Significant ransom payment by major Iranian IT firm underway

By SC Staff

Published: 2024-09-09 · Archived: 2026-05-01 02:03:04 UTC

Ransomware, Threat Intelligence

September 9, 2024

(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.

SC Staff

Related

KryBit retaliates against 0APT with extensive data leak

SC StaffApril 30, 2026

Newly identified ransomware-as-a-service operation KryBit has compromised fellow nascent RaaS gang 0APT and exposed its full operational information, including access logs, system files, and PHP source code, in retaliation for the latter's initial leak of some of its data earlier this month, reports Infosecurity Magazine.

Report sheds light on Chinese phishing campaigns against journalists, activists

SC StaffApril 30, 2026

Report sheds light on Chinese phishing campaigns against journalists, activists Chinese state-backed freelance hackers have launched a pair of phishing campaigns aimed at journalists and opposition activists in Taiwan, Hong Kong, Tibet, and China's Uyghur region in a span of nine months, according to The Record, a news site by cybersecurity firm Recorded Future.