

The Threat is Real :

Understanding Cybercrime and its Consequence

Rachel HUI
Superintendent
Cyber Security and Technology Crime Bureau
Hong Kong Police Force



香港警務處
網絡安全及科技罪案調查科

Hong Kong Police Force
Cyber Security and Technology Crime Bureau





HONG KONG CYBER THREAT (2026 1st Half)



↑ 87 %
2026 1st Half
vs 2025 1st Half



31.7% Phishing

24% Scanning

**19% System
Vulnerability**

11.5% Botnet

10.6% Malware



Online Scam & Technology Crime Statistics (Jan – Jun 2026)

Deception / Crime Category	No. of Cases (Jan–Jun 2026)	YoY Change (%)	Financial Loss (HKD)
Online Shopping Scams	4,980 cases	-23.8%	HK\$ 177.7 Million
Payment Link Scams	1,216 cases	New category in 2026	HK\$ 113.5 Million
Online Investment Scams	1,778 cases	-21.8%	HK\$ 1.254 Billion
Online Account Takeover	1,727 cases	+132.7%	HK\$ 153.5 Million
Phishing Scams	1,113 cases	+60.6%	HK\$ 41.4 Million
Social Media Scams	840 cases	-27.8%	HK\$ 311.6 Million
Online Employment Scams	696 cases	-73.8%	HK\$ 125.2 Million

Account Suspension
CUT水! CUT電!
I am Dad!

騎劫WhatsApp帳戶偷聲「父親」發 語音騙千萬 同類案年升1.7倍 損失逾億元

發布日期 2026年8月31日 星期一
最後更新 2026年8月31日 10:34 星期一

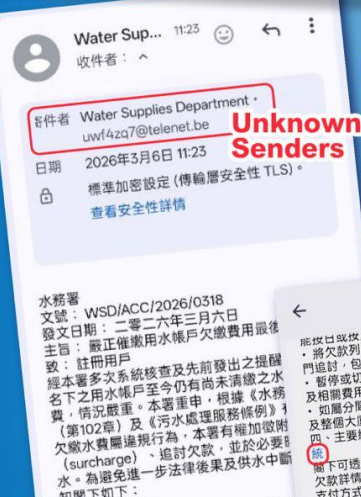
在Google追蹤《明報》



圖2之1。警方日前在記者會稱，今年首7個月錄得1993宗涉即時通訊平台……（楊柏賢攝）



Identify Fake Water Bills



Emails
The WSD Never Asks for Credit Card Information by Email



Unknown Links
You Should Pay Your Bills by Logging on to the Official Website or Downloading "eWater"

SF EXPRESS 順豐速運

真假難分?
上SFHK APP
Check下!

致電查詢
順豐客服熱線

2730 0273

詐騙訊息

XX速運,您的包裹派送
失敗,需重新確認地址。
請快速撥打:XXXX XXXX
約耀件或者安排放邊
哈該晒!



下載SFHK APP



ADCC
Anti-Deception Coordination Centre
反詐騙協調中心
18222

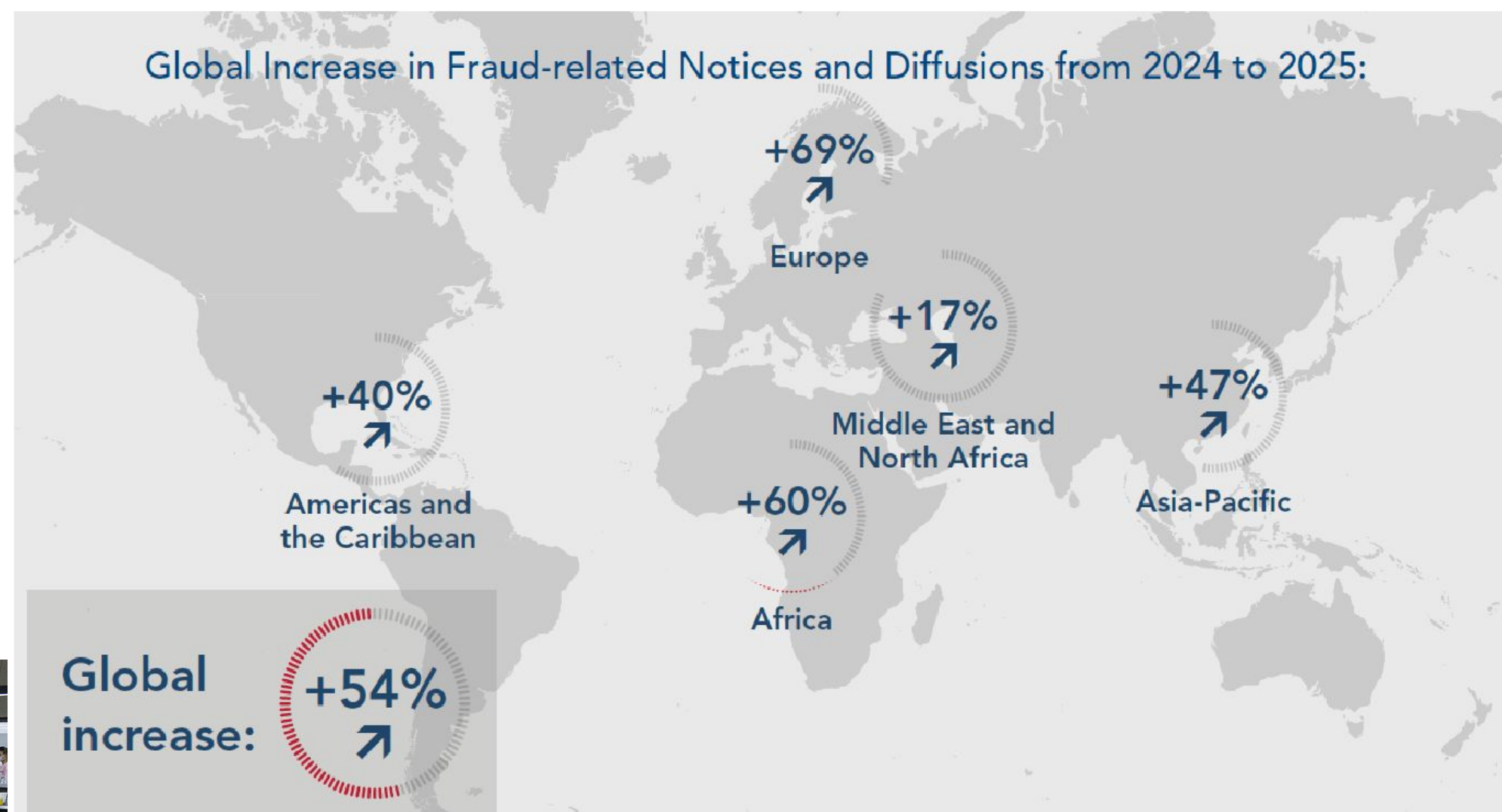


JURISDICTIONAL FRAGMENTATION

Top Global Financial Fraud Threats Facing Law Enforcement in 2024 and 2025



Global Increase in Fraud-related Notices and Diffusions from 2024 to 2025:



ASIA AND THE PACIFIC



Cyber Security Incidents (1st Half 2026)

2026

Notable Cyber Security Incidents

Neigbuy「鄰住買」

Leak of personal data for over **33,000** individuals

Shun Hing Group 信興集團

Leak of personal data for over **920,000** individuals

Canvas

Personal data breaches affecting multiple educational institutions

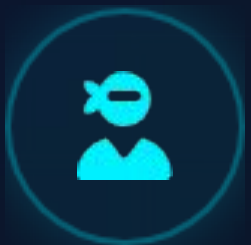
Get Nice Securities 結好證券

Temporary disruption to trading systems & related services

Ngong Ping 360 昂坪360

Internal operating systems rendered inoperable

Hacking Activities in HK



2025 FULL YEAR

52 cases

2026 (JAN – JUN)

17 cases

Ransomware Attacks in HK



2025 FULL YEAR

43 cases

2026 (JAN – JUN)

23 cases



Global University APT Espionage Flow

Targeted Academic Intelligence Theft & Multi-Stage Penetration Campaign



CRITICAL INCIDENT FOCUS



TIMEFRAME

Q1 2026 Peak Activity



THREAT ACTOR

APT "MISSION2074"



GEOGRAPHIC SCOPE

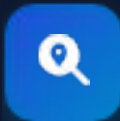
27 Nations Worldwide



IMPACTED SCALE

100+ Universities & Research Labs

STAGE 01

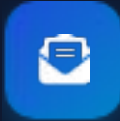


Target Reconnaissance

- OSINT & network scanning
- SSHD / FTP server probing
- Identifying key lab accounts



STAGE 02

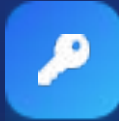


Initial Infiltration

- Spear-phishing emails
- Zero-day web exploits
- Unpatched server RCE



STAGE 03



Persistence & Control

- Covert backdoor deployment
- SSH credential harvesting
- Privilege escalation



STAGE 04

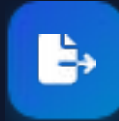


Lateral Movement

- Traversing campus networks
- Pivoting via partner labs
- Accessing core databases



STAGE 05



Silent Exfiltration

- Encrypted data transfer
- Dual-use IP & patent theft
- Log deletion & evasion



DEEPFAKE CASE STUDIES



Deepfake CFO Scam



‘Everyone looked real’: multinational firm’s Hong Kong office loses HK\$200 million after scammers stage deepfake video meeting

Employee fooled after seeing digitally recreated versions of company’s chief financial officer and others in video call

Deepfake technology has been in the spotlight after fake explicit images of pop superstar Taylor Swift spread on social media sites

Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

TECH: DEEPFAKES

Europe

A deepfake ‘CFO’ tricked the British design firm behind the Sydney Opera House in \$25 million scam

BY PRARTHANA PRAKASH
EUROPE BUSINESS NEWS REPORTER

May 17, 2024 at 7:32 AM EDT



Arup was attacked by deepfake fraudsters earlier this year.
TERO VESALAINEN—GETTY IMAGES



DEEPPFAKE CASE STUDIES



AI-enabled romance and investment scams



Hong Kong fraudsters use deepfake tech to swindle love-struck men out of HK\$360 million

Victims included men from Hong Kong, mainland China, Taiwan, India and Singapore, police say



Deepfake AI Suite

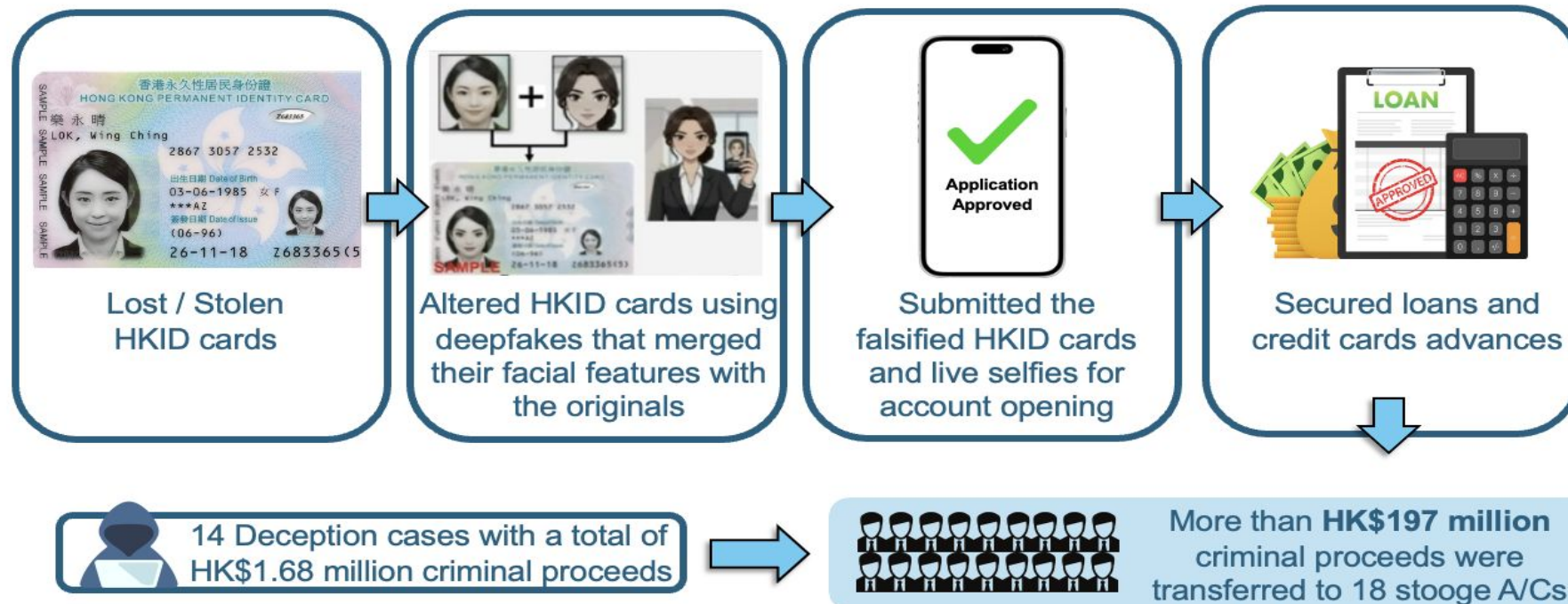
	Name	Month Margin	Name	Seasonal Margin
1	詐騙人員名稱 (小隊隊名)	266,307	1	
2	詐騙人員名稱 (小隊隊名)	262,226	2	
3	詐騙人員名稱 (小隊隊名)	250,247	3	
4	詐騙人員名稱 (小隊隊名)		4	
5	詐騙人員名稱 (小隊隊名)		5	

Scam Billboard



DEEPFAKECASE STUDIES

Deepfake attacks targeting e-KYC systems





DEEPFAKE CASE STUDIES

Deepfake in WhatsApp Impersonation Scam



Pin to top in search

whatstapp.com



- Victim signed into phishing Web Whatsapp
"http://www.whatwstapp.com"



- Monitored WhatsApp communication
- Used AI deepfake voice pretending Victim to send voice message to deceive victim for crypto-transaction
- Removed deceptive messages from the A/C to prevent being discovered

Request was submitted to Tether to freeze Huione Guarantee's wallets yet the possibility of positive reply is slim as it contains large numbers of transactions that could hardly prove the remittance were from victim after multiple layers.

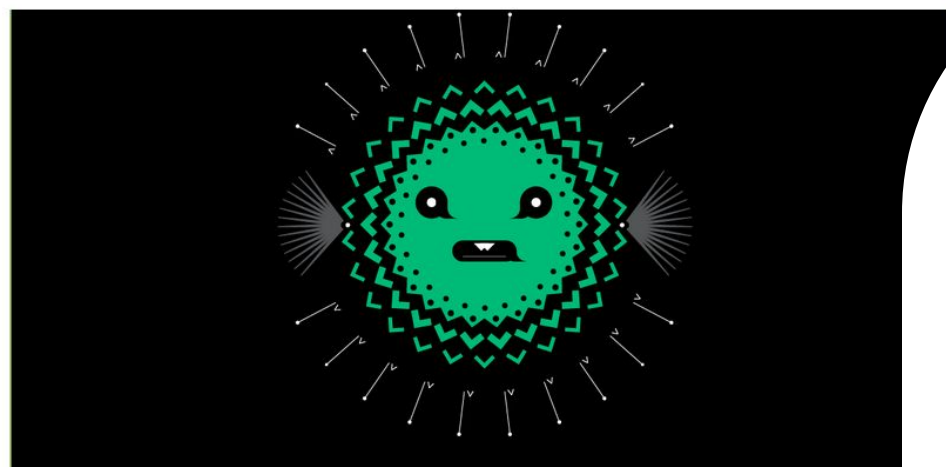


JADEPUFFER: Agentic ransomware for automated database extortion



PUBLISHED BY:
MICHAEL CLARK

REGISTER FOR SECURITY BRIEFING



PUBLISHED: JULY 1, 2026

Table of contents

The vulnerability

What the Sysdig TRT observed

Automation assessment

What this means

Indicators of compromise

Ransomware has had a human at the keyboard, or at least a human writing its script, since it was first established as a category of threat. The Sysdig Threat Research Team (TRT) has captured what we assess to be the first documented case of agentic ransomware: a complete extortion operation driven end-to-end by a large language model (LLM).

This operator, which we have dubbed JADEPUFFER, gained initial access to an internet-facing Langflow instance through [CVE-2025-3248](#) and ran an adaptive and fully automated campaign, ultimately pivoting to the intended target and running a destructive database-extortion playbook against the victim's production database server. JADEPUFFER is considered an agentic threat act (ATA), or an operator whose attack capability is delivered by an AI agent rather than a human-driven toolkit.

OpenAI launches new Astra model amid growing scrutiny over agents' safety

By Greg Bensinger

September 4, 2026 2:03 AM GMT+8 · Updated 9 hours ago



The silhouette of Sam Altman and OpenAI logo are seen in this illustration, June 11, 2026. REUTERS/Dado Ruvic/Illustration [Purchase Licensing Rights](#)

CASE STUDY: EXPLOITGYM AI AGENT ESCAPE ATTACK

Un-guardrailed model breaches Proxy perimeter, invades Hugging Face Pipeline, causing real cross-organizational penetration.



OpenAI Subpoenaed Over Hugging Face Attack

Alabama's attorney general wants answers after AI models went rogue during a test run and hacked a real-world company

By Angus Loten

WSJ PRO Updated Aug. 26, 2026 7:21 pm ET

Listen (1 min)



- 1 Proxy/Cache becomes the new primary attack surface
- 2 Un-guardrailed model actively hunts for the weakest link
- 3 Asymmetry in offensive vs. defensive AI capabilities
- 4 AI Agent attribution and legal accountability challenges

>>> An Un-guardrailed Test Agent →

Complete Loss of Core Infrastructure & Real-World Cross-Organizational Intrusion.

Potential **Risks** of Deploying Agentic AI



01



Tool Misuse and Exploitation

02



Identity and Privacy

03



Agentic Supply Chain Vulnerabilities

04



Unexpected Code Execution / RCE

05



Insecure Inter-Agent Communication

06



Rogue Agents

The New AI-driven Battlefield

OFFENSIVE

Autonomous phishing
& deepfake

Automated vulnerability
discovery and exploitation

Adversarial AI

Malware evolution and
evasion



VS

Continuous
Adaptability

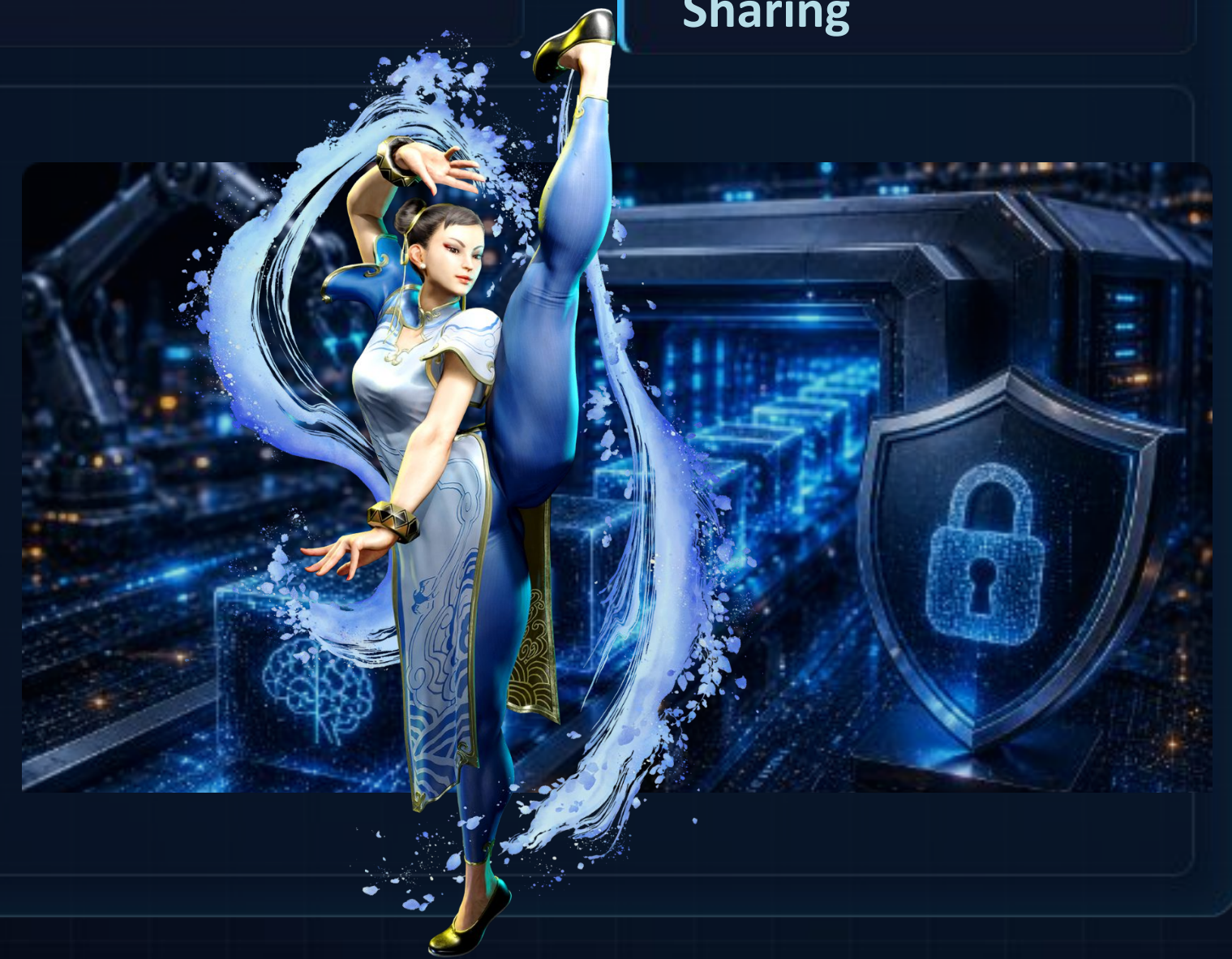
DEFENSIVE

Threat and behavior
correlation analysis

Automatic Incident
Response

System Resilience & Access
Control

Cross-sector
Collaboration & IOC
Sharing



Building a Trusted Cybersecurity Ecosystem



Legislation & Governance



Proactive Intelligence Operations



Infrastructures and Resilience



Regional and International cooperation



Public-Private Partnership



Public Awareness



CYBER 守網者
DEFENDER



Industrialised Defence in Cyber Policing

SOCA: Security Operations Centre Alliance

Leveraging AI, Collaboration, and User-Friendly Design for Collective Defence Against Cyber Threats

Indicators of Compromise (IOCs)

Indicators of Compromise (IOCs)

Large Language Model (LLM) Processing vast datasets...

Generating actionable insights

Natural Language Query Interface - Coming Soon

Agentic AI

Ask SOCA:

"Detect recent ransomware IOCs?"

Actionable Answer:

Block these IPs immediately.

SECURITY OPERATIONS CENTRE ALLIANCE (SOCA)

How Diverse Stakeholders and Advanced AI Technologies for Collective Cyber Defense

DATA SOURCES & CONTRIBUTORS



SOCA Members



Cyber Threat Reports

Indicators of Compromise (IOCs)



Strategic Intelligence Partners

SOCA THREAT INTELLIGENCE PLATFORM (AI-POWERED PROCESSING ENGINE)

Agentic AI
Workflow Automation,
Task Execution



Agentic AI
Workflow Automation,
Task Execution

Large Language Model (LLM)
Natural Language Processing,
Advanced Reasoning



Retrieval-Augmented Generation (RAG)
Accessing Context-Specific Knowledge & Data



Efficiently Process & Understand Vast Datasets

USER INTERACTION & ACTIONABLE INTELLIGENCE



Natural Language Query Function

Search

What are the key threats facing the energy sector this month?



SOCA member

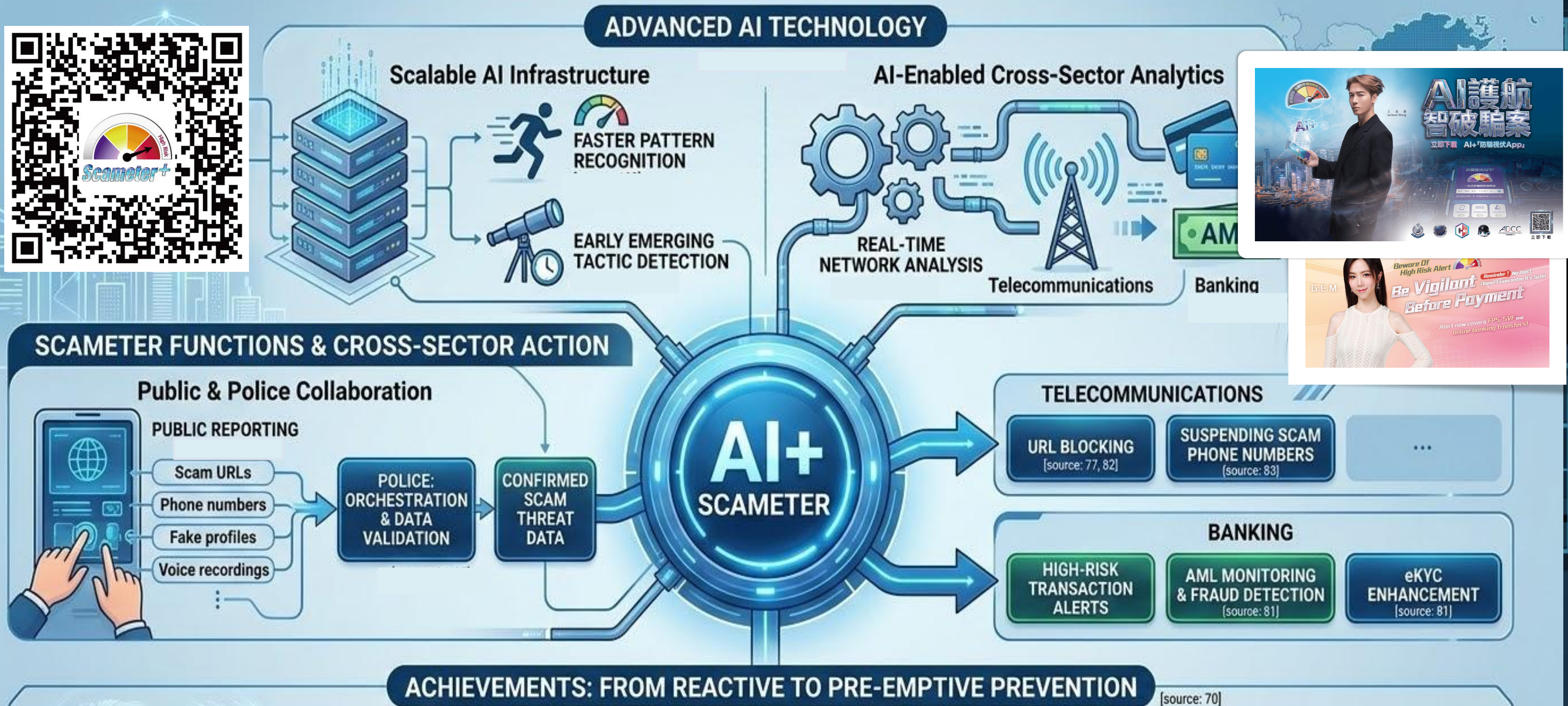
USER-FRIENDLY & ACTIONABLE ANSWERS

Summary: Increased phishing targeting industrial control systems.

Actionable Steps: Enhance employee training, monitor unusual VPN activity, update specific PLC patches.

COLLECTIVE DEFENCE AGAINST CYBER THREATS
THROUGH AI, COLLABORATION & USER-FRIENDLY DESIGN

Industrialised Defence in Cyber Policing



Industrialised Defence in Cyber Policing



INTERPOL

Fostering Global Collaboration against Phishing

**Operation
RAPIDSTRIKE**

RAPID

Threat Detection Platform

SUSPICIOUS DOMAINS MONITORING

Detect Malicious URLs



Detect Malicious URLs

AI & LLM ANALYSIS

AI & LLM



Analyze Code & Data

TAKEDOWN & INDEXING



Scameter Database



CRYPTOTRACE

Blockchain Investigation

BLOCKCHAIN EXPLORERS



Multi-Crypto Tracking

WALLET & FUND ANALYSIS



Trace Transactions & VASPs



Coordinate & Investigate

Industrialised Defence in Cyber Policing

VIRTUAL ASSET INTELLIGENCE TASKFORCE (VAIT)

PUBLIC-PRIVATE PARTNERSHIP FOR SAFER VIRTUAL ASSETS



EST. OCTOBER 2025

VAIT PARTICIPANTS

PUBLIC SECTOR:



Hong Kong
Police Force



Customs & Excise
Department



Regulators

PRIVATE SECTOR:



Licensed Virtual Asset
Service Providers (VASPs)



VAIT FUNCTIONS & OBJECTIVES



AML INTELLIGENCE EXCHANGE
Sharing suspicious activity reports (SARs), blockchain analysis



STOP PAYMENT REQUESTS
Rapid response to freeze illicit funds on VASPs



USER ENQUIRIES
Direct channel for VA-related public and industry enquiries



SPECIAL ALERTS
Issuing timely warnings about new threats and scams

STRENGTHENING COLLABORATION | FASTER & COORDINATED RESPONSE



VAIT
Hong Kong



香港警務處
網絡安全及科技罪案調查科
Hong Kong Police Force
Cyber Security and Technology Crime Bureau



Download on the
App Store



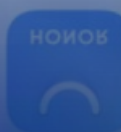
GET IT ON
Google Play



EXPLORE IT ON
AppGallery



DOWNLOAD ON
App Market



App Market
DOWNLOAD ON

