

Significant ransom payment by major Iranian IT firm underway

By SC Staff

Published: 2024-09-09 · Archived: 2026-04-05 17:54:45 UTC

[Ransomware](#), [Threat Intelligence](#)



(Adobe Stock)

Major Iranian IT vendor Tosan has been providing ransom payments on an installment basis following a significant cyberattack by the [IRLeaks](#) threat operation last month, which was reported to have compromised data from nearly 70% of the country's active credit entities but has been denied by the Iranian government, reports [CyberScoop](#).

Nearly \$561,000 worth of Bitcoin, or less than a third of the demanded ransom, has already been sent by Tosan to IRLeaks' cryptocurrency wallet since both parties began negotiations in early August, which commenced with the payment of a Bitcoin in exchange for the removal of IRLeaks' posting on Telegram before settling to a 3 Bitcoin per week arrangement until the 35 Bitcoin total is reached, according to emails between Tosan CEO Arash Babaei and IRLeaks provided by a third party and verified by a source close to the matter. At least two different Iranian exchanges provided payments to the wallet, which has also been used by threat actors for IT infrastructure purchases, noted Chainalysis Head of Cyber Threat Intelligence Jackie Burns Koven.

Get essential knowledge and practical strategies to protect your organization from ransomware attacks.

 SC Staff

Related





Get daily email updates

SC Media's daily must-read of the most current and pressing daily news

Source: <https://www.scmagazine.com/brief/significant-ransom-payment-by-major-iranian-it-firm-underway>