Remo Android Trojan Targets 50+ Banking Apps & Wallets

By daksh sharma

Published: 2023-08-29 · Archived: 2026-04-05 23:50:00 UTC

New Remo Android Banking Trojan Targets Over 50 Banking Applications And Crypto Wallets

New Remo Android Banking Trojan Targets Over 50 Banking Applications And Crypto Wallets

CRIL analyzes a newly discovered Remo Android Banking Trojan targeting over 50 banking and cryptocurrency wallet applications from Indonesia, Vietnam, and Thailand.

Key Takeaways

- A phishing site impersonating Binance distributes a new Android Banking Trojan “Remo” abusing the Accessibility service to steal sensitive information.
- The malware targeted more than 50 banking and cryptocurrency wallet applications in Thailand, Vietnam, and Indonesia, exfiltrating sensitive information from these apps.
- The malware leveraged the Accessibility service to capture screen text, and steal keystrokes from the targeted applications.
- Analysis of the admin panel and code strings in the apk file suggested a possible China-originated Threat Actor (TA) behind the malware.
- Malware can monitor clipboard data, which allows it to steal sensitive data without granting any permissions by the victim.

Overview

In today’s interconnected digital landscape, the threat of cyber phishing and scams has become a significant concern. Cybercriminals have cleverly exploited the convenience and connectivity that technology offers, crafting sophisticated schemes to trick unsuspecting individuals and organizations. Cyble Research and Intelligence Labs (CRIL) has been continuously monitoring crypto-based phishing and scams. In June 2023, we discovered a crypto mining scam distributing Roamer Android Banking Trojan targeting banking applications primarily in Vietnam and India.

CRIL subsequently discovered yet another Android Banking Trojan, the “gjf-p3.apk (f75e26936a8f3b55065cdad25ee3e37bdf94054bc5e242dc72ebb073e4f73c3d),” via a VirusTotal search. This new discovery showcased an expanded targeting scope, involving not only Vietnam but also Thailand and Indonesia.

Following an in-depth investigation, a phishing website was unearthed: hxxps://binancep2p[.]cc/, which imitates a legitimate Binance cryptocurrency platform distributing the same malicious APK file named “binance.apk (63e60c5c984dc379a273fc0e13be81bd3030466b7b2fc9695ec588edc24930e7)”.

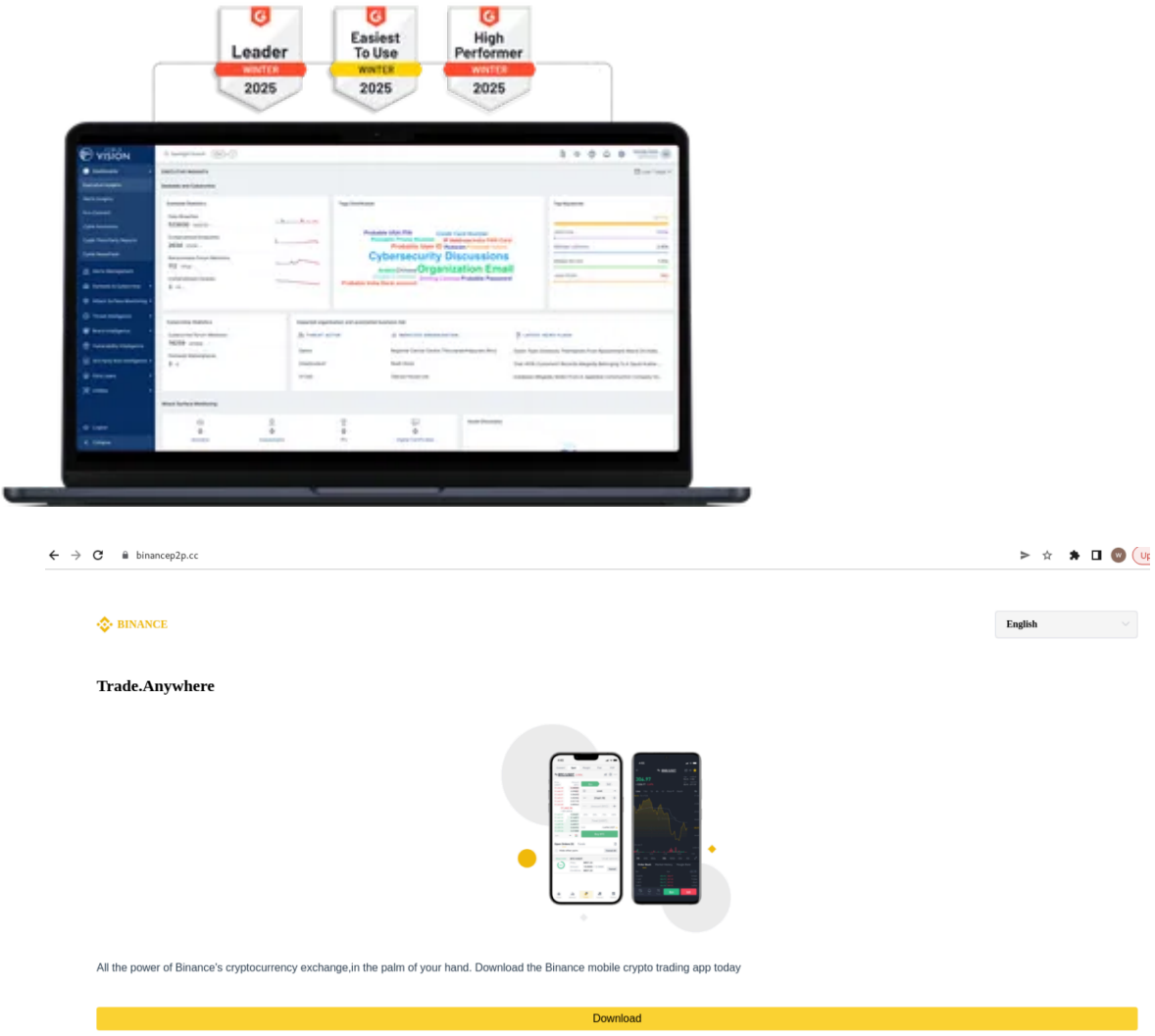

Figure 1 – Binance phishing site downloads malicious APK file

During the scrutiny of the initial phishing site, an additional three phishing websites were identified. As of the writing of this blog, the following mentioned sites are inactive:

- hxxps://binance-p2p[.]net/
- hxxps://binanceb2c[.]com/
- hxxps://vtelpuls[.]com/

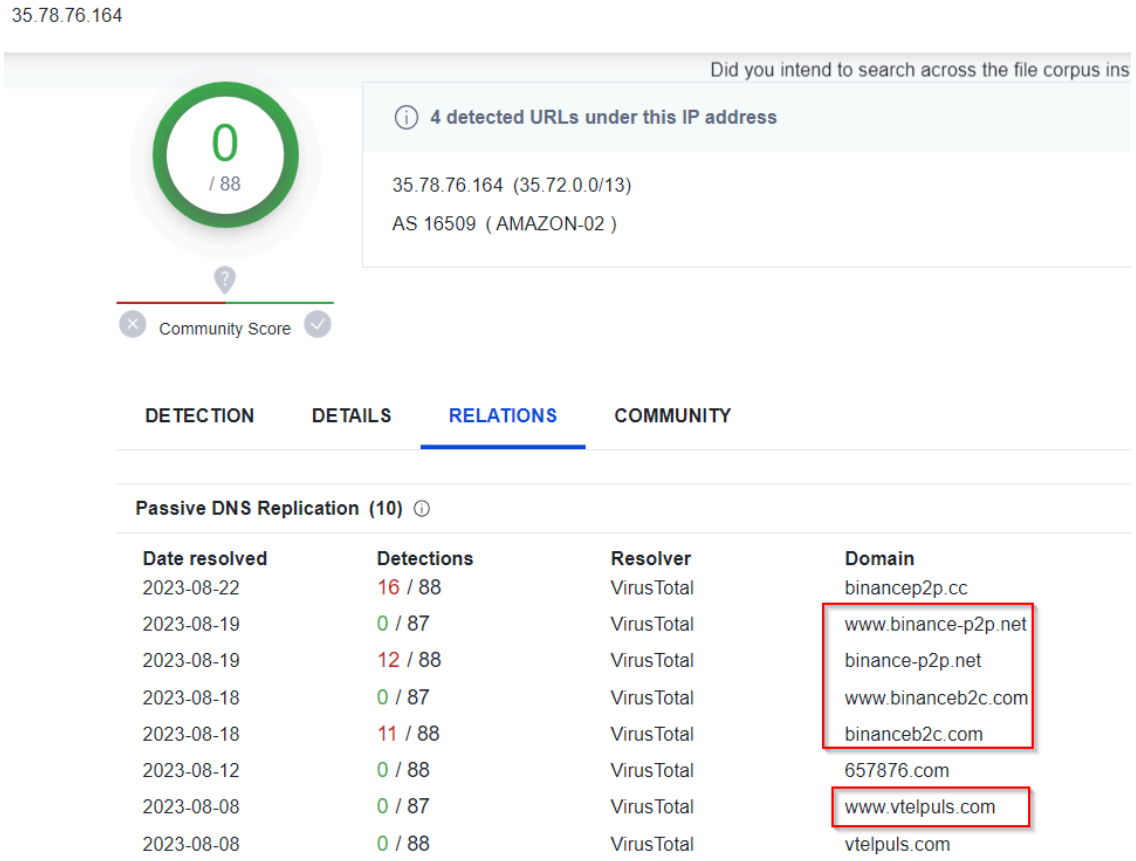

Figure 2 – Additional phishing sites

The phishing website hxxps://vtelpuls[.]com/ was distributing an APK file named “Vtel.apk (sha256: 3f7e87646dfc76784942e044d0468ba8f2bc9495fa2710779dc36f7e53f53708).” This APK file’s source code closely resembled the one obtained from the phishing website that was pretending to be Binance. We also have suspicions that the other two websites might have played a role in distributing this potentially harmful APK file.

Furthermore, we suspect that the targeted individuals might have encountered these phishing websites through SMS or other messaging applications, potentially making them susceptible to this threat.

After examining the downloaded APK file, it was discovered that the downloaded malicious application targets more than 50 banking applications and cryptocurrency wallets from Thailand, Vietnam, and Indonesia. Like several other banking trojans, this malware also uses the Accessibility service to steal the credentials of the targeted applications.

Since July 2023, the malware has been operational, and as of the time of composing this blog post, the malware samples have been detected at a notably low rate as shown in the below figure.

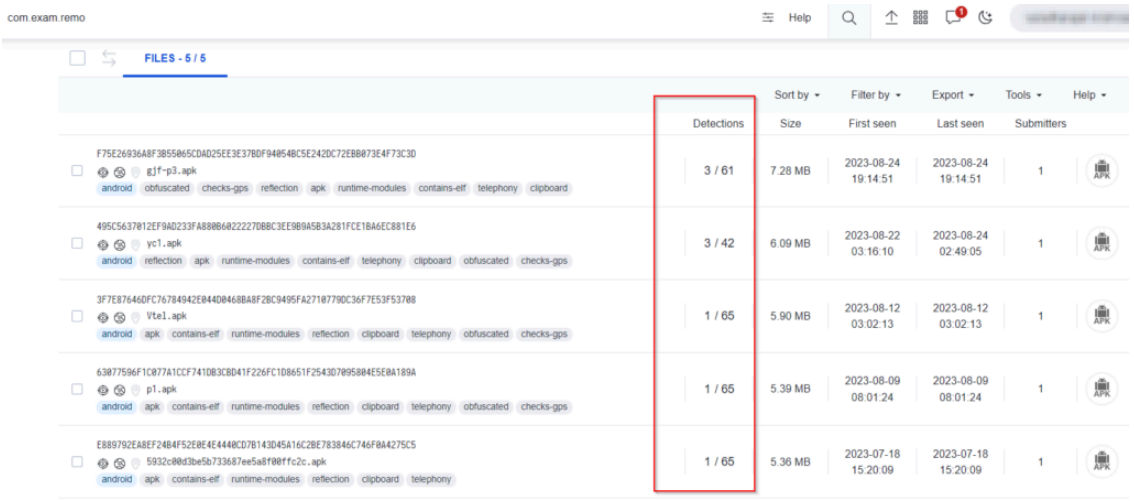

Figure 3 – Malware samples have low detection

The Threat Actor (TA) has kept some of the malicious code inside the Android Library under the “Remo” and “service” folders as shown in the below figure.

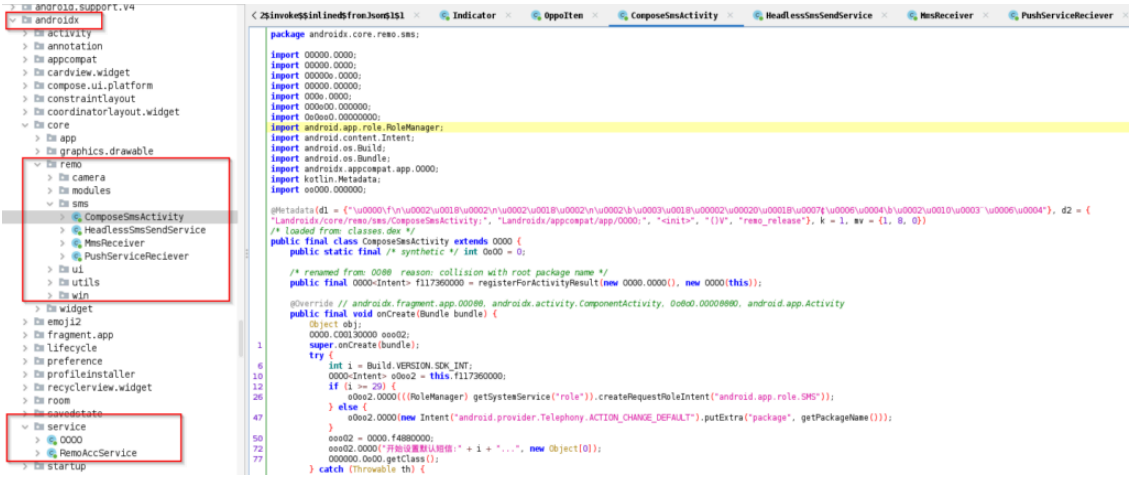

Figure 4 – Malicious module kept inside the Android Library

A comprehensive analysis of the malicious file revealed that this variant of malware is distinct and has not been encountered in the wild previously. Given this uniqueness, we have named the malware “Remo Banking Trojan,” a moniker name derived from the consistent package name observed across all malicious samples. This naming convention enhances our ability to monitor the malware’s activities effectively.

For the technical analysis, we are considering the most recent sample of the Remo Banking Trojan, namely “gjf-p3.apk (f75e26936a8f3b55065cdad25ee3e37bdf94054bc5e242dc72ebb073e4f73c3d)”. This specific sample establishes communication with a Command and Control (C&C) server located at *hxxps://vnoffs[.]cyou:8081*. Notably, the admin panel is also hosted on this URL. Upon examination of the admin panel, it becomes evident that certain strings are written in Chinese. Additionally, some strings present in the code are also in the Chinese language, suggesting that a TA could be of China origin.

The below figure shows the admin panel.

Figure 5 – Admin Panel

The malware employs strong obfuscation techniques to complicate reverse engineering and the strings present within the files are encrypted. Malware has implemented a custom decryption process to decrypt strings. The code snippet displayed in the figure below illustrates the specific logic that the malware employs to decrypt these encrypted strings.

Figure 6 – String decryption code

Technical Analysis

APK Metadata Information

- **App Name**: ARK
- **Package Name**: com.gjf2.office
- **SHA256 Hash**: f75e26936a8f3b55065cdad25ee3e37bdf94054bc5e242dc72ebb073e4f73c3d

Figure 7 – Application metadata information

After being installed, the Remo Banking Trojan establishes a connection with the C&C server at *hxxps://vnoffs[.]cyou:8081/device/getAllDeviceAppPackageSetting*. During this connection, it acquires a list of specific banking and cryptocurrency wallet applications that it aims to target. This list includes details such as the ID, package name, application name, and its disabled status, as shown in the figure below.

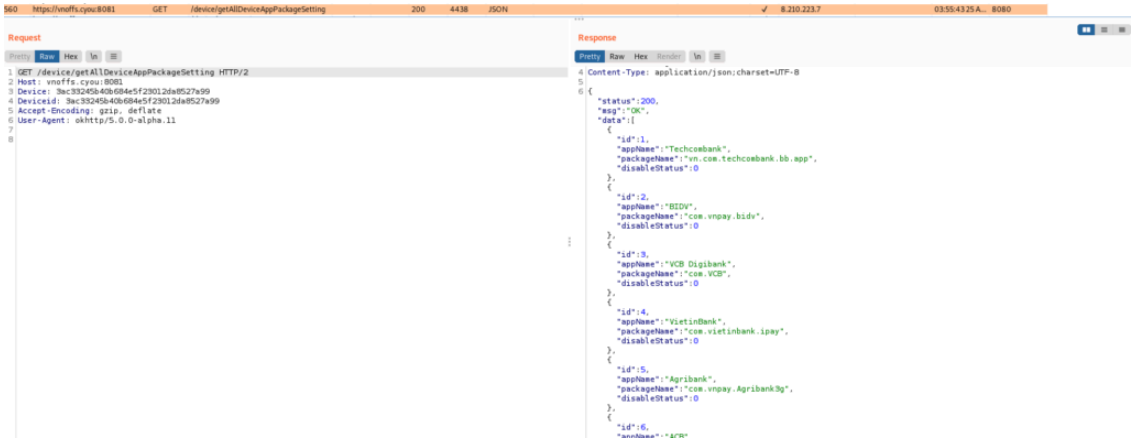

Figure 8 – Malware receives targeted application list

The table provided below lists the package names and application names of the targeted applications as targeted by the Remo banking trojan.

Package name	**Application name**
com.vnpay.bidv	BIDV
vn.com.techcombank.bb.app	Techcombank
com.VCB	VCB Digibank
com.vietinbank.ipay	VietinBank
com.vnpay.Agribank3g	Agribank
mobile.acb.com.vn	ACB
com.vnpay.vpbankonline	VPBank
com.tpb.mb.gprsandroid	TPBank
src.com.sacombank	Sacombank
com.mbmobile	MB Bank
com.vnpay.hdbank	HDBank
vn.com.msb.smartBanking	MSB
com.ocb.omniextra	OCB
com.mservice.momotransfer	MOMO

com.bca	BCA mobile
id.bmri.livin	Livin’ by Mandiri
src.com.bni	BNI Mobile Banking
com.jago.digitalBanking	Jago
com.bsm.activity2	BSI Mobile
com.ocbcnisp.onemobileapp	OCBC Mobile
id.co.bri.brilinkmobile	BRILink Mobile
id.com.uiux.mobile	M2U
com.bca.mybca.omni.android	myBCA
com.dbs.id.pt.digitalbank	Digibank Indonesia
com.alloapp.yump	allo bank
com.dbank.mobile	D-Bank PRO
net.myinfosys.PermataMobileX	PermataMobile X
id.co.bankbkemobile.digitalbank	SeaBank
com.bplus.vtpay	Viettel Money
vn.com.vng.zalopay	ZaloPay
wifi.gps.input	Input
th.or.gsb.coachaom	Coachaom
ktbcs.netbank	NEXT
com.bbl.mobilebanking	Bualuang mBanking
com.kasikorn.retail.mbanking.wap	K PLUS
com.scb.phone	SCB EASY
com.krungsri.kma	KMA
com.TMBTOUCH.PRODUCTION	Ttb Touch
com.kbzbank.kpaycustomer	KBZPay
com.uob.mighty.app	UOB TMRW
com.ktb.customer.qr	Paotang

im.token.app	imtoken
vn.shb.mbanking	SHB Mobile
com.bitpie	Bitpie Wallet
io.metamask	MetaMask
com.binance.dev	Binance
pro.huobi	HuoBi
com.bybit.app	Bybit
com.okinc.okex.gp	OKX
vip.mytokenpocket	TokenPocket
app.vitien.vitien	Vitien

Upon obtaining the list of targeted applications, the malware verifies the targeted application's existence on the compromised device. It then transmits both the application's name and package name along with the version number for each targeted application to the C&C server at *hxxps://vnoffs[.]cyou:8081/device/saveAppList as* shown below.

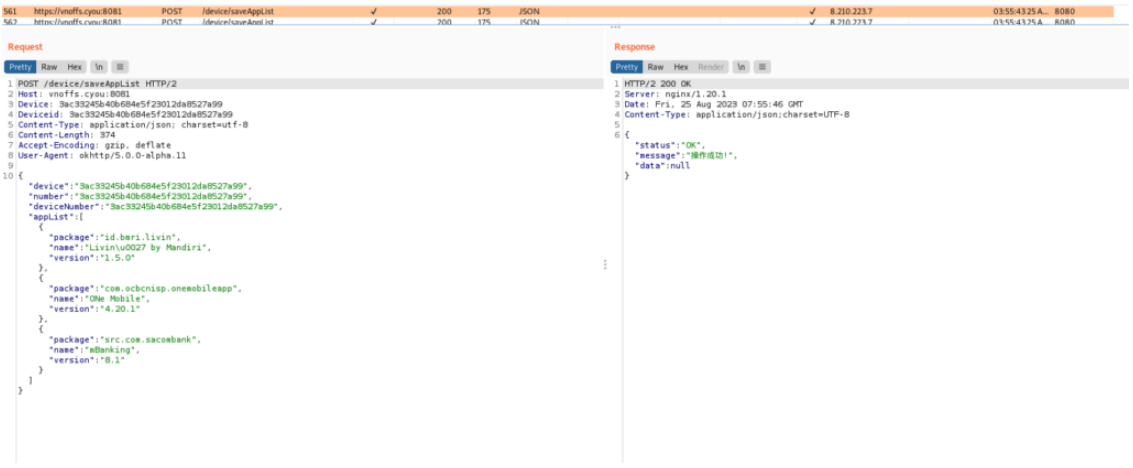

Figure 9 – Malware sends targeted application information installed on the victim's device to the C&C server

Simultaneously, malware prompts the victim to enable Accessibility service. Once the service is enabled, the malware abuses the service to execute banking Trojan activity, prevent uninstallation, and grant auto permissions as shown below.

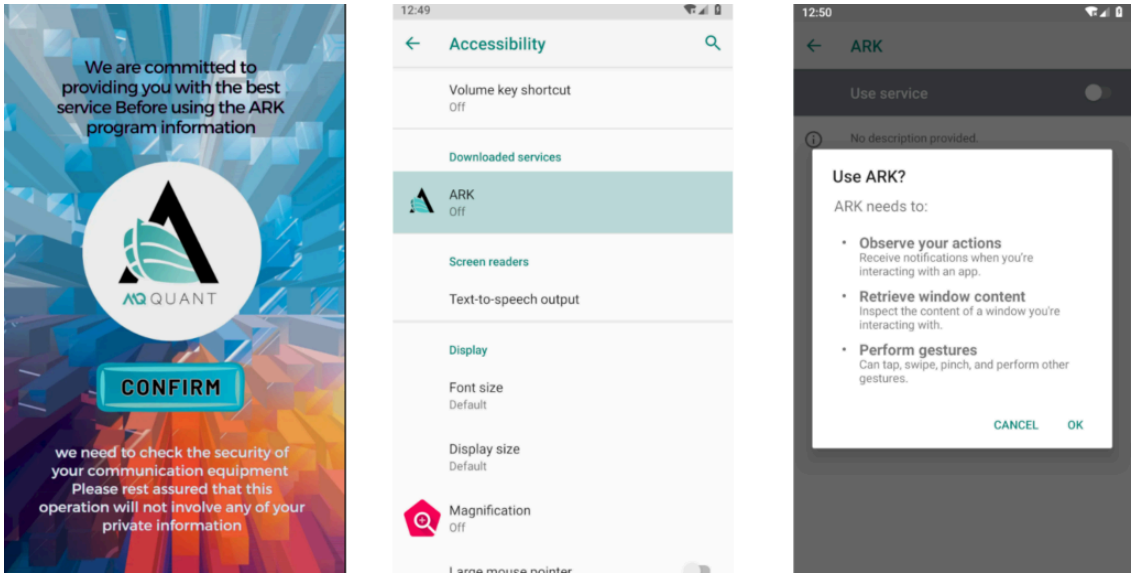

Figure 10 – Malware prompts to enable the Accessibility service

In the background, the malware continuously transmits data from the infected device to the C&C server *hxxps://vnoffs[.]cyou:8081/device/addOrUpdateDevice*. The data includes a wide range of information, such as the status of the Accessibility service, the package name of the currently running application, contents of the clipboard, time zone settings, and basic device details as shown in Figure 11. One notable aspect is the malware's persistent collection of clipboard content, enabling the TA to gather sensitive data from the victim's device without requiring any explicit permissions.

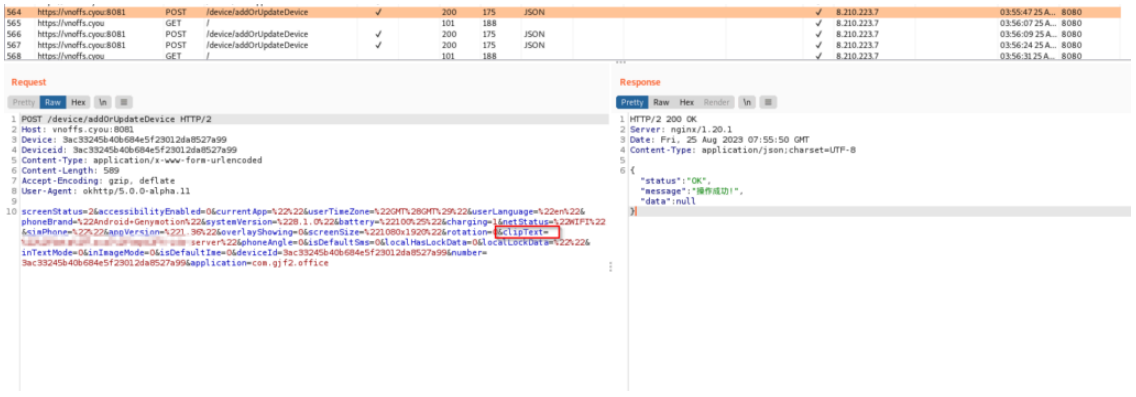

Figure 11 – Malware sends clipboard content with other device information

After gaining permission for the Accessibility service from the victim, the malware exploits this service to identify the targeted banking or cryptocurrency wallet applications installed in the victim's device. When the malware detects the victim's interaction with any of these applications, it captures all the visible text on the current screen.

Subsequently, the malware transmits this extracted text, along with the app name, package name, and current activity component name of the target application, to the C&C server *hxxps://vnoffs[.]cyou:8081/device/saveScreenText*. The compromised information can be used by the TA to exfiltrate credentials and other confidential data from the targeted application. The below figure shows an example of the exfiltration of screen text from the targeted crypto wallet application.

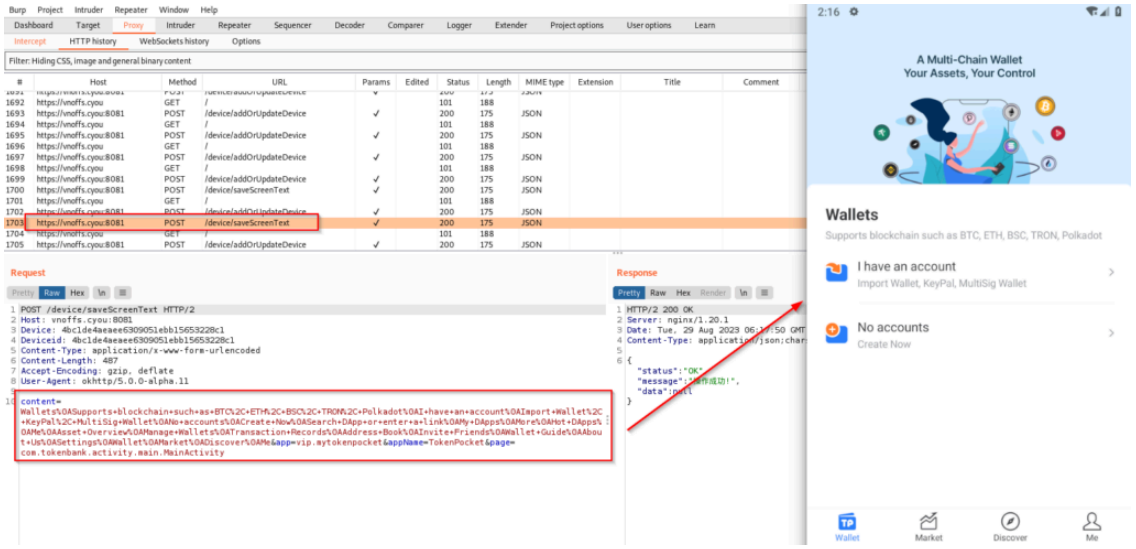

Figure 12 – Malware sends text from the targeted application's screen

The Remo Banking Trojan additionally monitors the edit text fields within the targeted applications and proceeds to transmit any sensitive information entered by the victim to the C&C server *hxxps://vnoffs[.]cyou:8081/device/saveKeyboardEvent*. The figure below depicts how the malware captures a victim's wallet mnemonic phrase through keylogging techniques.

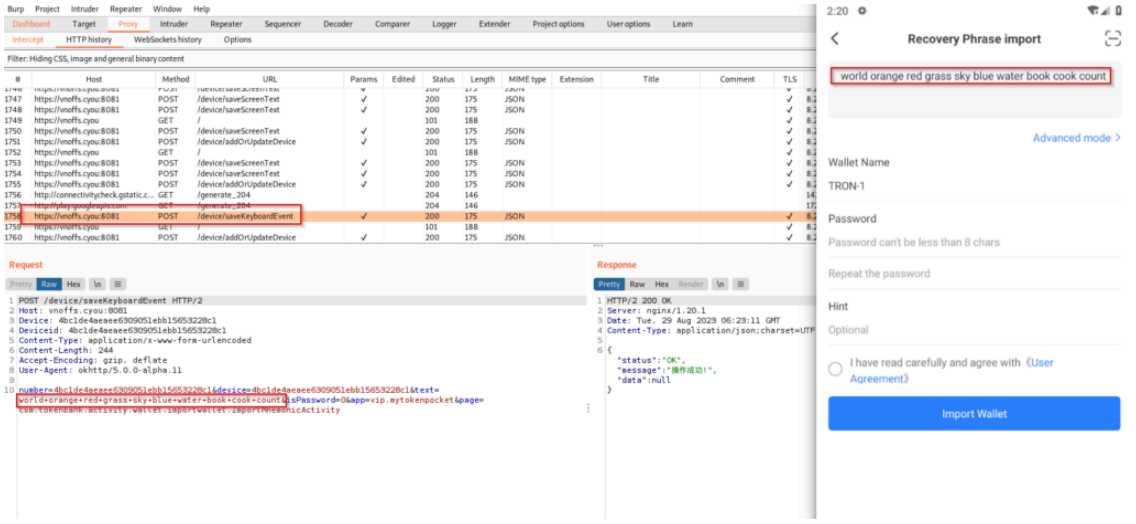

Figure 13 – Malware steals a mnemonic phrase from the targeted crypto application using keylogging

Additionally, Remo Banking Trojan also steals all the contacts stored from the infected device and sends them to the C&C server "*hxxps://vnoffs[.]cyou:8081/device/saveAddressBookList*". However, this particular URL is not available on the server, as shown in the below figure.

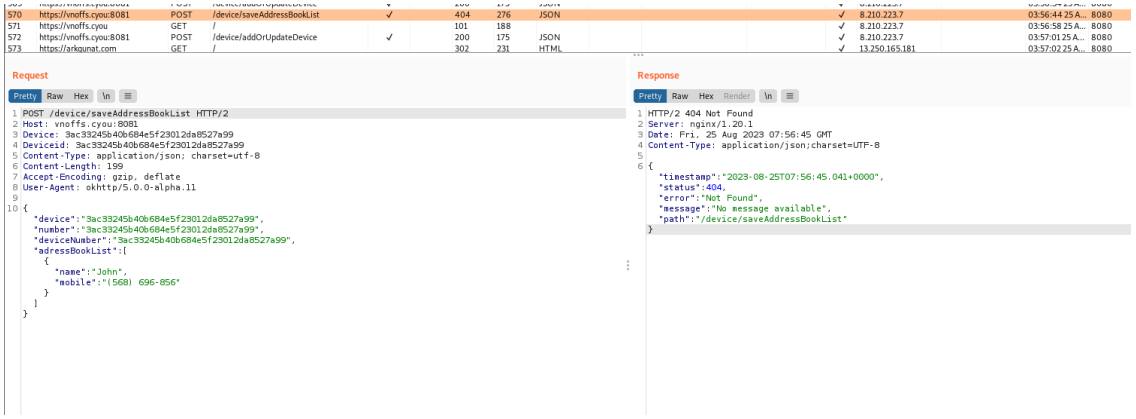

Figure 14 – Malware steals contact list

Conclusion

The Remo Banking Trojan represents a sophisticated cyber threat that specifically targets Android users in Southeast Asia, particularly in Thailand, Vietnam, and Indonesia. This malware employs various tactics, including phishing, keylogging, and accessibility service exploitation, to steal sensitive information from banking and cryptocurrency wallet applications. Notably, the malware's utilization of a counterfeit Binance platform, combined with its ability to evade detection effectively, highlights the increasing inventiveness of cybercriminals in developing powerful and dangerous threats.

The malicious APK, distributed through phishing websites, establishes a connection with a C&C server, allowing the malware to carry out its malicious activities. The Chinese origin implication, although speculative, suggests the involvement of a TA with an advanced level of sophistication. The use of custom encryption and decryption processes further highlights the malware's attempt to evade traditional security measures.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices given below:

- Download and install software only from official app stores like Play Store or the iOS App Store.
- Never share your Card Details, CVV number, Card PIN, and Net Banking Credentials with an untrusted source.
- Avoid copy pasting sensitive information such as ID Password of banking crypto, digital locker, or any other social media app.
- Using a reputed antivirus and internet security software package is recommended on connected devices, including PC, laptops, and mobile.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Be wary of opening any links received via SMS or emails delivered to your phone.
- Ensure that Google Play Protect is enabled on Android devices.
- Be careful while enabling any permissions.
- Keep your devices, operating systems, and applications updated.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Defense Evasion	T1629.001	Impair Defenses: Prevent Application Removal
Credential Access	T1414	Clipboard Data
Credential Access	T1417.001	Input Capture: Keylogging
Discovery	T1418	Software Discovery
Discovery	T1426	System Information Discovery
Collection	T1636.003	Protected User Data: Contact List
Exfiltration	T1646	Exfiltration Over C2 Channel

Indicators of Compromise (IOCs)

Indicators	Indicator Type	Description
63e60c5c984dc379a273fc0e13be81bd3030466b7b2fc9695ec588edc24930e7 bdfca6b4179daa865acd5c344ab6d44595994f2e 655c7f0f138675f81fae4eebea3a2b09	SHA256 SHA1 MD5	Binance.apk
hxxps://binancep2p[.]cc/	URL	Distribution site
f75e26936a8f3b55065cdad25ee3e37bdf94054bc5e242dc72ebb073e4f73c3d b5d780dc90fcc2534d331f1b369646fdafe523dd 0b7f5acaf4aa7dc5b5c4afa5c3c16f2d	SHA256 SHA1 MD5	Hash of analyzed file “gjf-p3.apk”
hxxps://vnoffs[.]cyou:8081	URL	C&C server
495c5637012ef9ad233fa880b6022227dbbc3ee9b9a5b3a281fce1ba6ec881e6 d96e6cf0af6720b272bca0befc4a72f2967531ec 1549b189b64abe469e8d002f524f0281	SHA256 SHA1 MD5	Remo Banking Trojan

3f7e87646dfc76784942e044d0468ba8f2bc9495fa2710779dc36f7e53f53708 b04b7af784c7dc6d8b3e2a9f8eed70bd72e12a01 9318046c62addc393bd411a14ea39dff	SHA256 SHA1 MD5	Remo Banking Trojan
hxxps://vtelpuls[.]com/apk/download/Vtel.apk	URL	Distribution URL
63077596f1c077a1ccf741db3cbd41f226fc1d8651f2543d7095804e5e0a189a 31c6fdf519e4e1012b27b752d128e4dd2df65c37 2d9d806404e30afacb8ccd82635c7ae7	SHA256 SHA1 MD5	Remo Banking Trojan
e889792ea8ef24b4f52e0e4e4440cd7b143d45a16c 2be783846c746f0a4275c5 29a046c8c0d500bd412d063a3c4daff0ff927929 5932c00d3be5b733687ee5a8f00ffc2c	SHA256 SHA1 MD5	Remo Banking Trojan

---

Source: https://cyble.com/blog/new-remo-android-banking-trojan-targets-over-50-banking-applications-and-crypto-wallets/