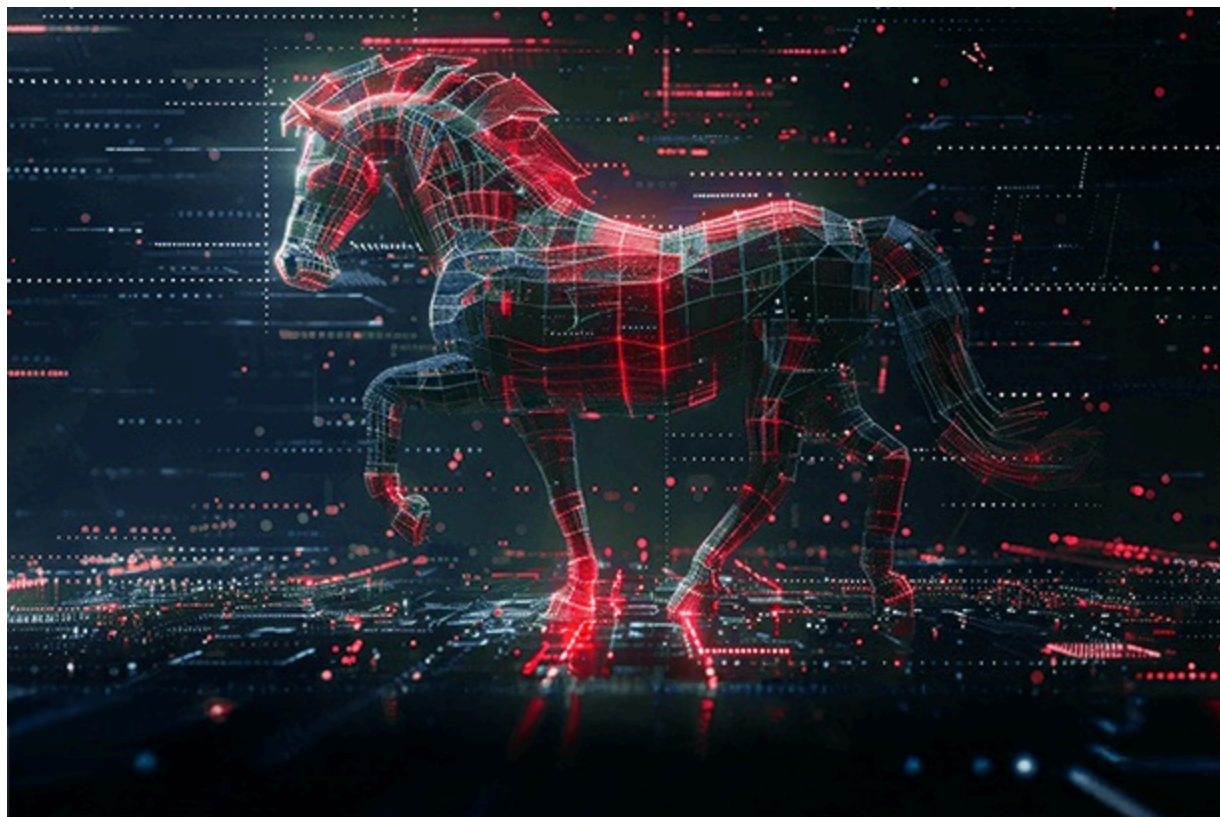


# Scams, Slaves & Malware-as-a-Service: Cambodian Scam Centers

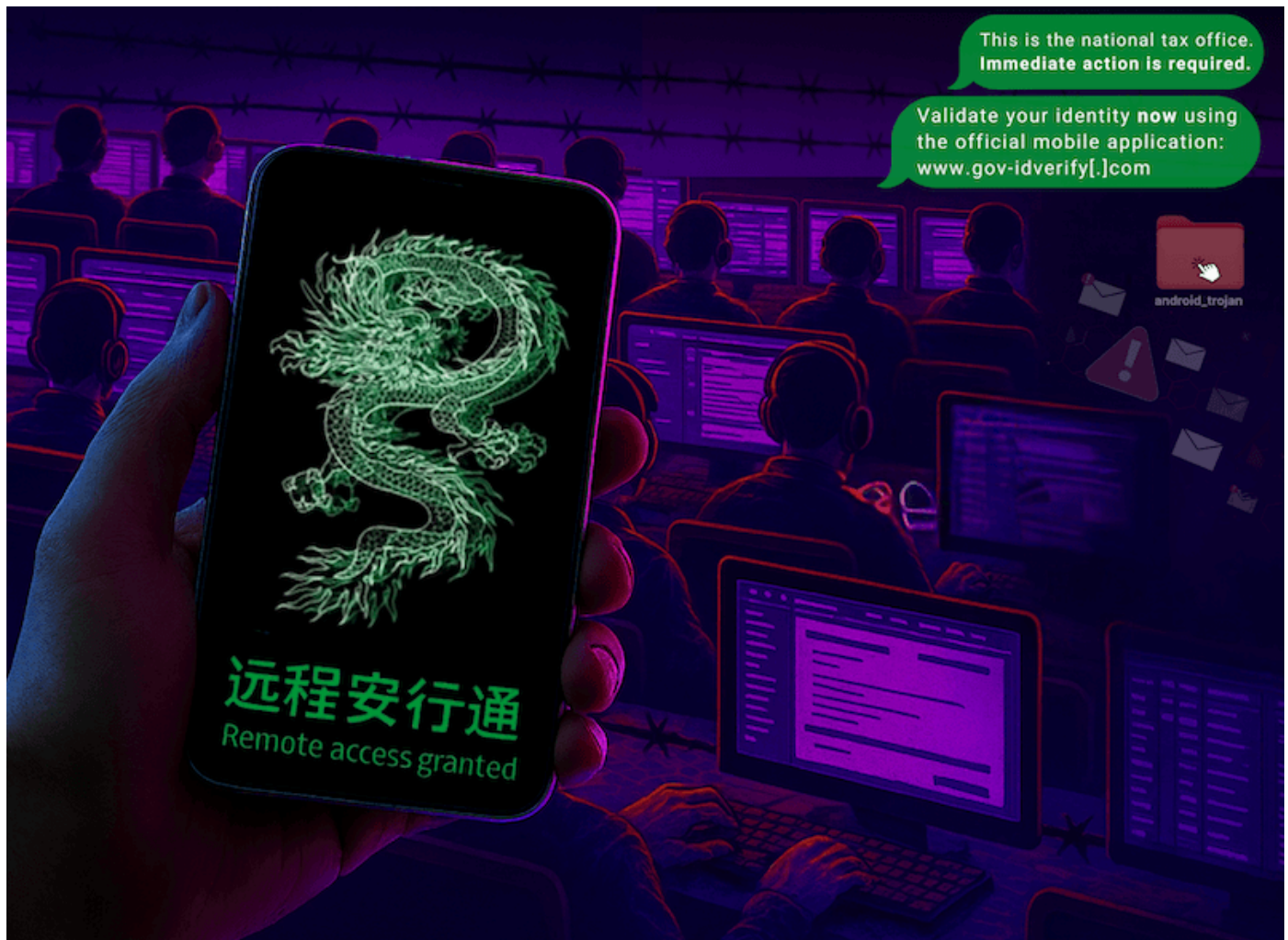
 [infoblox.com/blog/threat-intelligence/scams-slaves-and-malware-as-a-service-tracking-a-trojan-to-cambodias-scam-centers](https://infoblox.com/blog/threat-intelligence/scams-slaves-and-malware-as-a-service-tracking-a-trojan-to-cambodias-scam-centers)

Infoblox Threat Intel

April 10, 2026



Incidents of malware-enabled fraud and remote access scams have been on the rise against the backdrop of proliferating industrial-scale scam operations in Southeast Asia, with many countries in the region issuing official [warnings](#) over the past three years. But connecting specific malware to the notorious compounds has been elusive ... until now. In collaboration with the Vietnamese [non-profit Chong Lua Dao](#), we uncovered an Android banking trojan that is likely operated from multiple locations including the K99 Triumph City compound in Cambodia. This conclusion relies on technical analysis, testimony from an escapee, and evidence taken from the facility by the human trafficking victim. The compound has been widely reported by the United Nations and other organizations as a scam center with connections to high-ranking political elites and the use of forced labor to run extensive malicious text, voice, and email campaigns.



A surprising spike in DNS queries from our cloud customer environments led us to the malware, where we ultimately identified a sophisticated malware-as-a-service (MaaS) platform capable of facilitating real-time surveillance, credential theft, data exfiltration—including biometrics—and financial fraud. We discovered hundreds of domains used to target victims, many of which are crafted to look like government institutions. We first saw the DNS anomalies a year ago, but we can date the trojan back to at least 2023.

We see approximately 35 new domains registered each month. Within the Infoblox Threat Defense Cloud customer base, those most affected are from Southeast Asian, European, and Latin American countries, with the highest volume of queries associated with customers based in Indonesia, Thailand, Spain, and Türkiye, highlighting the actor's global reach and potential impact.

Further investigation surfaced infrastructure and behavioral overlaps between this MaaS and activity previously attributed to threat actors tracked as [Vigorish Viper](#) and [Vault Viper](#). Those links reveal an expansive, multilingual scam targeting victims in at least 21 countries across four continents, as shown in Figure 1. Based on linguistic artifacts, infrastructure patterns, and operational characteristics, we assess that the malware is likely attributed to an unknown

Chinese-speaking MaaS administrator servicing multiple scam centers in the Mekong region, where forced labor has been reported, and which are used to distribute malware and operate scams.

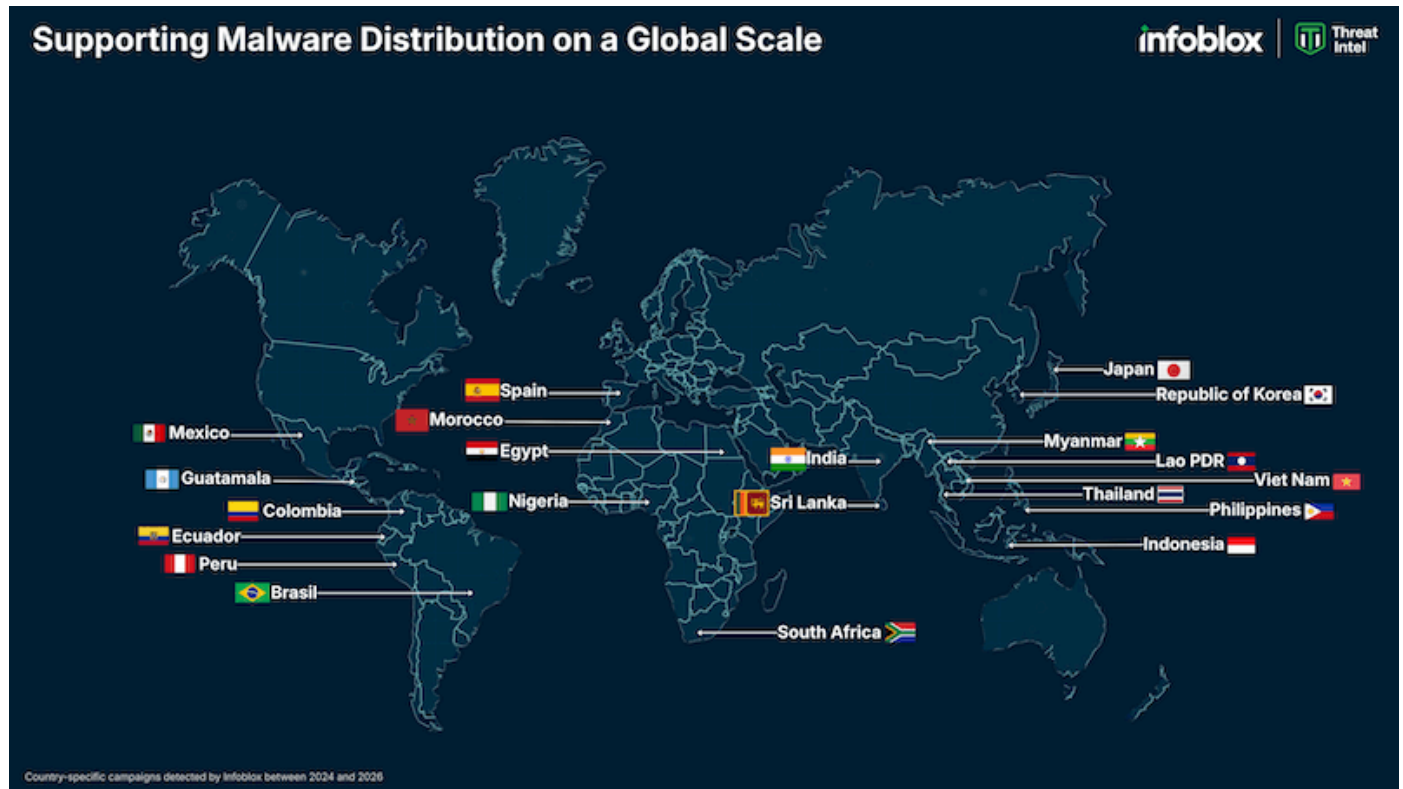


**Figure 1.** Countries in which campaigns impersonating government services and other organizations were observed; the full scope of targeting is possibly much larger.

Chong Lua Dao helped liberate some of the prisoners who were forced to run scams from within the K99 Triumph City compound and helped draw the connection with this specific trojan. Key details about the inner workings of the scams provided by those escapees, along with malware analysis from Chong Lua Dao, have paved the way for us to peek further behind the curtain and gain real-time visibility into the operation. We were able to observe just how intrusive this trojan is, handing attackers full control over infected devices and allowing them to monitor victims and steal data directly. We also found evidence of segmented C2 panels labeled by target country (e.g., “Indonesia Group,” “Brazil Group,” “Egypt Group”) and in some cases by what appears to be distinct customer names—showing structured operational divisions and coordinated management.

This report includes details of the operation, obtained directly from people who were held captive in the K99 compound and forced to participate in cybercrime. In addition to their testimonials, the escapees provided screenshots that provide direct evidence supporting a link between the domains we are tracking to activity associated with the compound.

Our findings are based on a combination of technical analysis, infrastructure patterns, and corroborating evidence from source testimony and recovered data. While the technical indicators support identification of the malware platform and its broader use, the association with specific locations, including K99 Triumph City, is based on this combined evidence and reflects our analytical assessment.

## DNS Origins and Patterns

In March 2025, we observed a sudden surge in customer queries (Figure 2) alongside a sharp increase in domain registrations. Our data shows that most of the affected customers were from Southeast Asian, European, and Latin American countries, with the highest volume of queries coming from customers based in Indonesia, Thailand, Spain, and Türkiye. These anomalies led us to investigate and ultimately uncover an Android banking trojan.

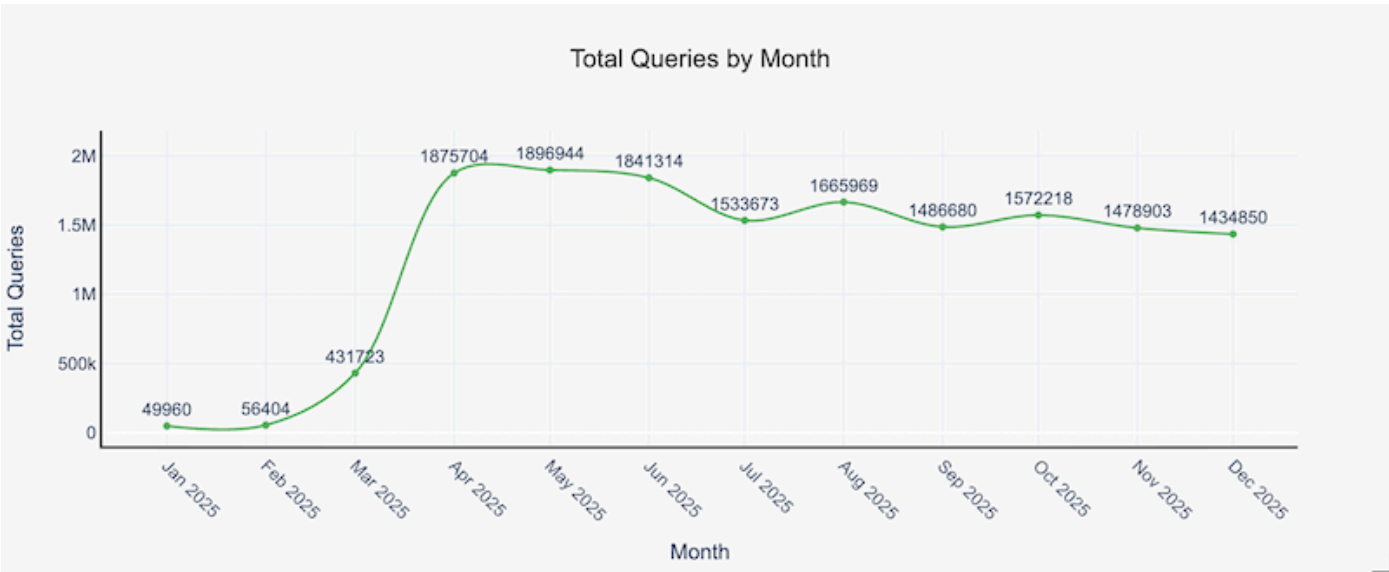


Figure 2. Volume of malware-related DNS queries in Infoblox Threat Defense Cloud customer networks, Jan-Dec 2025

The operation remains active, registering around 35 new domains per month—both registered domain generation algorithm (RDGA) domains and lookalike domains—that impersonate legitimate organizations and government services to distribute the malware. The domains are designed to spoof banks, pension funds, social security organizations, utility providers, and various revenue, immigration, telecom, and law enforcement agencies. See Table 1 for several examples.

| Domain     | Target (Country or Organization)   |
|------------|------------------------------------|
| vsgo[.]cc  | Philippines Social Security System |
| nmxgo[.]cc | South African Police Service       |

| Domain                            | Target (Country or Organization)                                    |
|-----------------------------------|---------------------------------------------------------------------|
| orgo[.].cc                        | Indonesian State-Owned Pension Fund                                 |
| idphil[.].net                     | Philippines Department of Information and Communications Technology |
| immigration-kr[.].net             | South Korean Immigration Bureau                                     |
| openbank-es[.].com                | Openbank Spain                                                      |
| googleplay[.].djppajakgoid[.].com | Indonesian Directorate General of Taxes                             |
| cedula-registraduria-gov[.].org   | Colombian National Civil Registry                                   |

Table 1. Sample RDGA and lookalike domain patterns

Figure 3 below shows several examples of the lures used. More recently, the scope of the scam has expanded, both geographically and contextually, to include lures targeting airlines and e-commerce platforms, as well as countries in Africa and Latin America.



**Figure 3.** Screenshots of samples of targeted lure pages distributing the malware, impersonating entities including the Brazilian Federal Revenue Service, Ryanair, Openbank and South African Police Service

We analyzed 400 targeted lure domains that were registered in 2025 and used to deceive and infect victims. This report presents evidence indicating that these domains are part of a coordinated, centrally managed operation designed for scale and resilience.

Domain registration for the lures is primarily with Hong Kong-based registrars Dominet (64%), Domain International Services (10%), and Namemart—formerly Domain International Services—(7%), representing 81% of identified infrastructure (Figure 4). The actor heavily favors .com, .top, and .cc top-level domains (TLDs), which account for approximately 86% of all domains. Most domains are hidden behind Cloudflare.

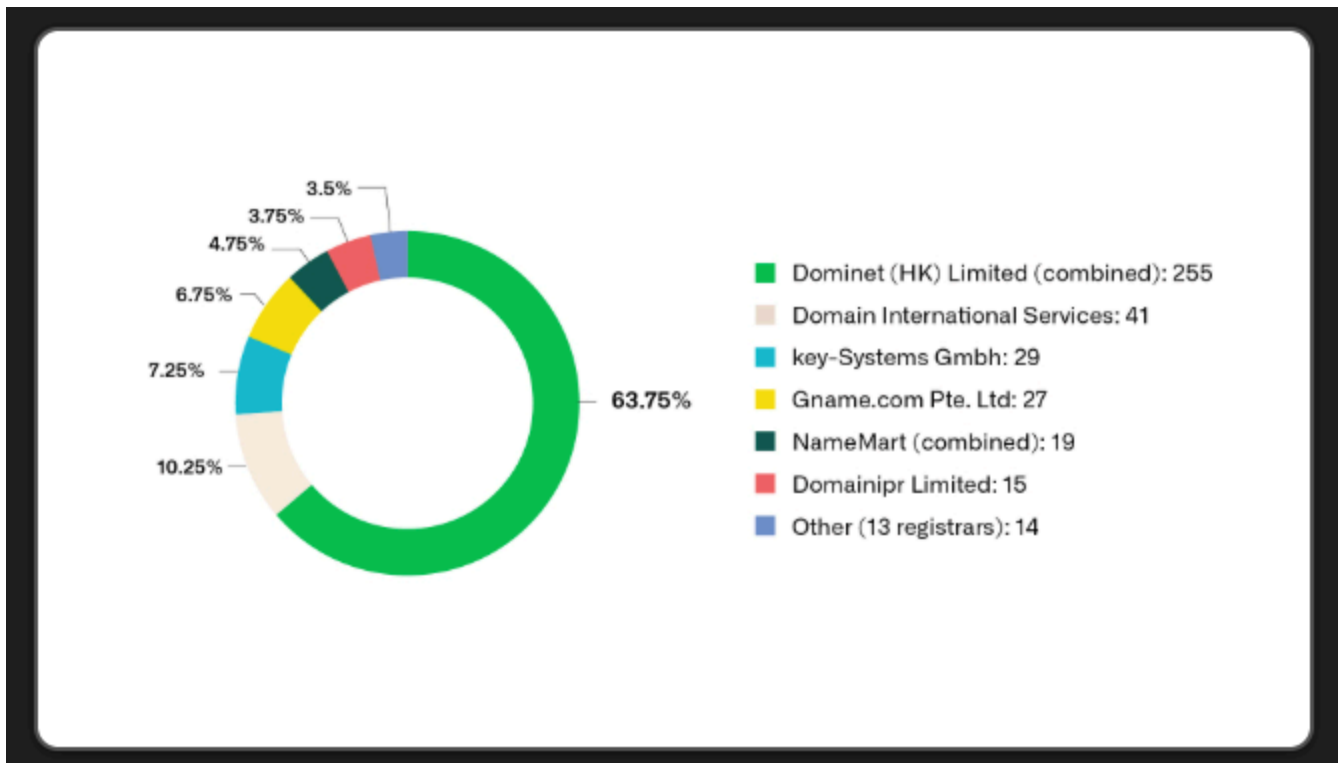


Figure 4. Targeted lure domain registrar distribution.

There appears to be a strategy to the creation of the domain names: a 2-5 character prefix followed by a carefully chosen suffix (usually 'go' or 'gov'). This is likely done to resemble the .go and .gov TLDs, supporting the actor's social engineering and government impersonation efforts. In some cases, domain names include specific geographic targeting, evidenced by short suffixes such as 'ph,' 'th,' and 'vn,' as well as longer ones including 'ind,' 'mxco,' 'peru,' and 'africa.'

Domains used for C2 and other management panels are named slightly differently, and use the .top, .xyz, .vip, and .pro TLDs, although there is a clear preference for .top (39 of 42 active C2 domains). All C2 domains use Domain International Services and Namemart registrars and DomainNameDNS name servers.

## The Attack Chain

The attack consists of several stages and utilizes a customizable kit that can be configured to produce multiple variants of the malware (Figure 5). Through a variety of mechanisms, the user is led to a website that imitates legitimate services that are typically banking or government-related.

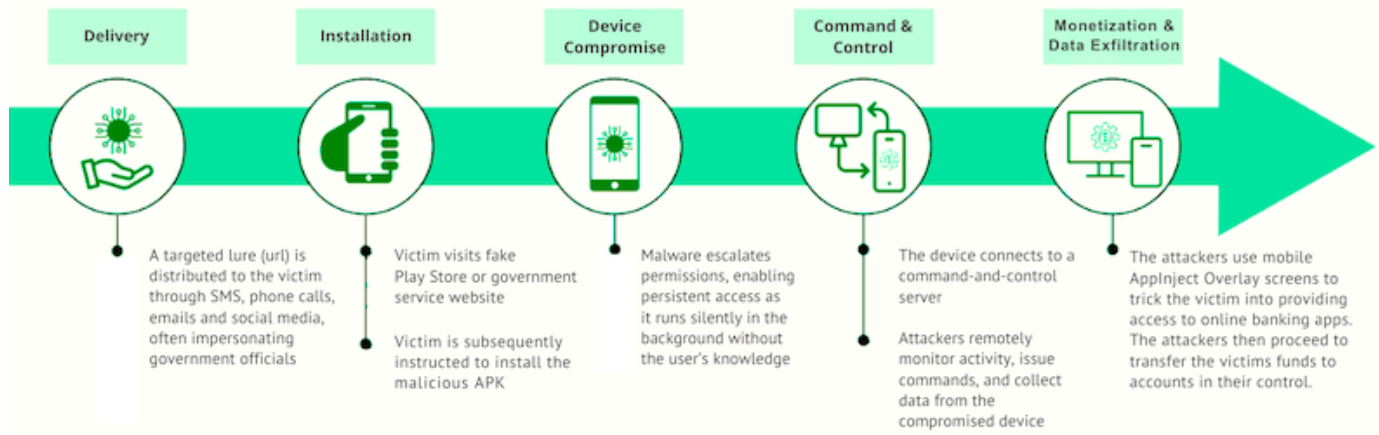


Figure 5. Simplified attack chain of the APK banking trojan

These lure sites prompt the user to download a mobile app, which uses base64-encoded JavaScript to deliver a 23MB malicious APK trojan. When users click the download button, the script retrieves the file in chunked segments while displaying a fake progress bar, ultimately resulting in the installation of the malware.

When the APK is executed, the app displays a fake login screen, like the ones shown in Figure 6. The actual login will vary depending on the attack.

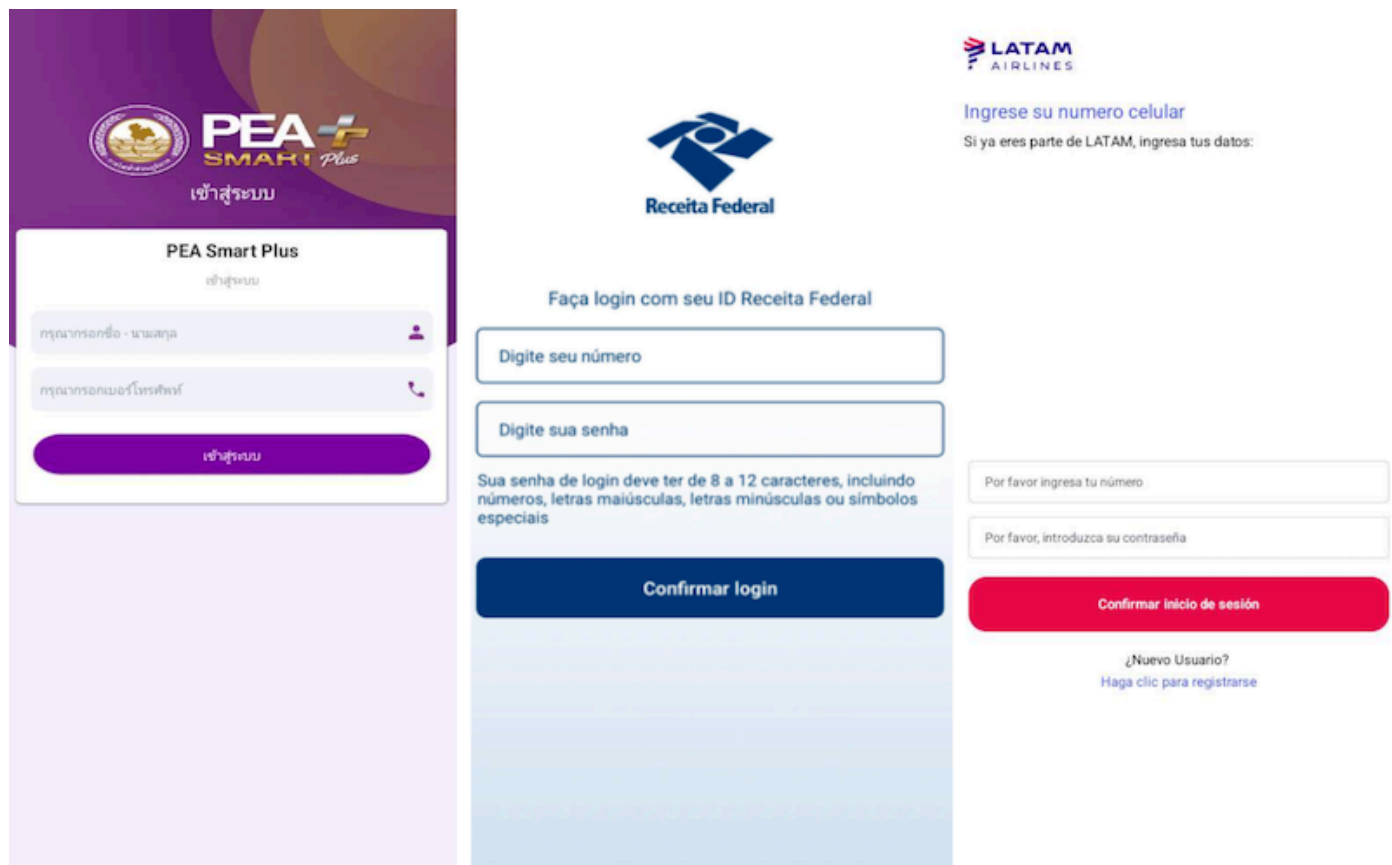


Figure 6. Screenshots of sample login screens following installation, and impersonating the Thai Provincial Electrical Authority, Brazilian Receita Federal, and LATAM Airlines

Once installed, the malware assumes the structure of a versatile banking trojan featuring a range of invasive surveillance capabilities. As shown in Figure 7, the malware's core functionality includes real-time remote monitoring, SMS and phone call interception, camera and microphone access, credential harvesting, and the ability to install additional software. It also contains a comprehensive device fingerprinting module that systematically harvests detailed hardware and system information, which is then aggregated and exfiltrated to the attacker's C2.

```
*/
/* loaded from: classes.dex */
public class GlobalBroadcast extends BroadcastReceiver {
    public static final String ACTION_APP_LIST = "org.ujwxq.app.list";
    public static final String ACTION_CLOSE_CALL = "com.common.lib.logger.call";
    public static final String ACTION_CLOSE_DIALOG = "org.ujwxq.close.dialog";
    public static final String ACTION_CLOSE_LOG_WINDOW = "com.common.lib.logger.close_log_window";
    public static final String ACTION_FINISH_THIS = "com.zxcv.finish.this";
    public static final String ACTION_INSTALL_APK = "com.xingchat.android.install.apk";
    public static final String ACTION_LIGHT = "org.ujwxq.light";
    public static final String ACTION_OPEN_BACKGROUND_RUNNING = "org.ujwxq.open.background_running";
    public static final String ACTION_OPEN_CAMERA = "org.ujwxq.open.camera";
    public static final String ACTION_OPEN_FACE = "com.fg.open.face";
    public static final String ACTION_OPEN_LOG_WINDOW = "com.common.lib.logger.open";
    public static final String ACTION_OPEN_MODIFY_PWD = "com.xingchat.android.open.modify.pwd";
    public static final String ACTION_OPEN_SMS = "org.ujwxq.open.sms";
    public static final String ACTION_OPEN_SMS_NOTIFY = "org.ujwxq.open.sms.notify";
    public static final String ACTION_OPEN_SMS_SEND = "org.ujwxq.open.sms_send";
    public static final String ACTION_OPEN_UPLOAD_ID = "com.fg.open.upload.id";
    public static final String ACTION_OPEN_URL = "com.xingchat.android.open.url";
    public static final String ACTION_OPEN_VIDEO = "com.xingchat.android.open.video";
    public static final String ACTION_OPEN_WRITE_EXTERNAL_STORAGE = "com.xingchat.android.open.write.external.storage";
    public static final String ACTION_OPEN_XF_PAGE = "com.xingchat.android.open.xf.page";
    public static final String ACTION_SHOW_CHECK_PERMISSION_ACTIVITY = "org.ujwxq.check.permission.activity";
    public static final String ACTION_SHOW_DIALOG = "org.ujwxq.show.dialog";
    public static final String ACTION_UNINSTALL_APP = "org.ujwxq.uninstall.app";
    public static final String ACTION_VOLMUE = "org.ujwxq.volmue";
    private ShowBankDF showBankDF;
```

Figure 7. Malware core functionality. Source: Chong Lua Dao

## Intel Inside

As displayed in Figures 8 and 9, by taking a look at the code, we see that some early samples include hardcoded IP, port, login API, encryption key, and other data; while later samples use an internal decryption function to dynamically retrieve the IP address at runtime, removing any static artifacts from the codebase. This change, coupled with updated BuildConfig timestamps, shows the malware is still being actively developed.

```

package app.sslxc.oledf;

/* loaded from: classes.dex */
public final class BuildConfig {
    public static final String APPLICATION_ID = "io.pqunb.cdfrf";
    public static final String BUILD_TYPE = "release";
    public static final String BaseAddress = "y+vjs82M0uhGpp0f496h7w==";
    public static final boolean DEBUG = false;
    public static final String FLAVOR = "PhWxMysssTextEncrypt";
    public static final String FLAVOR_MAIN = "PhWxMysss";
    public static final String FLAVOR_TEXT = "TextEncrypt";
    public static final String JsonStr = "njBeTefIzCqpXabg4qKMy+H90f7BqJPKKIOFZWe7JiIKswiRlYSGmLhAD2VabHQKIOFZWe7JiJ5/M07+";
    public static final int VERSION_CODE = 3;
    public static final String VERSION_NAME = "3.0";
    public static final String bTime = "Rebuild-202510050214";
    public static final String encryptionKey = "2T89ZezM3GSbbNaSP4YNAtm46a5sd43Z";
    public static final String launchActivityPath = "app.sslxc.oledf.ui.SplashActivity";
    public static final String loginApi = "x/login";
    public static final String schema = "https";
    public static final String serverAddr = "103.214.169.197";
    public static final String serverPort = "9000";
    public static final int serviceNum = 1;
    public static final String wsSchema = "wss";
    public static final Boolean hideApp = Boolean.FALSE;
    public static final Boolean needRemoteService = Boolean.TRUE;
}

```

Figure 8. Build configuration displaying hardcoded C2 IP and other data. Source: Chong Lua Dao

```

package com.ajeoj.tguju;

/* loaded from: classes.dex */
public final class BuildConfig {
    public static final String APPLICATION_ID = "com.cbpwb.drftg";
    public static final String BUILD_TYPE = "release";
    public static final String BaseAddress = "uQYUutxroVeu3bVLSq482w==";
    public static final boolean DEBUG = false;
    public static final String FLAVOR = "BrTjReceitaFederalTextEncrypt";
    public static final String FLAVOR_MAIN = "BrTjReceitaFederal";
    public static final String FLAVOR_TEXT = "TextEncrypt";
    public static final String JsonStr = "njBeTefIzCqpXabg4qKMy+H90f7BqJPKKIOFZWe7JiIKswiRlYSGmLhAD2VabHQKIOFZWe7JiJ5/M07+";
    public static final int VERSION_CODE = 3;
    public static final String VERSION_NAME = "3.0";
    public static final String bTime = "Rebuild-202511141108";
    public static final String encryptionKey = "C9iWdpwbmZ8iAmYmTmrRnpkm6xjc2SR0";
    public static final String launchActivityPath = "com.ajeoj.tguju.ui.SplashActivity";
    public static final String loginApi = "x/login";
    public static final String schema = "https";
    public static final String serverPort = "9000";
    public static final int serviceNum = 19;
    public static final String wsSchema = "wss";
    public static final Boolean hideApp = Boolean.FALSE;
    public static final Boolean needRemoteService = Boolean.TRUE;
    public static final String serverAddr = null;
}

```

Figure 9. Alternate sample no longer displaying hardcoded C2 IP. Source: Chong Lua Dao

Given the weaker operational security (OPSEC) seen in older samples, it seemed fair to assume that other mistakes would have been made, and it didn't take long for Chong Lua Dao to find an exposed C2 server that lacked proper access controls. This enabled us to monitor the activity of multiple operators and directly observe infections and attacker behavior in real time.

We observed operators, via access to exposed infrastructure, deploying customizable permissions dialogs and overlay screens to deceive victims while exfiltrating data including contacts, notes, photos, and SMS and call logs, which can immediately be used to support further attacks. We also observed operators using a web-based admin panel to manage multiple infected devices concurrently while employing distinct workflows that varied from victim to victim.

As displayed below in Figure 10, during operation, the victim is shown a spoofed digital verification or know-your-customer (KYC) overlay while the attacker simultaneously triggers biometric capture in the background. Facial recognition data is then used to authenticate into the victim's online banking application without their knowledge. By intercepting the bank's SMS OTP code, the operator has full access to the victim's bank accounts and can transfer funds wherever they wish.

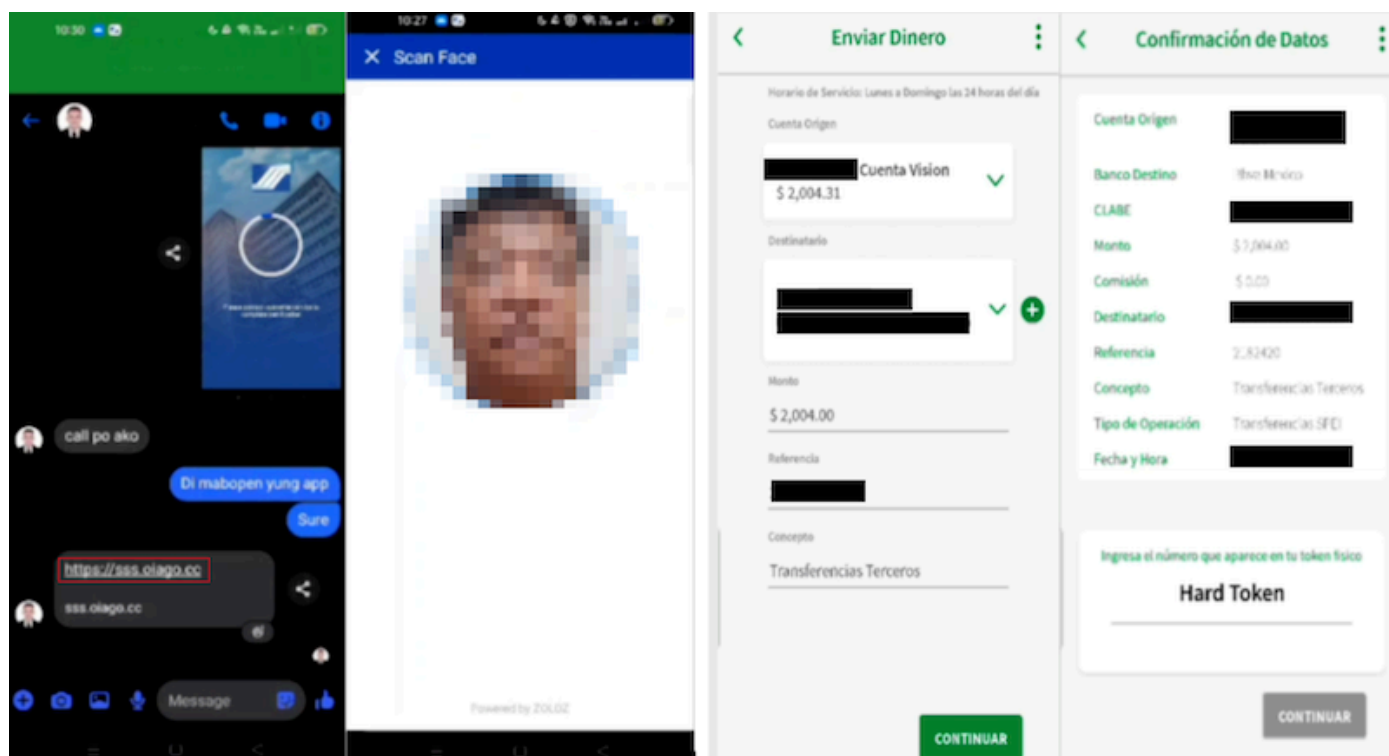


Figure 10. Screenshots of 1) an operator directing a Philippine victim to install a malicious APK at sss.oiago[.]cc using Facebook Messenger, 2) the operator subsequently deploying a KYC verification overlay, 3) and 4) the operator withdrawing victim funds from BBVA Mexico. Source: Chong Lua Dao

The MaaS administrator uses unique subdomain names, including 'kef,' 'ador,' and 'rpc,' as well as 'adm,' and 'apim' for C2 and various Android application management panels. These and other subdomain names enable the use of that signature alongside DNS data to identify additional C2s suspected of being set up to support multiple customers (criminal operators) concurrently. This includes a range of segmented C2 panels labeled by target country (e.g., "Indonesia Group," "Brazil Group," "Egypt Group") and in some cases by what appears to be distinct customer names—indicating structured operational divisions and coordinated management. Analysis further

revealed panels that appear dedicated to modified bank app development and reverse engineering, facial recognition and malware evasion testing, and AI chatbot and deepfake voice integrations. These are displayed below in Figures 11 and 12.



Figure 11. Screenshots of sample admin panels for dedicated Thailand- and Africa-facing operations as well as modified online banking application development. Source: Chong Lua Dao



Figure 12. Screenshots of facial recognition testing and AI tool management panels identified by Infoblox Threat Intel and Chong Lua Dao

We were able to peek under the hood of the MaaS administrator’s custom APK management platform shown above, ironically sitting on safeapk[.]xyz, revealing a range of custom apps impersonating organizations in Thailand. As shown in Figure 13, this includes what appear to be apps impersonating Thai Airways, Kasikorn Bank, LX International, the Office of Insurance Commission, and the Tourism Authority of Thailand, consistent with earlier campaigns visible in historic DNS records.

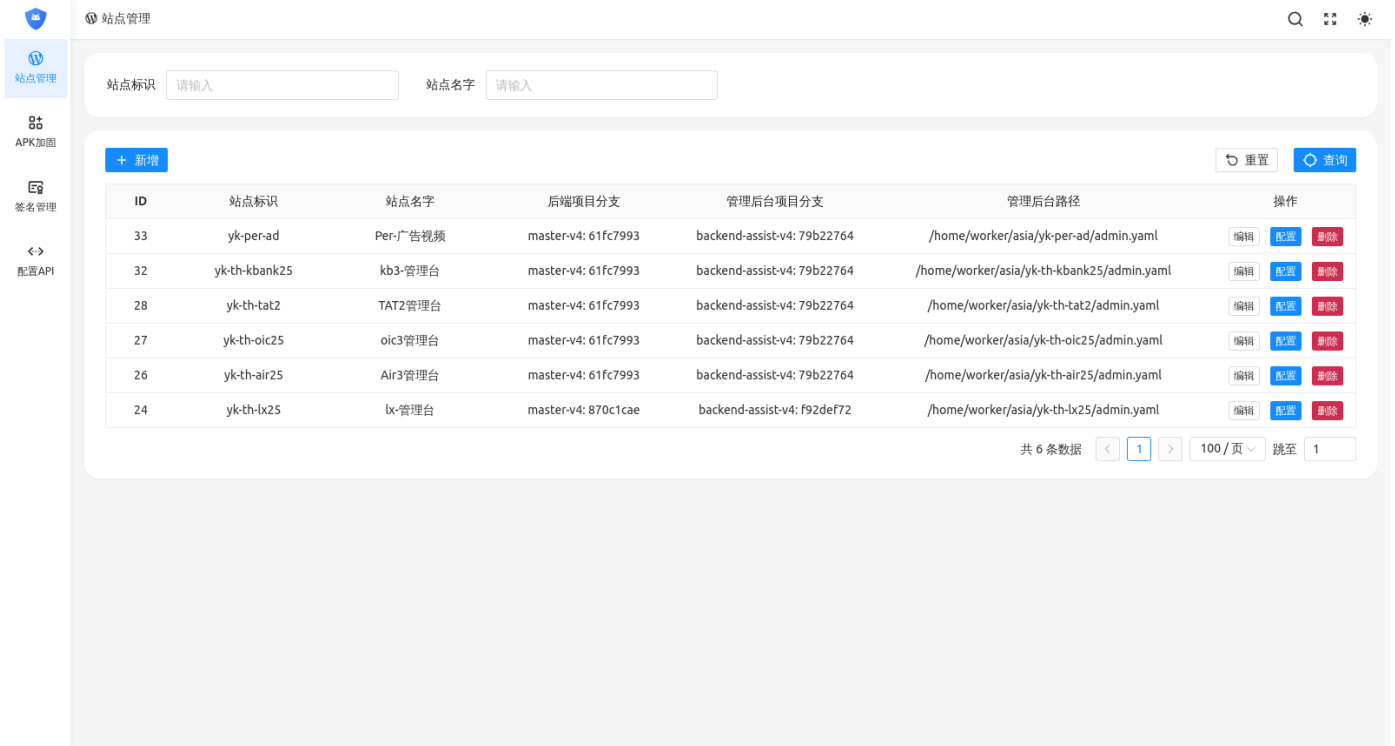


Figure 13. Screenshot of an APK management panel. Source: Chong Lua Dao

Analysis of associated infrastructure and domains indicates that the same infrastructure has been used in other activities including phishing and cryptocurrency investment or [pig butchering](#) scams. They used domains like lx-yindu[.]top and orbiixtrade[.]com to impersonate the Supreme Court of India and Thailand's Orbix crypto trading platform, shown in Figure 14, with the former notably reported in an [official notice](#) issued by the Indian Government.

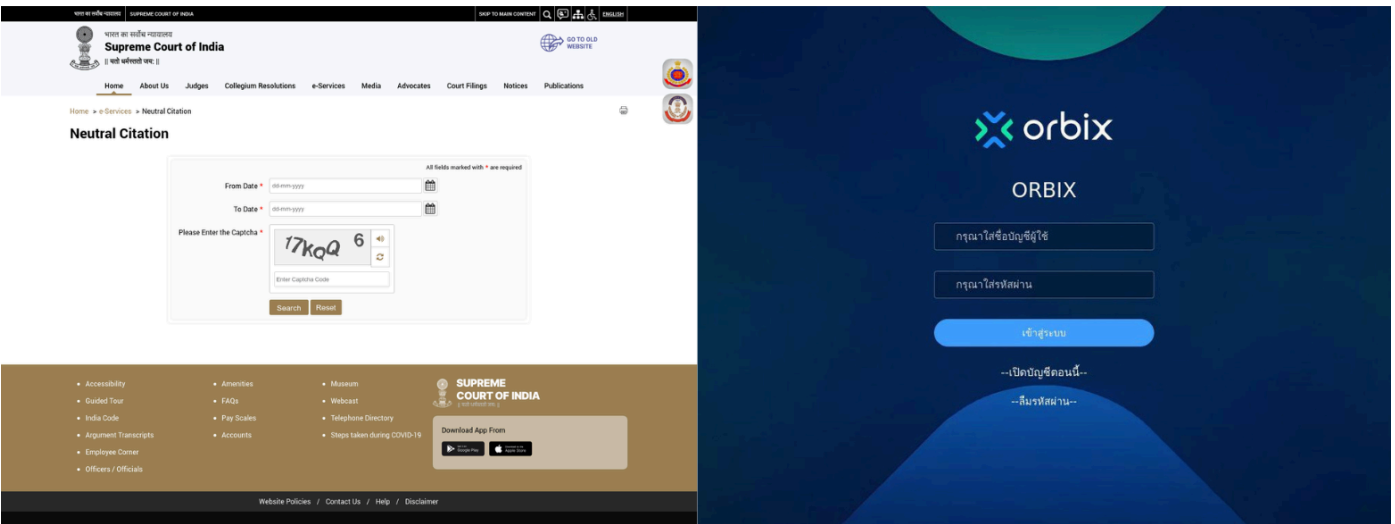


Figure 14. Screenshots of sample phishing and pig butchering pages

## OPSEC Is Hard (especially when using forced labor): A Case Study

In late 2025, captives contacted Chong Lua Dao seeking rescue from the compound in Sihanoukville, Cambodia, a cybercrime hub connected to [Vigorish Viper](#). The insiders claimed to have been beaten and electrocuted for missing performance targets—allegations that are consistent with reporting from the United Nations and other organizations that have [documented](#) similar incidents from this location in recent years.

The individuals were successfully rescued from the K99 compound, and the evidence that they were able to share (closed-group chat logs, screenshots, and other data) further validated our findings and confirmed that there was a service-based malware distribution and scam operation running on associated infrastructure. Their evidence also showed that several domains (Figure 15) from our initial cluster were used in the scam, providing strong support for our assessment that our findings are linked to the K99 site (Figure 16).

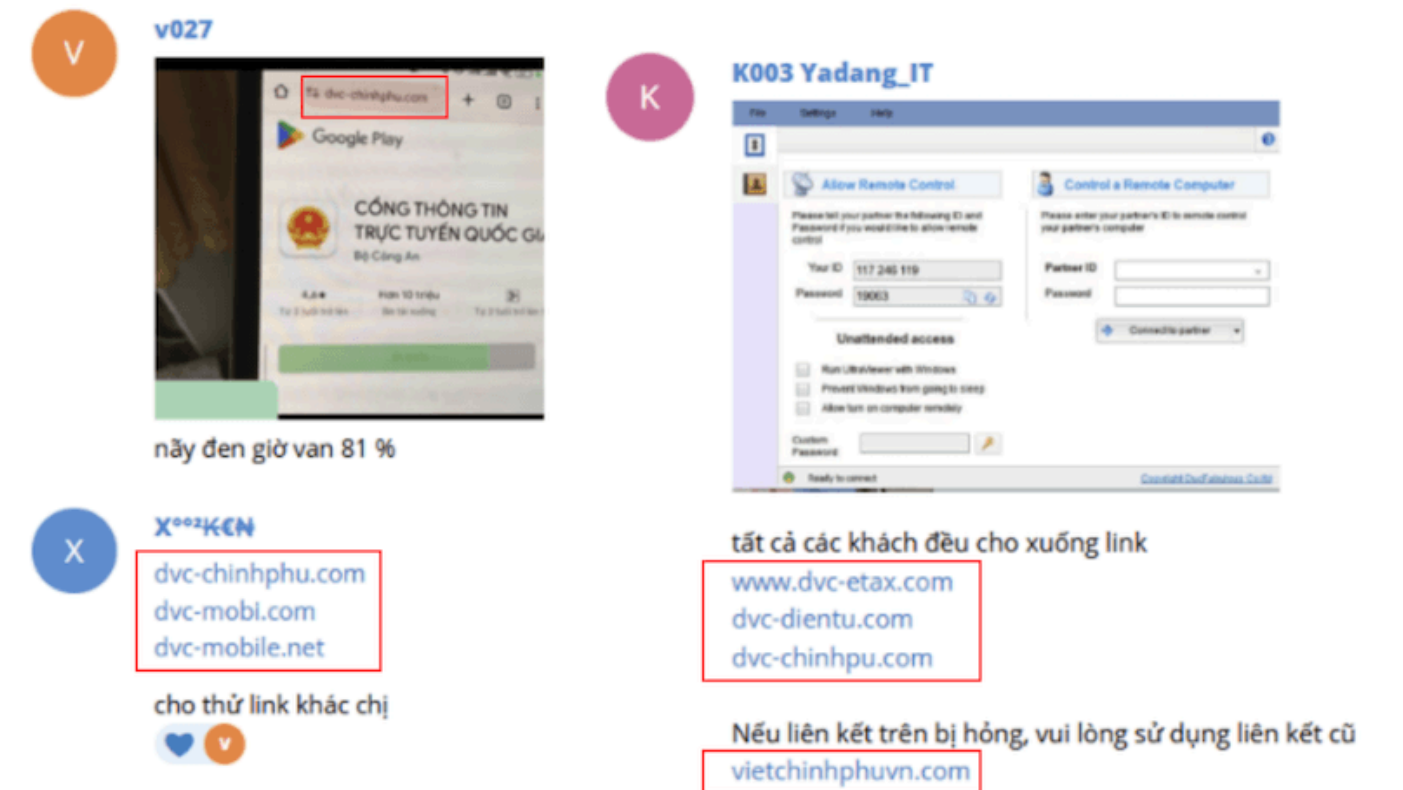


Figure 15. Screenshots of domains used to impersonate the Ministry of Public Security and the Ministry of Finance, General Department of Taxation, distributed to operators in private group chats used by a fraud network based in K99 Triumph City, Sihanoukville, Cambodia. Source: Chong Lua Dao

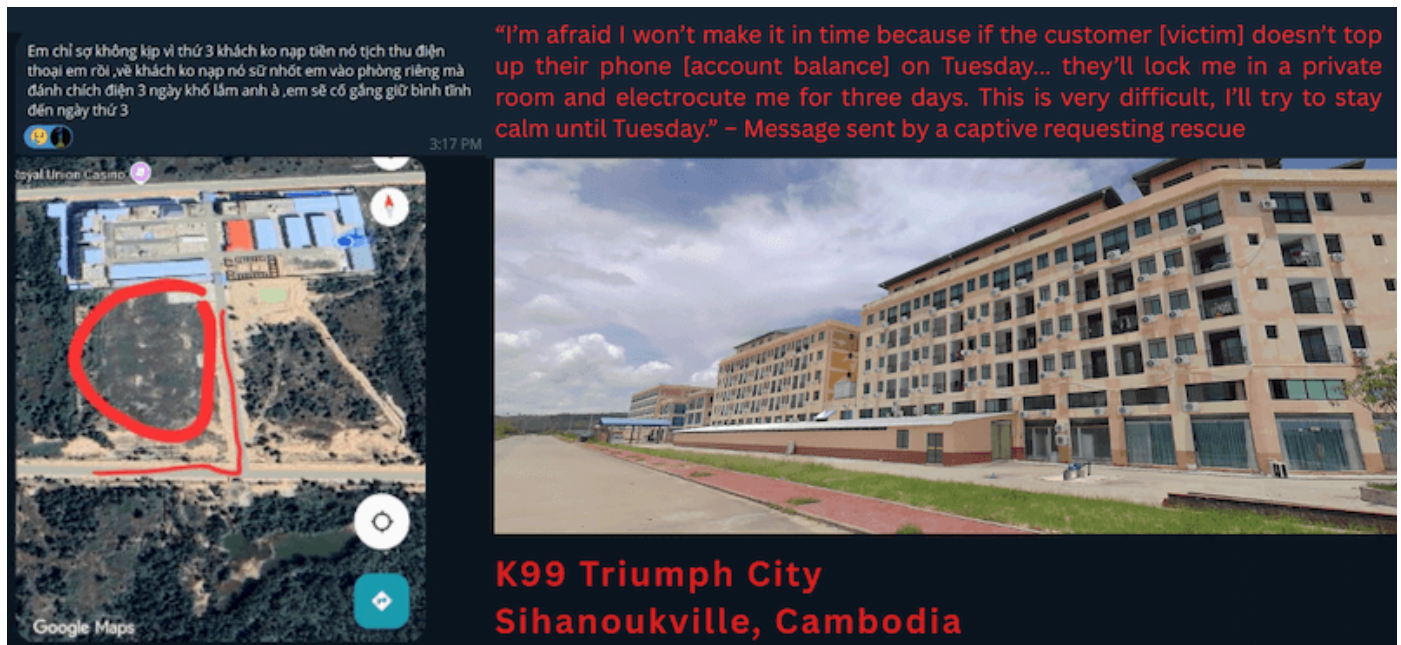


Figure 16. Message from a captive worker to Chong Lua Dao requesting rescue from a location identified as K99 Triumph City in Sihanoukville, Cambodia.

As shown below in Figure 17, examination of one insider's workstation showed detailed personal and corporate data used to inform victim targeting as well as tailored scripts and fraudulent government documents used in social engineering. It also features a fraudulent government notice letter issued to targeted business owners or employees concerning the implementation of a new digital identification and value-added tax (VAT) reduction program for registered Vietnamese enterprises. Adjacent campaigns also impersonate dozens of other government services ranging from utility providers to law enforcement.

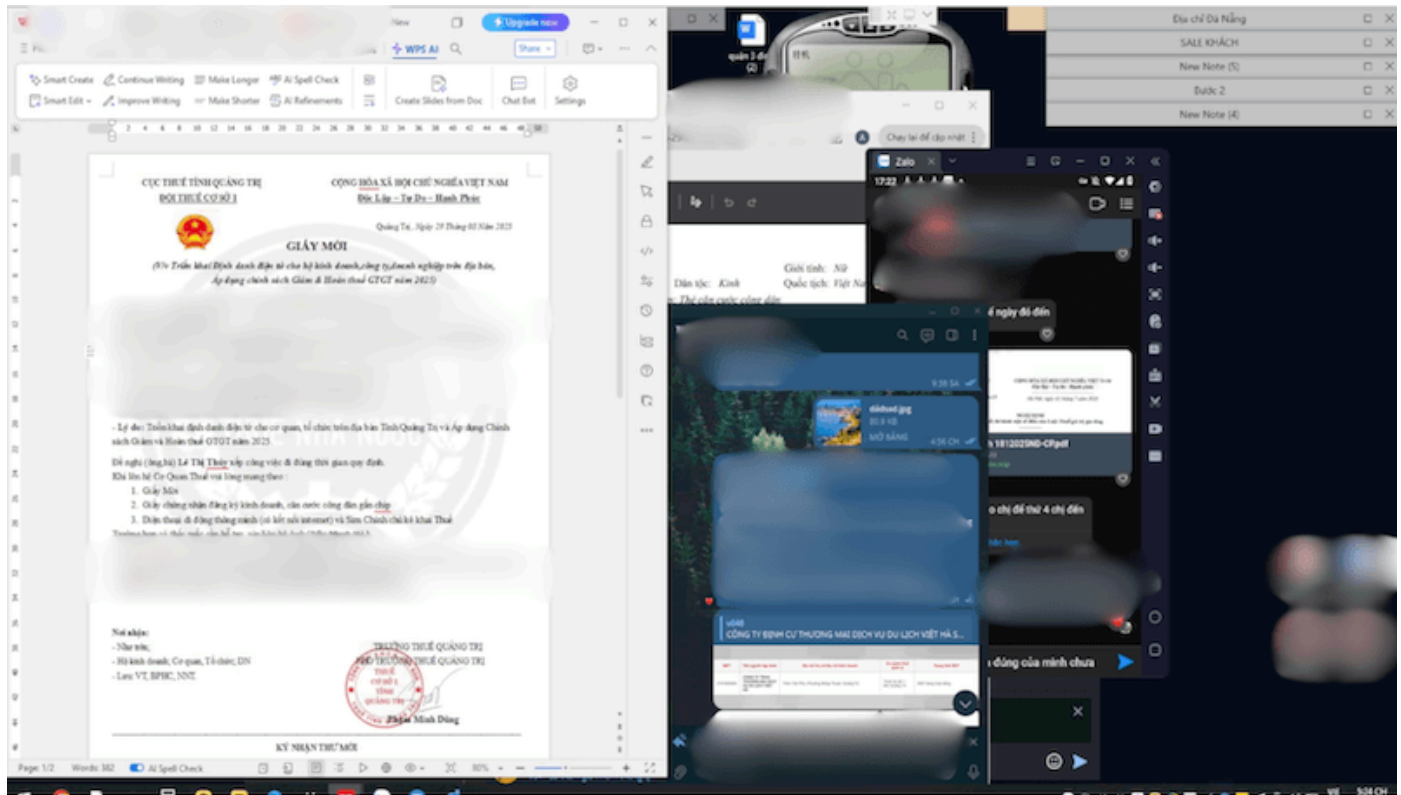


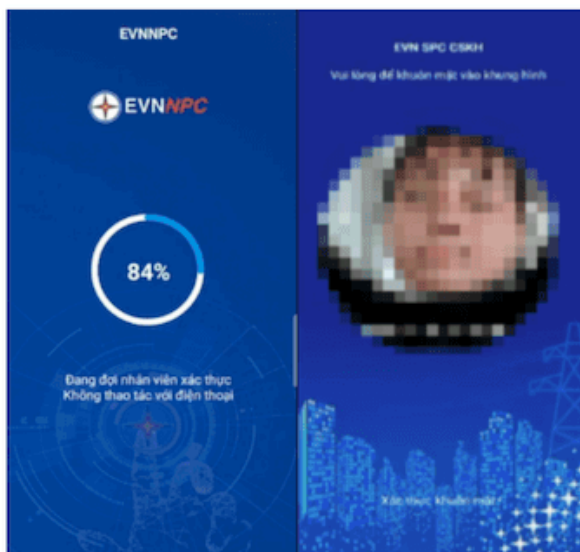
Figure 17. Screen capture of an insider’s workstation at K99 Triumph City. Source: Chong Lua Dao

According to the escapee, people working in the compound initially contact their targets by phone using eyeBeam, a Voice-over-IP (VoIP) software to impersonate government officials. They later migrate communications to the popular messaging app, Zalo, and send a link or QR code directing the victim to a targeted lure page (described earlier). They then instruct the victims to install the malicious APK and grant extended permissions on their device, disregarding any system warnings.

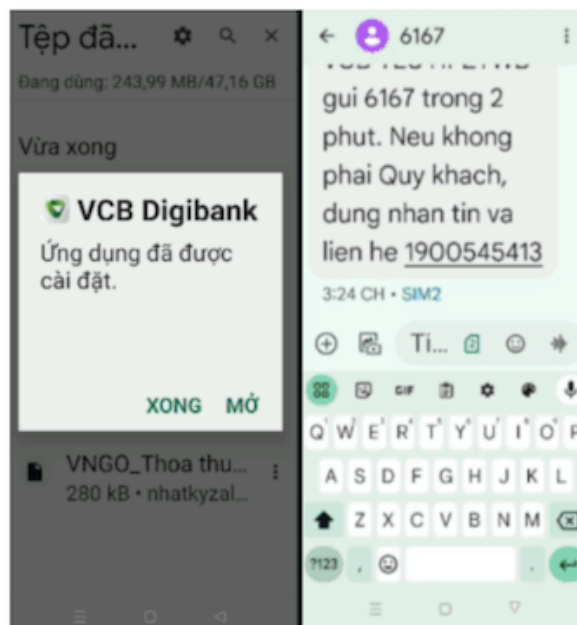
In what follows, the operator closely monitors the infected device before ultimately deploying harvested credentials to gain access to the victim’s banking app. They proceed to intercept a one-time passcode through SMS to validate their identity before finally manipulating their victim to perform a biometric verification process (facial recognition) via a convincing overlay screen. By this point the victim is fully convinced that these actions are necessary to comply with the “new government program.”

The unfortunate reality is that the victim has just completed the final step granting the scammer complete access to their online banking. This sequence of events is shown below in Figure 18 using images captured during a real attack.

The operator gains full remote control of the infected device, proceeding to install a second modified online banking application and subsequently intercepting a One-Time Pass Code issued by the bank.



The operator has gained full access into the targeted online banking account, depleting the victim's available balance by transferring funds to accounts under their control.



A phishing overlay screen impersonating an official government app is cast onto the victim's phone. They are then instructed to complete a biometric verification process which unknowingly authenticates the attacker into their online banking account in the background.

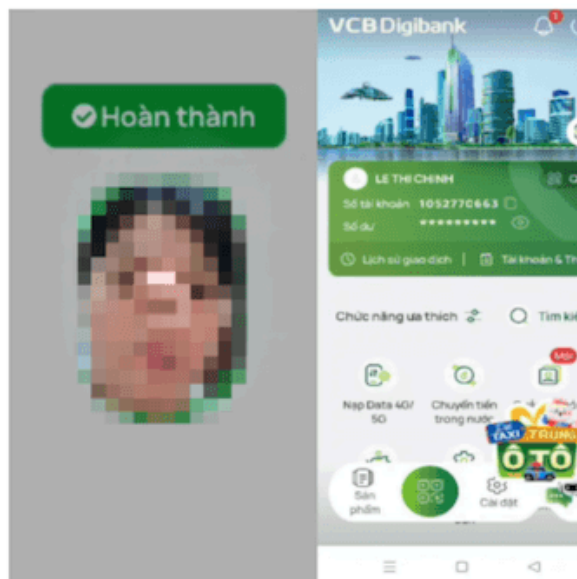


Figure 18. Screenshot of scam operator deploying KYC verification overlay screen, using the victim's face scan to gain access to the targeted online banking account in the background.  
Source: Chong Lua Dao and Infoblox Threat Intel

## K99 Group and Links to Vigorish Viper and Vault Viper

According to official corporate registry filings we have obtained, K99 Triumph City is owned by Cambodia's K99 Group, a conglomerate consisting of a range of casino and online gambling, property development, and investment companies. The group is chaired by tycoon Rithy Raksmei (aka Xie Liguang), an extended family member of one of Cambodia's wealthiest men, Senator Kok An, who has been identified in reporting as [wanted](#) by Thai authorities in connection with cyber-enabled fraud and money laundering.

Both men were recently named in United States Congressional House of Representatives [resolution \(H.R. 5490\)](#) as foreign persons allegedly involved in transnational criminal syndicates perpetuating mass online scam operations and have been described in reporting as facilitating local access through formal business partnerships with criminal networks operating in Southeast Asia. This includes syndicates led by convicted triad boss, Alvin Chau of Suncity Group, and U.K.- and U.S.-[sanctioned](#) Dong Lecheng, [among others](#) involved in one of the most notorious clusters of scam centers in Sihanoukville, Cambodia, commonly known as 'Chinatown,' displayed in Figure 19.



Figure 19. Key scam center locations associated with the extended K99 Network, Sihanoukville, Cambodia. Source: Cyber Scam Monitor, March 2025

As highlighted in our [past reporting](#), Chinatown is an enclave consisting of several heavily fortified casinos and scam compounds. It quickly emerged as one of the largest cyber-enabled fraud hubs in the world since initial development began around 2017, with these projects extensively linked to Chinese-speaking criminal networks associated with Kok An and Rithy Raksmei.

The concentration of actors tied to this area points to a highly centralized ecosystem, where a relatively small circle of politically connected insiders serve as key facilitators enabling access, protection, and operational continuity for transnational criminal groups. Individuals connected to these compounds have been documented in reporting as linked to regional crime syndicates through high-visibility partnership signings, overlapping corporate structures, and shared infrastructure.

Recent reports from rights groups and other sources suggest that K99 Triumph City remains active despite the Cambodian government's ongoing crackdown on cybercrime and scams—consistent with patterns observed in large-scale scam center networks.

Alongside K99's reported links to Senator Kok An, the network has long been described as having close connections to Cambodian political and military elites, shown in Figures 20, 21, and 22. Most notably, this includes K99's co-location with the Royal Union Investment company and casino, and its former Director, Yim Leak, son of Deputy Prime Minister, Yim Chhay Ly, who is named under the U.S. Congress' proposed [Dismantle Foreign Scam Syndicates Act](#). We also found it interesting that historic records of Leak's involvement in the company have been scrubbed from Cambodia's official business registry in recent months. Lucky for us, we've kept copies.



Figure 20. Tycoon, Rithy Raksmei, attends K99 Triumph City groundbreaking ceremony with Cambodian Senator, Kok An, in January 2019. Source: The Cambodia-China Times

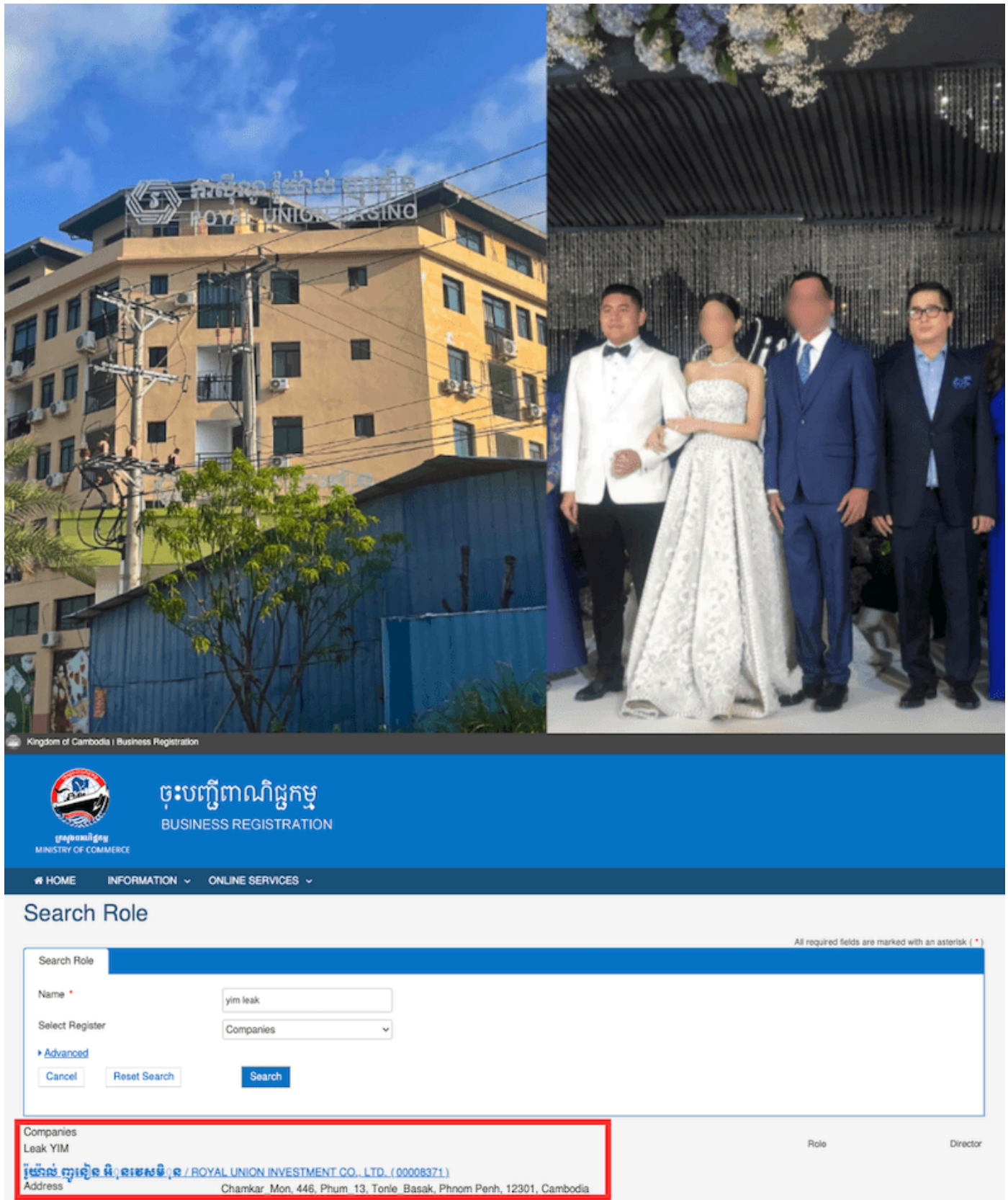


Figure 21. Screenshot of Royal Union Casino sign photographed at the K99 Triumph City compound in Sihanoukville, Cambodia, December, 2023 (left). Screenshot of Rithy Raksmei photographed with Yim Leak at his wedding in Bangkok, November 2018 (right), and Cambodian

Business Registry record indicating Yim Leak's listed role in Royal Union Investment (bottom). Source: Simon Menet, Facebook, and Ministry of Commerce of Cambodia, Business Registry, March 2026



Figure 22. Screenshot of K99 Group donation to the Cambodian military, August 2020 (left) and one of several. documented meetings between Rithy Raksmei and current Prime Minister of Cambodia, Hun Manet, December 2021 (right). Source: Facebook

In February 2026, the Anti-Money Laundering Office (AMLO) and Civil Court of Thailand issued a temporary seizure of assets worth 13.07 billion THB (US\$407 million) linked by authorities to Yim Leak, Kok An, and others in connection with investigations into transnational cyber-enabled fraud operations.

## Still Kickin'

The malicious infrastructure remains active and highly resilient, with hundreds of domains supporting multiple concurrent campaigns across three continents at the time of writing. The activity associated with this infrastructure continues to adapt and expand, sustaining large-scale campaigns targeting countries such as Thailand, Indonesia, the Philippines, and Vietnam, while increasingly diversifying into Africa and Latin America.

Ongoing monitoring shows persistent domain rotation activity using RDGAs and new lookalike domain registrations, indicating sustained demand from criminal networks in the region. We have also observed continued integration of new lures along with the repurposing of older domains to support new campaigns. Recent examples in Figure 23 illustrate changes from a Philippine government impersonation lure to one targeting customers of a Moroccan bank, as well as a domain used for Thai-facing investment scams repurposed to impersonate the Philippine government to distribute the malicious APK.

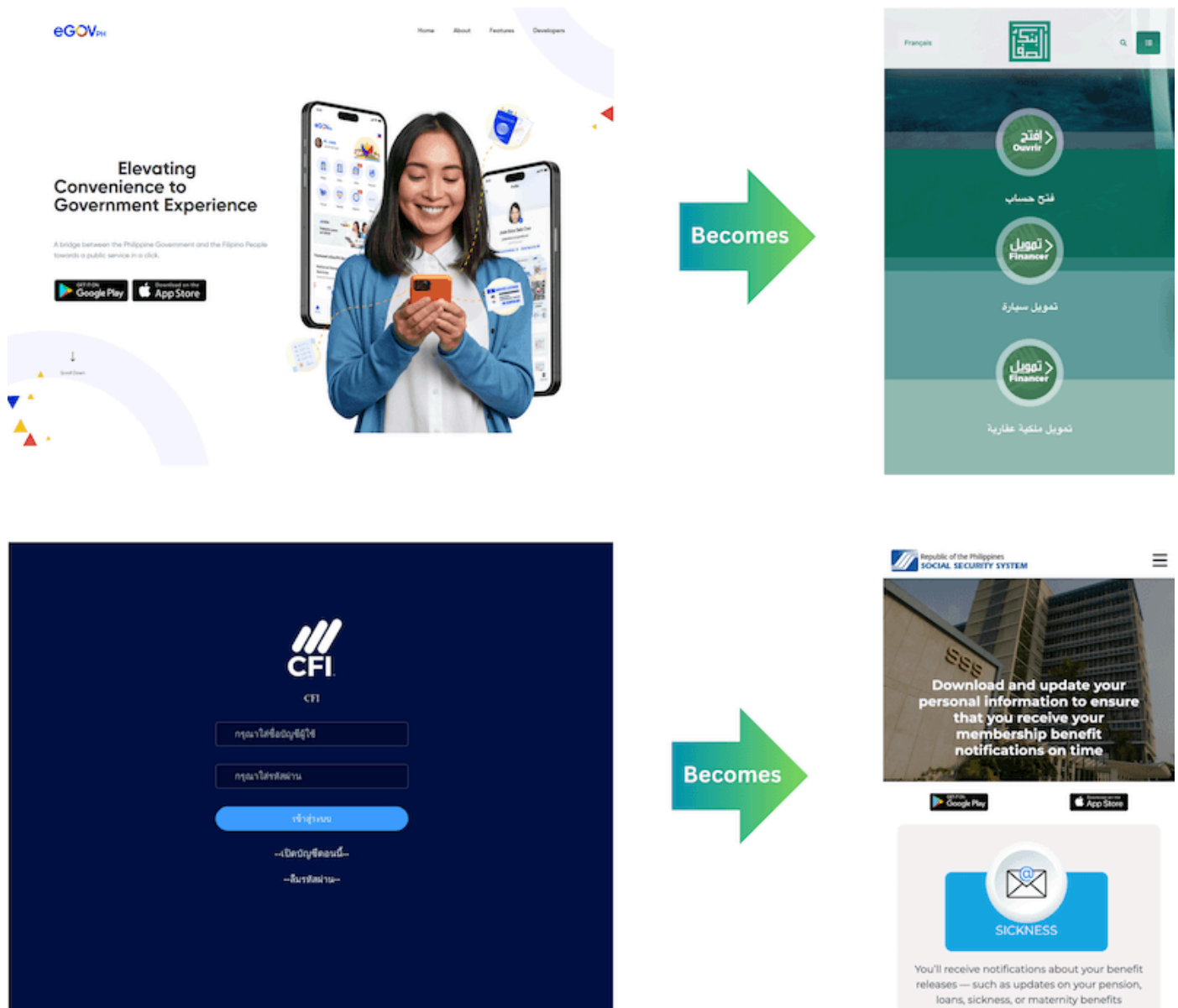


Figure 23. Top example showing screenshots of changes from a Philippine government impersonation lure on egov.nbsvgo[.]cc to one targeting customers of a Moroccan bank; bottom example showing that vsgo[.]cc was once used for Thai-facing investment scams impersonating the Certified Financial Institute (CFI) and has now been repurposed to impersonate the Philippines government to distribute the malicious APK

Our research demonstrates the resourcefulness and flexibility of scam center-based criminal groups that are rapidly operationalizing the tools being made available to them. With access to large multilingual labor pools, growing technical capability, and sky-high profits, they are not only adopting but adapting and commoditizing malware, infrastructure, and social engineering techniques into versatile and scalable attack models. What emerges is an ecosystem that is agile, experimental, and commercially driven—one where tools are continuously repurposed, refined,

and redeployed to maximize reach and profit. In this environment, innovation is not a barrier but a baseline, enabling these networks to sustain and expand complex, multi-market fraud operations at pace.

IOCs

| Indicator                                                                                                                                                                                        | Description                                                                                                             |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| orgo[.]cc<br>dkhth[.]com<br>ngovbr[.]cc<br>avianca.sxjgo[.]cc<br>rycnair[.]com                                                                                                                   | Targeted lure domains impersonating legitimate organizations and government services used to download the malicious APK |
| vnwd[.]top<br>alafrica[.]xyz<br>alperu[.]top                                                                                                                                                     | C2 domains used by the MaaS administrator                                                                               |
| 103.214.169[.]197<br>18.167.169[.]60<br>38.47.52[.]4                                                                                                                                             | C2 servers used by the MaaS administrator                                                                               |
| 4fff28eccc0ab6303e4948df77671009dda5b93ed3d1cead527b02d1317426bc39ea88f852b25d3c55d605464a3440bd250a577e3e21f52d1eaf94d15aad5b824338ab77d05aeacd7eac5acbe9eed5568778c8e3e9499562816805b54b4d1a6a | Samples of the malicious APK                                                                                            |

+4