¿Qué sucede realmente cuando el ransomware ataca un servidor de una empresa?

Respuesta breve: Cuando el ransomware ataca un servidor, los atacantes normalmente deshabilitan primero sus servicios y luego cifran sus datos mientras impiden que los equipos de TI y seguridad puedan intervenir, a veces utilizando docenas o incluso cientos de estaciones de trabajo comprometidas para llevar a cabo el cifrado de forma remota.

Las primeras señales de un ataque

Uno de los primeros indicadores de que un servidor ha sido comprometido es una pérdida repentina de servicio. Dado que los atacantes saben que el ransomware puede corromper archivos accidentalmente durante el cifrado, muchos deciden deliberadamente detener las aplicaciones que se ejecutan en un servidor antes de que comience el proceso de cifrado. Esto significa que los empleados o clientes que dependen de ese sistema —ya sea una plataforma de nómina, una aplicación web u otro servicio crítico para el negocio— pueden notar una interrupción antes de que nadie se dé cuenta de que se está produciendo un incidente de seguridad.

Bloqueando a los defensores mientras el cifrado se propaga

Una vez que el ataque está en marcha, el ransomware comienza a cifrar los datos almacenados en el servidor. Para evitar que los equipos de seguridad o los administradores intervengan, los atacantes suelen bloquear el acceso de red al servidor, aislándolo de las personas que normalmente responderían ante la amenaza. Esta táctica le da al atacante tiempo para terminar de cifrar los archivos antes de que los defensores puedan actuar.

Las estaciones de trabajo pueden ser el verdadero punto débil

Curiosamente, el servidor en sí no siempre es el origen del peligro. En muchos casos, los atacantes comprometen una gran cantidad de estaciones de trabajo de empleados —a veces 50, 70 o más— que ya cuentan con acceso legítimo al servidor. Estas estaciones de trabajo se utilizan luego simultáneamente para cifrar los datos del servidor de forma remota. Debido a que el ataque se lanza desde múltiples puntos finales a la vez, las estaciones de trabajo conectadas al servidor a menudo representan una vulnerabilidad mayor que la propia infraestructura del servidor.

Este patrón resalta por qué la defensa contra el ransomware no puede centrarse únicamente en los servidores. La seguridad de los puntos finales en todos los dispositivos con acceso al servidor desempeña un papel fundamental para detener los ataques antes de que el cifrado se propague. FortressAI de Cyber Crucible está diseñado para identificar e interrumpir estos comportamientos en las etapas más tempranas, ya sea que la amenaza se origine en un servidor o se propague desde estaciones de trabajo conectadas.

https://player.vimeo.com/video/1041172405?texttrack=es

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

Revision #2
Created 2026-07-24 02:13:48 UTC by Dennis Underwood
Updated 2026-08-06 18:34:42 UTC by Dennis Underwood