09/12/2024

’Hackers’ aseguran haber robado 560 GB de datos a la Agencia Tributaria y piden rescate

El grupo de ’hackers’ Trinity asegura haber robado millones de datos a la AEAT que, de momento, niega haber sido objeto de un ciberataque. Fuentes gubernamentales consultadas, sin embargo, le dan credibilidad



Un **grupo de hackers conocido como Trinity** asegura haber robado millones de datos de la Agencia Tributaria (AEAT). Según ha publicado en su web de filtraciones y han recogido varios servicios de seguimiento de ciberataques, se han hecho con 560 GB de información, han **secuestrado parte de los sistemas de la AEAT**, cifrado los datos y pedido un rescate por liberarlos, del que aún se desconoce la cifra exacta, pero podría rondar los varios millones de euros. Si no reciben el dinero, amenazan con publicar toda la información el 31 de diciembre. Consultada por este diario, la AEAT niega de momento haber sido objeto de ataque. Sin embargo, fuentes gubernamentales de lucha contra el cibercrimen, consultadas por El Confidencial, dan credibilidad al anuncio de robo por parte de Trinity.

A las pocas horas de conocerse el supuesto robo de datos, la Agencia Tributaria ha asegurado no tener conocimiento de ningún **incidente**. "En relación con el supuesto caso de ataque informático, se han revisado todos los sistemas y en estos momentos están funcionando todos los servicios sin ningún problema y **no se ha detectado ningún indicio de posibles equipos cifrados o salidas de datos**. La Agencia Tributaria mantiene bajo observación todos sus sistemas para hacer seguimiento", ha señalado un portavoz de la AEAT a este diario.

Fuentes consultadas de la lucha contra el cibercrimen señalan, sin embargo, que dado el historial del grupo Trinity, **dan credibilidad al anuncio de ataque**. "Es muy probable que la puerta de entrada haya sido un Ayuntamiento o una Diputación. De ahí, saltan a la red Sara y pueden colarse en la AEAT. Así es como están entrando en todas las instituciones públicas", explican estas fuentes.

Otros especialistas en ciberseguridad señalan además que **"el hecho de que no haya un incidente visible [como asegura la AEAT] no quiere decir que alguna base de datos no esté comprometida**. Puede ser un ataque que haya afectado a alguna réplica de bases de datos. Eso permite que sigan funcionando con normalidad, pero la exfiltración puede ser muy completa. Por ejemplo, imagina que el ransom es en un servidor con las copias de seguridad: todo va a seguir funcionando bien, pero ese fichero de datos es potencialmente muy, muy sensible. Fue lo que ocurrió con el hackeo masivo a Equifax en 2017". Ese año, los datos fiscales de casi 150 millones de contribuyentes estadounidenses, 15 millones de británicos y casi 20.000 canadienses, quedaron

totalmente expuestos. Equifax descubrió el agujero en julio de 2017, pero no lo hizo público hasta septiembre.

En España, la red Sara es un conjunto de infraestructuras de comunicaciones gestionado por el Ministerio de Transformación Digital y de Función Pública que interconecta distintas Administraciones Públicas españolas entre sí, facilitando el intercambio de información y el acceso a servicios. **No es la primera vez que se usa esta red para obtener el acceso ilícito a instituciones del gobierno**. Una de las más sonadas fue el robo de datos de más de 500.000 contribuyentes a la Agencia Tributaria realizado a finales de 2022 por José Luis Huertas Rubio, conocido como Alcasec. Tal y como quedó probado en la investigación, Alcasec logró acceder a la AEAT colándose primero en la red Sara, de ahí al sistema del Punto Neutro Judicial, obteniendo credenciales de acceso de varios funcionarios, y finalmente a la Agencia Tributaria.

"Si lo han publicado para venderlo, es muy posible que el ataque sea cierto por el historial que llevan. La cuestión es que la red Sara ya se ha visto comprometida más de una vez, como en el ataque al Servicio Público de Empleo Estatal (SEPE) hace unos años, o el de la DGT", señala un especialista en ciberseguridad consultado. Otra fuente, conocedora de la red Sara y del funcionamiento de los sistemas de la Administración Pública, **duda que esta red haya sido la puerta de entrada**. "La AEAT es el único organismo aislado de la red Sara. Se puede usar como pasarela, para entrar a otro organismo conectado y de ahí a la Agencia Tributaria, pero no daría opción a sacar toda la información que dicen haber sacado. En caso de que el hackeo sea cierto, me suena más al trabajo de un insider, de alguien desde dentro que haya dado algún vector de acceso".

Trinity es un grupo de hackers relativamente nuevo que ha ganado notoriedad por emplear un ransomware del mismo nombre y una estrategia de doble extorsión. Esto significa que, en primer lugar, extrae los datos de la víctima antes de iniciar el proceso de cifrado. Posteriormente, cifra los archivos robados mediante un algoritmo conocido como ChaCha20, **dejándolos inutilizables sin la clave de descifrado correspondiente**. Los archivos comprometidos suelen renombrarse con la extensión trinitylock, lo que permite identificar claramente cuáles han sido afectados.

Trinity se ha dado a conocer en los últimos meses por ataques a hospitales de EEUU y Reino Unido, forzando la Centro de Coordinación de Ciberataques del Departamento de Salud de EEUU a publicar un informe de alerta sobre su funcionamiento. "El ransomware Trinity fue detectado por primera vez en mayo de 2024. Este software malicioso se infiltra en los sistemas utilizando diversos vectores de ataque, como correos electrónicos de phishing, sitios web maliciosos y la explotación de vulnerabilidades en el software. **El impacto de Trinity es devastador**", explica el informe, "ya que no existen herramientas públicas para descifrar los datos afectados".

El modus operandi de Trinity suele ser filtrar unos días después de sus ataques la cantidad que piden por el rescate de los datos. En su publicación sobre el ataque a la AEAT, cifran en 38 millones de dólares el valor de la organización. Es la cantidad que usan para luego calcular una cifra de rescate, que fácilmente podría llegar a varios millones de euros.

Fuente: https://www.elconfidencial.com/

LINK DE LA NOTICIA