Un grupo de hackers y defensores de la transparencia, publicó 269 GB de datos presuntamente robados de más de 200 departamentos de policía, centros de fusión y otras agencias de aplicación de la ley en Estados Unidos.

Nombrado colectivamente como BlueLeaks, los datos expuestos filtrados por el grupo DDoSecrets, contienen cientos de miles de documentos confidenciales de los últimos diez años con información oficial y personal.

DDoSecrets, o Denegación de Secretos Distribuidos, es un colectivo de transparencia similar a WikiLeaks, que publica información clasificada y presentada por filtradores y piratas informáticos, mientras que asegura que la organización nunca se involucra en la exfiltración de datos.

Según el grupo hacktivista, el vertedero de BlueLeaks incluye *«informes policiales y del FBI, boletines, guías y más, lo que proporciona información única sobre la aplicación de la ley y una amplia gama de actividades gubernamentales, incluidos miles de documentos que mencionan COVID19».*

Un análisis rápido del volcado de BlueLeaks muestra que los datos contienen más de un millón de archivos, incluyendo imágenes, documentos, videos, páginas web, archivos de texto, correos electrónicos, archivos de audio y más, aunque aún no se ha investigado cuántos archivos están clasificados y no se supone que sean públicos.

Algunas alertas y guías filtradas en BlueLeaks también contienen información sobre las protestas, incluidas las recientes protestas de Black Lives Matter en todo el país tras la muerte de George Floyd en el momento en que estaba bajo custodia de la policía de Minneapolis.

Algunas de las agencias de Estados Unidos que aparecen en BlueLeaks son:

- Centro de fusión de Alabama

- Centro de Inteligencia Regional de Austin
- Centro de Inteligencia Regional de Boston
- Centro de Análisis de Información de Colorado
- Asociación de Oficiales de Narcóticos de California
- Centro de Información y Análisis de Delaware
- Asociación de Antiguos Alumnos de la Academia de Ciudadanos del FBI de Houston
- Capítulo de la Asociación de la Academia Nacional del FBI Arkansas/Missouri
- Capítulo de Michigan de la Asociación de la Academia Nacional del FBI
- Asociación de la Academia Nacional del FBI Texas

Al parecer, la fuente de estos datos masivos proviene de una violación de seguridad en la empresa de alojamiento web con sede en Houston, Netsential Inc, donde está alojado el servidor web de la Asociación Nacional de Centros de Fusión (NFCA), según informó el blog de seguridad Krebs.

Los centros de fusión son en esencia, centros de información que permiten el intercambio de inteligencia entre agencias locales, estatales, tribales, territoriales y federales, maximizando su capacidad de detectar, prevenir, investigar y responder a actividades criminales y terroristas.

En un comunicado, la NFCA confirmó a Krebs que las *«fechas de los archivos en la filtración en realidad abarcan casi 24 años, desde agosto de 1996 hasta el 19 de junio de 2020, y que los documentos incluyen nombres, direcciones de correo electrónico, números de teléfono, documentos PDF, imágenes y una gran cantidad de archivos de texto, video, CSV y ZIP»*.

Netsential confirmó que un actor de amenazas aprovechó una cuenta de usuario de cliente de Netsential comprometida y la función de carga de la plataforma web y extrajo los datos de clientes de Netsential, incluidas varias agencias de policía de Estados Unidos y los Centros Fusion.

Netsential es la misma compañía de alojamiento web que fue abusada anteriormente por los hackers para infectar a las víctimas con ransomware enviando correos de phishing

disfrazados de NFCA.