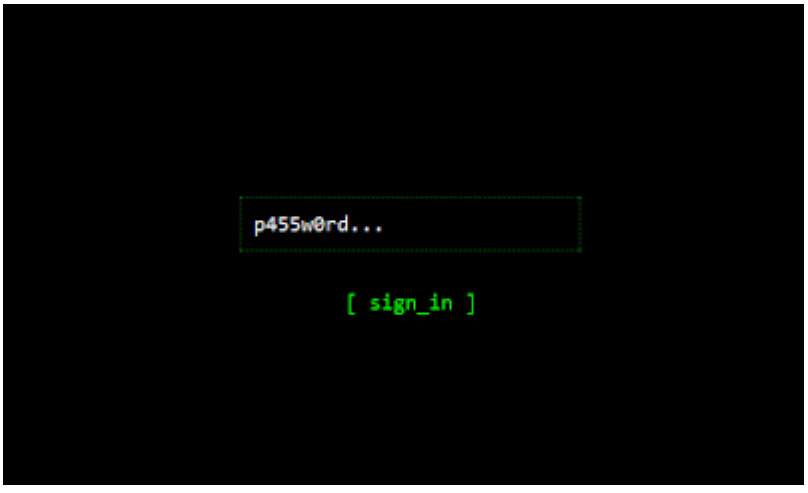
Negociaciones con el grupo de ransomware Akira: un enfoque desaconsejado

By newschu

Published: 2025-05-05 · Archived: 2026-04-05 16:58:49 UTC

Algunas entidades afectadas por ciberataques optan por negociar con actores de amenazas, como el grupo de ransomware Akira, una práctica que no es recomendable en absoluto. Negociar con estos ciberdelincuentes rara vez garantiza la recuperación de los datos o la no publicación de la información robada.

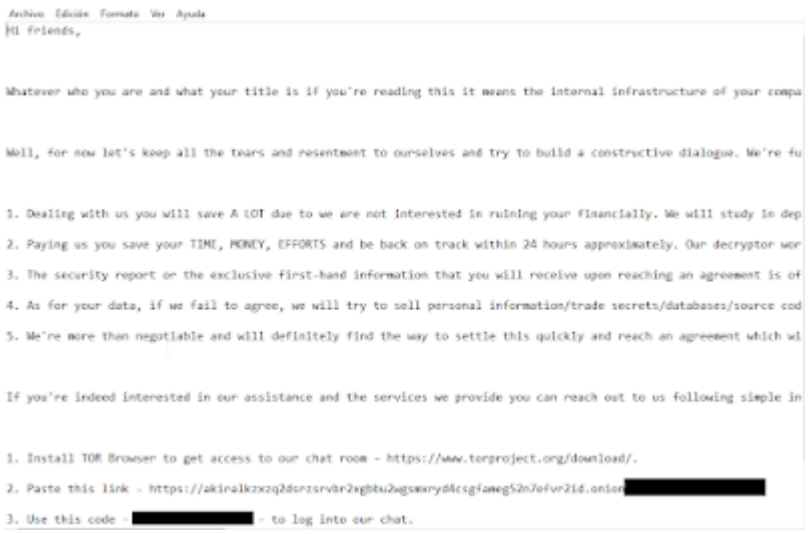
Cómo opera Akira: el archivo akira_readme.txt



Cuando una entidad es víctima de Akira, recibe un archivo de texto llamado **akira_readme.txt**. Este archivo contiene instrucciones detalladas para contactar a los ciberdelincuentes.

Habitualmente, incluye un ID único que permite a las víctimas iniciar sesión en una página de negociación en la Dark Web, diseñada por Akira para interactuar con sus objetivos. A través de esta plataforma, los atacantes

gestionan las demandas de rescate y, en muchos casos, presionan a las víctimas para que paguen.



Archivo Edición Formato Ver Ayuda

Hi friends,

Whatever who you are and what your title is if you're reading this it means the internal infrastructure of your compa

Well, for now let's keep all the tears and resentment to ourselves and try to build a constructive dialogue. We're fu

1. Dealing with us you will save A LOT due to we are not interested in ruining your financially. We will study in dep
2. Paying us you save your TIME, MONEY, EFFORTS and be back on track within 24 hours approximately. Our decryptor wor
3. The security report or the exclusive first-hand information that you will receive upon reaching an agreement is of
4. As for your data, if we fail to agree, we will try to sell personal information/trade secrets/databases/source cod
5. We're more than negotiable and will definitely find the way to settle this quickly and reach an agreement which wi

If you're indeed interested in our assistance and the services we provide you can reach out to us following simple in

1. Install TOR Browser to get access to our chat room - https://www.torproject.org/download/.
2. Paste this link - https://akiralkzxzq2dsrzsrvbr2xgbtu2wgsxmryd4csgfameg52n7efvr2id.onion[redacted]
3. Use this code - [redacted] - to log into our chat.

nota de rescate del grupo akira

Seguimiento de los intentos de negociación

Tras un análisis detallado, identificamos cuatro chats de distintas empresas que intentaron dialogar con Akira tras ser atacadas. Algunas de estas empresas aún figuraban como víctimas en el sitio web del grupo.

Días después de las negociaciones fallidas, en las que no se logró un acuerdo económico, los datos de estas compañías fueron publicados en el sitio de filtraciones de Akira, alojado en la Dark Web —una parte de internet no indexada, accesible solo mediante navegadores especializados como Tor, donde los ciberdelincuentes suelen compartir información robada.

De los cuatro casos analizados, tres entidades se negaron a negociar, mientras que solo una realizó un pago en Bitcoin. A continuación, presento algunos fragmentos de las conversaciones entre Akira y los negociadores de las entidades.

Primer caso: Las increibles "ofertas" que hace akira pero la entidad se negó a pagar

> Entidad: Nos gustaría saber qué datos nos robaste.
>
> Akira: Hola. Has contactado con el chat de soporte de Akira. Estamos preparando la lista de datos que obtuvimos de tu red. Por ahora, **debes saber que contactarnos es la mejor manera de resolver esto de forma rápida y económica**. Mantente en contacto y ten paciencia. Nos pondremos en contacto contigo pronto. **¿Tienes permiso para negociar en nombre de tu organización?** Una vez que recibamos una respuesta, te proporcionaremos todos los detalles.
>
> Entidad: Sí

> Akira: list().txt, Estos archivos se obtuvieron de tu red antes del cifrado. Puedes elegir de 2 a 3 archivos aleatorios de hasta 10 MB cada uno de la lista y los subiremos a este chat como prueba de posesión. **Para demostrar que podemos descifrar tus datos correctamente**, puedes subir de 2 a 3 archivos cifrados de hasta 10 MB cada uno a nuestro chat y **te enviaremos copias descifradas**.

A esta empresa le exigían **450,000 dólares**. Después de algunos días, le ofrecieron una "oferta" de **400,000 dólares**. La empresa dejó de responder, mientras el soporte intentaba apresurar el trato, hasta que **los datos fueron publicados**.

Los grupos de ransomware afirman que esta vía es más rápida y económica. Además, insisten en que **demostrar su descifrador** puede hacer que las víctimas caigan en esta charla tan cordial con el soporte de Akira.

Segundo Caso: víctima de Estados Unidos paga en Bitcoin

> Akira: Nosotros obtuvimos sus datos. Podemos descifrarlos correctamente y restaurar su infraestructura en poco tiempo.

> Entidad:Lo máximo que tenemos son entre 10 y 15 mil dólares, y podríamos pedir prestado un poco más. Pero como dije, somos una pequeña empresa que lleva más de medio año en una fase de baja actividad. Apenas estamos empezando nuestra temporada alta para ganar lo suficiente para el resto del año.

> Entidad: **Saben que tenemos sistemas muy antiguos y no podemos permitirnos actualizarlos**. **No tenemos copias de seguridad y no podemos trabajar en absoluto**.

Al final de esta conversación, el soporte de Akira aceptó la oferta de la empresa. Inicialmente, exigía **75,000 dólares**, pero redujo la cifra a **25,000 dólares**.

En una nueva dirección de Bitcoin, se transfirieron algunos bitcoins de prueba y, posteriormente, el resto de los bitcoins prometidos. Finalmente, **la empresa desapareció del sitio de Akira ransomware, el chat entre Akira y la entidad fue eliminado**.

Una víctima de ransomware pagando a Akira en su cuenta de Bitcoin

La víctima siguió preguntando sobre cómo restaurar sus sistemas encriptados. El soporte de Akira envió un desencriptador llamado **unlocker.exe** con instrucciones para proceder con la desencriptación de los sistemas.

Además, la entidad preguntó cómo habían sido atacados. El soporte proporcionó un informe inicial que decía lo siguiente:

> El acceso inicial a su red se **compró en la dark web**. Posteriormente, se realizó un **kerberoasting** y obtuvimos los **hashes de las contraseñas**. Después, los extrajimos y obtuvimos la contraseña de **administrador del dominio**.
>
> Tras semanas de análisis de su red, hemos detectado algunos fallos que recomendamos encarecidamente eliminar.

Tercer caso: entidad ignora pagar

La tercera entidad se puso en contacto con el soporte de Akira, preguntándoles directamente que encontró la nota de rescate y que estaba dispuesta a trabajar en una solución. Akira insistió en que la empresa debía mejorar su seguridad y le entregó una lista de los archivos comprometidos.

Además, preguntó a la empresa si trabajaría con ellos, adjuntando un precio de 550,000 dólares. El soporte volvió a preguntar si estaba lista para pagar. La empresa respondió que intentaba organizar sus archivos para poder proceder con el pago. Akira presionó nuevamente, advirtiendo que esperaba su decisión ese mismo día o, de lo contrario, los datos serían publicados. **Verificamos que la entidad aún no está listada ni filtrada en la página de Akira**.

Cuarto caso: Entidad solo negocia el costo

La cuarta entidad se puso en contacto con el chat de Akira, **solicitando únicamente el costo del pago para evaluar si era más conveniente que restaurar sus sistemas**. Akira exigió un pago de 1,000,000 de dólares y especificó que, si los fondos se retiraban de una cuenta bancaria, la empresa debía informar al banco que el dinero era únicamente para una inversión.

La empresa respondió que era demasiado dinero y añadió que **reconstruir todos los datos en un nuevo sistema le tomaría solo dos semanas**, por lo que no pagaría más de 50,000 dólares.

El chantaje continuó por parte de Akira, quien amenazó con publicar 22.5 GB de información en su blog. **Al verificar, constatamos que la entidad aún no ha sido publicada en el blog**.

Advertencia: Por qué no negociar y qué hacer en su lugar

Los intentos de negociación con Akira, como los documentados, demuestran que esta estrategia es arriesgada e ineficaz. Pagar un rescate no asegura que los datos sean recuperados ni que se evite su filtración. Además, financiar a estos grupos fortalece sus operaciones y aumenta la probabilidad de futuros ataques.

En lugar de negociar, las entidades deben priorizar:

Respuesta inmediata: Aislar los sistemas comprometidos y notificar a las autoridades de ciberseguridad.

Recuperación de datos: Utilizar copias de seguridad protegidas para restaurar la información.

Prevención: Implementar autenticación multifactor, aplicar parches de seguridad y capacitar al personal contra tácticas como el phishing.

Fortalecer la ciberseguridad es la mejor defensa contra grupos como Akira. Evitar el contacto con estos actores y adoptar medidas proactivas protegerá mejor a las organizaciones frente a estas amenazas.
