Research Threat intelligence Microsoft Defender Mobile threats
9 min read

Social engineering attacks lure Indian users to install Android banking trojans

By Microsoft Threat Intelligence

November 20, 2023

Microsoft Defender for Endpoint

Microsoft Defender XDR

Cybercrime

Social engineering / phishing

Android

Credential theft

Microsoft has observed ongoing activity from mobile banking trojan campaigns targeting users in India with social media messages designed to steal users' information for financial fraud. Using social media platforms like WhatsApp and Telegram, attackers are sending messages designed to lure users into installing a malicious app on their mobile device by impersonating legitimate organizations, such as banks, government services, and utilities. Once installed, these fraudulent apps exfiltrate various types of sensitive information from users, which can include personal information, banking details, payment card information, account credentials, and more.

While not a new threat, mobile malware infections pose a significant threat to mobile users, such as unauthorized access to personal information, financial loss due to fraudulent transactions, loss of privacy, device performance issues due to malware consuming system resources, and data theft or corruption. In the past, we observed similar banking trojan campaigns sending malicious links leading users to download malicious apps, as detailed in our blog Rewards plus: Fake mobile banking rewards apps lure users to install info-stealing RAT on Android devices.

The current active campaigns have pivoted to sharing malicious APK files directly to mobile users located in India. Our investigation focused on two malicious applications that falsely present themselves as official banking apps. Spoofing and impersonating legitimate banks, financial institutions, and other official services is a common social engineering tactic for information-stealing malware. Importantly, legitimate banks themselves are not affected by these attacks directly, and the existence of these attacks is not related to legitimate banks' own authentic mobile banking apps and security posture. That said, cybercriminals often target customers of large financial institutions by masquerading as a legitimate entity. This threat highlights the need for customers to install applications only from official app stores, and to be wary of false lures as we see in these instances.

In this blog, we shed light on the ongoing mobile banking trojan campaigns impacting various sectors by analyzing the attacks of two fraudulent apps targeting Indian banking customers. We also detail some of the additional capabilities of malicious apps observed in similar campaigns and provide recommendations and detections to defend against such threats. As our mobile threat

research continuously monitors malware campaigns in the effort to combat attackers' tactics, tools, and procedures (TTPs), we notified the organizations being impersonated by these fake app campaigns. Microsoft is also reporting on this activity to bring increased awareness to the threat landscape as mobile banking trojans and credential phishing fraud continues to persist, prompting an urgent call for robust and proactive defense strategies.

Case 1: Fake banking app targeting account information

We discovered a recent WhatsApp phishing campaign through our telemetry that led to banking trojan activity. In this campaign, the attacker shares a malicious APK file through WhatsApp with a message asking users to enter sensitive information in the app. The widely circulated fake banking message states "Your **[redacted]** BANK Account will be Blocked Today please update your PANCARD immediately open **[redacted]**-Bank.apk for update your PANCARD. Thank You." and includes a APK file named **[redacted]**-*BANK[.]apk*.

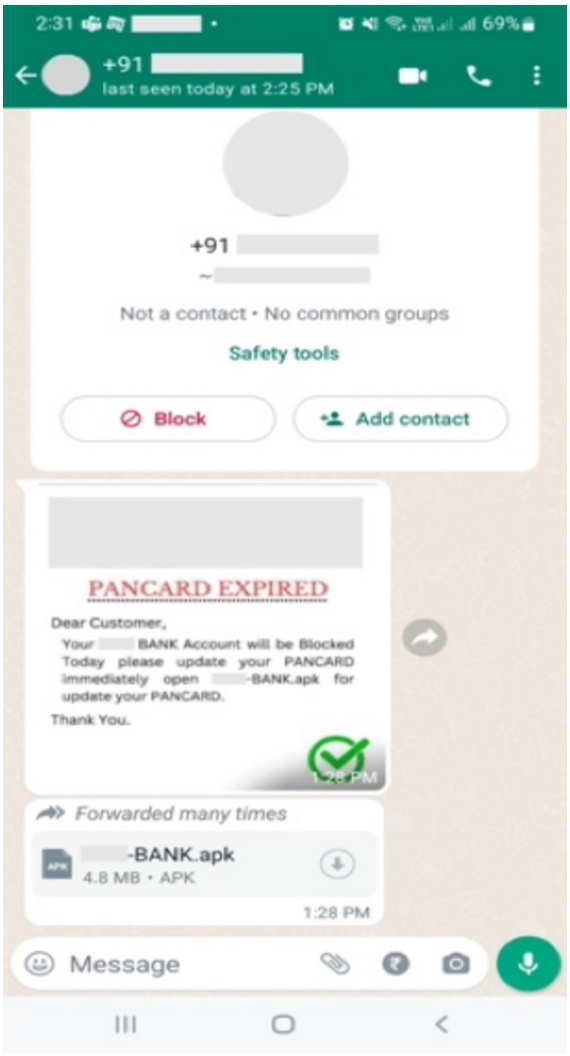


Figure 1. A fake WhatsApp message sent to user to update KYC using shared APK file.

Upon investigation, we discovered that the APK file was malicious and interacting with it installs a fraudulent application on the victim device. The installed app impersonates a legitimate bank located in India and disguises itself as the bank's official Know Your Customer (KYC) application to trick users into submitting their sensitive information, despite this particular banking organization not being affiliated with an official KYC-related app. This information is then sent to a command and control (C2) server, as well as to the attacker's hard-coded phone number used in SMS functionality.

Figure 2. The attack flow of this campaign.

What users see

Upon installation, the fake app displays a bank icon posing as a legitimate bank app. Note that the app we analyzed is not an official bank app from the Google Play Store, but a fake app that we've observed being distributed through social media platforms.

The initial screen then proceeds to ask the user to enable SMS-based permissions. Once the user allows the requested permissions, the fake app displays the message "Welcome to **[redacted]** Bank fast & Secure Online KYC App" and requests users to signin to internet banking by entering their mobile number, ATM pin, and PAN card details.

Figure 3. Once installed on a device, the fake app asks users to allow SMS permissions and to sign-in to internet banking and submit their mobile number, ATM pin, and PAN card to update KYC.

After clicking the sign-in button, the app displays a verification prompt asking the user to enter the digits on the back of their banking debit card in grid format for authentication—a common security feature used as a form of multifactor authentication (MFA), where banks provide debit cards with 2-digit numbers in the form of a grid on the back of the card. Once the user clicks the authenticate button, the app claims to verify the shared details but fails to retrieve data, instead moving on to the next screen requesting additional user information. This can trick the user into believing that the process is legitimate, while remaining unaware of the malicious activity launching in the background.

Figure 4. The fake app's authentication process asks the user to enter the correct digits as presented on their debit card.

Next, the user is asked to enter their account number followed by their account credentials. Once all the requested details are submitted, a suspicious note appears stating that the details are being verified to update KYC. The user is instructed to wait 30 minutes and not to delete or uninstall the app. Additionally, the app has the functionality to hide its icon, causing it to disappear from the user's device home screen while still running in the background.

Figure 5. The fraudulent app steals the user's account number and credentials and hides its icon from the home screen.

Technical analysis

To start our investigation and as part of our proactive research, we located and analyzed the following sample:

SHA-256	*6812a82edcb49131a990acd88ed5f6d73da9f536b60ee751184f27265ea769ee*
Package name	*djhgsfjhfdgf[.]gjhdgsfsjde[.]myappl876786ication*

We first examined the app's *AndroidManifest* file, which lists the permissions and components (such as activities, services, receivers, and providers) that can run in the background without requiring user interaction. We discovered that the malware requests two runtime permissions (also known as dangerous permissions) from users:

Permissions	Description
Receive_SMS	Intercept SMSs received on the victim's device
Send_SMS	Allows an application to send SMS

The below image displays the requested *Receive_SMS* and *Send_SMS* permissions, the activities, receivers, and providers used in the application, and the launcher activity, which loads the application's first screen.

Figure 6. AndroidManifest.xml file

Source code review

Main activity

The main activity, *djhgsfjhfdgf[.]gjhdgsfsjde[.]myappl876786ication[.]M1a2i3n4A5c6t7i8v9i0t0y987654321*, executes once the app is launched and shows as the first screen of the application. The *OnCreate()* method of this class requests permissions for *Send_SMS* and *Receive_SMS* and displays a form to complete the KYC application with text fields for a user's mobile number, ATM pin, and PAN card. Once the user's details are entered successfully, the collected data is added to a JSON object and sent to the

attacker's C2 at: *https://biogenetic-flake.000webhostapp[.]com/add.php*

The app displays a note saying "Data added successfully". If the details are not entered successfully, the form fields will be empty, and an error note will be displayed.

Figure 7. Launcher activity page, asking the user to sign-in with their mobile number, ATM pin, and PAN card.

Additionally, the malware collects data and sends it to the attacker's phone number specified in the code using SMS.

Figure 8. Collected data sent to the attacker's mobile number as a SMS.

Stealing SMS messages and account information

The malware collects incoming SMS messages from the victim's device using the newly granted *Receive_SMS* permission. These incoming messages may contain one-time passwords (OTPs) that can be used to bypass MFA and steal money from the victim's bank account. Using the *Send_SMS* permission, the victim's messages are then sent to the attacker's C2 server (*https[:]//biogenetic-flake[.]000webhostapp[.]com/save_sms[.]php?phone=*) and to the attacker's hardcoded phone number via SMS.

Figure 9. Steals incoming SMS to send to the attacker's C2 and mobile number via SMS.

The user's bank account information is also targeted for exfiltration—once the user submits their requested account number and account credentials, the malware collects the data and similarly sends it to the attacker's C2 server and hard-coded phone number.

Figure 10. Collecting the user's account number to send to the attacker.

Figure 11. Collecting the user's account credentials to send to the attacker.

Hiding app icon

Finally, the app has the functionality to hide its icon from the home screen and run in the background.

Figure 12. Hides app icon from home screen

Case 2: Fake banking app targeting payment card details

Similar to the first case, the second case involves a fraudulent app that deceives users into providing personal information. Unlike the first case, the banking trojan in the second case is capable of stealing credit card details, putting users at risk of financial fraud. User information targeted by the fraudulent app to be sent to the attacker's C2 includes:

- Personal information – Name, email ID, mobile number, date of birth
- Payment information – Card details (16-digit number, CVV number, card expiration date)
- Incoming SMS

What users see

When the user interacts with the app, it displays a launch screen featuring the app icon and prompting the user to grant SMS-based permissions. Once the requested permissions are enabled, the app displays a form for the user to enter their personal details, including their name, email address, mobile number, and date of birth. The data provided by the user is then sent to C2 server. After this, the app displays a form for the user to enter their credit card details, including the 16-digit card number, CVV number, and card expiration date, which is also sent to the attacker's C2.

Figure 13. Fake app collects SMS permissions, personal details and card details.

Additional features in some versions

In related campaigns, we observed some versions of the same malicious app include additional features and capabilities, such as capturing:

- Financial information – Bank details, bank ID, card details
- Personal information – PAN card, Aadhar number, permanent address, state, country, pin code, income
- Verifying and stealing one-time passwords (OTPs)

Similar campaigns

Based on our telemetry, we have been observing similar campaigns using the names of legitimate organizations in the banking, government services, and utilities sectors, as app file names to target Indian mobile users. Like the two cases discussed above, these campaigns involve sharing the fraudulent apps through WhatsApp and Telegram, and possibly other social media platforms. Moreover, these campaigns select legitimate and even well-known institutions and services in the region to imitate and lure users into a false sense of security. Spoofing and impersonating legitimate organizations and official services is a common social engineering tactic for information-stealing malware. While these banks and other organizations themselves are not affected by the attack directly, attackers often target customers by imitating legitimate entities.

Conclusion

Mobile banking trojan infections can pose significant risks to users' personal information, privacy, device integrity, and financial security. As the campaigns discussed in this blog display, these threats can often disguise themselves as legitimate apps and deploy social engineering tactics to achieve their goals and steal users' sensitive data and financial assets. Being aware of the risks and common tactics used by banking trojans and other mobile malware can help users identify signs of infection and take appropriate action to mitigate the impacts of these threats.

Finding unfamiliar installed apps, increased data usage or battery drain, unauthorized transactions or account settings changes, device crashes, slow performance, unexpected pop-ups, and other unusual app behaviors can indicate a possible banking trojan infection. To help prevent such threats, we recommend the following precautionary measures:

- Only install apps from trusted sources and official stores, like the Google Play Store and Apple App Store.
- Never click on unknown links received through ads, SMS messages, emails, or similar untrusted sources.
- Use mobile solutions such as Microsoft Defender for Endpoint on Android to detect malicious applications
- Always keep *Install unknown apps* disabled on the Android device to prevent apps from being installed from unknown sources.

Figure 14. Example of the Install unknown apps feature on an Android device

Additionally, various Indian banks, governments services, and other organizations are conducting security awareness campaigns on social media using promotional videos to educate users and help combat the ongoing threat presented by these mobile banking trojan campaigns.

Abhishek Pustakala, Harshita Tripathi, and Shivang Desai

Microsoft Threat Intelligence

Appendix

Microsoft 365 Defender detections

Microsoft Defender Antivirus and Microsoft Defender for Endpoint on Android detect these threats as the following malware:

- Trojan:AndroidOS/Banker.U
- Trojan:AndroidOS/RewardSteal.S
- Trojan:AndroidOS/RewardSteal.I
- TrojanSpy:AndroidOS/SpyBanker.Y

Indicators of compromise

SHA256	Description	Threat Name
6812a82edcb49131a990acd88ed5f6d73da9f536b60ee751184f27265ea769ee	Malicious APK	Trojan:AndroidOS/Banker.U
34cdc6ef199b4c50ee80eb0efce13a63a9a0e6bee9c23610456e913bf78272a8	Malicious APK	TrojanSpy:AndroidOS/SpyBanker.Y

MITRE ATT&CK techniques

Execution	Defense Evasion	Credential Access	Collection	Exfiltration	Impact
Scheduled Task/Job	Obfuscated Files/Information	Input Capture	Protected User Data: SMS Messages	Exfiltration Over C2 Channel	SMS Control
	Hide Artifacts: Suppress Application Icon				

References

- https://developer.android.com/guide/topics/permissions/overview#dangerous_permissions

Acknowledgments

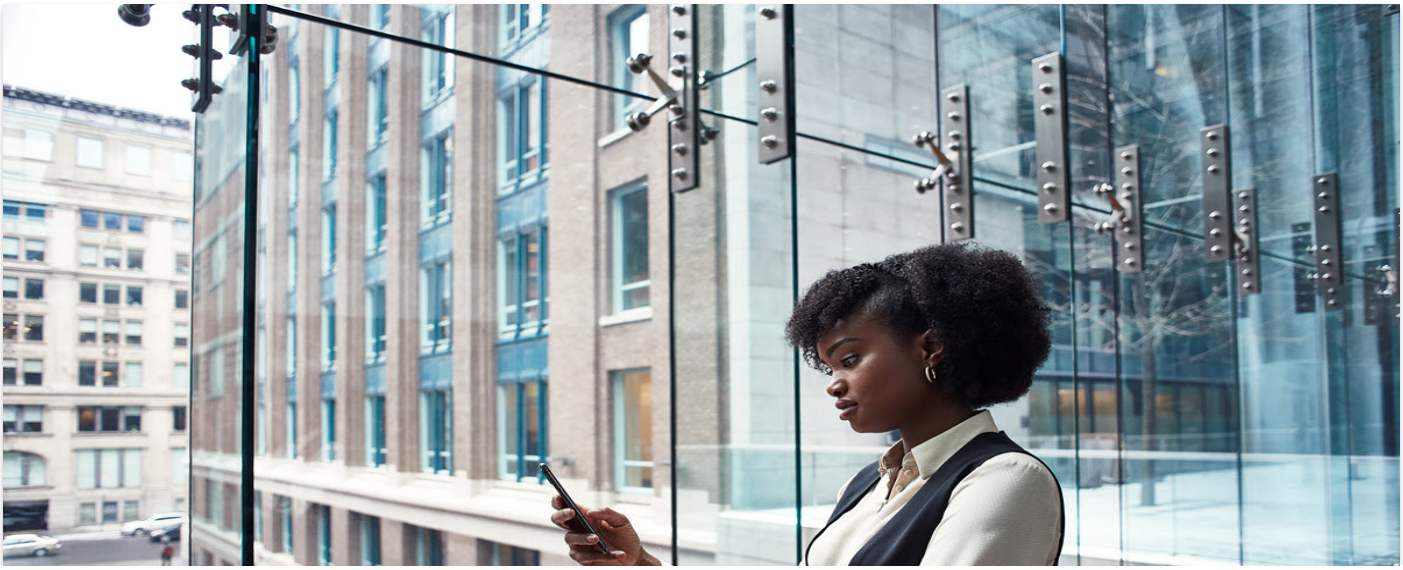
- https://cyble.com/blog/new-wave-of-finacial-fraud-scammers-monitoring-social-media-complaints/

Further reading

For the latest security research from the Microsoft Threat Intelligence community, check out the Microsoft Threat Intelligence Blog: https://aka.ms/threatintelblog.

To get notified about new publications and to join discussions on social media, follow us on X (formerly)Twitter at https://twitter.com/MsftSecIntel.

Related Posts



Research
Threat intelligence
Vulnerabilities and exploits

Mar 6
6 min read

Protecting Android clipboard content from unintended exposure

Microsoft discovered that the SHEIN Android application periodically read the contents of the Android device clipboard and, if a particular pattern was present, sent the contents of the clipboard to a remote server.

Research
Threat intelligence
Supply chain attacks

Sep 21
7 min read

Rewards plus: Fake mobile banking rewards apps lure users to install info-stealing RAT on Android devices

A fake mobile banking rewards app delivered through a link in an SMS campaign has been making the rounds, targeting customers of Indian banking institutions. Users who install the mobile app are unknowingly installing an Android malware with remote access trojan (RAT) capabilities.

Research
Threat intelligence
Vulnerabilities and exploits

Aug 31
11 min read

Vulnerability in TikTok Android app could lead to one-click account hijacking

Microsoft discovered a high-severity vulnerability in the TikTok Android application, now identified as CVE-2022-28799 and fixed by TikTok, which could have allowed attackers to compromise users' accounts with a single click.

Research
Threat intelligence
Attacker techniques, tools, and infrastructure

Jun 30
17 min read

Toll fraud malware: How an Android application can drain your wallet

Toll fraud malware, a subcategory of billing fraud in which malicious applications subscribe users to premium services without their knowledge or consent, is one of the most prevalent types of Android malware – and it continues to evolve.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy