


Significant ransom payment by major Iranian IT firm underway

 scmagazine.com/brief/significant-ransom-payment-by-major-iranian-it-firm-underway

September 9, 2024

Ransomware, Threat Intelligence

September 9, 2024

 Share

By SC Staff



(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.

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.

[Learn More](#)



[SC Staff](#)

Related



RANSOMWARE

[RaaS group Storm-0501 targets hybrid cloud environments in the US](#)

[Steve Zurier](#) September 27, 2024

Financially motivated group uses legit Python key and hash management tool to steal credentials.



RANSOMWARE

Global ransomware incidence spikes

SC Staff September 27, 2024

At least 117 countries were targeted by ransomware intrusions last year, up from 105 in 2022, with Iran, Pakistan, Brazil, and India having the highest growth in ransomware incidence, while recently disrupted LockBit and ALPHV/BlackCat operations were the most active of the 66 ransomware gangs that launched attacks last year.



BREACH

Over 3K U.S. congressional staffers' data exposed on dark web

SC Staff September 27, 2024

Aside from IP addresses and social media details, more than 1,800 plaintext passwords belonging to staffers have also proliferated across the dark web, findings from a joint Proton and Constella Intelligence report showed.

Related Events

GET DAILY EMAIL UPDATES

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

By clicking the Subscribe button below, you agree to SC Media [Terms of Use](#) and [Privacy Policy](#).