¿Por qué los ataques de ransomware son cada vez más comunes cada año?

Respuesta breve: Los ataques de ransomware están aumentando porque los grupos de ciberdelincuentes han evolucionado de actores desorganizados y oportunistas a operaciones disciplinadas que utilizan la automatización para atacar a muchas víctimas de manera eficiente y extraer el pago rápidamente.

De startups caóticas a operaciones organizadas

Cuando el ransomware se convirtió por primera vez en una amenaza generalizada, muchos atacantes eran inexpertos. Una ola de personas recientemente desempleadas durante la era de la pandemia intentó incursionar en el cibercrimen, a menudo con resultados inconsistentes. Como ocurre con cualquier industria emergente, solo los operadores más organizados y capaces sobrevivieron a ese período inicial de depuración. Con el tiempo, estos grupos comenzaron a funcionar menos como oportunistas dispersos y más como negocios estructurados enfocados en generar ingresos consistentes.

Para 2024, esta madurez se ha traducido en una fuerte dependencia de la automatización. Las operaciones de ransomware establecidas ahora utilizan herramientas automatizadas para incorporar a participantes menos experimentados en sus ataques, manteniendo al mismo tiempo procesos eficientes y repetibles. Esto les ha permitido escalar su actividad mucho más allá de lo que un pequeño equipo de hackers expertos podría lograr manualmente.

Calibrar el ataque para obtener el máximo pago

Una parte clave de esta evolución es aprender a dimensionar correctamente un ataque. Si una intrusión es demasiado leve, un equipo de TI bien preparado simplemente puede restaurar los sistemas y evitar pagar nada. Si un ataque es demasiado extenso y elimina toda la infraestructura de la empresa, es posible que no quede ningún negocio viable para emitir un pago de rescate. Los

grupos de ransomware modernos apuntan a un punto intermedio: suficiente disrupción para presionar a una empresa a pagar rápidamente, sin causar tanto daño que la recuperación o la negociación se vuelvan irrelevantes.

Por qué la automatización impulsa el aumento

Una vez que un proceso de ataque puede automatizarse, los ciberdelincuentes ya no se conforman con perseguir a una sola víctima a la vez. Utilizando herramientas que se asemejan a la inteligencia artificial, el aprendizaje automático y la automatización robótica de procesos, pueden atacar a docenas o cientos de organizaciones en paralelo. Muchas víctimas optan por no divulgar públicamente los incidentes, lo que permite a los atacantes completar un ciclo de extorsión y pasar a nuevos objetivos. Este modelo de negocio escalado y repetible—más que cualquier nueva tecnología en particular—es la razón principal por la que los ataques de ransomware continúan en aumento.

https://player.vimeo.com/video/1043463561?texttrack=es

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

Revision #2
Created 2026-07-24 02:15:36 UTC by Dennis Underwood
Updated 2026-08-06 18:34:58 UTC by Dennis Underwood