Negotiations with the Akira ransomware group: an ill-advised approach

databreaches.net/2025/05/05/negotiations-with-the-akira-ransomware-group-an-ill-advised-approach/

Dissent May 5, 2025

@Chum1ng0 took a look at four victims of Akira and what happened in terms of negotiations or not. In translation:

> After a detailed analysis, we identified four chats from different companies that attempted to communicate with Akira after being attacked. Some of these companies were still listed as victims on the group's website.
>
> Days after the failed negotiations, in which no financial agreement was reached, data from these companies was published on the Akira leak site, hosted on the Dark Web—an unindexed part of the internet, accessible only through specialized browsers like Tor, where cybercriminals often share stolen information.

> **Of the four cases analyzed, three entities refused to negotiate, while only one made a payment in Bitcoin.**

Because the responses of the four victims were different, Chu's post provides some insights as to how Akira may respond to different negotiation strategies. As one example, Chu reports:

> The fourth entity contacted Akira's chat, **requesting only the cost of payment to evaluate whether it was more convenient than restoring its systems** . Akira demanded a payment of $1,000,000 and specified that if the funds were withdrawn from a bank account, the company should inform the bank that the money was solely for investment purposes. The company responded that this was too much money and added that **rebuilding all the data on a new system would only take two weeks** , so it would not pay more than $50,000.
>
> The blackmail continued with Akira, who threatened to publish 22.5 GB of information on his blog. **Upon verification, we found that the entity has not yet been published on the blog** .

Read more at security-chu.com.