FBI Attributes Record Crypto Theft Exceeding $6 Billion to North Korea's TraderTraitor



The FBI has formally attributed the theft of more than $6 billion in virtual assets to TraderTraitor, a North Korea-aligned group. The USSS and IRS-CI joined the FBI in the statement.

- The FBI officially attributed the theft of more than $6 billion in virtual assets to TraderTraitor.
- The group is North Korea-aligned and also tracked as Jade Sleet, Pressure Chollima, PUKCHONG, Slow Pisces and UNC4899.
- The U.S. Secret Service and IRS Criminal Investigation were party to the announcement alongside the FBI.
- The headline links the activity to a record $6.43 billion heist involving Binance.

The U.S. Federal Bureau of Investigation has formally attributed the theft of more than $6 billion in virtual

assets to TraderTraitor, an elite hacking group aligned with North Korea. The U.S. Secret Service and the Internal Revenue Service Criminal Investigation unit were part of the statement. The source headline describes the case as a record $6.43 billion heist linked to Binance.

What is known

The group is tracked under several names across the industry: Jade Sleet, Pressure Chollima, PUKCHONG, Slow Pisces and UNC4899. Security teams that see these names in threat intelligence feeds should treat them as referring to the same actor cluster as TraderTraitor.

The excerpt available to us does not set out the technical methods, the timeline or the specific indicators of compromise. We therefore do not draw conclusions on how the thefts were carried out.

Why it matters for Saudi institutions

An official attribution of this scale is a useful reference point for institutions that hold, custody, transact in or finance virtual assets, and for any organisation whose staff or partners work with such platforms. It is a prompt to review exposure to state-aligned financial theft and to confirm that threat intelligence coverage includes these actor names. No action is required beyond routine review unless your institution has digital-asset exposure.

What to do now

1. Add TraderTraitor and its aliases (Jade Sleet, Pressure Chollima, PUKCHONG, Slow Pisces, UNC4899) to threat intelligence watchlists.
2. Confirm whether your institution or its partners have exposure to virtual assets or crypto platforms.
3. Review privileged access and approval controls around any digital-asset or high-value transfer workflows.
4. Check that incident response plans cover large-scale financial theft by state-aligned actors.