Craxs Rat, the master tool behind fake app scams and banking fraud | Group-IB Blog

Archived: 2026-05-05 02:29:24 UTC

Introduction

Since April 2023, a series of scams involving fake Android apps have targeted Singapore. These fake apps are banking trojans used to harvest victims' banking credentials and personal information, as well as to take control of their devices. In this specific case, threat actors have been observed using phishing websites as part of their campaign to deliver fake apps posing as known brands. Abusing popular brands and imitating Android trojans as legitimate-looking apps has been a notable trend in cybercriminal activity in recent years.

The Android fake apps were introduced as part of the scam scheme to lure victims with fraudulent advertisements of services or goods. The threat actors would then request the user to download fake Android apps in the pretense of making a payment or making an order.

Group-IB's High-Tech Crime Investigation team has been closely analyzing the early campaigns. The fake Androids apps were initially detected as **Spymax** by most antivirus products. However, after further analysis into the code, the apps were in fact a Remote Access Trojan (RAT) built using **Craxs Rat**.

Spymax is a mobile RAT built by threat actor "**✶ s c я є α м"** in 2019**.** The source code of Spymax was leaked in 2020 and was used by other actors to customise the software. The actor "**EVLF**" created his version of malware named **Craxs Rat** using the leaked code. As of April 2023, EVLF advertised new versions of Craxs Rat on his Telegram channel.

During the research into the Singapore phishing campaign involving Craxs Rat, Group-IB's High-Tech Crime Investigation team revealed that there were at least **10 different brands** abused by threat actors, ranging from **multiple online shopping platforms, an anti-scam center, pet grooming salons, dumpling shops and many others**. All these phishing campaigns required victims to download and install the fake Android app (which was built using Craxs Rat) onto their Android mobile device.

What is Craxs RAT malware?

Craxs Rat is a potent Remote Access Trojan (RAT) created by EVLF, a threat actor that enables cybercriminals to remotely control an infected device without the victim's knowledge. Unlike many conventional malware tools, the Craxs Rat malware is specifically designed to hijack Android devices, allowing attackers to extract sensitive data, monitor user activities, and even manipulate the device's settings remotely.

Originally emerging as a derivative of Spymax RATs, Craxs Rat has become notorious for its adaptability and strong control mechanisms. With its latest iteration, Craxs Rat v7, the malware now features amplified capabilities that make it even more difficult to detect and mitigate.

How Does Craxs RAT Work?

At its core, Craxs Rat operates by exploiting vulnerabilities in the Android mobile operating system. Cybercriminals typically deploy the malware via phishing campaigns, where victims are tricked into downloading fake applications from third-party websites or through deceptive emails. Once installed, the malware silently connects to a Command and Control (C&C) server, allowing attackers to:

- **Gain remote access**: Control the device in real-time.
- **Harvest sensitive data**: Steal banking credentials, personal information, and contact details.
- **Manipulate device functions**: Change system settings, take screenshots, and even record audio.
- **Persist on the device**: Implement stealthy persistence mechanisms to survive reboots and updates.

The sophistication of Craxs Rat malware is evident in its ability to encode network parameters and utilize encrypted communications, making it a formidable threat that continuously adapts to bypass traditional security measures.

Features of Craxs RAT

The robustness of Craxs Rat lies in its wide range of capabilities. Key features include:

- **Complete remote control**: Once the malware is installed, attackers can manipulate nearly every function on the victim’s device.
- **Extensive permission requests**: Fake apps built using Craxs Rat often require access to SMS, call logs, contacts, cameras, microphones, geo-location, and more. These permissions are critical for executing fraudulent activities.
- **Command and control connectivity**: The malware encodes its C&C server details (often using base64 encoding) to evade detection and ensure a secure channel for remote commands.
- **Customizable payloads**: Using a free or paid version of the Craxs Rat builder, cybercriminals can tailor the malware’s functionality. This flexibility has led to the emergence of multiple variants, including the highly publicized Craxs Rat v7.
- **Multi-language support**: The malware interface often supports multiple languages—such as English, Arabic, Turkish, and Simplified Chinese—to target victims across different regions.

Key discoveries in the blog

- Group-IB Investigation team analyzed **the fake scam campaign targeting Singapore** including the threat actor’s infrastructure, and the fake apps used in the scam scheme.
- The scam campaign targeting Singapore used **a fake app built by Craxs Rat** and started no later than April 2023.
- Phishing websites used in the Singapore Craxs Rat campaign were probably controlled by **Chinese speaking threat actors**.
- Craxs Rat has been developed by the threat actor **EVLF** and sold on his Telegram Channel. We did the threat profiling of threat actor EVLF, and revealed in-depth information about the Craxs Rat tool.

- **EVLF's Telegram channel** was bought over on 5 September 2023. We assume that the actors behind the Singapore attacks could be related to it.
- There is a new channel created by EVLF where he released the latest version of Craxs Rat 7.5 on 17 April 2024.
- Our team constantly tracked and noted the latest updates on Craxs Rat, which have been detailed in the blog.

Who may find this article interesting:

- Cybersecurity analysts and corporate security teams
- Malware analysts
- Threat Intelligence specialists
- Cyber investigators
- Computer Emergency Response Teams
- Law enforcement investigators
- Cyber Police Forces

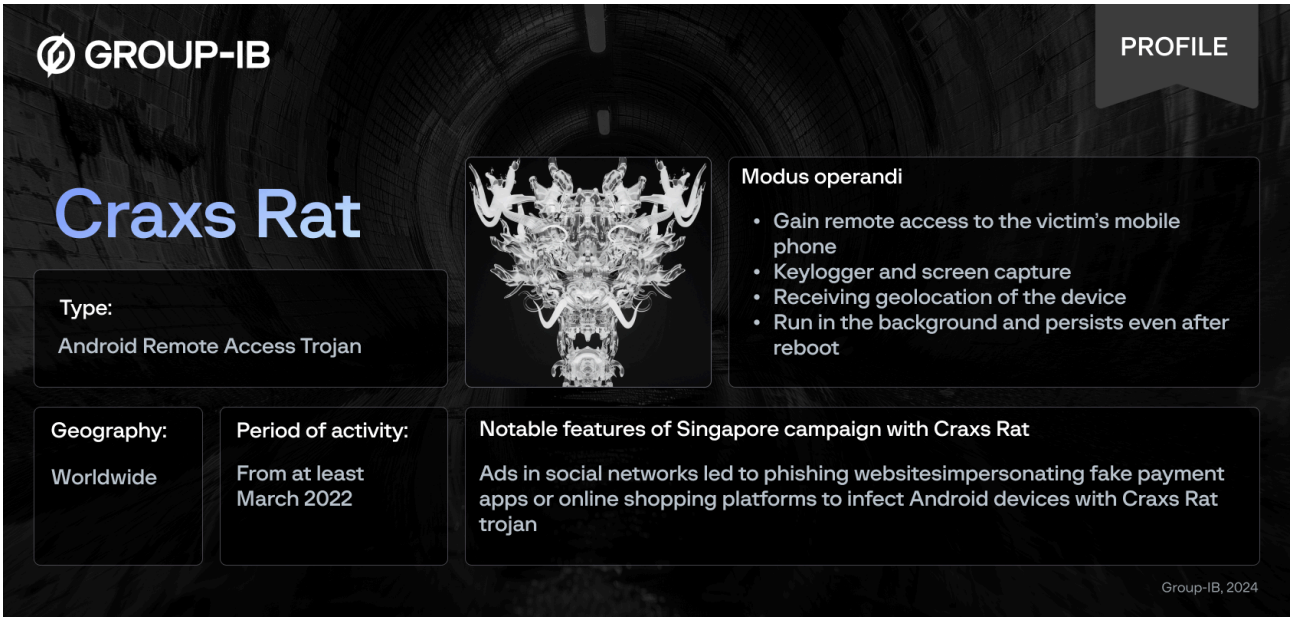

Figure 1. Craxs Rat profile made by Group-IB Threat Intelligence

What malware was used in the phishing campaign targeting Singapore?

The Singapore campaign with Android trojans garnered increasing attention in May 2023.

The fake applications were detected by antivirus engines as "SpyMax." Group-IB specialists found that the code of these apps was different from the known "SpyMax" samples. So, we dived deeper into the evolution of the "SpyMax" malware and discovered the latest popular version of it, named "**Craxs Rat.**" We further analyzed one of the fake apps from the scam campaign and compared its features with an app built by Craxs Rat free builder (hereinafter – replicated fake app).

Here are some of the comparisons of the results:

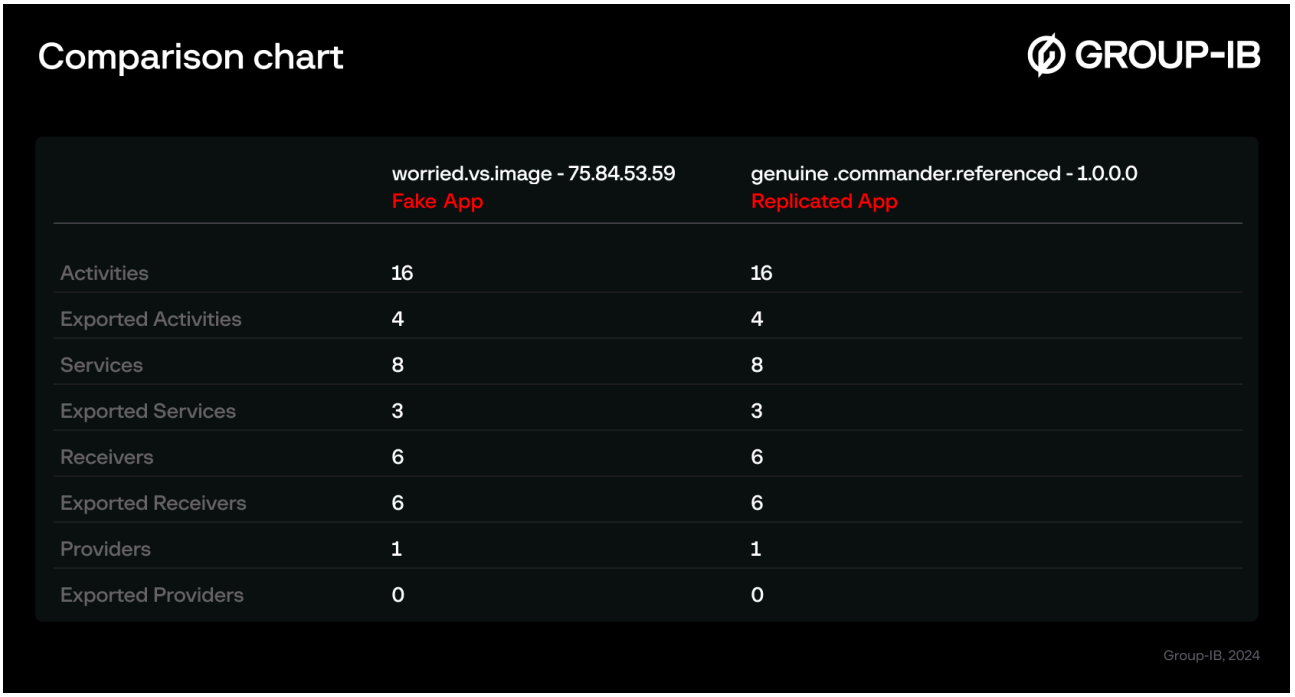

Figure 2. Comparing components of fake app and replicated app built using Craxs Rat builder.

As can be seen from the table above, the number of exported functions and components match.

Using the free version of Craxs App builder, we can see the minimum list of permissions required:

- Send SMS
- Record Calls
- Change Wallpaper
- Read SMS
- Read call logs, contacts and accounts
- Access to camera, microphone
- Access to geo-location
- Permission to make calls.

More extensive list of permissions is expected for the paid version buyers.

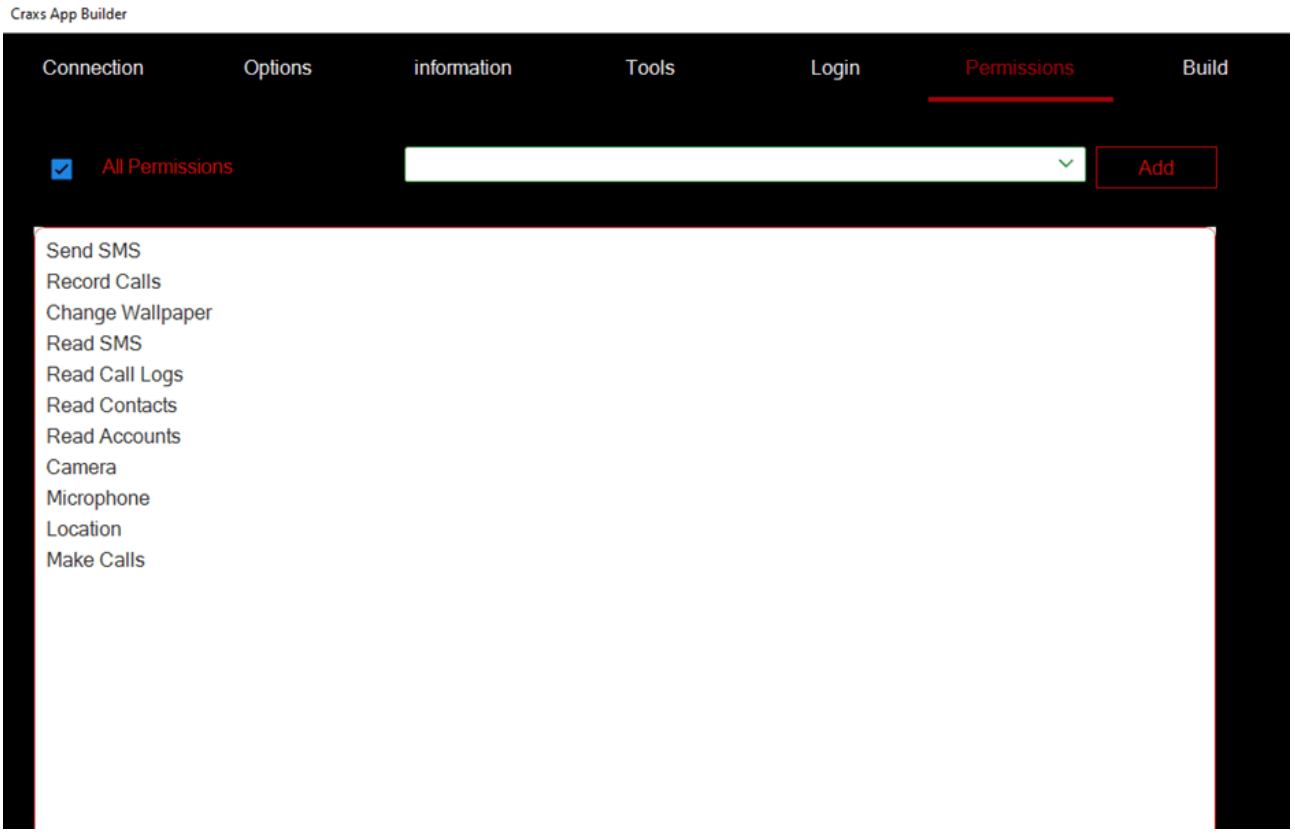

Figure 3. List of permissions for selection in Crax App builder

The permission list from the analyzed fake app includes the ones listed above.

The comparison of the AndroidManifest.xml is presented below. As we see there are complete similarities between the permissions of both fake app and a replicated app for access to SMS, camera, contact list, recording audio, call log, access to files, etc.

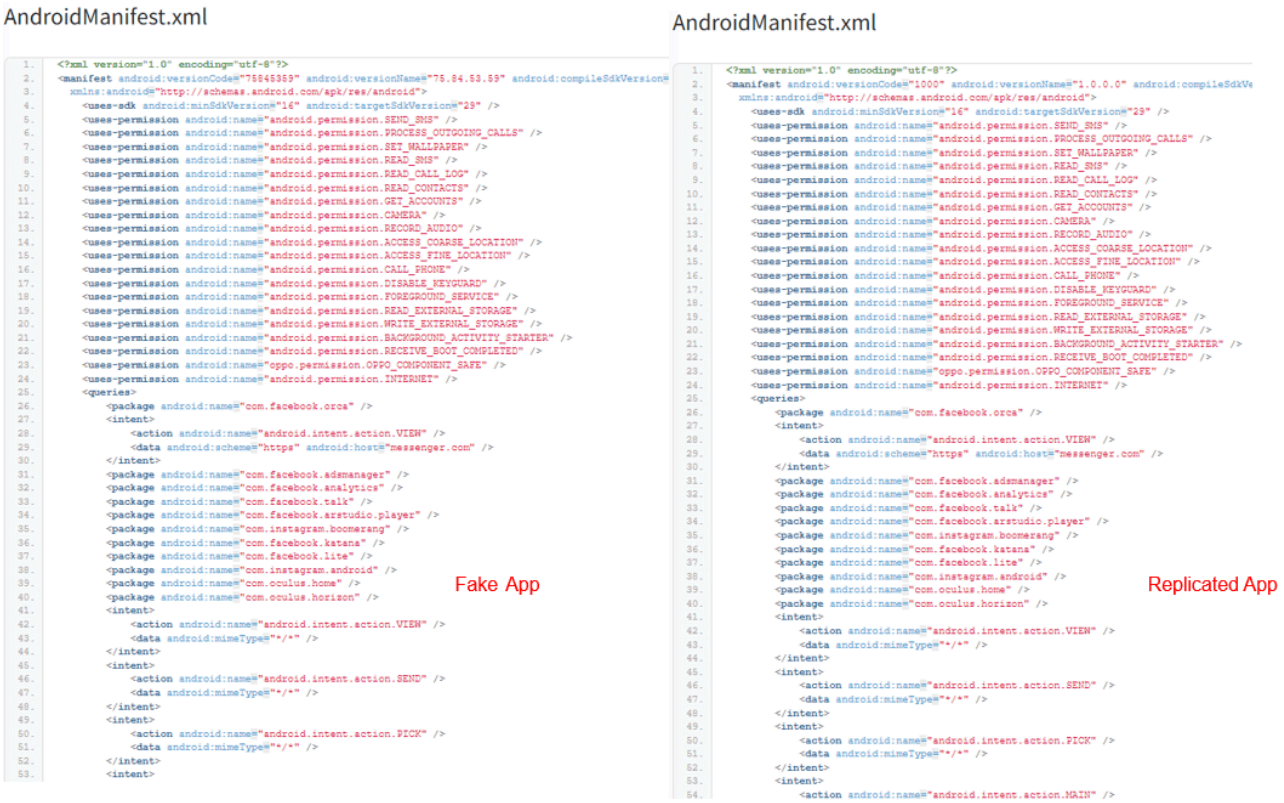

Figure 4. Comparing AndroidManifest.xml of fake app and a replicated app built using Craxs Rat builder.

Below showcases the similarities in the AlertDialog Message with languages in English, Arabic, Turkish and Simplified Chinese for both the fake app and replicated app.

Figure 5. Comparing source code of fake app and a replicated app built using Craxs Rat builder.

To get the Accessibility Service permissions which allows remote control functions, the following window appears on the victims' device:

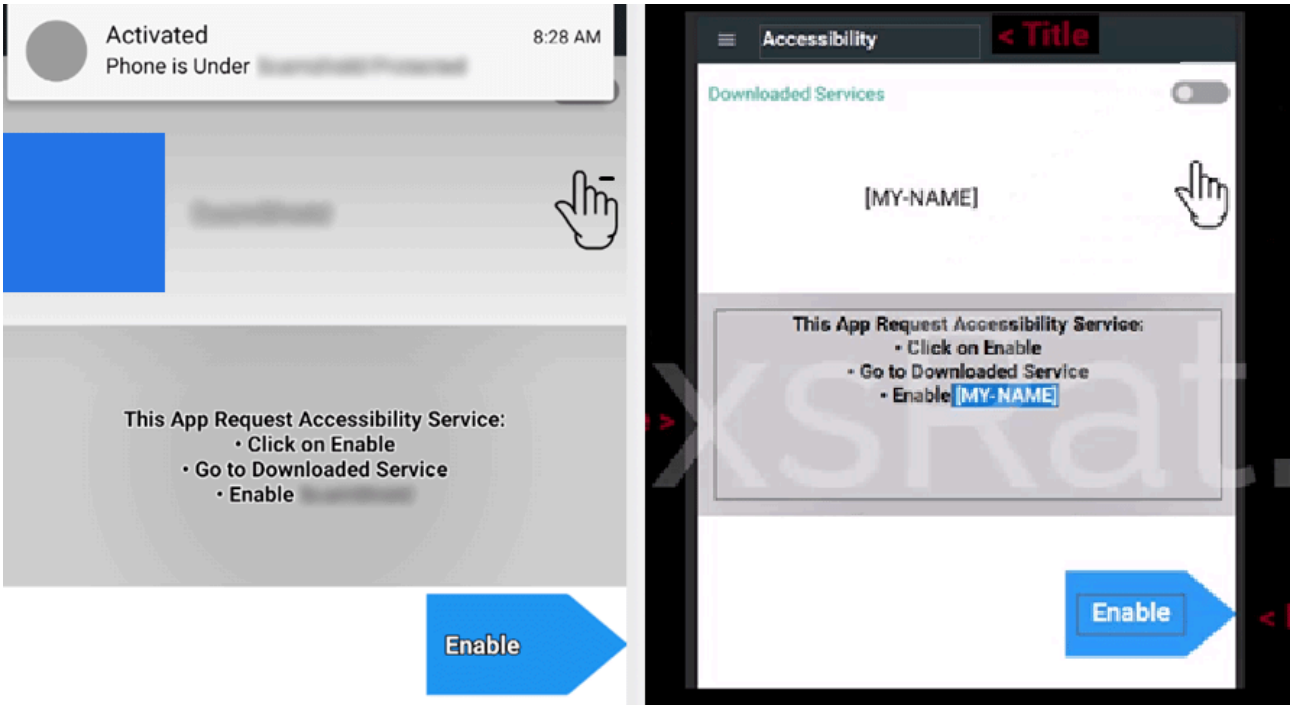

Figure 6. Comparison of the template design in a fake app and a replicated app using Craxs Rat builder

In terms of network indicators, a Craxs Rat sample contains a link to a website whose content it displays to a victim, and an encoded IP address of the Command and Control server (hereinafter – C2 server) controlled by a threat actor.

In both fake app and replicated app, the C2 IP address is base64 encoded.

```
/* renamed from: edgar.pdt.
public class C71 extends Service {
    public static String b = d.n("VHhUeFQ=");
    public static String c = "C";
    public static String d = "
    public static String e = "M:
    public static String f = "    dMQ==";
    public static List<e> g;
```

Fake App

```
public class uvryttllnbcfhugulhcudmyonjglerlh
    public static String b = d.n("VHhUeFQ=");
    public static String c = "T";
    public static String d = "
    public static String e = "M
    public static String f = "    MQ==";
```

Replicated App

The parameter “b” in a replicated app was changed manually to a value from a fake app. The parameter “d” contains the name of the app. The parameter “e” contains the IP address of the C2 server while the parameter “f” reflects the port number on the C2 server. We customised all these parameters in the replicated app through Craxs Rat builder to showcase the similarity of C2 configuration format.

While analyzing the network infrastructure of the C2 IP addresses obtained from malware samples used in a Singapore scam campaign, we discovered that all of the C2 IP addresses were hosting a Windows Server 2019, whereby the language of the system was in Chinese.

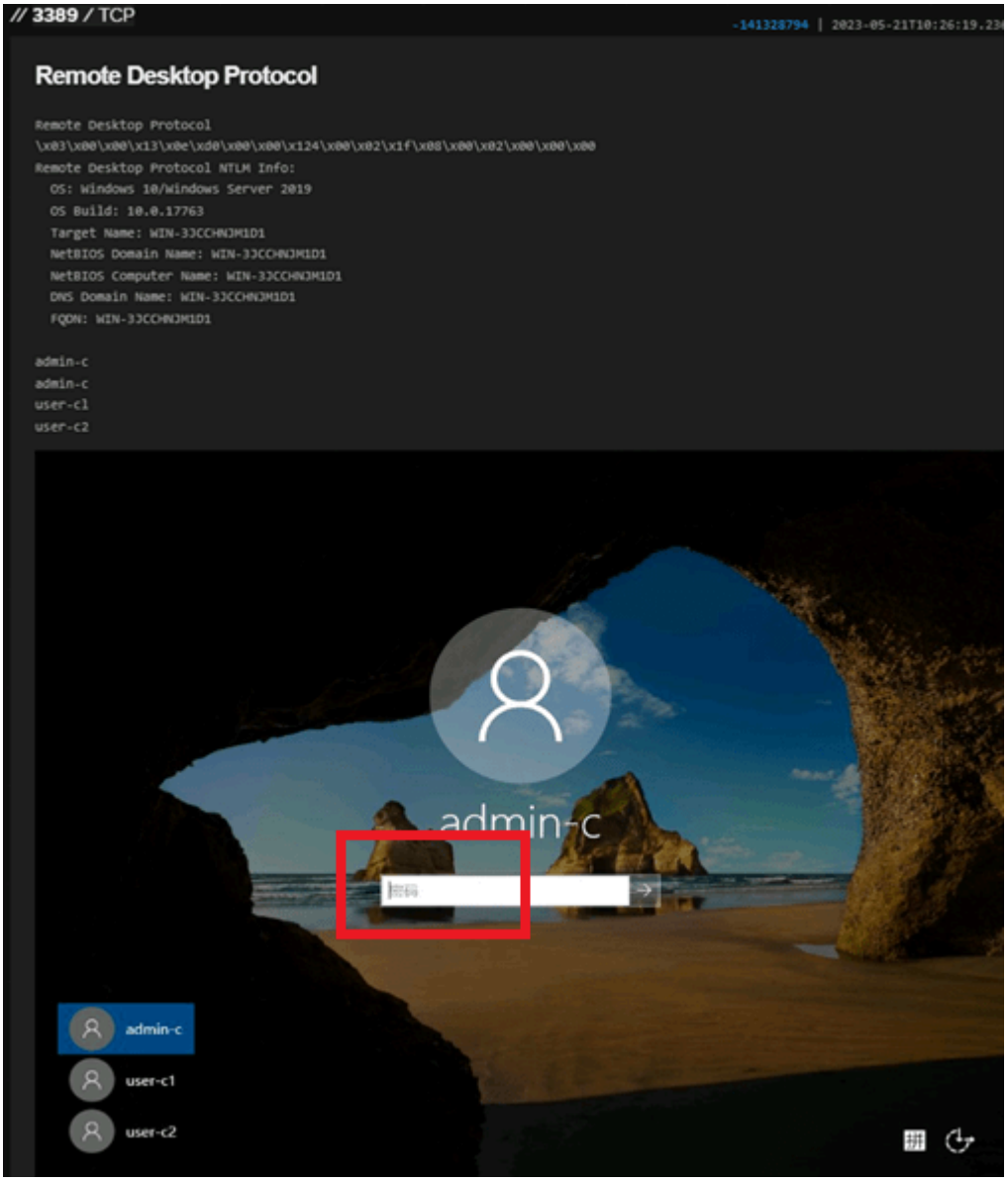

Figure 8. RDP connection to one of the C2 IP addresses showing Windows Server login where password field is in Chinese

A panoramic view of the correlation between the C2 IP addresses in the Singapore scam campaign is shown through Group-IB's patented Graph technology.

Figure 9. C2 IP addresses sharing the same settings with other IP addresses belonging to the threat actor’s network infrastructure

So, our comparison of the samples used in the Singapore scam campaign and Craxs Rat app showed similarities. **The analysis of its C2 infrastructure brought us to the conclusion that the Chinese speaking threat actors could be behind this campaign.**

Phishing infrastructure in the attacks

Analysing dozens of Craxs Rat samples used in a Singapore scam campaign, we discovered a lot of phishing pages impersonating different brands including some widely-known ones. The websites impersonated were online shopping platforms, anti-scam center, pet grooming salon, dumpling shop and many others. Example of one of the phishing pages positioned as 1st Mall is presented below:

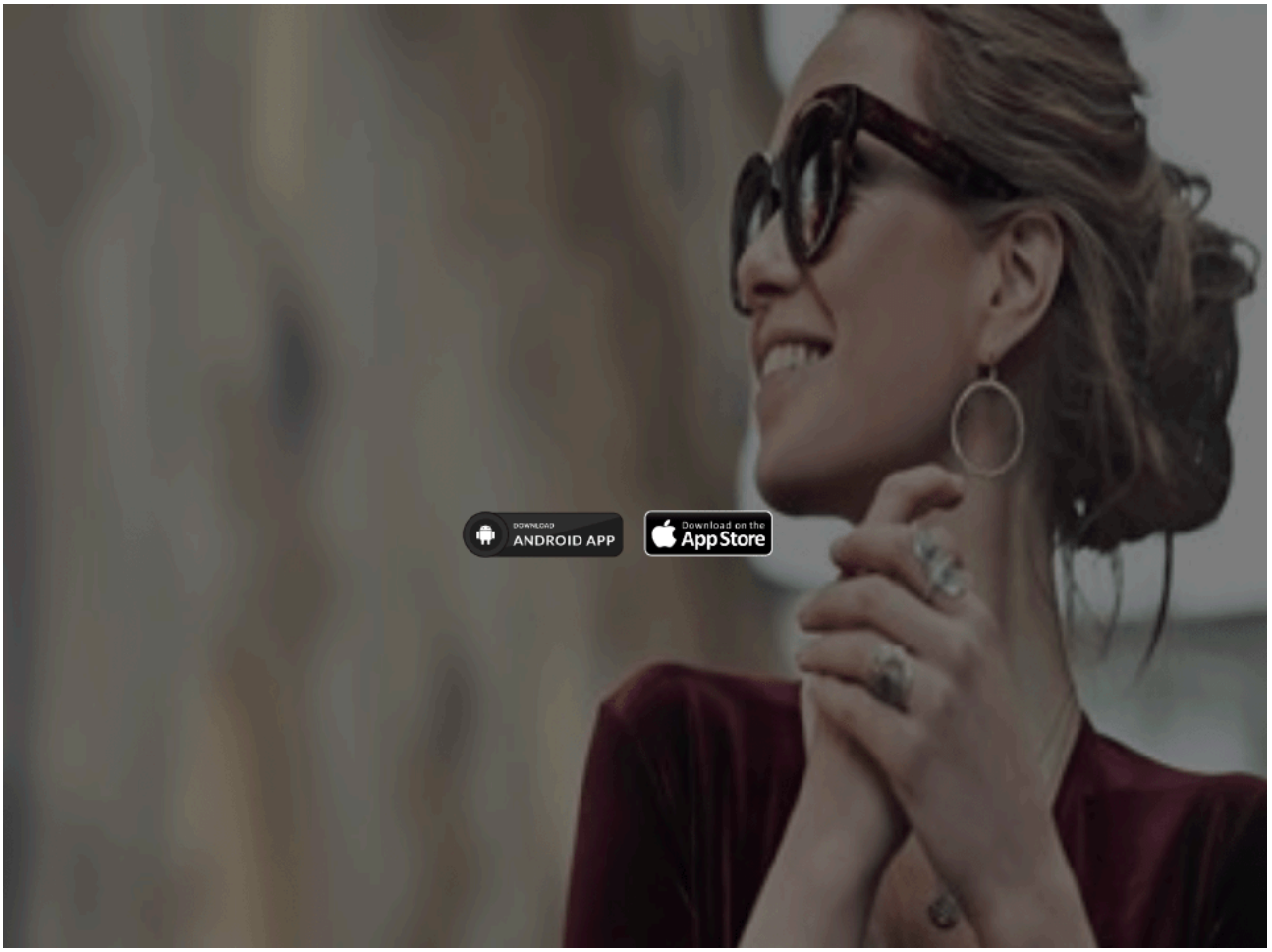

Figure 10. Phishing webpage positioned as 1st Mall website

The brands include the following but are not limited to:

- 1st Mall
- Anti-Scam center
- E2 Mall
- Shopnow
- Choose
- SG-Furniture
- Mall 1st
- Grab & Go
- 第一商城
- etc.

Examples of the samples whose names represent the impersonated brand are presented below:

Scanned	Detections	Type	Name
2023-06-01	26 / 62	Android	1st%20Mall%20v7.2.apk
2023-05-30	22 / 64	Android	1st%20Mall%20v7.1.apk
2023-05-28	26 / 64	Android	tmpW9onfi.tmp
2023-05-04	17 / 63	Android	tmpAsRpPn.tmp
2023-05-22	25 / 63	Android	Scamshield (1).apk
2023-05-28	23 / 64	Android	1st%20Mall%20v7.0.apk
2023-05-18	16 / 64	Android	Scamshield (2).apk
2023-05-27	24 / 63	Android	1st%20Mall%20v6.0.apk
2023-06-25	25 / 64	Android	1st Mall v8.5.apk
2023-05-29	24 / 64	Android	1st Mall v4.0.apk
2023-05-31	25 / 64	Android	1st%20Mall%20v7.6.apk
2023-05-27	24 / 64	Android	[redacted]20v6.2.apk
2023-05-29	26 / 64	Android	[redacted]apk
2023-05-28	24 / 64	Android	1st%20Mall%20v6.2.apk
2023-05-29	23 / 63	Android	1st%20Mall%20v4.6%20(3).apk
2023-05-08	21 / 63	Android	E2 Mall v6.4.apk
2023-05-05	15 / 63	Android	[redacted] v5.1.apk
2023-05-30	23 / 63	Android	1st Mall v7.8.apk
2023-05-29	24 / 63	Android	ScamShield (9).apk
2023-06-08	27 / 64	Android	1st Mall v8.0.apk
2023-05-29	25 / 64	Android	[redacted] (1).apk

Figure 11. Screenshot showing list of APK files communicating with fake app's C2 IP addresses

In one phishing page, we discovered the following languages supported: "China Hong Kong", "China", "English", "French", "Thai" and "Laos". It can be assumed that these are the languages of the target victims.

Figure 12. Languages supported by the phishing online shopping platform

The earliest web pages which we link to the Singapore Craxs Rat campaigns were discovered in April 2023, impersonating an application used to track phone location just by it’s phone number. The phishing service used the names **Backfinder** and **Backtracker.**

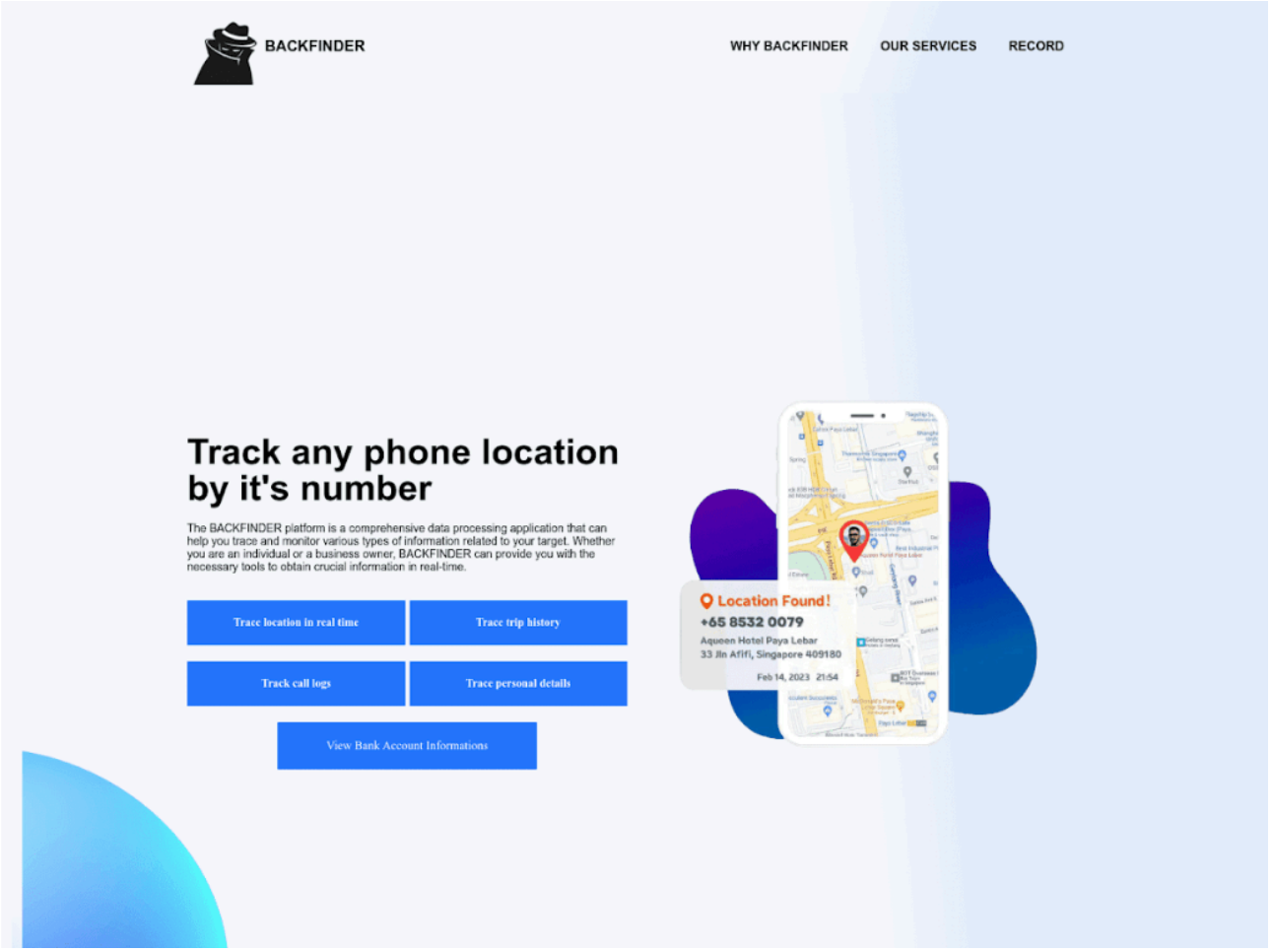

Figure 13. A screenshot of a website impersonating as Backfinder

Our experts also discovered that the admin panel behind the phishing websites is CRMEB – which is popular among the Chinese-speaking community of developers.

Figure 14. Example of CRMEB admin login page for a phishing website

So, based on the presented analysis, we concluded that phishing websites were administered via CRMEB admin panel by the threat actors who are likely to be Chinese-speaking. The first traces of the phishing infrastructure we discover to be registered not later than April 2023.

From Spymax to Craxs Rat

To clarify the roots of the Craxs Rat used in the Singapore campaigns we researched the malware evolution by analysing Dark Web forums.

We discovered that Spymax, also known as **Spy max or SpyNote,** was first developed by a threat actor nicknamed ✶ s c я є α м in 2019 and was advertised on a popular Syrian forum, which had been shut down already. Since then, the activity of Spymax has been ongoing especially with the source code of Spymax being published online in 2020. Many threat actors have taken the source code of Spymax and customised it to release new versions or to create their own RAT.

Amongst them is a threat actor named **EVLF**, who took the source code of Spymax and released his own updated version. Meanwhile, he was also behind new Remote Access tools such as Cypher Rat and Craxs Rat. The timeline below shows how the events unfolded from the creation of Spymax to the birth of Craxs Rat.

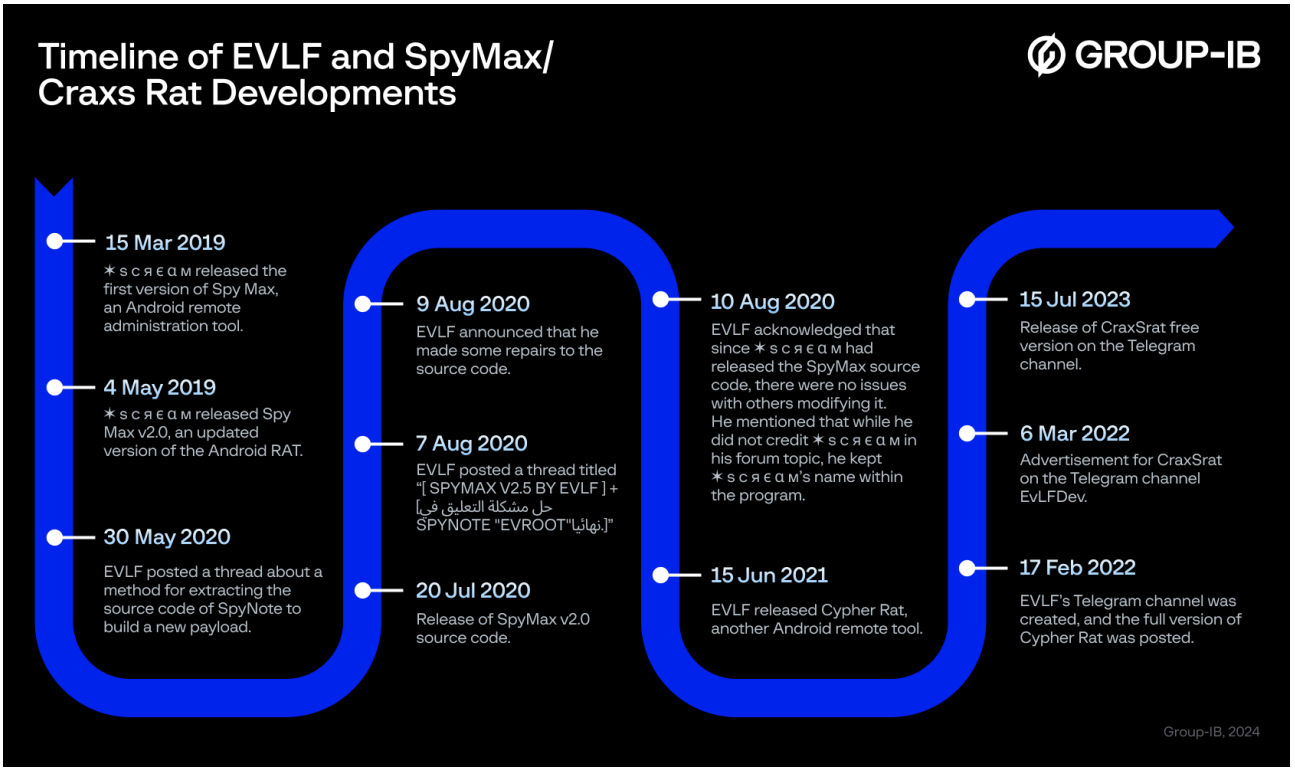

Figure 15. Timeline of EVLF and SpyMax / Craxs Rat development

Below you can find one of the EVLF's post with comments about his malware built on the source code of Spymax and SpyNote.

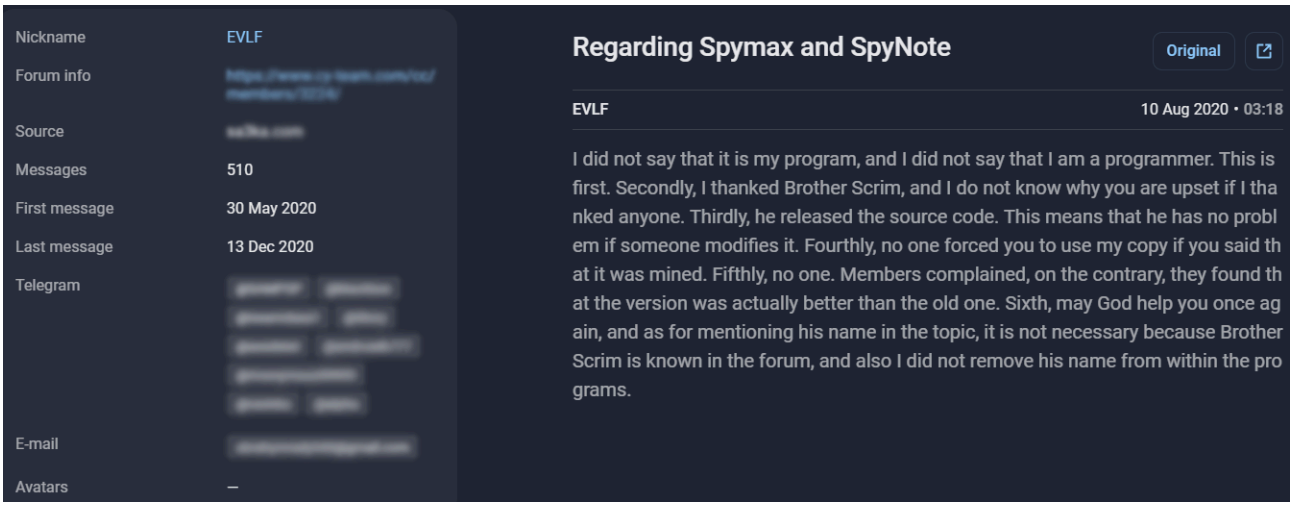

Figure 16. Screenshot from Group-IB Threat Intelligence Platform about EVLF clarifying about the source code for Spymax. Original post was written in Arabic.

After the forum shutdown, new advertisement posts from EVLF appeared on his Telegram channel. Since March 2022, this account was the main source of updates about Craxs Rat.

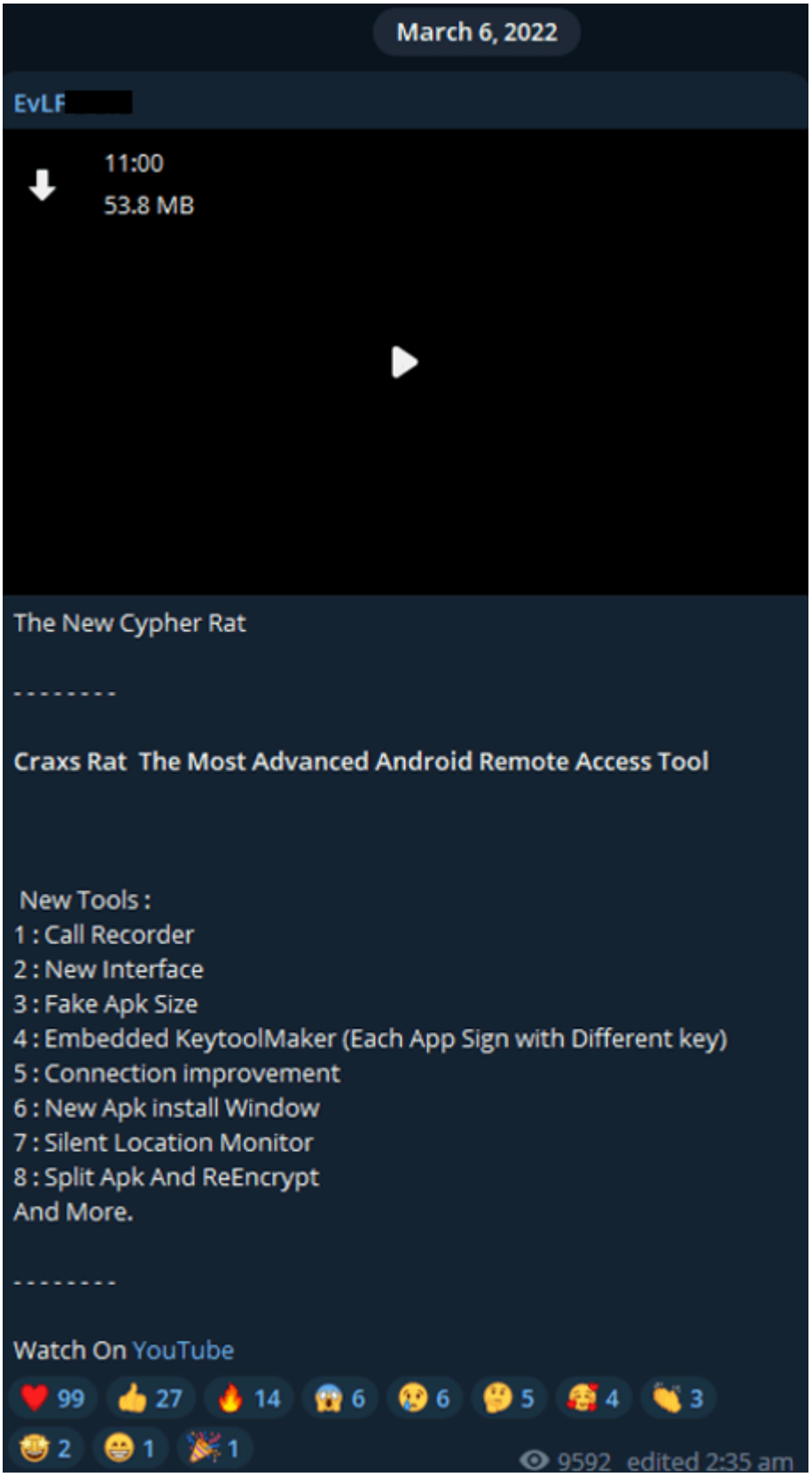

Figure 17. Screenshot from EVLF's Telegram channel showing the first message about Craxs Rat.

Group-IB's team have analyzed the posts more precisely to get more personal insights about the author.

One of the posts lets us figure his geolocation, which could be Syria:

Through the videos that he posted on his Telegram channel, there was other evidence indicating that EVLF could be from Syria. The geographic location of Mezze, a municipality in Syria, is shown on a mobile phone in one of his video.

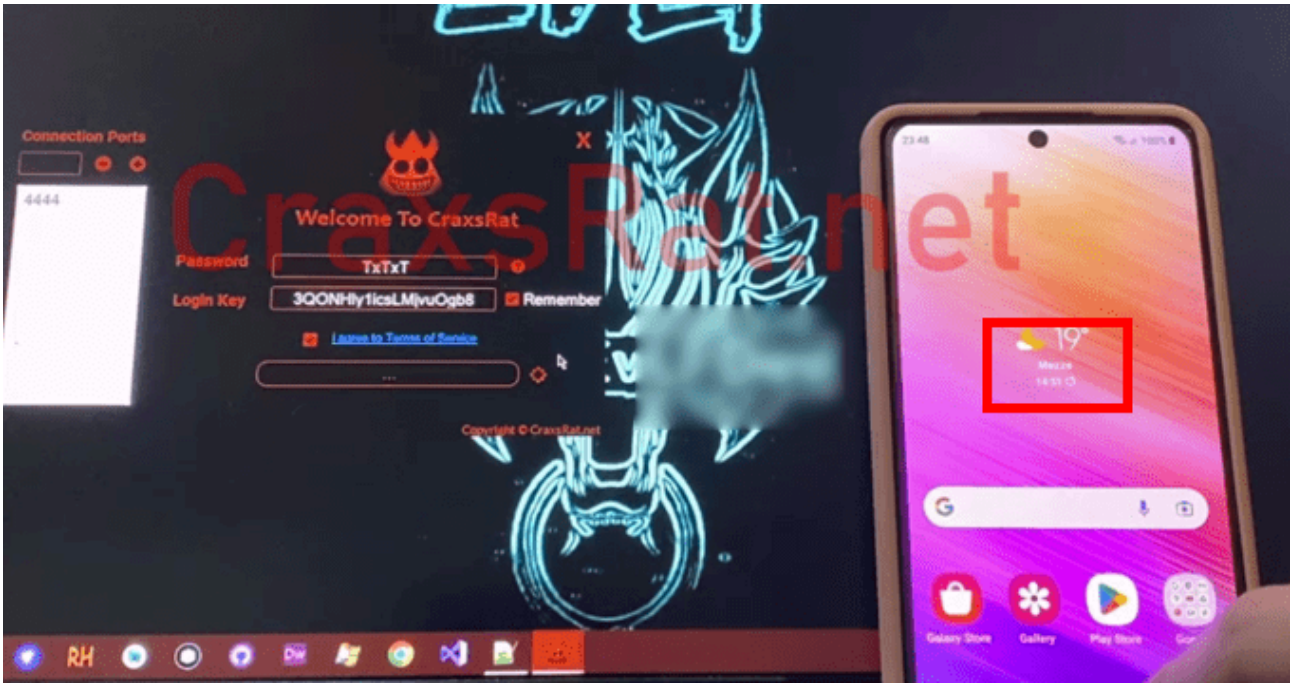

Figure 19. Screenshot of video in EVLF's Telegram channel showing geolocation Mezze

On 23 August 2023 the message was posted by EVLF about stopping his activity:

Figure 20. Screenshot of EVLF's message on stopping his activity

One of the deleted messages saved by our Threat Intelligence Platform:

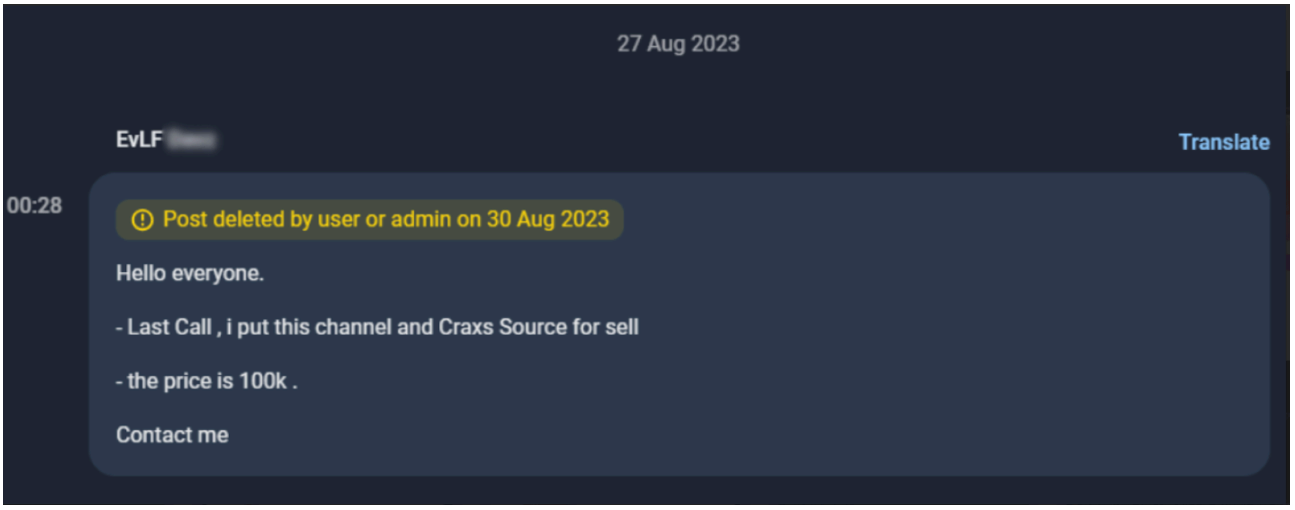

Figure 21. Screenshot from Group-IB Threat Intelligence Platform showing EVLF's deleted message about selling the channel and Craxs Rat source code

On 5 September 2023, a message was posted on EVLF's Telegram channel that the channel had been bought over.

Figure 22. Screenshot from EVLF's Telegram channel announcing that the channel has been bought over

The Telegram username of EVLF, which was used as a contact for buying, was changed to a new contact information. After the buy-over, Telegram messages on the channel have been incorporating Chinese language and have also published video tutorials in Simplified Chinese.

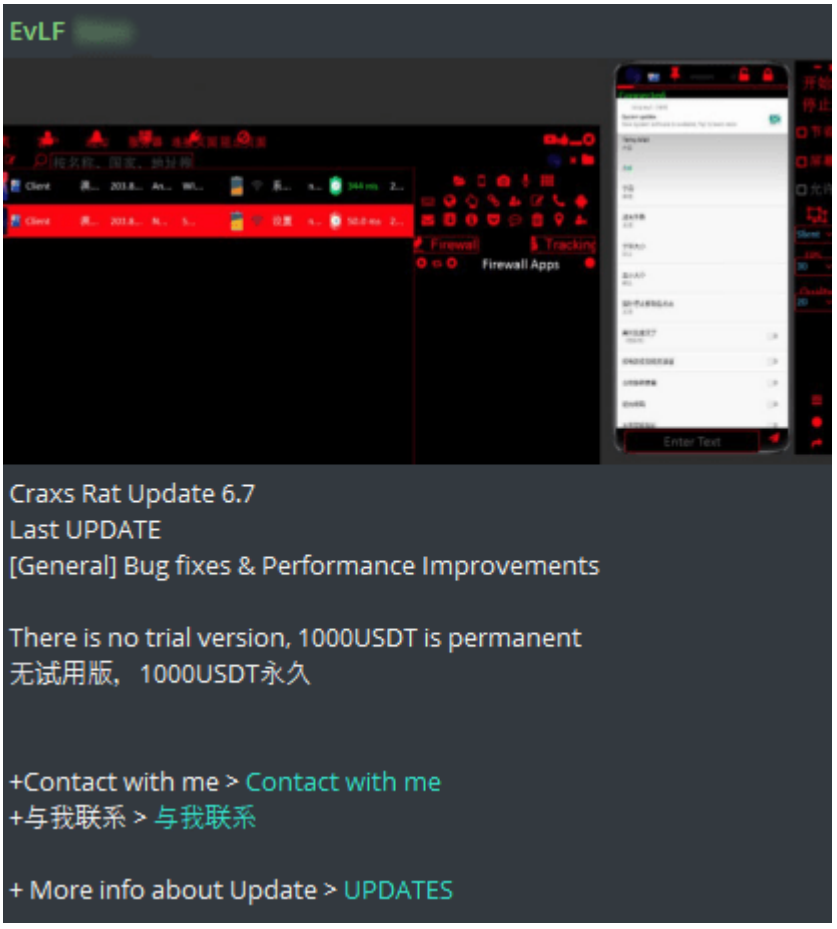

Figure 23. Screenshot from EVLF's Telegram channel with messages containing Simplified Chinese characters

The advertisement of new capabilities for the Craxs Rat malware started to be duplicated in Chinese as well:

- New interface and logo
- New update for MIUI + ColorOS phones. Enabling background permissions is easier than ever
- Automatic screen unlock: needs to be detected once
- Monitor selected applications
- Send notification to mobile phone
- Cut off internet access for any app
- Helps connections last longer

Common Functions:

- Manager: Files, SMS, Contacts, Calis, Accounts, Apps, Permission
- Monitor: screen controls, camera, microphone, keylogger, location, web browser, call recorder, auto-clicker, screen reader

- Admin: Request admin rights, lock screen, wipe data keylogging
- Tools: Call Number, Download Apk, Show Message, Clipboard, Open Link, Shell Command
- Extras: notification list, social media hunter, phone messages.

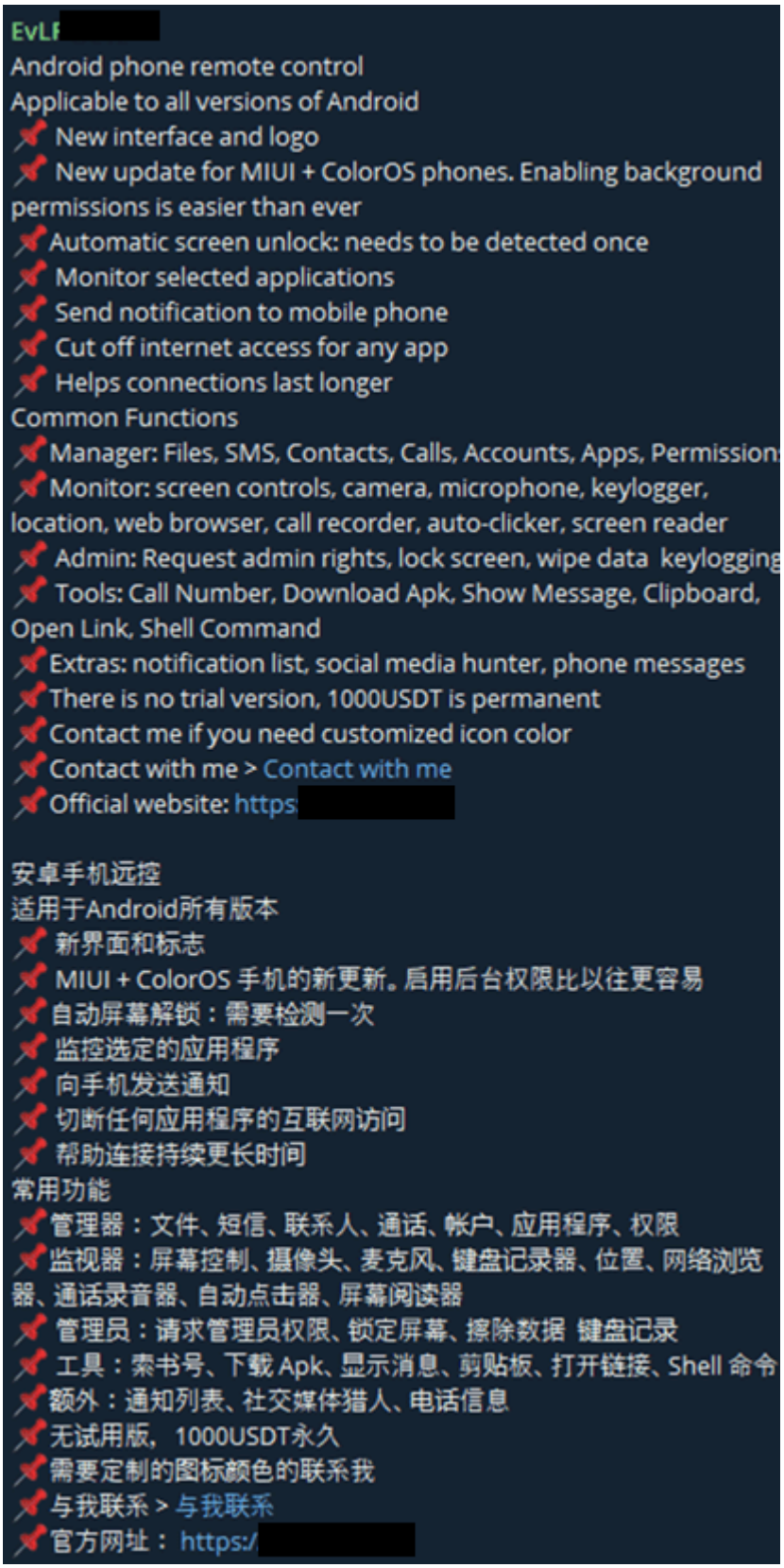

Figure 24. Screenshot from EVLF's Telegram channel with messages containing Simplified Chinese characters explaining the features.

We suppose that the new buyer is from Asia and that the group targeting Singapore could be potentially behind the buy-over.

On 30 November 2023, the attempt to sell source code was made by a new owner of the channel:

Figure 25. Screenshot from EVLF's Telegram channel about selling of Craxs Rat source code

However, based on the contact details in the latest posts, the owner wasn't changed.

Since then there were no updates of Craxs Rat malware in this channel, until April 2024. The latest version of Craxs Rat published on the Telegram Channel on 7 April 2024 is v7.4. However, the demonstration video stated 18 January 2024 as the date of recording:

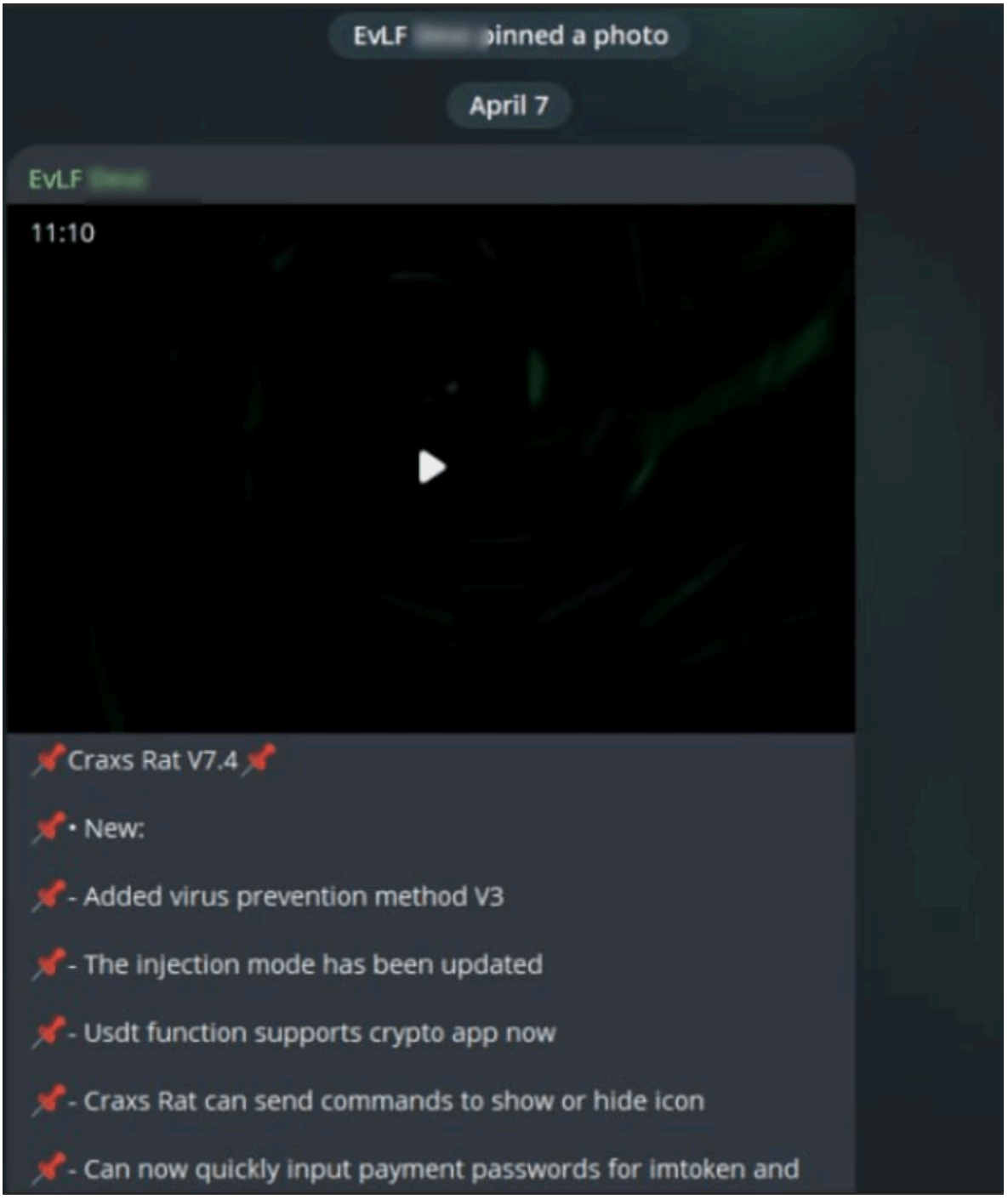

Figure 26. Screenshot from EVLF's Telegram channel about Craxs Rat v7.4

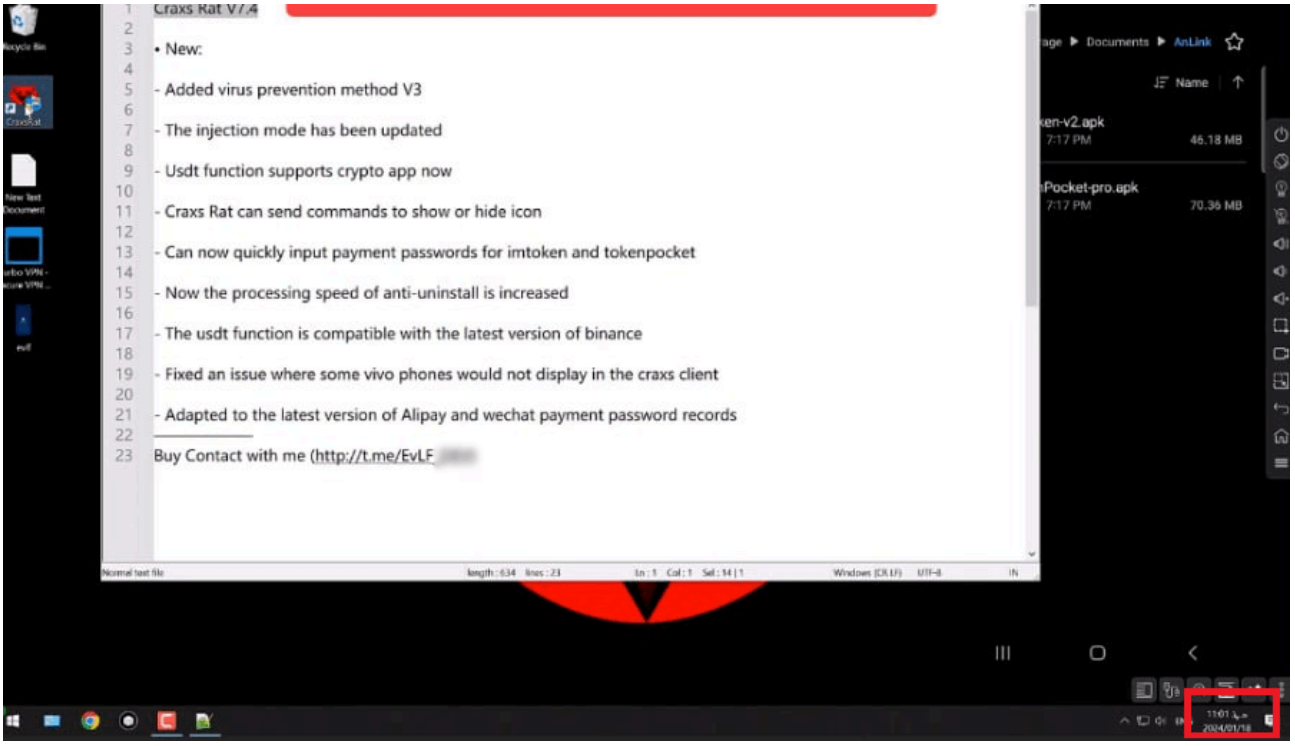

Figure 27. Craxs Rat v7.4 demonstration video on 18 January 2024

Note: The above message has since been deleted from the channel.

So, since 5 September 2023, the EVLF channel was controlled by a new owner, who is presumably a Chinese speaking one.

Making a reappearance promptly: ELVF's new Telegram Channel

When the original EVLF's Telegram channel was bought over on 5 September 2023, another Telegram channel was created by EVLF on the same day.

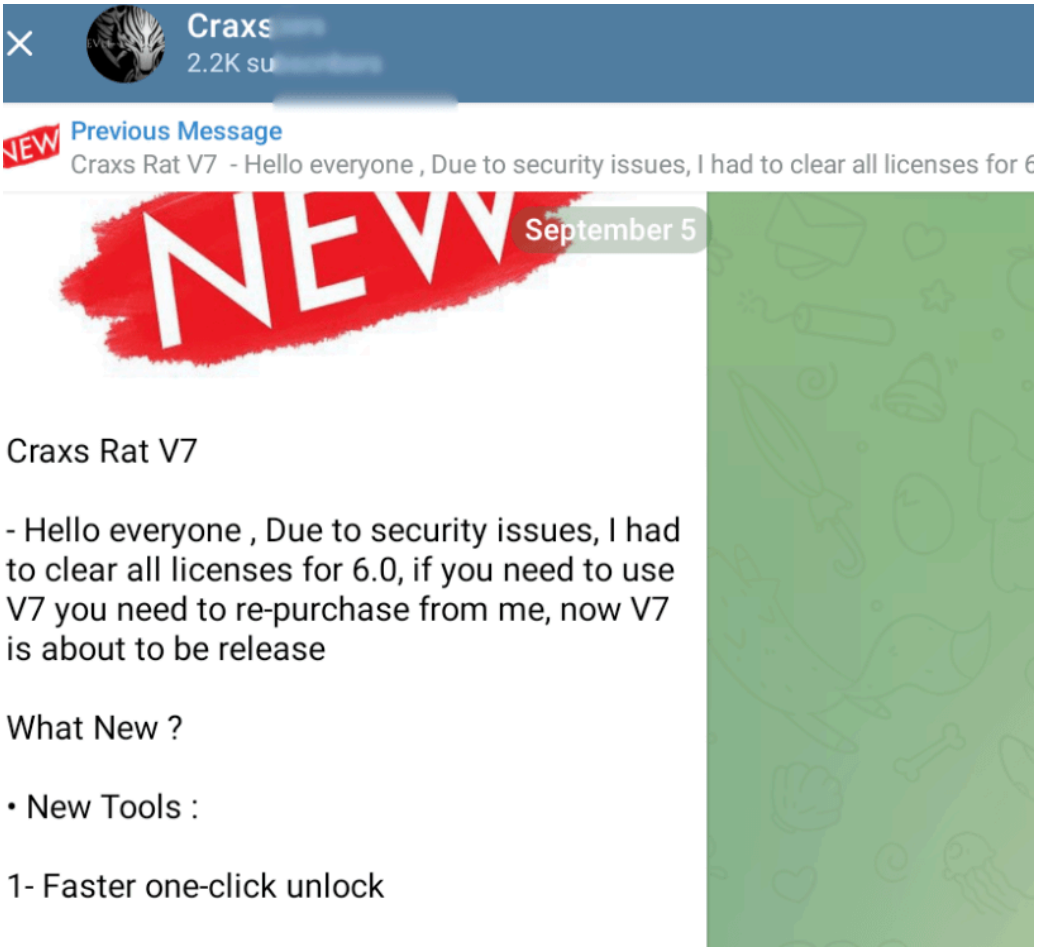

Figure 28. New EVLF's Telegram channel

The contact information written on the profile was the same Telegram username belonging to the original EVLF. Telegram ID of the channel's admin matches with the ID of the original EVLF account. It is not clear if EVLF's personal Telegram account was also sold along with the channel.

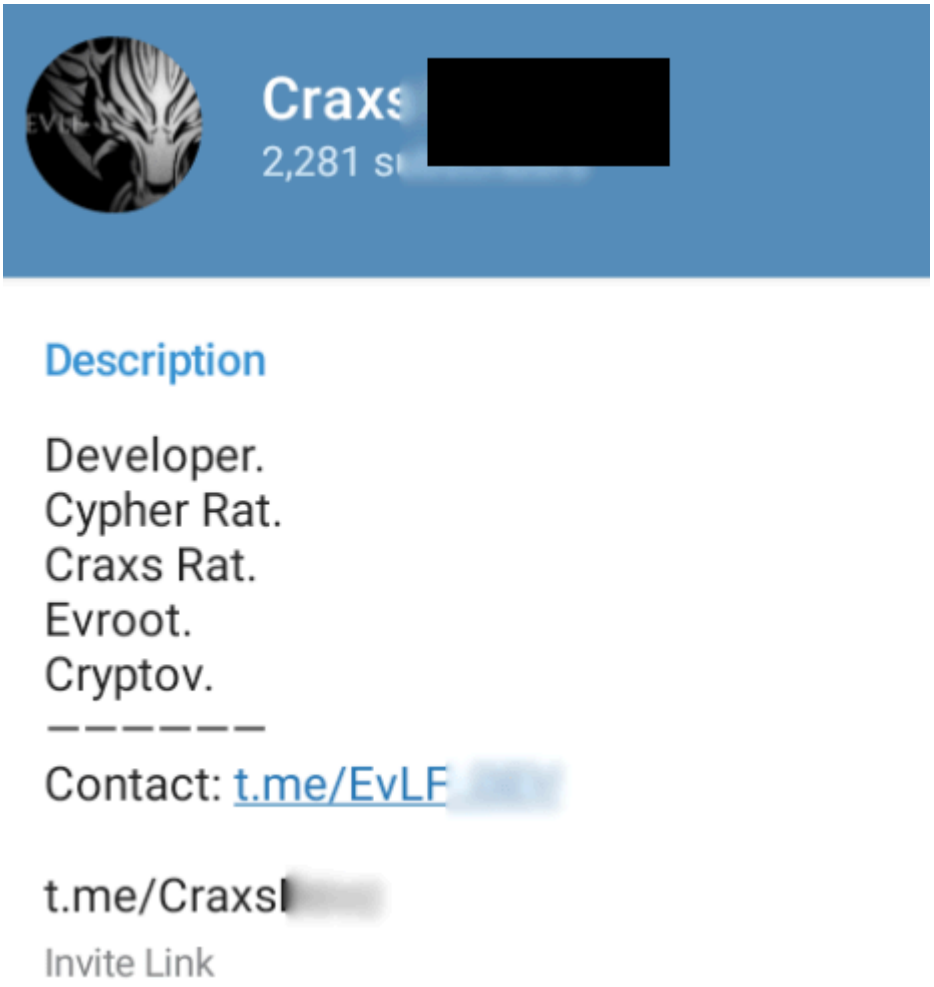

Figure 29. New EVLF's Telegram channel

In his messages in the new Telegram channel, the actor said that he was the real author of Craxs Rat.

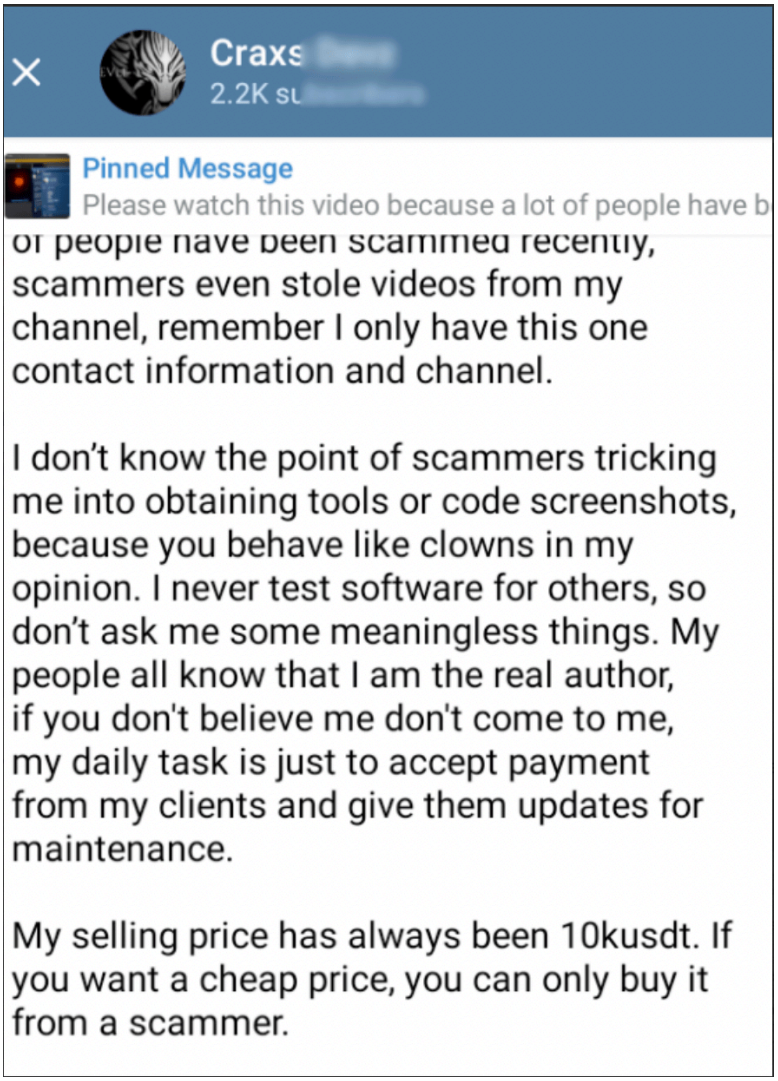

Figure 30. Screenshot from EVLF's new Telegram channel about him being the real author

Version 7.4 of Craxs Rat was published in this channel on 18 January 2024 which matches with a new date of recording.

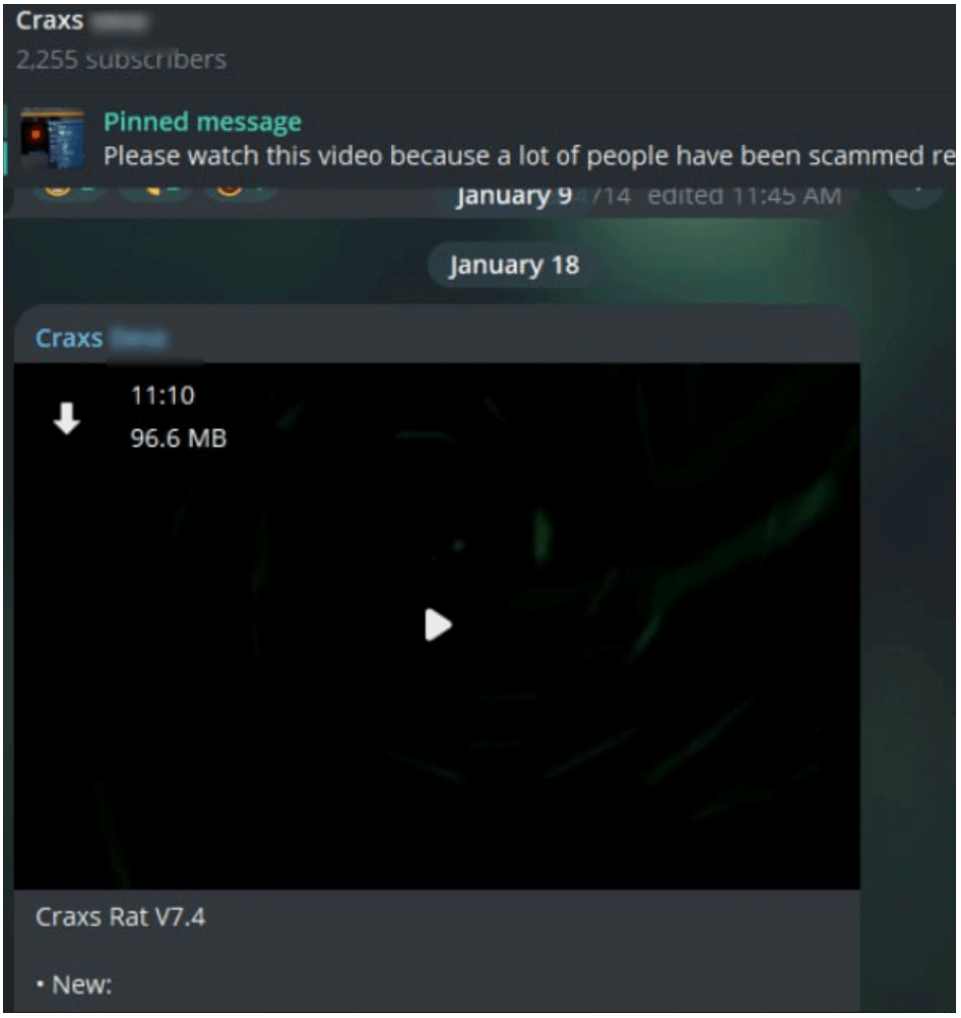

Figure 31. Screenshot on EVLF's new Telegram channel about v7.4 published on 18 January 2024

On 01 March 2024, a new message advertised that v7.5 was ready and will be released soon. The message was signed off by "EVLF". Craxs Rat v7.5 was released on this Telegram channel on 17 April 2024. This latest version has not been seen anywhere else at that time. Hence, it is highly likely that this Telegram channel belongs to the original EVLF.

On 18 May 2024, EVLF said that he decided to stop developing Craxs Rat because of scammers and cracked versions of Craxs Rat. However, he is working on a web version of Craxs Rat. Once this is completed, we foresee a new wave of this malware emerging.

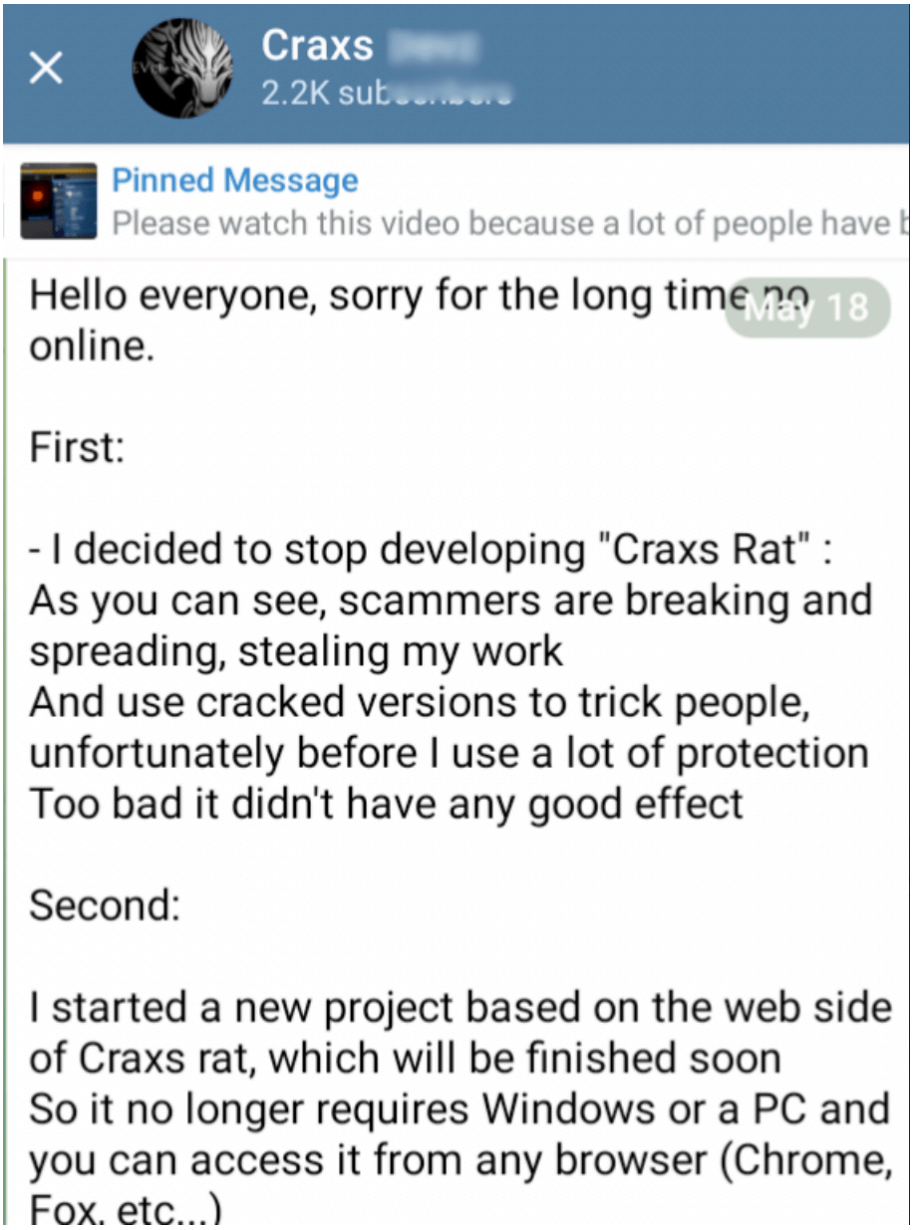

Figure 34. Screenshot of EVLF's new Telegram channel about stopping development of Crax Rat

So, as of now, **the initial channel of EVLF doesn't provide updated information about Craxs Rat**. Supposedly, it is still developed by **the same actor from Syria** who published information in the new channel.

Keeping in mind the new security measures from banks, **Craxs Rat can still be used by fraudsters for remote control of an infected device**. That is why other types of fraud and manipulations will continue to be used by fraudsters. **Craxs Rat is being sold as a malware-as-a-service and it continues to evolve.** (Not yet known) Buyers from different parts of the world will likely cause more damage in the near future.

Best practices for organizations to prevent RAT infections

These are some best practices we recommend that not only secure your devices against Craxs Rat, or any other forms of mobile malware.

Stick to trusted App Stores

Always download mobile applications from authorized sources like Google Play or the official Apple App Store. These platforms implement rigorous vetting procedures that significantly reduce the risk of fake app scams. By avoiding third-party sites, you steer clear of applications that could be designed to hijack your device through malicious permissions.

Be cautious with digital communications

Whether it's an unexpected email or a pop-up advertisement, maintain a healthy skepticism toward unsolicited digital content. Cybercriminals often use phishing emails and malvertisements to trick users into clicking on malicious links or downloading harmful attachments. Always verify the source of any message before engaging with it—this simple habit can save you from a lot of trouble.

Educate your team and customers

Knowledge is your best defense. For businesses, especially those in the financial sector, educating customers about the dangers of fake apps and phishing scams is crucial. Regular training sessions and awareness campaigns can help everyone understand how to identify suspicious behavior. When your team and customers know what red flags to look for, you create an environment where security is a shared responsibility.

Monitor and control app permissions

It's common for fake apps to request excessive permissions, like enabling Accessibility services or granting remote access to your device. These permissions can give cybercriminals complete control over your smartphone.

Work with reliable vendors

Group-IB's Fraud Protection utilizes a combination of threat intelligence, signature analysis, behavioral analytics, and cross-channel analytics to detect threats that traditional anti-fraud systems may miss. With Group-IB's Fraud Protection, strengthen your network security by proactively identifying and mitigating threats.

When businesses and their customers are being incessantly targeted, simply closing each security gap as it appears is insufficient. Instead, a comprehensive approach is necessary. Identifying the patterns of RAT activity, complete scope of the attack, IOCs, and conducting malware forensics is crucial. Detailed cyber investigations into the activity can help develop the best combative response against the specific type of attack initiated.

To learn more about Group-IB's Cyber Investigations, our solutions or to build holistic cybersecurity defenses against RATs and other threats, contact our experts here.
