La 'madre de todas las filtraciones' descubierta después de la filtración de 26 mil millones de registros

Una de las filtraciones de datos más grandes hasta la fecha podría comprometer miles de millones de cuentas en todo el mundo, lo que genera preocupaciones sobre un ciberdelito generalizado.

por Katrielle Soussana 25 de enero de 2024 en Noticias del editor, Artículos

El nuevo servicio AT&T Cybersecurity USM Anywhere Advisors ayuda a establecer y mantener la eficacia en la detección y respuesta a amenazas

Compartir en Facebook

Compartir en Twitter

Ayer, el equipo de seguridad de Cybernews anunció lo que probablemente resultará ser la mayor violación de datos de todos los tiempos. En un esfuerzo conjunto con el investigador de seguridad Bob Dyachenko, el equipo de Cybernews encontró una instancia abierta en la web que contenía miles de millones de registros expuestos. Esta violación, que representa la increíble cantidad de 12 terabytes de información y 26 mil millones de registros, está siendo apodada como la Madre de Todas las Infracciones (MOAB para abreviar).

Desde Twitter y LinkedIn hasta Adobe y Wattpad y muchos más, se encontraron datos filtrados de estas importantes marcas en línea incluidos en la instancia de MOAB. Tencent, la aplicación de mensajería china, fue la que tuvo el mayor número de registros expuestos: sólo 1.400 millones. Además, también se encontraron registros de organizaciones gubernamentales globales.

Greg Day, vicepresidente senior y CISO de campo global de Cybereason, comentó que: “A medida que nos acercamos a los 6 años de GDPR, está claro que numerosas empresas enfrentan desafíos para detectar rápidamente ciberataques cada vez más complejos, y el tiempo promedio de respuesta a menudo se extiende a cientos de días."

Como resultado, los registros combinados de todos estos consumidores ahora están expuestos a cualquier persona en la web. Y, si bien gran parte de esta información probablemente se originó en violaciones anteriores, sin duda también hay algunos datos aún no vistos en la mezcla.

La persona (o personas) detrás del MOAB es una de las preguntas que quedan por resolver. Podría ser un actor de amenazas o un intermediario de acceso. En resumen, es probable que se trate de alguien interesado en tener fácil acceso a tantos miles de millones de registros.

Aunque en algunos casos el MOAB puede contener datos duplicados, su impacto apenas disminuye. No se pueden subestimar las consecuencias que afrontan los consumidores tras esta infracción. Para los piratas informáticos, este tesoro escondido de una mina de datos se convertirá en una forma increíblemente fácil de obtener PII (información de identificación personal) sobre sus objetivos.

Según Paul Bischoff, defensor de la privacidad del consumidor en Comparitech, “con una sola consulta, un hacker podría descubrir todo lo que se ha filtrado en línea sobre usted, desde contraseñas antiguas hasta sus pasatiempos e intereses. Estas bases de datos se volverán más completas a medida que pase el tiempo, lo que hará más difícil para las víctimas defenderse del fraude y otros delitos”.

Y esta información podría usarse de manera maliciosa para phishing, relleno de credenciales y robo de identidad personal.

Las implicaciones de esto podrían resultar inmensas. De hecho, considerando que muchos consumidores reutilizan nombres de usuario y contraseñas en múltiples plataformas en línea, las consecuencias de este MOAB podrían tener un alcance aún mayor de lo que ya es.

Erfan Shadabi, experto en ciberseguridad de Comforte AG, está de acuerdo y explica que “el impacto potencial del MOAB en los consumidores no tiene precedentes, y los investigadores destacan el riesgo de un tsunami de ataques de relleno de credenciales. Esta amenaza es particularmente potente debido a la práctica generalizada de reutilización de nombres de usuarios y contraseñas”.

Entonces, ¿qué se puede hacer en respuesta a esto? ¿Se puede hacer algo?

Según Roger Grimes, evangelista de la defensa basada en datos de KnowBe4, la falta de privacidad de los datos es casi un hecho en este momento. “Creo que la mayoría de la gente en este mundo ahora piensa correctamente que al menos una parte de su información personal está disponible en Internet. Es una triste realidad de la vida y me pregunto cómo afecta a los más jóvenes y a la sociedad en general crecer en un mundo donde nuestra información privada ya no lo es”.

Pero eso no significa que sea inútil.

Chris Hauk, defensor de la privacidad del consumidor en Pixel Privacy, sugiere algunas formas integrales en las que los usuarios pueden protegerse. “Durante mucho tiempo he instado a todos los usuarios de Internet a actuar como si sus datos personales estuvieran disponibles en algún lugar de la web. Esto significa que los usuarios deben verificar su información de inicio de sesión para cada sitio... Los usuarios también deben estar alerta a los correos electrónicos de phishing, mensajes de texto y llamadas telefónicas de partes que utilizan los datos de la base de datos”.

También es importante que las personas preocupadas verifiquen si su información personal está involucrada en la violación. Esto se puede hacer con la práctica herramienta de verificación de datos personales en el sitio Cybernews. Al ingresar un correo electrónico o un número de teléfono, los consumidores pueden descubrir si alguna de sus PII relacionadas está expuesta en línea.

Tamara Kirchleitner, analista senior de operaciones de inteligencia de Centripetal, añade que no sólo los individuos deben estar en guardia, sino también las organizaciones. “Es crucial que las organizaciones prioricen la protección de datos e inviertan en estrategias integrales de ciberseguridad. Esto incluye capacitación en concientización, administradores de contraseñas seguros, auditorías de seguridad, cifrado sólido e incidencias.

t planes de respuesta”.

Tom Gaffney, experto en ciberseguridad de F-Secure: “Un caso como este enfatiza la necesidad de que las personas sean proactivas a la hora de salvaguardar sus datos y comprender cómo reducir su riesgo. Una investigación que realizamos recientemente encontró que casi un tercio de los británicos (29%) no saben qué medidas pueden tomar para mitigar los riesgos de que sus datos se vean comprometidos”.

El panorama tras la Madre de Todas las Infracciones es, sin duda, nefasto. Pero sólo el tiempo dirá cómo se desarrolla todo. Mientras tanto, si los consumidores y las organizaciones en riesgo toman las medidas adecuadas hoy, puede haber una posibilidad para que todos, colectivamente, salgamos ilesos.

Darren Guccione, director ejecutivo y cofundador de Keeper Security: “Esta filtración masiva subraya los persistentes y crecientes desafíos cibernéticos que enfrentan las organizaciones a la hora de salvaguardar datos confidenciales. La magnitud de la filtración es asombrosa: abarca 12 terabytes y 26 mil millones de registros. Esta violación debería servir como una llamada de atención para que las organizaciones reevalúen sus estrategias de ciberseguridad, enfatizando las medidas proactivas sobre las respuestas reactivas. A medida que las amenazas cibernéticas continúan evolucionando, no se puede subestimar la importancia de una inteligencia sólida sobre amenazas, un monitoreo continuo y una respuesta rápida a incidentes.

“Las organizaciones deben implementar una arquitectura de seguridad de confianza cero y una política de acceso mínimo para ayudar a prevenir la escalada de privilegios no autorizada y garantizar que las funciones de acceso de los usuarios se apliquen estrictamente. Las empresas también deberían contar con un monitoreo de eventos de seguridad para detectar y analizar escaladas de privilegios para que se pueda detectar y bloquear comportamientos anómalos”.