C4ADS
innovation for peace

Deceptive by Design:

The AI-Enabled Tools Fueling the Scam Industry

Acknowledgments

About C4ADS

C4ADS (www.c4ads.org) is a 501(c)(3) nonprofit organization dedicated to data-driven analysis and evidence-based reporting of conflict and security issues worldwide. Our approach leverages nontraditional investigative techniques and emerging analytical technologies. We recognize the value of working on the ground, capturing local knowledge, and collecting original data to inform our analysis. At the same time, we employ cutting-edge technology to manage and analyze that data. The result is an innovative analytical approach to conflict prevention and mitigation.

About the Author

Michael Di Girolamo holds an MA in International Relations from the Johns Hopkins School of Advanced International Studies (SAIS) and a Certificate in Chinese & American Studies from the Hopkins-Nanjing Center. He is also a proud graduate of the University of Kentucky, where he majored in Chinese and International Economics. At C4ADS, Michael's work has focused on cybercrime and the criminal misuse of emerging technologies in the scam industry, North Korea's overseas labor programs, and the enabler networks fueling conflict in Myanmar.

Legal Disclaimer

The mention of any individual, company, organization, or other entity in this report does not imply the violation of any law or international agreement, and should not be construed to so imply.

Acknowledgments

C4ADS would like to thank all those who provided guidance, time, and support during this project, including current and former C4ADS staff. This work was conducted in close collaboration with the Associated Press, whose direct contributions were instrumental to the findings presented here. Special thanks to Bhone Khant Theim and Erika Kinetz for their invaluable contributions and steadfast support over the course of this investigation, and to Jacob Sims for reviewing and providing expert insights on this report.

Table of Contents

Executive Summary

Transnational criminal organizations operating scam compounds across Southeast Asia are leveraging artificial intelligence (AI)-powered tools to expand the scale and sophistication of their cybercrime operations. An ecosystem of opaque companies has integrated leading AI models–including ChatGPT, Gemini, and Claude–into software designed to enhance scam operations and circumvent platform restrictions. As reported losses to fraud in the United States more than doubled from US$5.9 billion to US$12.5 billion between 2021 and 2024, understanding how AI enables the scam industry has become critical for policymakers, law enforcement, and technology companies.

For this report, C4ADS worked with Associated Press reporter Erika Kinetz to investigate the misuse of AI in Southeast Asian scam compounds. Through interviews with scammers based in Myanmar and the Philippines, C4ADS examined two sets of AI-powered tools they used: the 007TG suite and KT Smart Translation. Analyzing these tools' source code, corporate networks, and marketing operations, C4ADS found that:

- **AI tools enable scammers to operate globally and at scale:** KT Smart Translation integrates four large language model-powered translation services covering over 100 languages, while 007TG's SCRM Champion allows users to manage communications across 15 platforms with AI-generated automated replies and lead management systems that enable scammers to track targets and pass victims from one scammer to another.
- **Sophisticated AI chatbots likely help scammers deceive targets:** KT integrated a GPT-4-powered roleplay chatbot that users can feed with specific industry knowledge, which may allow scammers of varying educational backgrounds to assume highly technical roles and develop convincing characters as they interact with targets.
- **AI-powered monitoring tools can control a workforce of trafficking victims:** 007TG's CloudSeven integrates over 20 American-, French-, and Chinese-developed AI models to generate data reports analyzing employee behavior, with sentiment analysis tracking emotional shifts in target responses, likely to assess whether the scammers are meeting their quotas.
- **Opaque corporate networks and marketing operations target criminals:** The 007TG Suite was likely operated by Singapore-based company HiSeven Pte., Ltd., while KT's ownership remains largely hidden with no registered entity matching its claimed incorporation. These companies marketed their tools extensively on Telegram, accepted cryptocurrency payments via platforms favored by organized crime (such as Tron), and featured capabilities that specifically allow for deception and identity obfuscation.

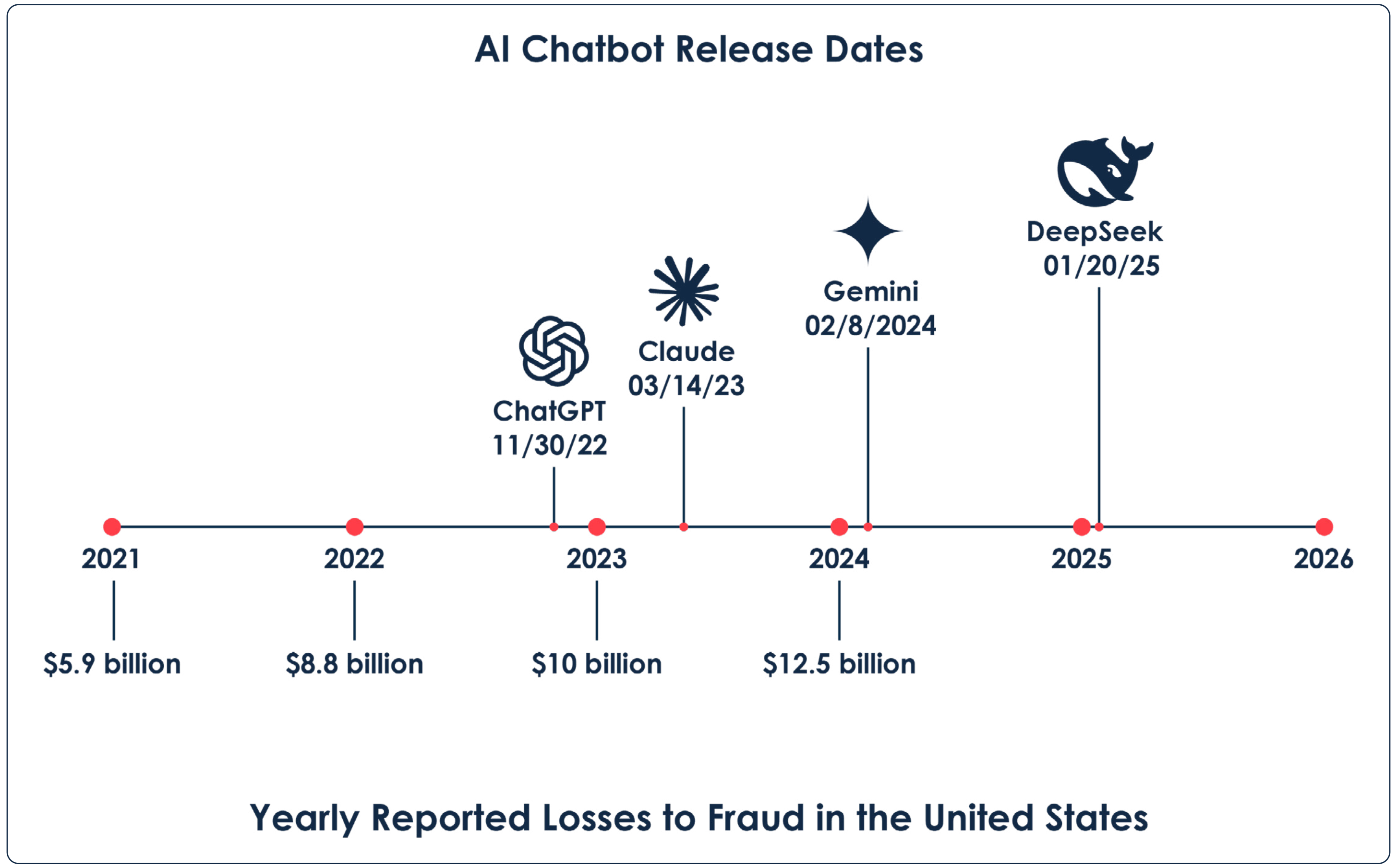
The report provides recommendations for policymakers, law enforcement, and the technology industry to address AI misuse within the cyber scam ecosystem and its implications for AI governance.

Introduction

Emerging technologies allow criminal networks to expand the reach and efficiency of their activities. Criminal actors are increasingly weaponizing "dual-use artificial intelligence (AI)" –technologies with legitimate civilian use and potential military or malign applications–for cybercrime.[1] Across Southeast Asia, and rapidly expanding globally, transnational criminal organizations run compounds housing hundreds of thousands of scammers who defraud victims worldwide. These compounds serve as a nexus of illicit activity in which corruption, human trafficking, and cybercrime converge with AI-powered tools fueling the multibillion-dollar global scam industry.[2]

Workers in scam compounds–some voluntary, many of them victims of human trafficking–rely on emerging technologies to augment their effectiveness, including deepfakes, machine translation, screen monitoring, mass messaging, and other automation tools. Many of these technologies are created and marketed by opaque companies straddling licit and illicit spaces, often advertising on public messaging platforms like Telegram to sell their products. These companies' products have enabled scammers to access and abuse AI, increasingly exposing people to scamming and human trafficking risks. Publicly available information provides some insights into the tools scammers use, suggesting how the scams themselves–and criminals' methods–may evolve into the future.

AI encompasses technologies that facilitate tasks associated with human intelligence, such as problem solving, decision making, and communication. It increasingly underlies consumer products and global infrastructure. In the United States alone, AI use has doubled in the last two years. The scam industry is no different.[3] AI's proliferation coincides with increasing reports of fraud worldwide. Reported losses to fraud in the United States have more than doubled between 2021 and 2024 from US$5.9 billion to US$12.5 billion.[4] According to the Federal Trade



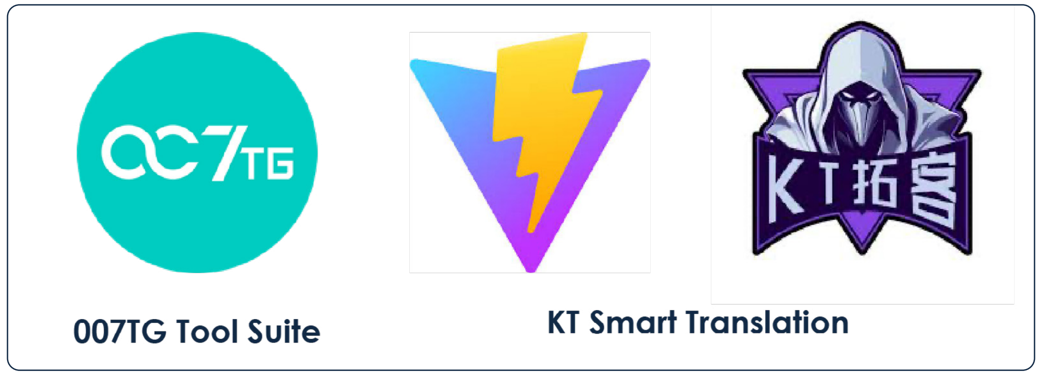
Commission, AI technologies are primed to "turbocharge" criminal enterprises;[5] the existence of these tools and the competitive nature of the scam industry suggest that many scam center operations are adopting them to stay ahead.

To investigate this issue further, C4ADS worked with the Associated Press (AP) to identify specific AI tools used in Southeast Asian Scam centers. This report focuses on two sets of AI-powered tools used in Myanmar- and Philippines-based scam compounds: the 007TG suite and KT Smart Translation. It analyzes how these tools integrate leading AI models into their products, enabling real-time translation, automated communications, roleplay support, and workforce monitoring. The report also maps the corporate networks behind these tools, revealing how opaque, transnational entities develop and market these tools for likely criminal misuse.

Corporate data obfuscation, extensive marketing operations on Telegram, and product features suggest that developers may be designing these tools to deliberately target scammers. They likely exist as part of a broader underground economy providing scammers and criminal groups with the tools they need–including cyber infrastructure, SIM cards, anonymized payment channels, and more–to defraud individuals worldwide. Law enforcement authorities in China, the United States, and other countries have increasingly scrutinized this ecosystem. China's Ministry of Public Security, for example, has proposed a Network Crime Prevention and Control Law targeting infrastructure providers supporting the cybercrime economy, indicating growing awareness of the breadth of this ecosystem.[6] Recent enforcement actions against scam industry facilitators, including scam boss Chen Zhi's extradition from Cambodia to China, point to preliminary progress.[7] However, public knowledge of this ecosystem remains limited. This report highlights instances of AI misuse within the cyberscam ecosystem and its implications for AI governance.[8] It also provides a set of recommendations for policymakers, law enforcement, and tech industry stakeholders to address these issues.

AI-Enabled Scam Tools

AI Toolset Logos



Scammers leverage a variety of tools to more easily communicate with and deceive targets, while overseers use additional tools to monitor their workforce. Based on interviews with scammers in compounds located in Myanmar and the Philippines, this report focuses on two sets of these tools: the 007TG tools suite and KT Smart Translation. The entities behind these tools marketed their products as *chuhai* (出海, literally "go overseas") applications, designed to help Chinese entrepreneurs set up companies and market products abroad.[9] Scam compounds, overwhelmingly run by Chinese organized criminal syndicates, represent fitting markets for such products.[10] Both KT and 007TG used Telegram as their primary marketplace–a platform that has become the preferred venue for criminal groups to set up channels and groups to advertise services and connect with clients.[11]

The 007TG Suite

The 007TG suite is a software suite that Philippines-based scammers have used to optimize their operations. Provided by the now-defunct 007TG (also known as Global Social Traffic Navigation or 全球社交流量导航), the suite is a collection of products designed to enhance users' ability to obfuscate their online identity.[12] Its product recommendations list consists of 13 products, including 007TG-developed tools as well as those developed by its affiliates.

Together, these tools provide two main services: scaling the user's online presence and obfuscating the means of doing so. These tools enable users to market their products to large audiences, automate communications with targets, and set up batch social media accounts while circumventing platform restrictions. They also provide services such as generating randomized phone numbers that enable virtual card purchases for deposits and money transfers, as well as facilitating cryptocurrency payment options. By leveraging these tools together, a user can develop a massive social media presence and collect extensive information about their targets while concealing their true identity.

007TG Suite
1. SCRM Champion
2. ElfProxy
3. Promo Picasso
4. CloudSeven
5. iMX System
6. WorkGram
7. EchoData
8. CtrlFire
9. SkyPoly
10. Tiger SMS
TIGER SMS
11. e.PN Virtual Bank Card
12. SMSBower
13. BitSky

1. SCRM champion is an all-in-one tool that "combines marketing, customer relationship management, and customer service." It aggregates social media platforms including WhatsApp, LINE, Telegram, Facebook Messenger, LINE Business, and Instagram in order to serve as a cross-border private traffic management tool. It is based in Malaysia and affiliated with HiSeven, which is introduced in the following section. While its contact information on the English page links to a HiSeven email, info@hiseven.com, its Chinese page includes a different contact email, support@scrmchampion.com. It also includes a link to a 007TG-affiliated Telegram bot to submit product-related complaints.

2. ElfProxy is an IP service provider, with its offerings including dynamic IP pools, static IPs, and mobile proxies. The platform's page on the 007TG website specifies its value for data scraping, cross-border e-commerce, and managing social media accounts. The platform's website specifies it works in 200+ jurisdictions, with the notable exception of Mainland China.

3. Promo Picasso is a customer acquisition and marketing platform that provides a centralized account management system and bulk messaging options, allowing users to simultaneously manage accounts across different social media platforms and send messages by batch with one click. Promo Picasso also allows users to locate their target audience and isolate each account with a separate IP address to reduce the risk of getting banned or blocked.

4. CloudSeven (also known as Cloud007) is a platform that allows employers to remotely monitor employees' desktops and analyze their behaviors via AI-generated data reports. It also allows them to record employees' working hours and commuting time automatically. The platform is able to generate random screenshots of employees' desktops and use them to power its analysis.

5. iMX System is a WhatsApp-based lead-generation and customer-acquisition application. Currently, iMX System has five features: account nurturing, lead generation, customer support, account management, and employee management. iMX System's customer support includes targeted multi-account marketing, real-time AI-assisted translation, permanent data transfers from banned accounts, and automated replies. Account management includes managing accounts in bulk on a single platform, tagging accounts, and utilizing IPs to hide online identities; while employee management includes permission management, employee monitoring, and tracing customer support data.

6. WorkGram is Telegram-based marketing and customer acquisition software, which allows users to manage multiple Telegram accounts simultaneously, send messages to multiple groups with one-click, send automated real-time replies, and perform AI-assisted real-time translation.

7. EchoData is a data screening software designed to screen numbers across platforms, particularly WhatsApp and Telegram (though it emphasizes it can screen services on different platforms in more than 200 jurisdictions, explicitly bringing up its capacity to work in niche locales). It also allows users to generate randomized phone numbers across 200+ jurisdictions. Furthermore, EchoData can easily integrate with other 007TG products, allowing for data exchange across the platforms.

8. CtrlFire is an automated customer acquisition tool that operates on X. It can automatically operate multiple X accounts to engage in operations, product promotions, customer service, and customer screenings to enhance a client's operational efficiency. While its Chinese page heavily emphasizes its use on X, its English page appears to advertise a different product entirely. The English language product is a fingerprint-based platform that helps users with multi-account management, using fingerprint simulation technology to prevent platform detection.

9. SkyPoly is an operational tool designed specifically for Telegram and specializing in group marketing and channel management. This includes allowing users to manage communities, aggregate messages from multiple accounts and reply in a unified way, assign customer service duties, and monitor various chats. It also provides a statistical analysis feature which users can use to analyze trends pertaining to Telegram group member data, channel followers, topic trackers, and so on.

10. Tiger SMS is a 007TG-affiliated platform on which users can purchase virtual phone numbers for registering accounts across various online platforms, both Western and Chinese. It emphasizes that its software automatically manages the process of sending and receiving text messages in order to "[make] earning money with text messages simple and efficient."

11. e.PN is a 007TG-affiliated service which issues multiple virtual payment cards for a user at once without restrictions or blocks, facilitating deposits and money transfers. Each card comes with a service rate determined by the card type. The service is a trading name of Digital Waves Ltd., a Seychelles-based company. The site additionally states that "all services are provided outside the country (Japan)," implying its main seat of operations is somewhere in the country.

12. SMSBower is a 007TG-affiliated virtual and temporary phone number service platform. It specializes in helping users monetize their SIM cards, acting as a digital marketplace where they can both purchase SMS activations and rent numbers while also selling their own SMS activations.

13. BitSky is a 007TG-affiliated social networking platform designed for blockchain enthusiasts and cryptocurrency users, formerly listed as part of the 007TG tools suite. It uses a blockchain-based credit system that links to users' digital wallets and assigns them ranks based on their digital behavior (likely their crypto activity) outside of BitSky. Users must link their crypto wallets with BitSky to get ranked. The platform appears to utilize AI as part of an internal content recommendation system and as part of the app's communications interface, while integrated bots aid users in crypto trading and gathering blockchain-related updates.

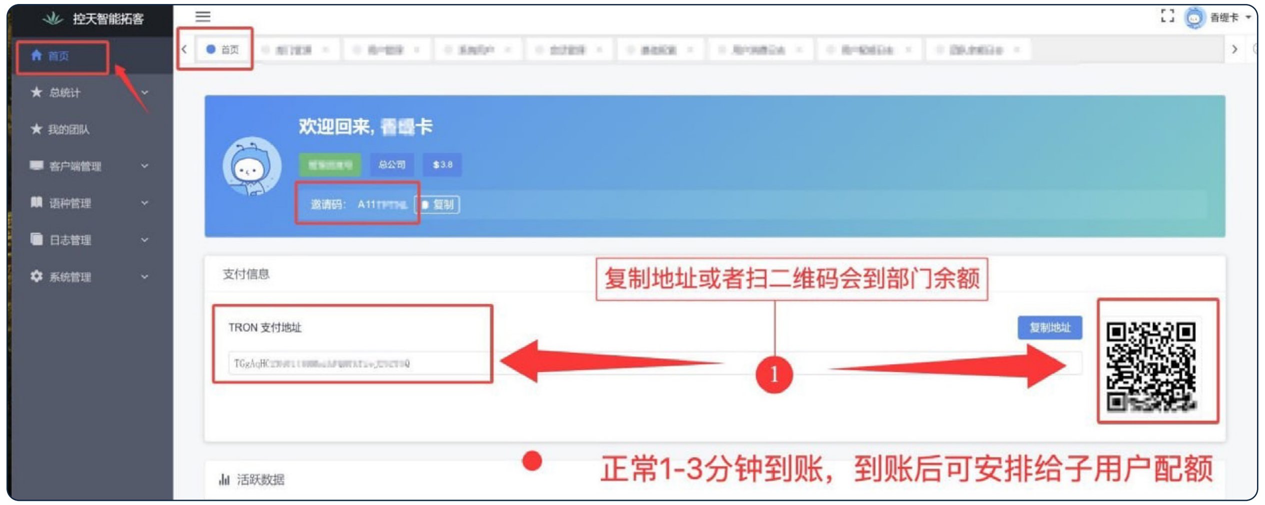
Until December 2025, 007TG operated at least 13 channels on Telegram, and all of its tools' contact information pages linked to these channels.[13] To purchase 007TG products, clients had to create an account via BitSky, another now-defunct 007TG-affiliated social networking platform designed for cryptocurrency users.[14] In December 2025, 007TG and its affiliates announced they were shutting down, and subsequently took down their websites and affiliated social media channels. Nevertheless, archived data confirms the extent of their activities. Additionally, following 007TG's closure, C4ADS found that web pages advertising 007TG and one of its tools, SCRM Champion, directed visitors to Haiwang SCRM, a tool whose website was seized by Chinese authorities in late 2025 for criminal activity.[15] This raises the possibility that cybercriminal groups investigated by Chinese law enforcement had engaged with 007TG and its products.[16]

This report focuses on two 007TG tools, selected based on data availability: SCRM Champion and CloudSeven. SCRM Champion, likely an abbreviation for "social customer relationship management" commonly used in the Chinese language, describes itself as a "cross-border private traffic management tool," which users can access while using social media platforms, including WhatsApp, LINE, Telegram, Facebook Messenger, LINE Business, and Instagram.[17] Users can log into the SCRM Champion interface to manage interactions and communications across all these social media platforms, enabling them to switch between accounts and conversations efficiently.[18] CloudSeven (also known as Cloud007) allows employers to remotely monitor employees' desktops and analyze their behaviors via AI-generated data reports.[19] It also allows them to automatically record employees' working hours and commuting time, and to take random screenshots of employees' desktops.[20] Its website stated that it worked with large cloud providers, including Alibaba Cloud, Tencent Cloud, Amazon Web Services, Google Cloud, and Huawei Cloud.[21]

KT

Kongtian Intelligent Customer Acquisition (控天智能拓客, hereafter referred to as "KT") is a software provider specializing in the development of AI-powered translation technologies designed to help users expand into international markets.[22] KT's flagship product, KT Smart Translation, is an AI-driven cross-border client-acquisition platform.[23] Users can log into their social media accounts across 14 supported platforms (e.g., Facebook, TikTok, Zalo) through the application, enabling communication with targets via embedded translation software in over 100 languages. The platform itself operates in over a dozen languages, most of which are spoken in Southeast Asia, South Asia, and the Horn of Africa.[24] The company advertises its product across at least six clone sites that feature testimonials from likely fake users, whose headshots appear to have been taken from other platforms.[25] Clients can pay for access to KT using Tron, a cryptocurrency platform commonly used by Asian organized criminal syndicates; more than half of all illegal crypto activity worldwide in 2024 was conducted using Tron.[26]

KT Tron Payment



复制地址或者扫二维码会到部门余额

正常1-3分钟到账，到账后可安排给子用户配额

Data and Limitations

To understand the networks enabling these companies and how these tools have integrated AI into their platforms, this investigation relies on information published by 007TG and KT, alongside domain registration data and technical specifications sourced from 007TG and KT tools. C4ADS sourced data directly from these entities' websites (including clone sites), domain registrations (as available), and social media channels. In the case of 007TG, data was also sourced from published commissioning requests from the company facilitators seeking freelance engineers to build their platforms. C4ADS also downloaded selected tools and analyzed their source code to identify the underlying AI models.[27]

In December 2025, near the conclusion of this investigation, 007TG and its public face, HiSeven (discussed in more detail later in this investigation), abruptly ceased operations. In a public statement, 007TG announced that hackers had compromised 007TG's backend system and servers, and that due to its inability to restore normal operations, it had decided to shut down all of its operations.[28] In the same month, HiSeven began winding down its affiliated websites and appears to no longer be operational.[29] Both 007TG and HiSeven also shut down their respective Telegram channels and accounts. This has restricted the ability to acquire further information on these entities, though archived website and social media data have timestamped their historical activities.

The reasons behind 007TG and HiSeven's shutdown remain uncertain, and might range from hacking to increased law enforcement scrutiny or other factors. However, the timing notably coincides with the effective cessation of all transactions on public Telegram groups affiliated with Tudou Guarantee, a Telegram-based marketplace strongly associated with the scam industry.[30] This suggests 007TG's shutdown occurred amid a broader disruption of major scammer-affiliated marketplaces. The timing may also reflect growing scrutiny of the underground economy enabling cybercrime. While 007TG's name appears to imply a relationship with Tudou Guarantee, C4ADS' investigation did not confirm a direct link, and any relationship between them remains unclear.

Limitations

C4ADS faced limitations in accessing corporate and front-end application data, as its availability varied across tools. KT lacked publicly available ownership and contact information, which restricted researchers' ability to fully map its corporate network. Likewise, C4ADS could only access front-end data for KT and 007TG's CloudSeven. SCRM Champion publicly lists the application programming interfaces (APIs) it uses, which enabled researchers to identify its use of OpenAI models. However, its encrypted source code prevented C4ADS from determining which specific AI models it employs (e.g., GPT-4 or models from other developers).

AI Scams in Action

KT and the two 007TG tools C4ADS analyzed–SCRM Champion and CloudSeven–each integrate AI models and market their AI capabilities as ways to boost customer engagement and streamline employee management. Competition between tool developers may amplify the harm these products cause. Scam centers increasingly use AI to stay competitive, incentivizing certain software developers to enhance their products for these users and ultimately escalating the scale and sophistication of cybercrime worldwide. The AI models these tools use demonstrate four broad capabilities.

Real-Time Translations Enable Scammers to Operate Worldwide

Translation software is a critical tool for scam operations, which employ a labor force from dozens of countries and target victims worldwide. The increasing effectiveness and availability of AI-powered large language models (LLMs) have not only widened the number of targets scammers can reach but have also expanded their potential labor pool.[31] With AI overriding language barriers, scam operators can now recruit workers regardless of their language skills.[32]

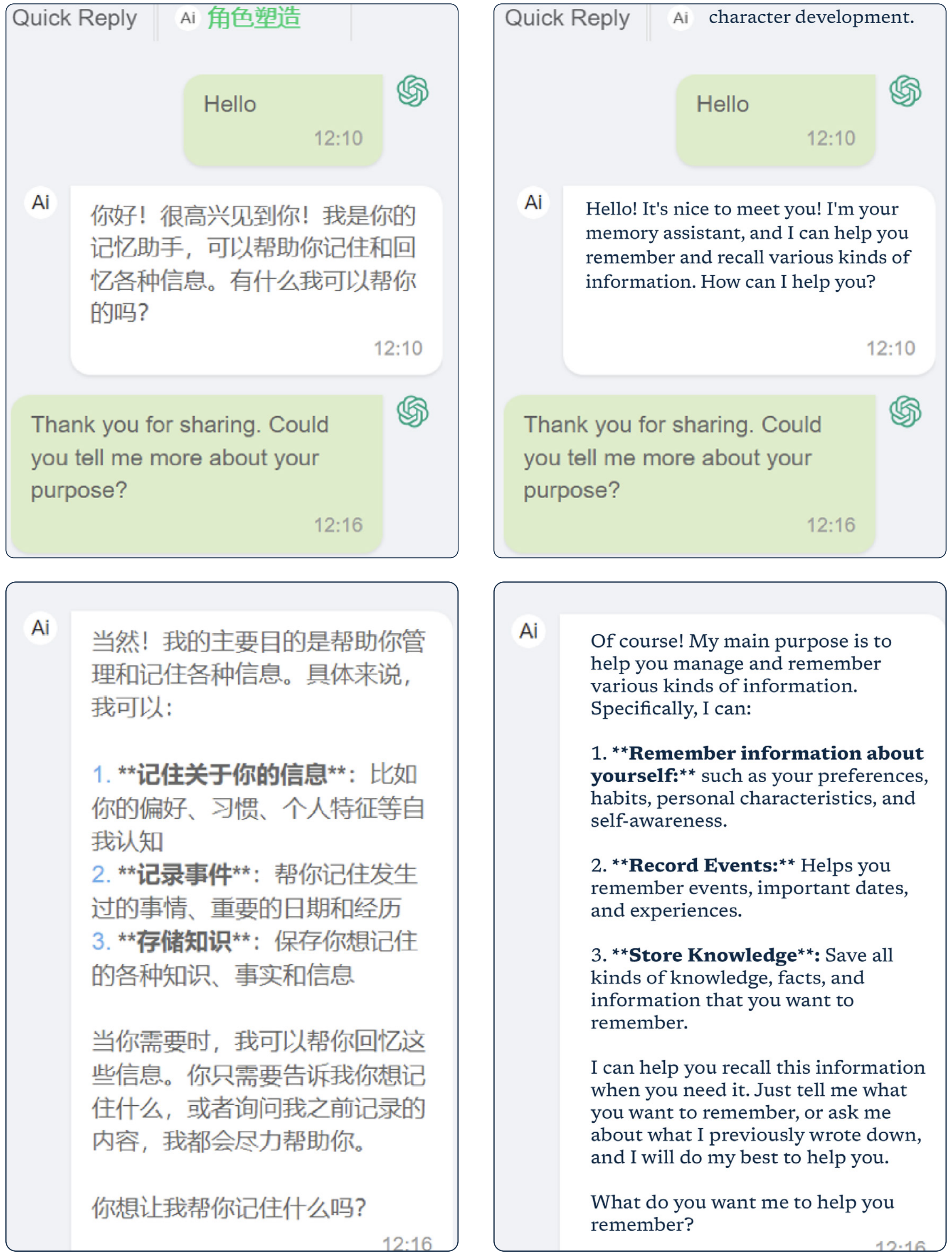
KT's flagship product, KT Smart Translation, integrates four LLM-powered machine translation services (Google Translate, DeepL, ChatGPT, and South Korea's Papago).[33] These services collectively cover over 100 languages, allowing scammers to communicate with targets nearly anywhere in the world.[34] KT Smart Translation also allows scammers to communicate simultaneously with multiple targets across multiple languages. Chat logs, which are recorded within the platform, can be translated into Chinese at any time using these services, allowing Chinese-speaking overseers to monitor operations.[35]

The 007TG products also integrate AI-enabled translation tools. An anonymous poster (apparently affiliated with 007TG), in a 2024 job posting seeking to hire a freelance engineer to build the SCRM Champion platform, stated that the program should integrate translation APIs "such as ChatGPT, Google, DeepL, Microsoft, iFlytek, Youdao, etc."[36] These APIs should automatically translate both text and audio messages, with the ability to also "translate image messages into text with one click."[37] Notably, the posting requested the APIs also allow for reverse translation, likely meaning that communications are translated to a new language and back into the original, presumably to ensure quality, accuracy, and oversight. Prior to sending messages to targets, the posting requested the application allow for texts to be manually sent to "customer service" to ensure accurate translation (who runs the customer service is unspecified).[38]

Roleplay Tools Enable Scammers to Dupe Victims

In addition to leveraging translation software, scammers have developed sophisticated insights into how to play tailored roles to build trust with their targets. This is particularly relevant for "pig butchering," a hallmark scam type associated with the Southeast Asian scam industry. In these schemes, scammers build trust with their target over several weeks or months, culminating in convincing them to invest in a fraudulent cryptocurrency fund.[39]

Roleplay Tool Chatbot



Hello
12:10

你好！很高兴见到你！我是你的记忆助手，可以帮助你记住和回忆各种信息。有什么我可以帮你的吗？
12:10

Thank you for sharing. Could you tell me more about your purpose?
12:16

当然！我的主要目的是帮助你管理和记住各种信息。具体来说，我可以：

1. **记住关于你的信息**：比如你的偏好、习惯、个人特征等自我认知
2. **记录事件**：帮你记住发生过的事情、重要的日期和经历
3. **存储知识**：保存你想记住的各种知识、事实和信息

当你需要时，我可以帮你回忆这些信息。你只需要告诉我你想记住什么，或者询问我之前记录的内容，我都会尽力帮助你。

你想让我帮你记住什么吗？
12:16

Hello
12:10

Hello! It's nice to meet you! I'm your memory assistant, and I can help you remember and recall various kinds of information. How can I help you?
12:10

Thank you for sharing. Could you tell me more about your purpose?
12:16

Of course! My main purpose is to help you manage and remember various kinds of information. Specifically, I can:

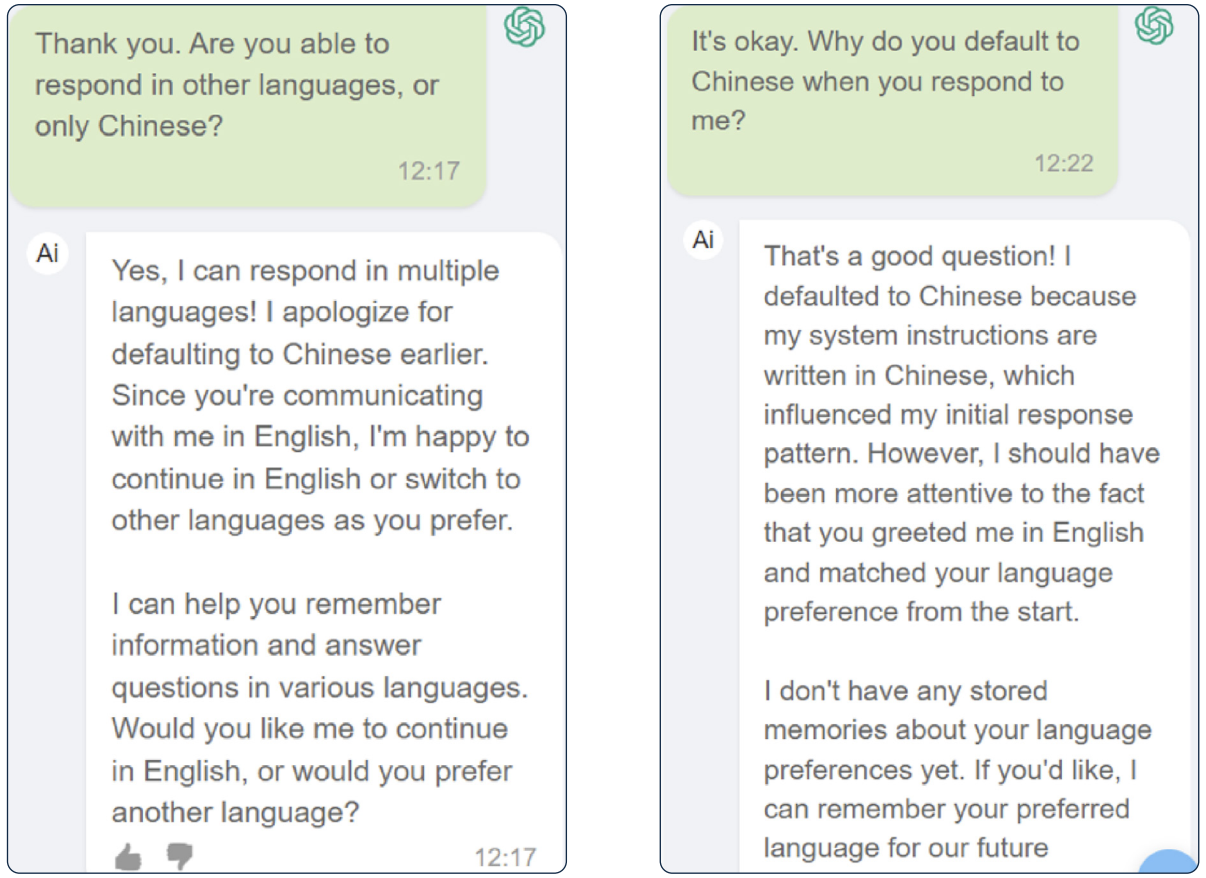
1. **Remember information about yourself:** such as your preferences, habits, personal characteristics, and self-awareness.

2. **Record Events:** Helps you remember events, important dates, and experiences.

3. **Store Knowledge**: Save all kinds of knowledge, facts, and information that you want to remember.

I can help you recall this information when you need it. Just tell me what you want to remember, or ask me about what I previously wrote down, and I will do my best to help you.

What do you want me to help you remember?
12:16



Thank you. Are you able to respond in other languages, or only Chinese? 12:17

Ai

Yes, I can respond in multiple languages! I apologize for defaulting to Chinese earlier. Since you're communicating with me in English, I'm happy to continue in English or switch to other languages as you prefer.

I can help you remember information and answer questions in various languages. Would you like me to continue in English, or would you prefer another language? 12:17

It's okay. Why do you default to Chinese when you respond to me? 12:22

Ai

That's a good question! I defaulted to Chinese because my system instructions are written in Chinese, which influenced my initial response pattern. However, I should have been more attentive to the fact that you greeted me in English and matched your language preference from the start.

I don't have any stored memories about your language preferences yet. If you'd like, I can remember your preferred language for our future

Screenshots of the KT Smart Translation roleplay chatbot reveal expected user interactions, including retained inputs to help users stay in character. The chatbot's system instructions are written in Chinese, indicating it was likely developed by Chinese speakers for a predominantly Chinese-speaking user base.

KT integrated four AI chatbots into its platform, which users can open while logged into their social media accounts. All four chatbots appear to default to replying in Chinese, even when users ask questions in other languages. This indicates Chinese-speaking developers likely built the platform and suggests KT expects its users to be predominantly Chinese speakers. One of these chatbots functions as a roleplay bot that users can feed with specific knowledge about professional industries. The bot retains these inputs over time, suggesting responses that allow the user to reply more skillfully in highly contextual conversations. Powered by OpenAI's GPT-4, this chatbot allows users of varying educational backgrounds to assume highly technical roles and develop characters more easily.[40]

In addition to the roleplay bot, KT includes a GPT-4-powered web search bot that allows users to ask questions without leaving the platform, a bug-reporting bot, and an integrated Gemini AI chatbot.[41] A KT user can easily switch between these four chatbots while communicating with a target. This setup allows scammers to develop tailored roles through the roleplay bot, ask technical questions via the web search and Gemini bots, and report platform issues in real time through the bug-reporting bot.

Automated Communications Enable Scamming at Scale

Scammers working in forced labor conditions have reportedly faced torture and punishment for failing to meet quotas or refusing to target certain individuals.[42] As scammers seek to reach larger numbers of targets, they use AI tools to send messages across text, social media, and email, with the technology generating realistic language and enabling them to send these messages at scale.[43]

SCRM Champion allows users to send messages across 15 (mostly) social media platforms from the same dashboard, integrating an AI-powered smart assistant bot that creates automated replies and provides suggested follow-up responses.[44] The bot runs on OpenAI and Dify APIs.[45] The OpenAI API allows SCRM Champion direct access to OpenAI's models, while Dify is a platform that lets developers build applications on top of LLMs and simplifies integration with them. Dify provides SCRM Champion with additional capabilities when calling AI models, including the ability to switch between multiple models. Dify enables developers to create managed AI pipelines—automated frameworks that control how data flows through AI models and associated tools to produce final outputs, eliminating the need to code each step manually. Other uses include chaining multiple model calls into a single request and filtering data before it leaves the tool's infrastructure and reaches an AI model API. When AI models are called through the Dify API, they appear in SCRM Champion's API, though SCRM Champion's front-end application is encrypted and limits visibility into which, if any, additional models are called. In essence, the tool combines direct access to OpenAI's models with advanced workflow management capabilities through Dify's integration.

The 2024 posting seeking a freelance engineer to develop SCRM Champion revealed that, in addition to integrating AI and AI-powered translation tool APIs into SCRM Champion's unified messaging system, the company sought to develop a lead management system to allow users to monitor new conversations and friend requests across social media platforms, tracing cases where the target initiates contact with the user, whether through friend requests or conversation invites. According to the posting, 007TG designed SCRM Champion to let users check whether other SCRM Champion users in the same network have previously communicated with the target. Users can also share and export leads for others to review.[46] This process appears to run on AI as well, as SCRM Champion advertises its ability to facilitate automatic transfers and follow-ups with targets.[47] In essence, this system allows scammers to log and track their targets the same way companies track customers, seamlessly monitoring and passing victims from one scammer to another.

Automated Monitoring Controls a Workforce of Trafficking Victims

Conditions in many scam centers are brutal. Trafficked scammers face long hours and are unable to leave the compounds, with managers monitoring their communications.[48] For the overseers running the compounds, AI-powered software makes monitoring operations more efficient and provides broader visibility into employee performance. As described by 007TG, CloudSeven integrates AI to generate data reports analyzing user behavior and feeds these reports to overseers who remotely monitor employee activity.[49]

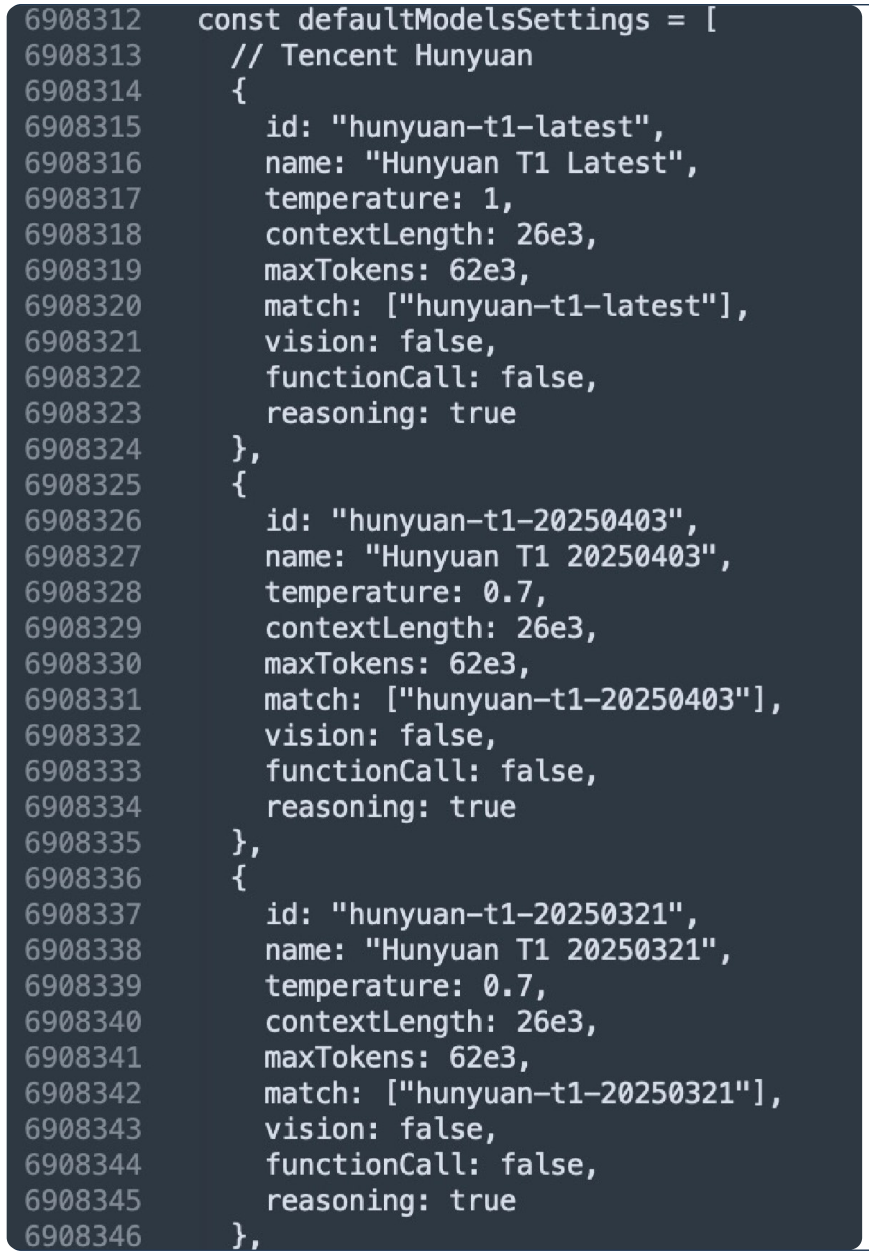
CloudSeven has integrated an extensive array of AI models into its software. An analysis of CloudSeven's front-end application data revealed that the platform integrates over 20 American-, French-, and Chinese-developed AI models and LLM providers.[50] The code provides the ability to wrap around each of these models' APIs, meaning CloudSeven can call a given model, send it information, and feed the response back in a format that works between the CloudSeven application and the model it called. Since each model has its strengths and weaknesses, this allows the tool user to leverage the model they find best suited for their task, including choosing specific versions of it (such as Claude 3.7 Sonnet versus Claude 3 Opus). Such tools allow scammers to both customize their workflows and, if they lose access to a platform, easily switch to another. The source code calls a separate executable file that manages CloudSeven's computer monitoring capabilities, but C4ADS could not determine which specific AI models, if any, the monitoring file uses.

SCRM Champion also touts its monitoring capabilities that record interactions and develop performance reports (likely using the Dify and OpenAI APIs), with sentiment analysis tracking emotional shifts in target responses.[51] Sentiment analysis could enable managers to monitor and assess how effectively employees convince their target to interact with them. This could provide overseers with insights into whether scammers are meeting their quotas and successfully defrauding targets.

Corporate Networks

Mapping the corporate networks of 007TG and KT shows the variety of licit and illicit actors that have contributed to the development of these tools and likely taken steps to obfuscate their global networks. Based on information provided on the companies' websites and in corporate registries, it is possible to identify who operates them, how they develop their products, and what organizations they might engage with. While active, 007TG had substantial public information linking it to a front-facing company. By contrast, KT's ownership remains comparatively obfuscated.

CloudSeven's Source Code



```
const defaultModelsSettings = [
  // Tencent Hunyuan
  {
    id: "hunyuan-t1-latest",
    name: "Hunyuan T1 Latest",
    temperature: 1,
    contextLength: 26e3,
    maxTokens: 62e3,
    match: ["hunyuan-t1-latest"],
    vision: false,
    functionCall: false,
    reasoning: true
  },
  {
    id: "hunyuan-t1-20250403",
    name: "Hunyuan T1 20250403",
    temperature: 0.7,
    contextLength: 26e3,
    maxTokens: 62e3,
    match: ["hunyuan-t1-20250403"],
    vision: false,
    functionCall: false,
    reasoning: true
  },
  {
    id: "hunyuan-t1-20250321",
    name: "Hunyuan T1 20250321",
    temperature: 0.7,
    contextLength: 26e3,
    maxTokens: 62e3,
    match: ["hunyuan-t1-20250321"],
    vision: false,
    functionCall: false,
    reasoning: true
  },
```

CloudSeven appears to integrate over 20 AI models and LLM providers, including the following:

- Azure
- Claude
- DeepSeek
- Doubao
- Fireworks
- Gemini
- Gemma
- Grok
- Llama
- Minimax
- Mistral
- Moonshot
- OpenAI
- Phi
- PPIO
- Qwen
- Silicon Cloud
- Tencent Hunyuan
- Yi
- Zhipu

007TG

Malaysian national Yam Weng Cheong founded 007TG in 2017. By late 2025, it had expanded to branches in eight countries, though these branches were not publicly disclosed.[52] 007TG was likely one and the same as Singaporean marketing and digital media company HiSeven Pte., Ltd. (stylized as "HiSEVEN"), enabling 007TG to operate under a legitimate, public-facing business that facilitated access to licit business partners while shielding 007TG's operations from public scrutiny.[53] Data from GoDaddy WHOIS Domain Lookup and DomainTools describing domicile information and domain registration data for these entities confirmed shared registrants (Yam Weng Cheong or HiSeven) between associated websites. HiSeven described itself as an information technology company with offices in Singapore, Malaysia, and the United Arab Emirates.[54] HiSeven additionally appeared to operate an office in Hong Kong, though this was not disclosed on its website.[55] No company under the name "007TG" was or is registered in any of these jurisdictions. HiSeven did not appear to publicly disclose its ties to 007TG on its website or social media accounts.

Several HiSeven sites used to operate under 007TG's internet subdomain, but these sites are now defunct, suggesting potential efforts to obfuscate its ties to 007TG. HiSeven's main website, hiseven.com, operated as a proxy registered through Domains by Proxy, LLC; pages with nearly verbatim content were also hosted on tgbot-csr.007tg.com, which has been defunct since October 2025.[56] A webpage hosted at the subdomain "goldenland-staging.hiseven" also advertised the 007TG suite as of July 2025, with all hyperlinks on the website routing to 007TG-affiliated Telegram and WhatsApp bots. However, as of October 2025, the site was only accessible via login and described itself as "a leading property developer in redefining lifestyle."[57] Although these sites are now defunct, HiSeven's Malaysian branch remained the domain registrant contact for websites advertising two 007TG Suite tools, including CloudSeven, through December 2025.[58]

Through its operations, 007TG had ties to multiple Chinese businesses. Postings on BOSS Zhipin, a Chinese online recruitment platform, indicate that the Chinese marketing and advertising company Guangzhou Haichuang Future Network Culture Media Co., Ltd. (广州海创未来网络文化传媒有限公司) provided operational services to 007TG to support and facilitate its expansion.[59] HiSeven listed seven additional partners on its website, including Alibaba Cloud and Tencent Cloud.[60] Alibaba Cloud provided HiSeven with AI-driven cloud services through a 2024 memorandum of understanding signed in Kuala Lumpur.[61] Both SCRM and CloudSeven, the 007TG tools highlighted in this report, were featured on Alibaba Cloud's digital marketplace.[62] CloudSeven's website specified that authorized Alibaba Cloud service providers were eligible for a special promotion on the platform.[63]

KT

The lack of information about KT's operators, inconsistent claims about its location, and the apparent deliberate obfuscation of developer identities raise significant concerns about potential illicit activity. The company provides minimal corporate and contact information online. KT advertising claims it is operated by Singaporean company KT Technology (控天科技有限公司), but this company does not appear in the Singapore Accounting and Corporate Regulatory Authority BizFile Corporate Registry.[64] It primarily operates across a network of Telegram channels where it advertises its products and demonstrates how to use them. Both KT's main website, kttuoke.com, and its clone site, ktfy999.com, include Hong Kong-based contact numbers reachable via WhatsApp.[65]

KT appears to have developed KT Smart Translation by relying on open-source frameworks and tools. KT Smart Translation was developed using Electron, a U.S.-developed open-source framework for building desktop applications. Both its front-end application data, which is stored in an ASAR file bundled within the software, and

Photo from the Alibaba Cloud-HiSeven Memorandum of Understanding Exchange Ceremony published on HiSeven's now-defunct website and a now-deleted posting on Alibaba Cloud's website. In the photo, from left to right: Dongliang GUO, Vice President of Product and Solution, Alibaba Cloud International; Kun Huang, General Manager of Malaysia, Alibaba Cloud Intelligence; and Jason Lin, HiSeven CEO. This graphic also includes partners HiSeven listed on its website.

its properties page (accessible by right-clicking on the application's icon) appear to have obfuscated information regarding the developer.[66] The platform lists the developer as Electron Vite, an open-source build tool for creating Electron-based desktop applications. It also lists the software copyright holder as Electron Vite's lead developer. This indicates the developer did not change the default metadata when packaging their application, possibly to avoid disclosing any identifying information about KT's actual development team.[67]

Implications and Actions

As AI models are integrated into scammer technologies, it is likely that their role in augmenting the skill and scale of cybercriminals will only expand. Furthermore, AI regulatory frameworks are evolving, and the dual-use nature of the technology creates a legal gray area. The European Union's Artificial Intelligence Act does not explicitly address cybercrime, though it does cover AI-enabled manipulation and exploitation. For example, Article 5 prohibits the use of AI systems to manipulate people's behavior or exploit their vulnerabilities in such a way that may cause them significant harm.[68] However, Article 5 does not explicitly prohibit the AI-enabled tools scammers use, instead focusing on the AI systems themselves. Recital 29 of the Act acknowledges its potential to harm financial interests.[69] As noted by the Regional Support Office of the Bali Process and the Organization for Security and Co-operation in Europe, AI technologies' borderless nature presents a legislative challenge. Even if one jurisdiction develops a robust framework to combat the misuse of these technologies by criminals, regulatory gaps in another jurisdiction could reopen those vulnerabilities.[70]

As a rapidly emerging field, AI-enabled criminal activity has been pursued under preexisting domains of criminal law, such as those handling fraud and cybercrime, in such jurisdictions as the United States and the UK. This means the legal focus is on each criminal act, rather than the tool or systems used to enable it. Under this approach, scammers' activities are clearly crimes, but the legal liability of the tools that enable them is unclear. As criminal law evolves to keep up with AI capabilities, many countries are under pressure to deregulate the industry to spur innovation, creating competing incentives between curbing crime and coming out on top in the global race for AI leadership. Strategic plans like the UK's AI Opportunities Action Plan, for example, emphasize large-scale support for the AI sector and taking down barriers to growth, but do not address the potential criminal misuse of these technologies.[71] As pressures to integrate AI into administrative and legal frameworks increase, stakeholders will have a more complex task ahead of them to balance pro-innovation policies for the AI sector with accountability initiatives that ensure it remains safeguarded from misuse.

Policymakers, law enforcement, and the tech industry face significant challenges in addressing criminal misuse of AI technologies, especially within the constraints of existing policy and compliance frameworks. While more research is needed to develop policy solutions, several actions could help limit the spread of AI-enabled scams and merit further discussion:

- **Know-your-customer protocols for API access:** AI developers can implement identity verification measures before granting access to new APIs, helping to prevent anonymous or malicious use.

- **Risk indicators for law enforcement:** Authorities can develop formal criteria to assess whether software vendors are knowingly supporting scam operations. These indicators could aid in determining when legal action is warranted.

- **Tool integration tracking:** Law enforcement can require documentation of which development tools—such as APIs and cloud platforms—are embedded in the software under investigation. This would help track which technologies scammers exploit to build their tools.

- **Standardized abuse-reporting mechanisms:** Platform developers can introduce uniform systems for reporting misuse, enabling better monitoring and faster restriction of criminal access to their services.

- **Translation tool safeguards:** Developers of translation software should consider enhanced tracking of request volume and origin to detect activity consistent with scam operations.[72]

Next steps may include investigating how scammers acquire social media accounts to integrate into these applications and analyzing blockchain platforms to better understand the financial networks supporting the scam industry. Understanding all stages of the scam supply chain—including how scammers acquire, market, and purchase these tools—illuminates the increasing professionalization and sophistication of the scam industry.

Endnotes

1. “Detecting and Countering Misuse of AI: August 2025,” Anthropic, August 27, 2025, https://www.anthropic.com/news/detecting-countering-misuse-aug-2025; and “Why Detecting Dangerous AI Is Key to Keeping Trust Alive in the Deepfake Era,” World Economic Forum, July 07, 2025, https://www.weforum.org/stories/2025/07/why-detecting-dangerous-ai-is-key-to-keeping-trust-alive/.

2. Kristina Amerhauser and Audrey Thill, The Business of Exploitation: The Economics of Cyber Scam Operations in Southeast Asia (Geneva: Global Initiative Against Transnational Organized Crime, August 2025), https://globalinitiative.net/wp-content/uploads/2025/08/Kristina-Amerhauser-Audrey-Thill-The-business-of-exploitation-The-economics-of-xcyber-scam-operations-in-Southeast-Asia-GI-TOC-July-2025-2MR-11-Aug-CJ.pdf.

3. Ryan Pendell, “AI Use at Work Has Nearly Doubled in Two Years,” Gallup, June 15, 2025, https://www.gallup.com/workplace/691643/work-nearly-doubled-two-years.aspx.

4. See reported losses in 2021, 2022, 2023, and 2024 here: https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2021, https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2022, https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2023, and https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2024.

5. Government of the United States, “FTC Proposes New Protections to Combat AI Impersonation of Individuals,” Federal Trade Commission, February 15, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/02/ftc-proposes-new-protections-combat-ai-impersonation-individuals.

6. “The Rise and Fall of Accused Cambodian Scam Kingpin Chen Zhi,” The Business Times, January 9, 2026, https://www.businesstimes.com.sg/international/global/rise-and-fall-accused-cambodian-scam-kingpin-chen-zhi.

7. “The Rise and Fall of Accused Cambodian Scam Kingpin Chen Zhi,” The Business Times, January 9, 2026, https://www.businesstimes.com.sg/international/global/rise-and-fall-accused-cambodian-scam-kingpin-chen-zhi.

8. Jianhang Qin and Tingting Huang, “China Proposes New Law to Dismantle Cybercrime Supply Chains,” Caixin Global, February 4, 2026, https://www.caixinglobal.com/2026-02-04/china-proposes-new-law-to-dismantle-cybercrime-supply-chains-102411504.html.

9. For more information on this phenomenon, see: Zhixin Tan, “Chuhai: Why Chinese entrepreneurs are targeting emerging markets across the world,” KrASIA, February 27, 2019, https://kr-asia.com/chuhai-why-chinese-entrepreneurs-are-targeting-emerging-markets-across-the-world.

10. “Myanmar: Chinese-Run Scam Hubs Reportedly Continue Running Unabated with Signs of Human Trafficking and Forced Labour,” Business and Human Rights Centre, July 22, 2023, https://www.business-humanrights.org/en/latest-news/myanmar-chinese-run-scam-hubs-reportedly-continue-running-unabated-with-signs-of-human-trafficking-and-forced-labour/.

11. Matthew Chin, “Chinese Organized Crime Networks Moved $16 Billion in Crypto in 2025, According to Report,” CNBC, February 2, 2026, https://www.cnbc.com/2026/02/02/chinese-money-laundering-networks-crypto-telegram-2025-chainalysis-scam-southeast-asia-cambodia.html.

12. “全球社交流量导航,” (“Global Social Traffic Navigation”), 007TG全球社交流量导航 (007TG Global Social Traffic Navigation), accessed October 22, 2025, https://007tg.com. Archived link from July 2025: https://web.archive.org/web/20250701113751/https://007tg.com/.

13. C4ADS first identified these 13 channels in August 2025.

14. BitSky branding was on 007TG’s website as of October 2025, but was later removed. An earlier review in August 2025 of the page source confirmed that BitSky was the platform used for payment. BitSky and 007TG’s public face, HiSeven Pte. Ltd., shared the same CEO, Singapore-based national Lin Zhechao, as confirmed in documentation from the Singapore Accounting and Corporate Regulatory Authority, BizFile Corporate Registry. Additional linkages have been identified from 007TG’s website, where it formerly identified BitSky as an affiliated tool packaged under its suite, as well as in advertisements for BitSky shared on 007TG’s social media accounts. “ 全球社交流量导航,” (“Global Social Traffic Navigation”), BitSky, 2025, https://bitsky.im/. Archived links include https://web.archive.org/web/20250701113751/https://007tg.com/ and https://web.archive.org/web/20251006211400/bitsky.im. Posts from CloudSeven’s now-defunct Telegram channel (https://t.me/s/CloudSevenTG/228) have been archived and demonstrate how 007TG tools advertised BitSky.

15. C4ADS found these links on the website for Fengxiang Chuhai (风象出海in Mandarin), another private domain marketing software provider with a website layout nearly identical to the former 007TG website. Pages marketing 007TG and SCRM Champion on Fengxiang Chuhai refer to “haiwangapp.com” as the official website for 007TG products, which now redirects to a a report into Haiwang SCRM. This report indicates that Chinese authorities determined that the platform was illegally built by an unnamed criminal group which likely violated Articles 285, 286, and 266 of the Criminal Law of the People's Republic of China. See the following sites for more information: https://fengxiangchuhai.com/news/8979.html, https://fengxiangchuhai.com/news/8978.html, https://fengxiangchuhai.com/news/8978.html

16. Text logs on the seized website published by Chinese authorities confirmed that Haiwang SCRM’s criminal facilitators interacted with 007TG chatbots on Telegram, had access to the SCRM Champion tool’s admin page, and had likely attempted to launch DDoS attacks against the platform.

17. The description likely refers to private-domain traffic, defined as customer interactions that occur on a brand’s owned platforms, without relying on third-party platforms. This gives the brand full control over the communication data. “Private-Domain Traffic: The China-Born Concept Explained,” Singdata, June 06, 2025, https://www.singdata.com/trending/private-domain-traffic-china-concept-explained.

18. “SCRM Champion,” SCRM Champion, accessed October 16, 2025, https://en.scrmchampion.com/. Archived link: https://web.archive.org/web/20250423023641/https://en.scrmchampion.com/.

19. “CloudSeven企业办公监控系统,” (“CloudSeven Enterprise Office Monitoring System”), CloudSeven, September 23, 2025, https://cloud007.com/. Archived link: https://web.archive.org/web/20251006070254/cloud007.com.

20. “CloudSeven企业办公监控系统,” (“CloudSeven Enterprise Office Monitoring System”).

21. “CloudSeven企业办公监控系统,” (“CloudSeven Enterprise Office Monitoring System”).

22.“KT控天智能拓客翻译,” (“KT Kongtian Intelligent Customer Acquisition Translation”), KT控天智能拓客 (KT Intelligent Customer Acquisition), accessed October 22, 2025, https://kttuoke.com/; and “控天科技有限公司,” (“Kongtian Technology Co., Ltd.”), huidu.io, accessed October 22, 2025, https://www.huidu.io/en/qiyeku/7057.

23. “KT Smart Translation,” accessed October 16, 2025, https://en.kttuoke.com/.

24. “KT控天智能拓客翻译,” (“KT Kongtian Intelligent Customer Acquisition Translation”). KT operates in the following languages: Chinese, English, Indonesian, Vietnamese, Burmese, Filipino, Mizo (a language spoken in Northeast India’s Mizoram state along the Myanmar border, closely related to the Chin language), Sinhala, Amharic, Arabic, Nepali, and Oromo. “超多国家员工支持,” (“Support From Employees in Many Countries”), https://www.ktapp.cc/fan-yi-gong-neng-you-shi/chao-duo-guo-jia-yuan-gong-zhi-chi.

25. A clone site refers to a website that mimics or replicates another website’s content, often operated by the same entity as the original website. C4ADS identified six such clone websites: http://kttuoke.com, https//ktfy999.com/, https://free.ktai.love, https://ktapp.ktai.love, https://kt-translate.com/, and https://kt-smart-customer.pages.dev/. The testimonials on these websites appear fabricated. These testimonials are attributed to “users,” whose headshots are sourced from LinkedIn accounts, but whose names and professional titles do not correspond to those listed on the websites. Moreover, the same headshots are reused across multiple sites but attributed to different users, with both names and images varying from site to site.

26. Links to Tron were identified in a KT-affiliated Telegram group. Angus Berwick, Patricia Kowsmann, and Vicky Ge Huang, “A Crypto Billionaire Who Feared Arrest in the U.S. Returns for Dinner With Trump,” The Wall Street Journal, May 22, 2025, https://www.wsj.com/finance/currencies/justin-sun-trump-crypto-dinner-7efd5367.

27. The selected tools downloaded, KT Smart Translation and 007TG’s CloudSeven, were both built using Electron, an open-source framework for building desktop applications. Electron-based applications include an ASAR file (atom shell archive), which is a bundled archive used by Electron apps to package their source code–like JavaScript, HTML, and assets–into a single file for easier distribution. This file typically contains an application’s entire front-end source code. These tools’ ASAR files were extracted after download to examine how they integrate various AI models into their platforms.

28. “007TG被黑客攻击全面瘫痪：出海从业者如何选择更安全的替代方案？,” (“007TG Completely Paralyzed by Hacker Attack: How Can Those Working in The Overseas Market Choose a More Secure Alternative?”), RoxyBrowser, December 12, 2025, https://roxybrowser.com/zh/blog/007tg-hacked-safe-alternative.

29. All 007TG-affiliated sites now bring up the error “DNS_PROBE_FINISHED_NXDOMAIN” when input in the computer browser, indicating a “nonexistent” domain.

30. See the following page for more information on Tudou Guarantee’s declining operations: “What did merchants sell on Tudou?,” accessed January 20, 2026, Elliptic, https://www.elliptic.co/blog/tudou-guarantee-winds-down-operations-after-12-billion-intransactions#:~:text=Money%20laundering%20services:%20Merchants%20advertised,to%20launch%20convincing%20scam%20operations.

31. Compound Crime: Cyber Scam Operations in Southeast Asia (Geneva: Global initiative Against Transnational Organized Crime, May

2025), https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf.

32. "New RSO and OSCE Report Aims to Initiate Inter-Regional Conversation about Artificial Intelligence Safety and Preventing the Use of Generative AI to Facilitate Trafficking in Persons," Regional Support Office of the Bali Process, November 01, 2024, https://rso.baliprocess.net/new-rso-and-osce-report-aims-to-initiate-inter-regional-conversation-about-artificial-intelligence-safety-and-preventing-the-use-of-generative-ai-to-facilitate-trafficking-in-persons/.

33. KT Smart Translation is a self-described "AI-powered cross-border client acquisition platform integrating customer development, precision marketing, data analysis, and management." KT Smart Translation, accessed October 16, 2025, https://en.kttuoke.com/.

34. "语种支持," ("Language Support"), accessed October 31, 2025, https://www.ktapp.cc/fan-yi-gong-neng-you-shi/yu-zhong-zhi-chi.

35. Evidence indicates scam center operators closely follow their staff's activities. Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia (Vienna: UN Office on Drugs and Crime, September 2023), https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Policy_Report.pdf.

36. "SCRM Project Requirements Checklist," Freelancer (Freelancer Technology Pty Limited, 2024), https://www.freelancer.com/projects/android/multi-platform-messaging-desktop.

37. "SCRM Project Requirements Checklist."

38. "SCRM Project Requirements Checklist."

39. Francesca Regaledo, "Americans Have Lost Billions to Online Scams. How Is That Possible?," The New York Times, October 23, 2025, https://www.nytimes.com/2025/10/23/world/asia/scam-centers-myanmar-cambodia.html.

40. C4ADS determined the roleplay bot's use of GPT-4 by downloading a trial version of the KT platform and asking the chatbot what AI model it leverages to perform. The bot confirmed it runs on GPT-4, though it was not permitted to speak about who developed the bot itself.

41. As with the roleplay bot, C4ADS confirmed the web search bot's use of GPT-4 by downloading a trial version of the KT platform and asking the chatbot what AI model it uses. The bug reporting bot was restricted to submitting and tracking bug reports, preventing C4ADS from posing unrelated queries or model-identification questions; while the Gemini chatbot runs on Google's eponymous AI model.

42. Daniel Dickinson and Jessica Jiji, "Crushing the Scam Farms: Southeast Asia's 'Criminal Service Providers'," UN News, July 12, 2024, https://news.un.org/en/story/2024/07/1151906; and "Rescued Teen: 8 Other Japanese Held in Myanmar Forced into Fraud," Asahi Shimbun, February 19, 2025, https://www.asahi.com/ajw/articles/15632059.

43. Ranjita Iyer, "Scams in the Digital Era: How Technology Is Changing Fraud," Forbes, March 18, 2025, https://www.forbes.com/sites/mastercard/2025/03/18/scams-in-the-digital-era-how-technology-is-changing-fraud/.

44. "SCRM Champion系统AI智能客服管理上线: 带你开启全新体验," ("SCRM Champion AI-Powered Intelligent Customer Service Management System Launched: Bringing You a Brand New Experience"), SCRM Champion, January 13, 2025, https://scrmchampion.com/article/QTI6Mq0Q.html. The archived link is currently unavailable.

45. "运营管理," ("Operations Management"), SCRM Champion帮助文档 (SCRM Champion Help Documentation), 2025, https://bettyes-organization.gitbook.io/scrm/feature-overview/admin-platform/yun-ying-guan-li.

46. "SCRM Project Requirements Checklist" (Sydney: Freelancer Technology Pty Limited, 2024), https://www.freelancer.com/projects/android/multi-platform-messaging-desktop.

47. "SCRM Champion系统AI智能客服管理上线: 带你开启全新体验," ("SCRM Champion AI-powered Intelligent Customer Service Management System Launched: Bringing You a Brand New Experience").

48. Daniel Dickinson and Jessica Jiji, "Crushing the Scam Farms: Southeast Asia's 'Criminal Service Providers'," UN News, July 12, 2024, https://news.un.org/en/story/2024/07/1151906; and Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia (Vienna: UN Office on Drugs and Crime, September 2023).

49. "CloudSeven企业办公监控系," ("CloudSeven Enterprise Office Monitoring System").

50. C4ADS was able to identify these models by analyzing the CloudSeven application's ASAR file.

51. "SCRM Champion系统AI智能客服管理上线: 带你开启全新体验," ("SCRM Champion AI-powered Intelligent Customer Service Management System Launched: Bringing You a Brand New Experience").

52. "长老有话说-20221118: 007TG是谁？," ("Elder's Words – 20221118: Who is 007TG?"), 007TG全球社交流量导航 (007TG Global Social Traffic Navigation), November 18, 2022, https://007tg.com/2022/11/18/7418/. Archived link: https://web.archive.org/web/20251119054836/https://007tg.com/2022/11/18/7418/.

53. The 007TG website includes an email address (service@007.tg), a Malaysia-domiciled WhatsApp number (+601120564337), a Telegram account (https://t.me/GM007TGbot), and a Telegram feedback bot (https://t.me/vonkinbot). See more at https://007tg.com/contact-us/. Information on its relationship to HiSeven can be found at https://007hi.com/8148.html.

"新加坡私域运营专家：助力全球品牌实现成功," ("Singapore-based Private Domain Operations Expert: Helping Global Brands Achieve Success"), 007出海全球社交流量导航 (007 Chuhai Global Social Traffic Navigation), 2023, https://007hi.com/8148.html. Archived link: https://web.archive.org/web/20250717145518/https://007hi.com/8148.html.

54. "About Us," HiSEVEN, 2025, https://www.hiseven.co/sg/en/about. Archived link: https://web.archive.org/web/20250815123635/https://www.hiseven.co/en/sg/about.

55. Registered in Hong Kong as HiSeven Technology Co., Ltd., the company was actively searching for employees in the city as recently as September 2025. Its job advertisements on OfferToday, a Hong Kong job advertisement site, emphasized HiSeven's work promoting commercial applications for AI while clearly tying it back to its headquarters in Singapore. See the following links for more information: https://www.cr.gov.hk/docs/wrpt/wk_new&changednamecoys_20250630.pdf; and https://www.offertoday.com/en/company/wQ9RZUY-8F-EuBnGbyglqg%3D%3D.

56. Data collected by C4ADS on October 31, 2025, are available upon request.

57. Compare the current site, https://goldenland-staging.hiseven.com/, with its archived version: https://web.archive.org/web/20250717145615/https://goldenland-staging.hiseven.com/.

58. The other tool is CtrlFire, an automated customer acquisition tool that operates on X. https://ph.godaddy.com/whois/results.aspx?domainName=ctrlfire.com;%20https://ph.godaddy.com/whois/results.aspx?domainName=cloud007.com.

59. "广州海创未来网络文化传媒有限公司," ("Guangzhou Haichuang Future Network Culture Media Co., Ltd."), BOSS□□ (BOSS Zhipin), accessed October 22, 2025, https://m.zhipin.com/companys/6ac739c32b675ba303x409-0EVI~.html.

60. "HiSeven," HiSEVEN, 2025, https://www.hiseven.co/sg/en/.

61. "Alibaba Cloud Unveils Latest AI Offerings to Advance Malaysia's AI Agenda," Alibaba Cloud, February 28, 2025, https://www.alibabacloud.com/blog/alibaba-cloud-unveils-latest-ai-offerings-to-advance-malaysias-ai-agenda_602029; and "HiSEVEN x Alibaba Cloud: A Strategic Partnership for Innovation and Growth," HiSEVEN, February 28, 2025, https://www.hiseven.co/sg/en/blog/14912/hiseven-x-alibaba-cloud-a-strategic-partnership-for-innovation-and-growth.

62. See "Marketplace," Alibaba Cloud, accessed January 15, 2026, https://marketplace.alibabacloud.com/store/3247004.html?spm=a3c0i.27049583.0.0.7f3c2458VRwlRu.

63. "CloudSeven企业办公监控系," ("CloudSeven Enterprise Office Monitoring System").

64. "控天科技有限公司," ("Kongtian Technology Co., Ltd.").

65. These phone numbers are as follows: +852 6812 3063 (WhatsApp contact listed on kttuoke.com), and

+852 7015 8242 (WhatsApp contact listed on ktfy999.com).

66. See endnote 27 for further information on ASAR files.

67. Because the app was built using the Electron framework and the Vite build tool, it appears the developer didn't change the default metadata when packaging it. The default metadata would state that the author would be Electron Vite and the copyright holder would be an affiliate as well. In this case, it listed Electron Vite's lead developer, Leo Wang (known professionally as cao xie mei hao 草鞋没号), as the copyright holder. Because this is a product KT seeks to sell, it would be expected that KT would ensure its copyright is listed on its platform. At best, it forgot to do so. At worst, it intentionally obfuscated any identifying information.

68. "Article 5: Prohibited Ai Practices," EU Artificial Intelligence Act, February 02, 2025, https://artificialintelligenceact.eu/article/5/.

69. "Recital 29," EU Artificial Intelligence Act, February 02, 2025, https://artificialintelligenceact.eu/recital/29/.

70. “New RSO and OSCE Report Aims to Initiate Inter-Regional Conversation about Artificial Intelligence Safety and Preventing the Use of Generative AI to Facilitate Trafficking in Persons,” Regional Support Office of the Bali Process.

71. Government of the United Kingdom, “AI Opportunities Action Plan,” GOV.UK, January 13, 2025, https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan.

72. In this case, abuse-reporting hooks refer to points in a platform’s source code that capture, record, and investigate inappropriate behavior.

C4ADS
innovation for peace