

¿Qué sucede realmente en los momentos durante un ataque de ransomware?

Respuesta breve: La fase de cifrado real de un ataque de ransomware es sorprendentemente rápida, y a menudo se completa en aproximadamente 60 a 90 segundos una vez activada, aunque los atacantes dedican un tiempo considerable y no visible previamente a posicionarse dentro de una red. Para el momento en que aparecen síntomas visibles, el daño ya está ocurriendo en tiempo real, razón por la cual la detección debe producirse antes del desencadenante final, no después.

La calma antes del ataque

Antes de que el ransomware se active, los atacantes suelen pasar tiempo moviéndose silenciosamente por los sistemas de una empresa, identificando datos valiosos, desactivando copias de seguridad y estableciendo las condiciones necesarias para un ataque exitoso. Este trabajo preparatorio puede pasar inadvertido porque las operaciones normales del negocio continúan como de costumbre. La red puede parecer estable y saludable justo hasta el momento en que el atacante decide lanzar la etapa final. De manera similar a un inquietante silencio justo antes de que ocurra algo catastrófico, este período de calma puede ser engañoso, ya que no refleja la interrupción que está por ocurrir.

La rápida aparición del daño

Una vez lanzado, un evento de ransomware puede desarrollarse en menos de dos minutos. En esa breve ventana de tiempo, los empleados pueden notar interrupciones súbitas: el correo electrónico deja de funcionar, los sistemas telefónicos quedan en silencio, las aplicaciones se comportan de manera errática o las conexiones de red se vuelven inestables. Estos son síntomas del cifrado y del compromiso del sistema ocurriendo simultáneamente en todo el entorno. Debido a que el proceso avanza con tanta rapidez, normalmente no hay suficiente tiempo para que una persona intervenga manualmente una vez que comienza.

Por qué algunos sistemas siguen funcionando

Un detalle inquietante de muchos incidentes de ransomware es que no todo falla al mismo tiempo. Algunos servicios pueden seguir funcionando con normalidad incluso mientras otros colapsan. Esto suele ocurrir porque esos sistemas no afectados son precisamente donde el atacante todavía está operando, utilizándolos como punto de apoyo o área de preparación. Reconocer este patrón es importante, ya que asumir que un problema es "solo parcial" puede crear una falsa sensación de seguridad mientras el compromiso está activamente en curso. La prevención eficaz depende de identificar y detener la actividad maliciosa antes de que comience la etapa destructiva final, ya que, una vez activada, la ventana de acción es extremadamente breve.

<https://player.vimeo.com/video/1046658956?texttrack=es>

[Ver en Vimeo](#) · Subtítulos: English, Français, Español, العربية

Revision #2

Created 2026-07-24 02:13:35 UTC by Dennis Underwood

Updated 2026-08-06 18:34:40 UTC by Dennis Underwood