GROUP-IB

← Blog

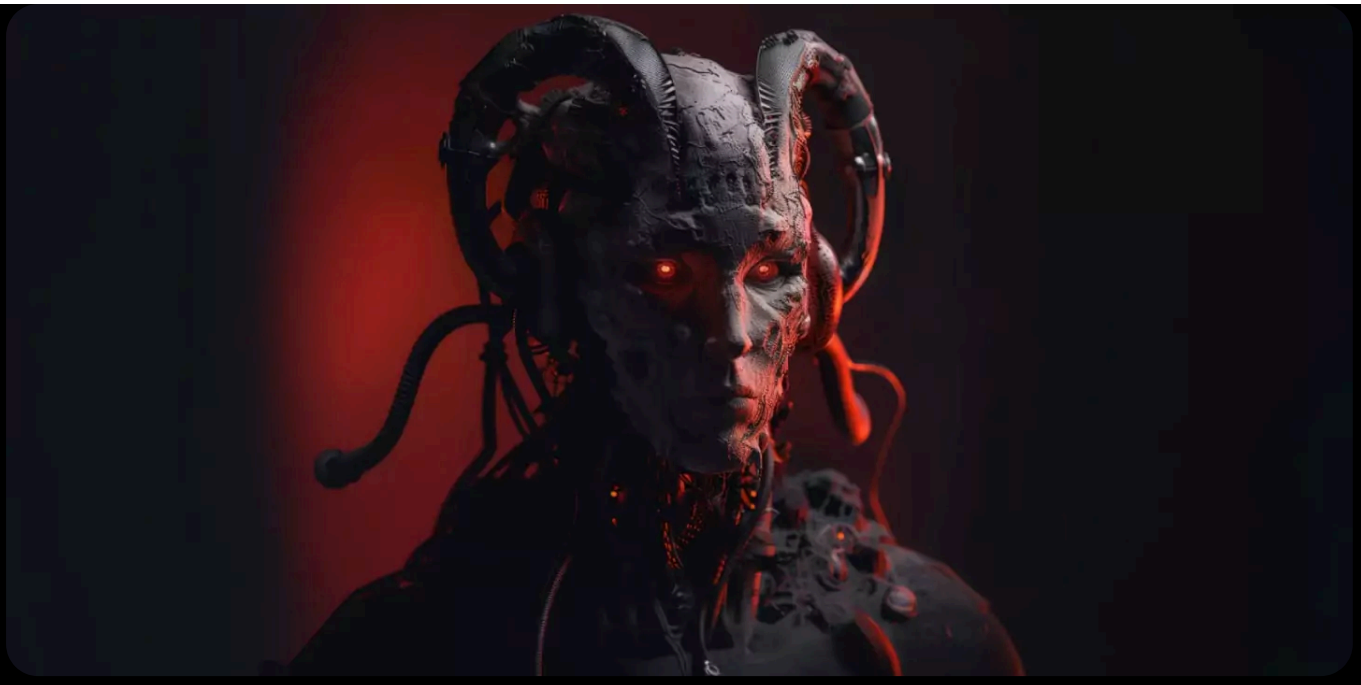
Boris Martynyuk

Cyber Threat Intelligence Analyst, Europe

Ajina attacks Central Asia: Story of an Uzbek Android Pandemic

Discovered by Group-IB in May 2024, the Ajina.Banker malware is a major cyber threat in the Central Asia region, disguising itself as legitimate apps to steal banking information and intercept 2FA messages.

September 12, 2024 · min to read · Malware Analysis



Android malware Central Asia

Introduction

In May 2024, **Group-IB analysts discovered suspicious activity targeting bank customers in the Central Asia region**. The threat actors have been spreading **malicious Android malware** designed to steal users' personal and banking information, and potentially intercept 2FA messages. During the investigation, Group-IB discovered .APK files masquerading as legitimate applications that facilitated payments, banking, deliveries, and other daily uses. These malicious files were spread across Telegram channels.

After the initial analysis of this trojan, we discovered thousands of malicious samples. All the found samples were divided into several activity clusters, each to be separately studied and investigated in a series of articles. **This article examines one of these clusters: meet the Ajina.Banker malware.**

Ajina *is a mythical spirit from Uzbek folklore, often depicted as a malevolent entity that embodies chaos and mischief. According to local legends, this spirit is known for its ability to shape-shift and deceive humans, leading them astray or causing them harm. We chose the name Ajina for this malware campaign because, much like the mythical spirit, the malware deceives users by masquerading as legitimate applications, leading them into a trap compromising their devices and causing significant harm.*

Key Findings

During our research, we uncovered the ongoing malicious campaign that started from November 2023 to July 2024.

We found and analyzed approximately 1,400 unique samples of Android malware and identified changes between versions of the same malware.

The attacker has a network of affiliates motivated by financial gain, spreading Android banker malware that targets ordinary users.

Analysis of the file names, sample distribution methods, and other activities of the attackers suggests a cultural familiarity with the region in which they operate.

Analysis also shows that the evolution of this malware campaign is causing attacks to expand beyond the original region, causing more victims in other countries as well.

Threat Actor Profile

The starting point of the research

As part of its continuous monitoring and hunting procedures, Group-IB analysts discovered a malicious Android sample (SHA1 b04d7fa82e762ea9223fe258fcf036245b9e0e9c) that was

uploaded to the VirusTotal platform from Uzbekistan via a web interface, and had an icon of a local tax authority app.

Figure 1. Screenshot of the sample found on the VirusTotal platform

Behavioral analysis has shown that the application tries to contact 109.120.135[.]42. Group-IB's proprietary Graph Network Analysis tool reveals similar files that contacted the same server.

Figure 2. Screenshot of graph analysis of network infrastructure of the detected server

Our attention was also drawn to the package when our Fraud Protection solution detected the package *org.zzzz.aaa* in one of our client sessions. During our investigation, we found more samples on the VirusTotal platform. Our Fraud Analysts continued researching this malware and constructed a timeline of the campaign, identifying methods of distribution and targets.

Figure 3. Screenshot of Android Info summary with unique package name

Timeline

Ajina's malicious campaign commenced in November 2023 and has persisted to present day. Initially the activities detected included the malware distribution through Telegram, encompassing a range of threats from malware-laden attachments to phishing attempts.

Ajina refined their tactics as the campaign progressed into February through March 2024, demonstrating heightened sophistication Social engineering techniques and the scale of the attack were increasingly leveraged to enhance the campaign's efficiency. Based on Group-IB's Fraud Protection system, we have plotted the following timeline of new infections.

Figure 4. New infections timeline

The timeline above illustrates the daily count of new infections, indicating a persistent and ongoing threat. This trend reveals that many users continually fall victim to the malware, leading to a steady increase in infections over time. The data shows that the adversary's distribution techniques remain effective, successfully targeting new victims daily.

Malware distribution

Our analysis has revealed intensive attempts by Ajina to utilize messaging platforms, including Telegram, as a channel for disseminating malicious samples. Ajina orchestrated a widespread campaign by creating numerous Telegram accounts, leveraging these accounts to disseminate malware within regional community chats. Evidence suggests that this distribution process may have been partially automated, allowing for a more efficient and far-reaching spread of the malicious software.

To enhance their deception, Ajina crafted messages and sent links and files to lure unsuspecting users. The malware is often disguised as legitimate banking, government, or everyday utility applications, designed to exploit the trust users placed in these essential services in order to maximize infection rates and entice people to download and run the malicious file, thereby compromising their devices. This targeting method resulted in a widespread and damaging malware campaign that compromised numerous devices in the Central Asia region.

Techniques

Files with themes

To further entice potential victims, the adversary shared these malicious files in local Telegram chats, using a variety of deceptive methods. They crafted enticing giveaways and promotional messages that promised lucrative rewards, special offers, or exclusive access to sought-after services. In the following example, one of the following text messages was used for spreading files mimicking the local finance application (SHA1 5951640c2b95c6788cd6ec6ef9f66048a35d6070).

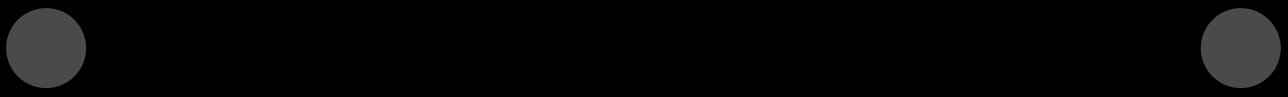


Figure 5.1 Screenshot of the message with the malicious file

Translated from Uzbek:

These messages were designed to create a sense of urgency and excitement, prompting users to click on the links or download the files without suspecting any malicious intent. The use of themed messages and localized promotion strategies proved to be particularly effective in regional community chats. By tailoring their approach to the interests and needs of the local population, Ajina was able to significantly increase the likelihood of successful infections.

File spamming

Further analysis of Ajina's distribution techniques revealed instances where they spammed messages containing only a malicious file attachment devoid of any accompanying text. This approach aimed to exploit the curiosity of users who might be inclined to open an unsolicited file or open it accidentally.

These spam campaigns were conducted across multiple accounts, sometimes even simultaneously, suggesting a highly coordinated effort. The simultaneous and widespread nature of these spam messages hints at the potential use of an automated distribution tool.

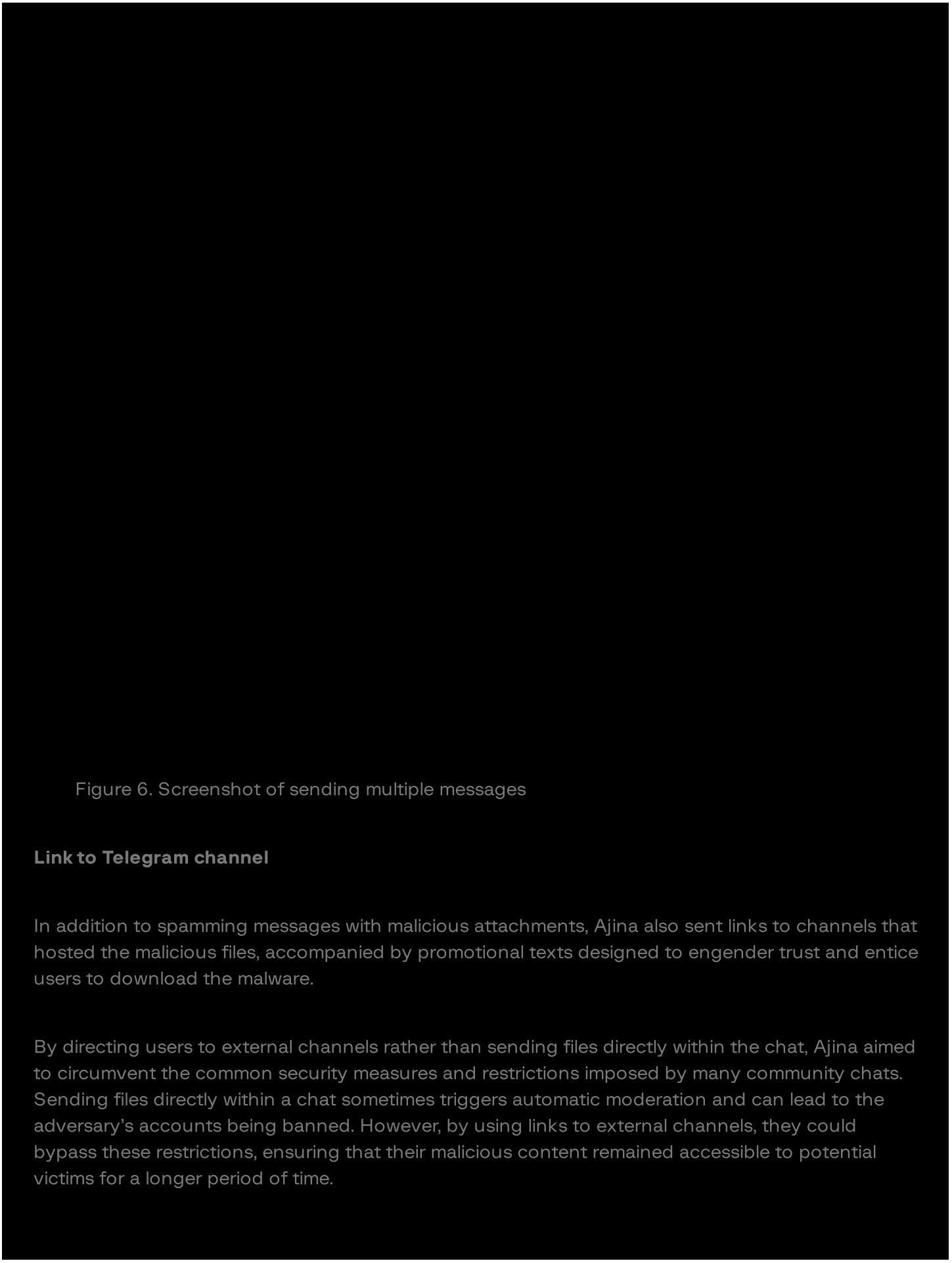


Figure 6. Screenshot of sending multiple messages

Link to Telegram channel

In addition to spamming messages with malicious attachments, Ajina also sent links to channels that hosted the malicious files, accompanied by promotional texts designed to engender trust and entice users to download the malware.

By directing users to external channels rather than sending files directly within the chat, Ajina aimed to circumvent the common security measures and restrictions imposed by many community chats. Sending files directly within a chat sometimes triggers automatic moderation and can lead to the adversary's accounts being banned. However, by using links to external channels, they could bypass these restrictions, ensuring that their malicious content remained accessible to potential victims for a longer period of time.

This approach helped the adversary avoid detection and leveraged the trust users have in seemingly legitimate channels. Once users clicked on the link and entered the channel, they were inclined to believe that the files shared there were safe, especially when presented with convincing promotional texts. This strategy highlights the adversary's adaptability and continuous efforts to refine their methods to evade security measures and maximize the reach of their malware campaign.

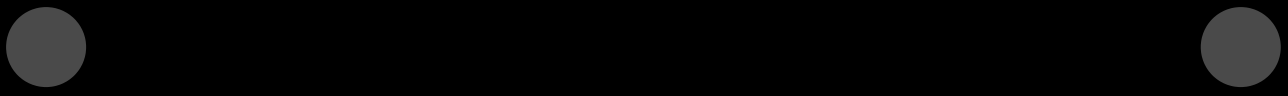


Figure 7.1 Screenshot of sending a link to channel

Link to web-resource

Some examples were found when the adversary sent links to web resources.

Figure 8. Screenshot of a message containing a link to web-resource

Accounts

Our investigation uncovered that the adversary established multiple accounts to execute their malicious campaign effectively. These accounts were meticulously set up to blend in with regular users and evade detection for as long as possible. Below, we provide detailed information on some of the identified accounts, including their account names, usernames, and user IDs, along with the volume of messages sent from each account.

Last Seen Name	INFINITOSSS MILLENNIUM	—	Barno Umarova	—	Оксана Цветкова
Last Seen Username	infinitosss	—	—	—	—
User ID	6571903171	6856449327	6824678523	6477339333	7027991392
Number of messages	238	175	76	54	25

Last Seen Name	Ренат	Алевтина!	Эмилия!	Святослав Пономарев	Eduard Bocan
Last Seen Username	—	—	—	—	EduardBocan
User ID	6406880636	7119728862	6556126401	7158481885	6125515928
Number of messages	16	48	46	10	43

Last Seen Name	Никон Дементьев	Эрнест Щербаков	شوكت	Лукия Рыбакова	Нинель Мамонтова
Last Seen Username	—	—	—	—	—
User ID	7133377920	6887020479	5526643036	6344107060	6701781993

Number of messages	7	2	2	9	13

Last Seen Name	Jason99	Linda Castaneda	Alicia Willis	Андреева Родригес
Last Seen Username	—	—	—	Andreeva_5676
User ID	6553097862	6574219148	5668418863	6716964266
Number of messages	2	1	3	1

These accounts were used to distribute the malware through various local community chats. By using multiple accounts, sometimes simultaneously, the adversary was able to increase the reach and frequency of their malicious content. The adversary's ability to maintain and operate numerous accounts simultaneously, while consistently delivering tailored messages, suggests the possible use of automated distribution tools. These tools enabled the adversary to manage large-scale operations with precision, further amplifying the impact of their malicious campaign. This approach to account management indicates a high level of planning and coordination.

Malware analysis

Fraud Protection telemetry found 1,402 packages with package names *com.example.smshandler* (187 samples) and *org.zzzz.aaa* (1,215 samples) between 30 November 2023 and 31 July 2024 across 5,197 devices. Analyzed samples share a common code structure and subset of permissions that are requested.

The first known infection occurred at 30 November 2023 via package name *com.example.smshandler* (SHA1 cc6af149f1da110a570241dde6e3cfd0852cb0d8) with permission list:

```
[
        "android.permission.READ_PHONE_STATE",
        "android.permission.RECEIVE_BOOT_COMPLETED",
        "android.permission.RECEIVE_SMS",
        "android.permission.ACCESS_WIFI_STATE",
```

```
            "android.permission.BROADCAST_SMS",
            "android.permission.DUMP",
            "android.permission.INTERNET",
            "android.permission.READ_PHONE_NUMBERS",
            "android.permission.ACCESS_NETWORK_STATE",
            "android.permission.CALL_PHONE",
            "com.example.smshandler.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION",
            "android.permission.READ_SMS"
    ]
```

Ajina.Banker.A

According to Fraud Protection telemetry data, the first known sample of this malware uploaded to VirusTotal is "*Узбек ◆екс ???*" (SHA1 84af2ce3a2e58cc8a70d4cc95916cbfe15f2169e). It was uploaded to the VirusTotal platform in January 2024, providing the initial glimpse into this malicious campaign.

Figure 9. Detections at the moment of analysis

Once the trojan is launched it connects to the gate server *79[.]137[.]205[.]212:8080*, generates AES encryption key, and sends it to the gate server along with a hard-coded worker's name and userId that is also stored into SharedPreferences.

Figure 10. Initialization of the trojan

Figure 11. Base-64 encoded string sent to server

Figure 12. Decoded payload

This message is base64-encoded JSON:

```
{
        "key": "base64-encoded AES key",
        "action": 1,
        "worker": "Ares",
        "id": "c23aaac5774d4992a8d68de5eaf28535"
}
```

All messages except *action 1* are encrypted with *AES/GCM/NoPadding* cipher suite.

Further research shows that messages are JSON-encoded, but are sent via raw TCP socket, not wrapped in HTTP. The general structure of messages contains a numeric *action* field with action type and other fields with arbitrary data depending on the action type. For example, if something goes wrong, the trojan sends a message to the gate server with the following structure:

```
{
        "action": 5,
        "msg": "string representation of the occured exception"
}
```

From the victim's point of view, once the trojan is initiated, it loads a background image from an external legit resource and requests the user to grant these permissions:

```
[
"android.permission.READ_PHONE_STATE",
"android.permission.CALL_PHONE",
"android.permission.READ_PHONE_NUMBERS",

"android.permission.RECEIVE_SMS",
"android.permission.READ_SMS"
]
```

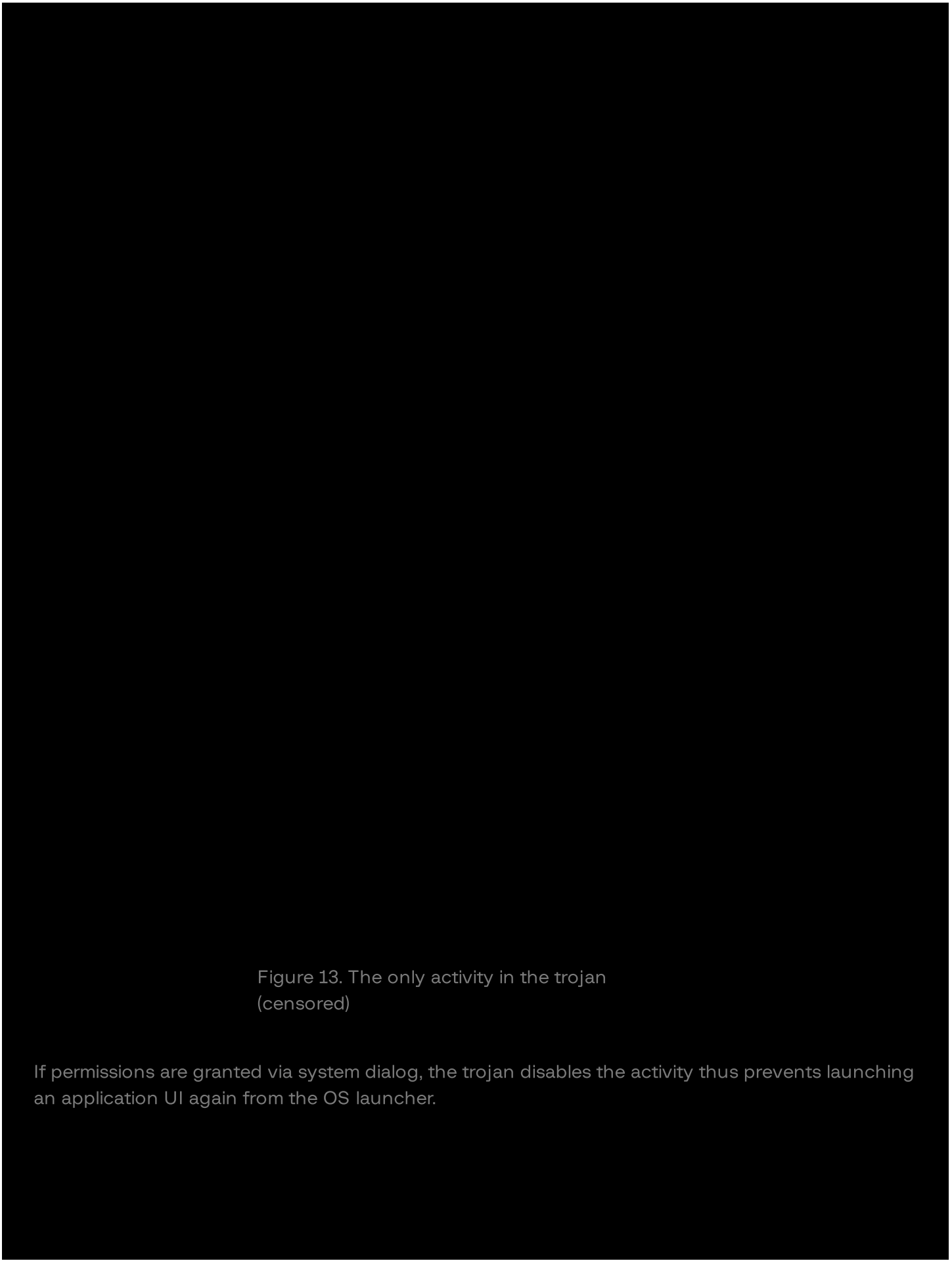


Figure 13. The only activity in the trojan (censored)

If permissions are granted via system dialog, the trojan disables the activity thus prevents launching an application UI again from the OS launcher.

```
setComponentEnabledSetting(componentName, PackageManager.COMPONENT_ENABLED_STATE_DISABLED
```

Figure 14. Prevention of further launching

If the user grants permissions via their mobile device's operating system settings menu, the trojan then launches an intent that activates a third-party application related to trojan's legend:

Figure 15. Starting a third-party activity

If permissions are not granted, the trojan sends a notification to the gate server (*action 6*).

When permissions are granted, the trojan collects information from the infected device and sends it to the gate server (*action 3*). The following is the list of information collected:

for each active SIM card

- MCC+MNC codes of current registered operator
- Name of the current registered operator
- ISO-3166-1 alpha-2 country code equivalent of the MCC (Mobile Country Code) of the current registered operator or the cell nearby
- ISO-3166-1 alpha-2 country code equivalent for the SIM provider's country code
- MCC+MNC codes of the provider of the SIM

Service Provider Name (SPN)

Phone number

Is SPN “known” or not

list of installed financial applications originated from Armenia, Azerbaijan, Iceland, Kazakhstan, Kyrgyzstan, Pakistan, Russia, Uzbekistan and some international ones

sent SMS

Recipient

Body

Date

received SMS

Sender

Body

Date

The trojan abuses the *<queries>* element in the app’s manifest instead of abusing *QUERY_ALL_PACKAGES* permission, and therefore it can get information only about what is declared in manifest packages. However, it does not prevent the expansion of the list of targets for a particular sample because Trojan will send to the gate server every incoming SMS, including for banks not included in the list of targets (*action 2*). This allows, for example, the initial registration of accounts in organizations that are not the target of the trojan.

Figure 16. Broadcast receiver for incoming SMSes

While collecting SIM-card info, the trojan checks if the SPN is “known” and, if it is, sends a Unstructured Supplementary Service Data (USSD) request to get the phone number of the active SIM cards from the victim’s device.

Country	USSD
	*187#
Armenia	*420#
	*525#
	*137#
Azerbaijan	*540#
	*666#
Kazakhstan	*160#
	*112#
Kyrgyzstan	
	*212#

After this USSD response is received, the trojan sends the response info to the gate server (*action 4*):

Figure 17. USSD response callback

There is no difference between samples with com.example.smshandler package name from first and last infections with publicly available samples.

Ajina.Banker.B

We gathered several samples from the *org.zzzz.aaa* group and found little differences in the code structure. Further analysis of the appearance of new samples and code similarities lead us to the conclusion that this family is still under active development, and we can suggest that *org.zzzz.aaa* is the new version of the same family as *com.example.smshandler*.

Figure 18. New samples stats

As shown above, another group of samples has the *org.zzzz.aaa* package name. The first known infection occurred on February 18 2024, while the earliest publicly available sample was detected on 20 February 2024, and is still the most downloaded for now.

One of the freshest samples has an interesting but less popular difference. It is a new execution flow branch showing another view instead of just a background image. Based on the names of variables of type TextInputEditText, we assume that this is something like a phishing page, but we are not able to trigger this branch.

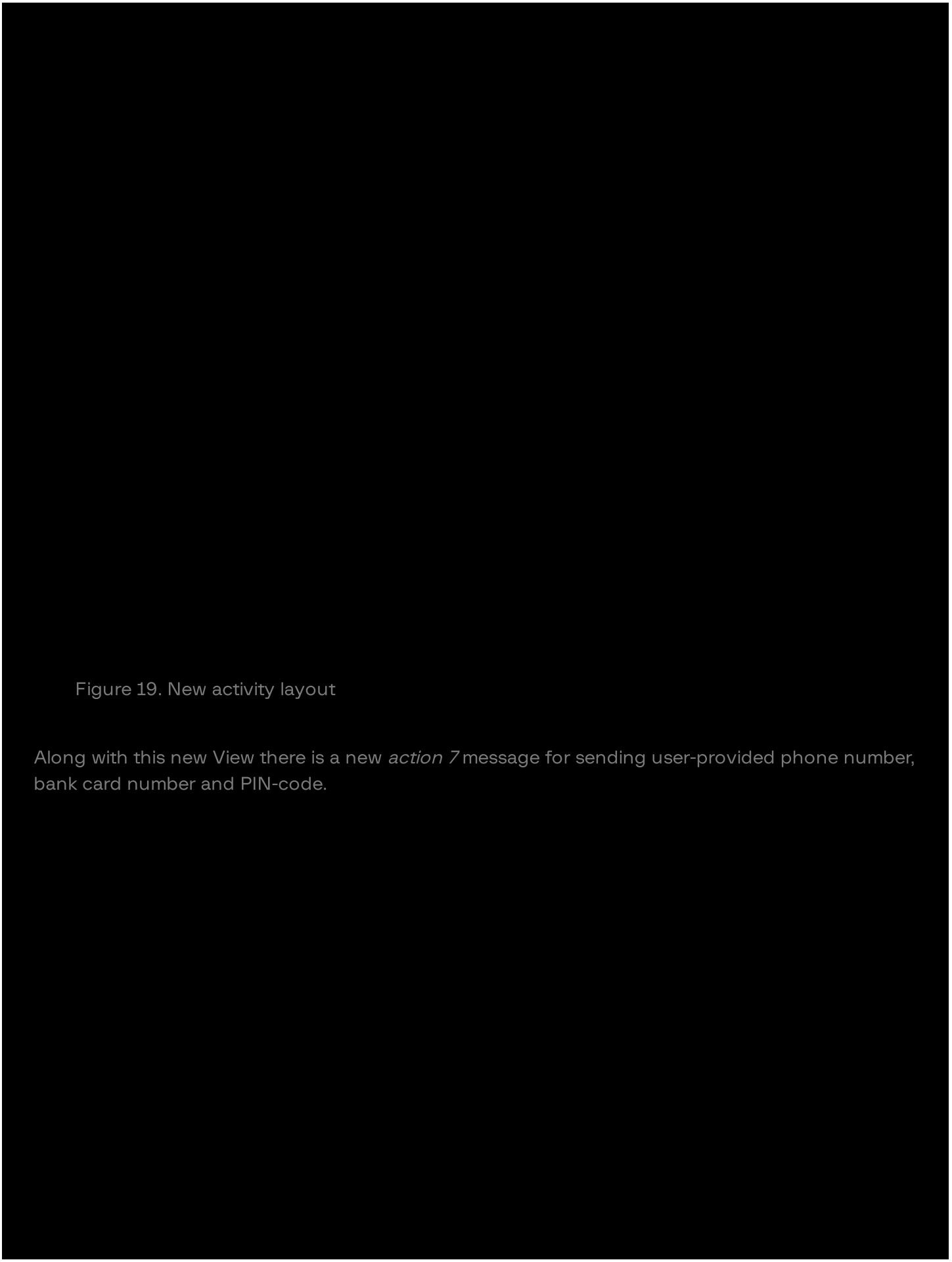


Figure 19. New activity layout

Along with this new View there is a new *action 7* message for sending user-provided phone number, bank card number and PIN-code.

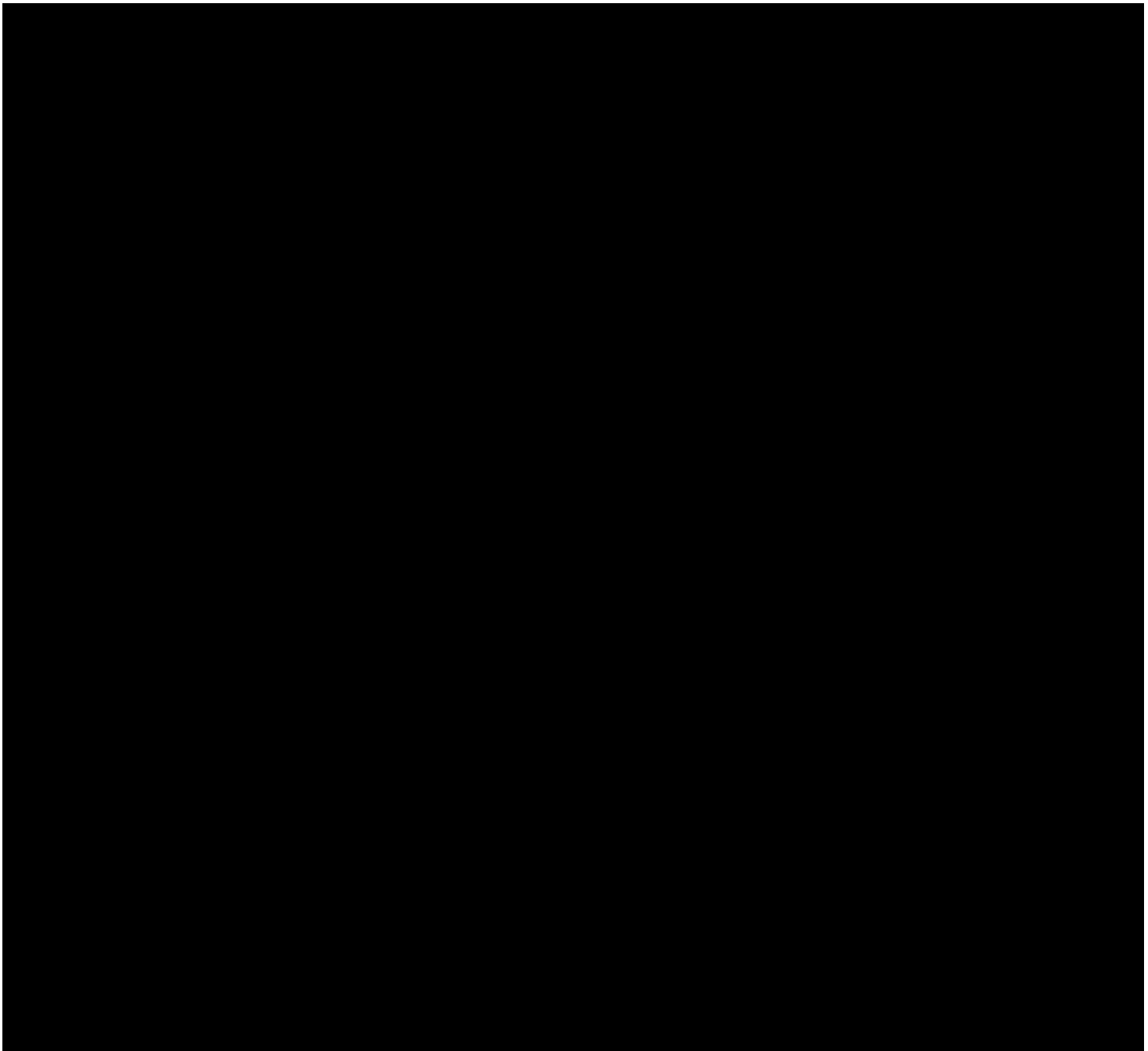


Figure 20.The user-inputed card info is sent to gate server

It appears that this new feature is developed to primarily target users in Azerbaijan because of the hard-coded phone number prefix and text language on the Toast popup.

There are some additional features that are common for most of analyzed org.zzzz.aaa samples:

- new packages of interest
- Accessibility Service abuse:
  - prevent uninstallation

grant permissions

Requests for additional permissions. However, we did not found calls of Android Platform API in the analyzed samples that requires such permissions

READ_CALL_LOG

GET_ACCOUNTS

READ_CONTACTS

Opens another legitimate app instead of a browser when permissions are granted

There are several examples of layouts from discovered samples with various legends:

Figure 21.1 Example of interface of the new samples

Infrastructure

As mentioned before, the malware only sends exfiltrated data over raw TCP in JSON to the gate server. There were no capabilities to receive commands found. But we've managed to find a web panel of "SMS handler", which refers us to the version of package name *com.example.smshandler*. It's possible to find further servers by the same response, using search by body hash (SHA1 1a9c98808a547d4b50cc31d46e19045bcd2cfc1b).

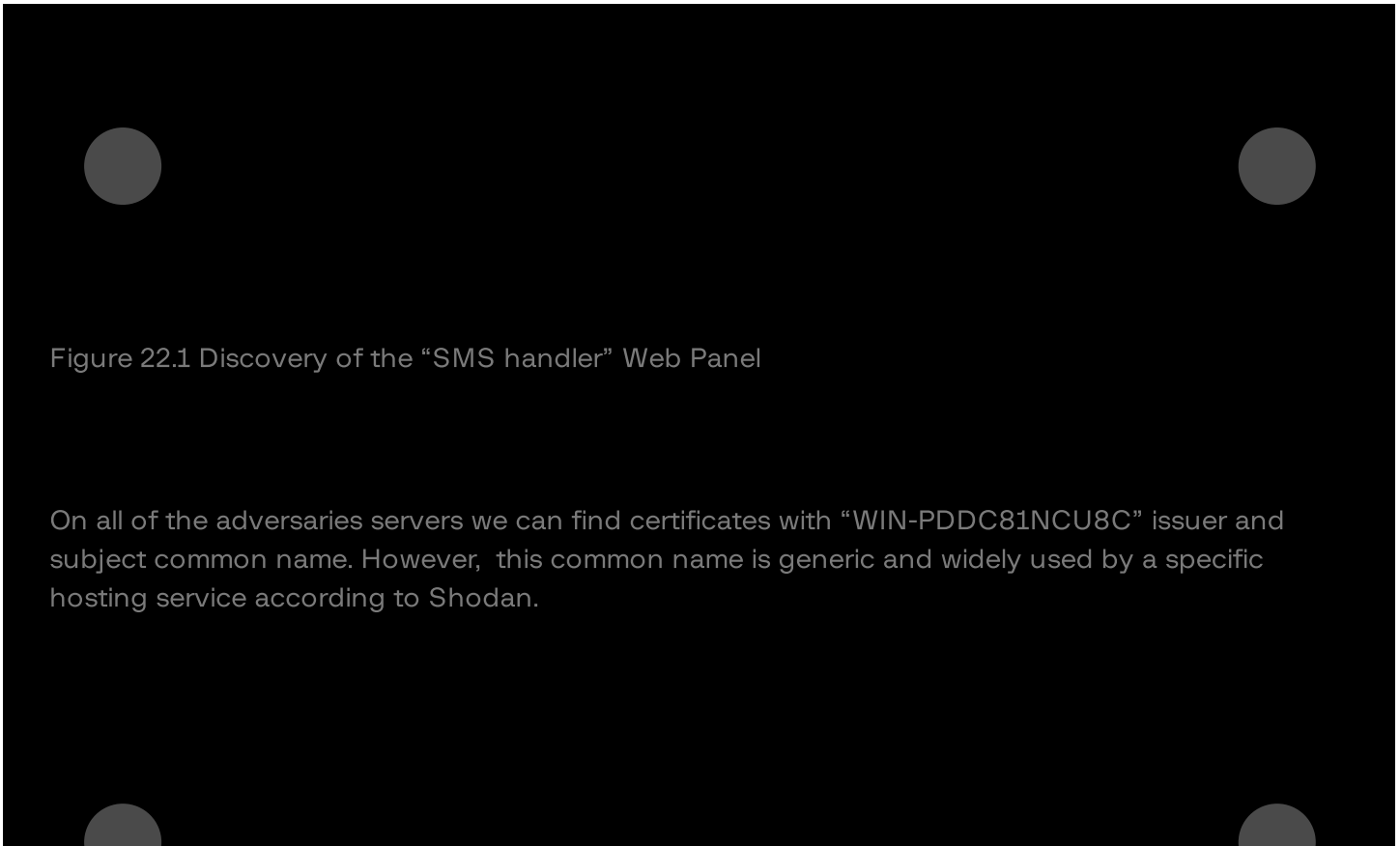


Figure 22.1 Discovery of the “SMS handler” Web Panel

On all of the adversaries servers we can find certificates with “WIN-PDDC81NCU8C” issuer and subject common name. However, this common name is generic and widely used by a specific hosting service according to Shodan.

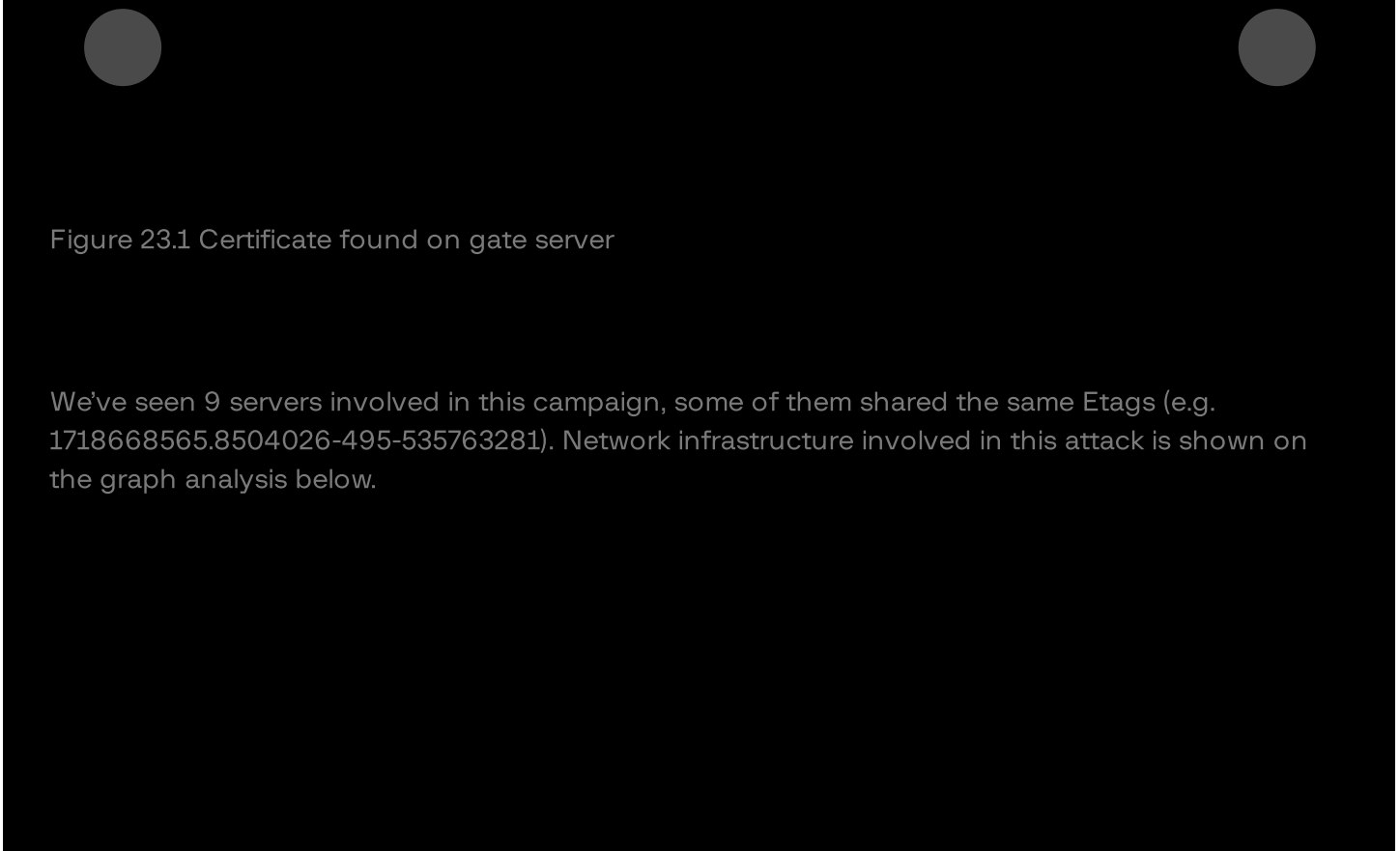


Figure 23.1 Certificate found on gate server

We’ve seen 9 servers involved in this campaign, some of them shared the same Etags (e.g. 1718668565.8504026-495-535763281). Network infrastructure involved in this attack is shown on the graph analysis below.

Figure 24. Screenshot of graph analysis of network infrastructure

Targets

As we've mentioned above, one significant aspect of our findings is based on the analysis of Android package names utilized in this campaign. Many of these packages mimicked popular regional apps, such as local banking applications, government service portals, or everyday utility tools. By replicating the appearance of these trusted applications, the adversary increased the likelihood of users downloading and installing the malware. So the displayed names can be a trustworthy indication of the target region.

Analysis indicates that most of these malware samples were specifically designed to target users in Uzbekistan, suggesting that the adversary deliberately focused on this region. But there are also a few other regions that have been targeted by the adversary. The main reason is that the samples have hardcoded checks for attributes distinctive for other countries. We've also seen *AM-CERT (National CERT/CSIRT Armenia) reporting this campaign*.

During the analysis we've also found the use of specific country phone provider codes embedded within the malicious APKs. These codes indicate that the adversary has an even wider pool of target countries. The adversary checks for Service Provider Network (SPN) and then sends a Unstructured

Supplementary Service Data (USSD) request to get the phone number of the active SIM cards from the victim's device. Based on this we can assume potential regions of interest, from where the user data could be possibly stolen.

Figure 25. Distribution of supported SPNs and apps of interest per country hardcoded in sample

Attribution

The analysis of the malware has shown that the malicious files contain data about different affiliates. This leads us to conclude that it's based on an affiliate programme, where the support for the initial project is led by a small group of people, and all the distribution and infection chains are made by affiliates working for the percentage.

Sample named "Вип Контент.apk" – "VIP Content.apk" in english – (SHA1 b4b9562a9f4851cba5761b1341f58f324f258123) was seen by MalwareHunterTeam and mentioned in *Twitter post* in January 28, 2024. One of the replies written *to the post by APK-47* highlights an interesting username hardcoded as a name of one of the workers. The username

“@glavnyypouzbekam” leads to the Telegram account named “Travis Bek” with description “Главный по узбекам” which means “Chief for Uzbeks”.

Figure 26.1 Screenshot of the Twitter post by APK--47

Group-IB Threat Intelligence system has found the following activity related to the Telegram account mentioned. Adversary participated in programmers chats, searched for “Java coder” and, according to his message, to an existing team. Detected user activity is shown on the figures below.

Figure 27.1 User activity found by Group-IB Threat Intelligence

We’ve also found a Telegram bot connected to this campaign by username “@glavnyypouzbekam” contained in its description. Bot with the username “@glavnyypouzbekambot” has information about the possibility of earning money online and an invitation to join written in Russian.

Figure 28.1 Telegram bot found during the investigation

We assume that highly likely due to its uniqueness, the hardcoded worker's name "@glavnyypouzbekam" is connected to the discovered Telegram activity. Based on our findings, we assume that the adversary standing behind this account is one of the operators of the Ajina malicious campaign. The hiring of Java coders, created Telegram bot with the proposal of earning some money, also indicates that the tool is in the process of active development and has support of a network of affiliated employees. Worth noting, that soon after the adversary's name was posted on Twitter, current Telegram account was deleted.

Prevention

To protect Group-IB customers from threats related to Ajina.Banker malware and other similar threats, Group-IB Fraud Protection uses events/rules to detect and prevent Ajina.Banker and other similar malware:

For confirmed malware samples Ajina.Banker:

Group-IB's Fraud Protection maintains an extensive database of all detected malware. When our system detects applications from the list of mobile Trojans downloaded to an end-users device, we trigger the appropriate events to notify our customers promptly.

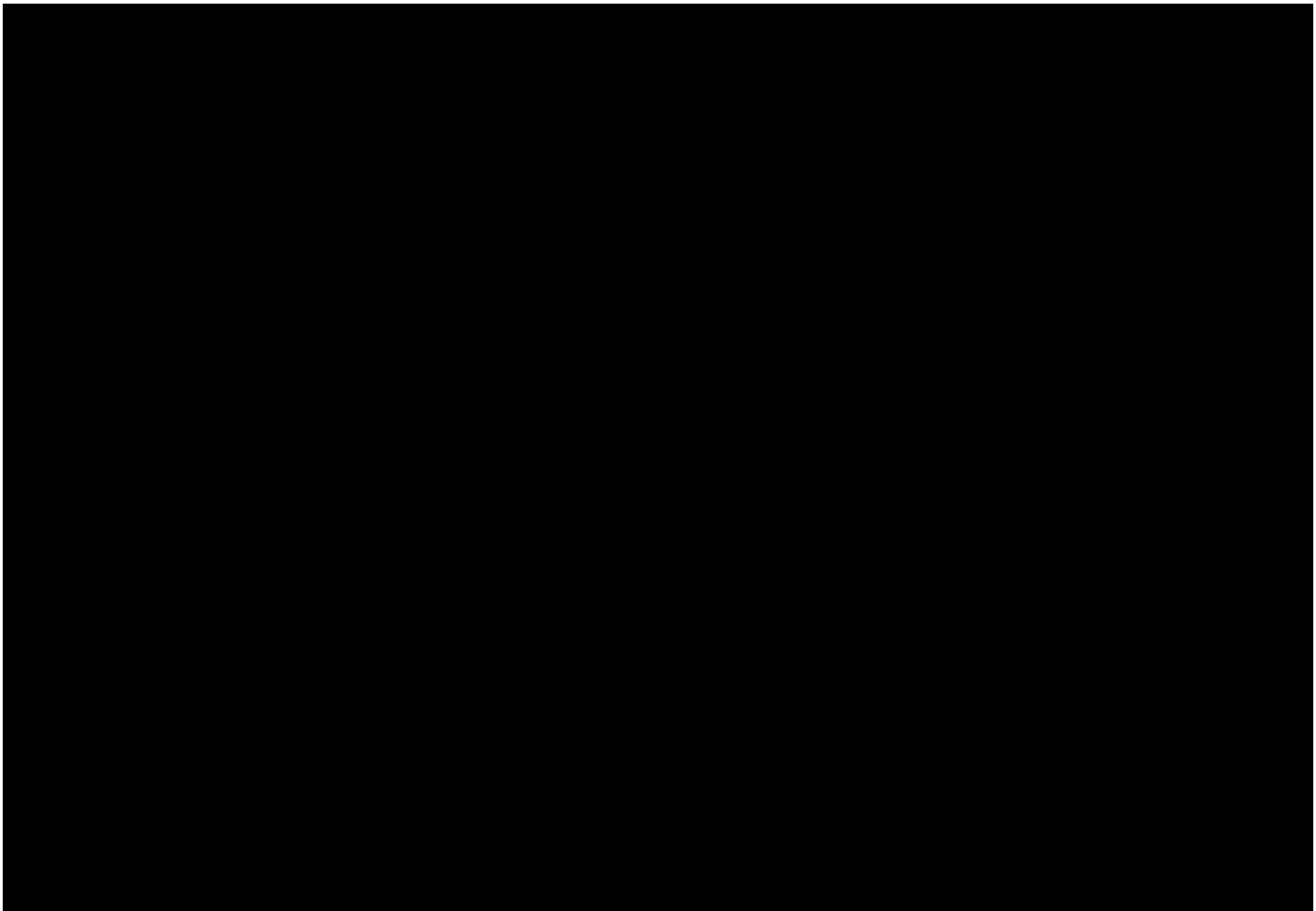


Figure 29. Screenshot of event from Group-IB Fraud Protection system

When the malware is detected on the user's device:

Once the trojan is successful, sensitive customer data typically falls into the hands of the threat actor, who then seeks to monetize this data. Often, the threat actor or their software will log into the stolen account. In such cases, a new device may appear when accessing the user account. Consequently, a rule has been developed to monitor accounts where a mobile banking trojan has been confirmed and to detect logins from new devices.

When new versions of a given Trojan family appear:

For cases where the malware has not yet been added to the malware database, a new rule has been developed that focuses on the trojan's specific characteristics. In particular, we check the characteristics of all software from a non-legitimate source for the ability to read SMS. These alerts are also transmitted to banks in the form of specific event types, increasing the likelihood of preventing fraudulent transactions by threats.

Figure 30. Screenshot of event from Group-IB Fraud Protection system

Conclusion

The case of Ajina highlights how quickly malware developers can appear, set up distributional chains and evaluate their tools. The direct communication between the threat actor and victim also makes Ajina.Banker an effective malware type in terms of keeping low detect rate on the first stages. While Group-IB does not have definitive data on the amount of money stolen by Ajina, the methods harnessed by malicious actors are cause for concern.

Recommendations

The security of mobile applications and operating systems is improving rapidly. However, it is premature to completely write-off Android banking Trojans entirely. In our experience, **banking Trojans are still highly active, with threat actors widely distributing modified Trojans based on publicly available source code**.

A good example of this trend is Ajina.Banker, which poses a significant threat not only to end-users of banking applications but also the entire banking sector itself.

For users

Below are some **basic recommendations on protecting mobile devices from banking Trojans like** Ajina.Banker.

- Always check for updates on your mobile device. Maintaining your mobile devices updated will make them less vulnerable to such threats.
- Avoid downloading applications from sources other than Google Play. However, it's important to note that even Google Play cannot guarantee complete security. Always check the permissions that an application requests before installing it.
- Do not click on links contained within suspicious SMS messages.

If your device has been infected, do the following:

1. Disable network access.
2. Freeze any bank accounts that may have been accessed from your device.
3. Contact experts to receive detailed information about the risks that the malware could pose to your device.

For organizations

The **Group-IB Threat Intelligence team will continue to track Ajina.Banker and update our database with new indicators related to this trojan**. Additionally, our Threat Intelligence team will notify customers when their application is targeted by Ajina.Banker, or any other Android malware we track.

For organizations that wish to protect their customers, implementing a solution that monitors user sessions – such as Group-IB Fraud Protection – can prevent malware operators from defrauding their clients and damaging their reputations.

Group-IB's Fraud Protection detects the latest fraud techniques, phishing preparation, and other types of attacks. The platform integrates data from Group-IB's attribution-based Threat Intelligence system. Exclusive information about cybercriminals, malware, adversary IP addresses, and compromised data (logins, passwords, bank cards) helps develop anti-fraud systems and cybersecurity teams, which allows the latter to identify intruders and their actions.

In this way, Fraud Protection "catches" banking Trojans and detects unauthorized remote access, web injections, cross-channel attacks, and personal data collection. Group-IB's solution implements patented algorithms that help detect infected devices without the client's involvement and without installing additional software.

Fraud Matrix

Tactic	Technique	Procedure
	Malware	Attackers use Ajina.Banker malware to gain access to user accounts
Resource development	Scam workers	Attacker has a network of affiliated employees acting with financial motivation, spreading Ajina.Banker that victimizes ordinary users
	Social Network Account	Attackers use Telegram accounts to spread Ajina.Banker
Trust abuse	Bluffing	Attackers promise easy earnings and lucrative offers to convince end users to install Ajina.Banker

	Fake application	Ajina.Banker mimics popular banking apps and payment systems

MITRE ATT&CK® Matrix

Tactic	Technique	Procedure
Initial Access (TA0027)	Phishing (T1660)	Ajina spreaded malicious applications via Telegram.
Persistence (TA0028)	Event Triggered Execution: Broadcast Receivers (T1624.001)	Ajina.Banker registers to receive system-wide broadcast intents such as receiving SMS message, device boot completion, network changes, battery charging state changes, locking and unlocking the screen.
Defense-evasion (TA0030)	Indicator Removal on Host: Uninstall Malicious Application (T1630.001)	Ajina.Banker can uninstall itself.
	Masquerading: Match Legitimate Name or Location (T1655.001)	Ajina.Banker mimics legitimate applications, trying to match their names and icons.
Credential-		

Indicators of compromise

md5	sha1	sh
4b0256974d7250e3ddc3d13d6c506f4f	cc6af149f1da110a570241dde6e3cfd0852cb0d8	a5

a61c0d53f624024d401c987032270e7d	2405e7b762e65011f7d107b2b2bcf069a18a5278	4
34a42857113ab2c856d533105494eb41	8a3c5e0c0438588640fbf4afe3a9c176a8204eec	1
bf20e58236c2020cd5eeceff0bf7974c	209aa1222bf59dd397aa38779cb0f48dcc961424	3
7f2e9aa66f802727a52eeec72ed2d458	84af2ce3a2e58cc8a70d4cc95916cbfe15f2169e	8
00241d7334d78340cd5eb721f40b8682	15de15a6f4af9c32cccbee23d99b80d33f3dcb50	2
48eb80adac9c2c9bd046c8f3da8c7f58	7f4b4f2b941e4472ece092a409099716aadcf16b	f4
bf1cb7d7c3bccaca23a652bd69feb539	5765162d8e5c5f903b4a297c5d2d2bbb5fedaa0f	3

Network indicators

MEA: +971 4 568 1785

info@group-ib.com