

INVESTIGATION REPORT

CASE: DATA BREACH

(MONEYPRO SDN BHD)



Incident Report

Date: 13 June 2025

Target: MoneyPro Sdn Bhd (Malaysia)

Threat Actor: TigerP4tch (Advanced Persistent Threat Group)

Incident Summary:

On June 13, 2025, MoneyPro Sdn Bhd, one of Malaysia's largest financial institutions, suffered a significant cyberattack orchestrated by the hacker group known as TigerP4tch. This sophisticated group, active since 2020, executed a targeted breach resulting in the theft of sensitive personal data of over 10,000 clients and a financial loss nearing RM15 million.

Impact Overview:

- Data Compromised: Personal and financial records of ~10,000 clients
- Estimated Financial Loss: RM15,000,000
- Current Status: Under investigation by national cybersecurity and law enforcement agencies




Threat Actor Background:

TigerP4tch is a Malaysian-based cybercriminal group known for its strategic data breaches, digital extortion, and infiltration of financial infrastructures. Their emblem—a tiger with a cyberpunk eyepatch—has become synonymous with advanced cyber sabotage and underground network operations.

Group Logo:



TigerP4tch Team Members:

PICTURE	SURNAME / FULL NAME/ HANDLER	POSITION	CURRENT LOCATION
	Surname: Alpha Full Name: ??? Social media handler: ???	Leader / Master Mind / Former Malaysia Defense Force Hacker	Unknown / Hiding
	Surname: Bravo Full Name: Brian Davis Social media handler: @InitialB_	Graphic Designer / Malware Expert	Arrested On 16 August in Johor / in Custody for investigation
	Surname: Charlie Full Name: Alice Red Social media handler: Unidentified / Probably Deleted	Accountant at Bintang Bank / Social Engineering Expert / insider Threat	Tracked / Last seen in Penang

Common Technique used:

- Social Engineering
- Spear Phishing
- C2 Attack
- Trojan
- Ransomware