a todas las variantes de ransomware conocidas.
2. Las nuevas variantes de ransomware se bloquean incluso antes de afectar a los primeros clientes. Ni siquiera sabemos cómo llamar a la mayoría del software contra el que nos defendemos durante aproximadamente 120 días, hasta que los investigadores “se ponen al día”.

3. Los desarrolladores de ransomware y herramientas de extorsión a veces nos llaman para ver qué estamos haciendo, en un intento de encontrar un ángulo. Lamentablemente, la frustración causada por nuestra presencia parece a veces impulsar su evolución, lo que hace que otras herramientas sean incluso menos efectivas.

4. Damos la bienvenida a las pruebas de nuestro software. Cuando profesionales de pruebas de penetración, analistas de malware o especialistas en emulación de adversarios entran en el proceso de venta, ¡nos entusiasma!

Revision #1

Created 2026-07-24 01:53:43 UTC by Dennis Underwood

Updated 2026-07-24 01:53:43 UTC by Dennis Underwood