TECHNICAL BRIEF

The Rise of Mobile Malware and How to Stop It

Malicious mobile apps — masquerading as legitimate apps — have spread like wildfire around the globe in 2023. Many of these trojans are designed to perform injection operations, like screen overlays, which collect user credentials, one-time passcodes (OTPs) and user data. By injecting malicious code or scripts into legitimate processes, the malware can hijack functions of the app and manipulate financial transactions, even changing the amount and recipient of a money transfer, for example.

We first saw an uptick in malware-infected apps in 2022 as the number of mobile banking trojans spiked 100% YoY. Likewise, remote access trojans (RATs) are growing in number and sophistication. For instance, Gigabud RAT is able to record the screen of an infected device and evade detection by delaying the execution of its malicious payload, which contains strings and commands obscured by encryption.

Complicating matters, criminals now wield the power of generative AI (GenAI). Tools on the dark web, like FraudGPT, scan for security vulnerabilities, create malware and scale attacks. With it, hackers are building malicious mobile apps that slip past security screenings on official and unofficial app stores. They're also creating flawless phishing campaigns and fraudulent ads that lure more victims to download their malware.

The growing prevalence of malicious mobile apps, primarily on unofficial app stores, underscores the need for better fraud and malware protection on customer-facing apps.

In this technical brief, we'll uncover the types of malicious apps that are on the rise and new compliance requirements on the horizon. Most importantly, you'll learn how cutting-edge, AI-driven security stops mobile malware.

What's driving the uptick in mobile malware?

With new tools at their fingertips, scammers are tricking victims to download malicious mobile apps commonly disguised as popular games, office utilities and retail apps. In some cases, they post ads, often on social media or third-party sites, enticing victims with discounts or promotions. Once installed, these side-loaded apps are used by hackers to remotely access the victim's device and steal data.

The malware often includes a keylogger, infostealer or other forms of spyware that abuse accessibility permissions to record input or extract information, including usernames, passwords and personal data. Later, bad actors login and take over accounts to transfer funds or purchase goods with the victim's credit card. These scams are evasive, damaging and fast, thanks to advanced tools and tactics, including:

GenAI scams: ChatGPT-like tools, including image generation apps and language translation services, enable fraudsters to create polished, eye-catching ads for fake goods or services. They also use bots and social media accounts to build trust, mimicking local dialects, professional language or gamer lingo, for example. They can even respond to direct messages and create positive, but fake, reviews.

GenAI phishing: Threat research shows phishing attacks have increased 1,265% in the past 12 months — a meteoric rise attributed largely to GenAI. Image generation and translation tools are making it easier for fraudsters to design and perfect phishing campaigns that trick more users to download malicious apps.

Remote access trojans (RATs): Threat actors use RATs to gain remote access to the device's operating system, screen and keystrokes. When the victim logs into any account, the criminal can steal their credentials and OTP codes. They simply log in to take over the account and use or transfer the victim's funds.

Among the most devious RATs, DroidJack enables bad actors to read and write WhatsApp messages on Android devices, whereas OmniRAT, which supports multiple platforms, enables remote calls. Both enable criminals to inflict serious damage.

Banking trojans: Advanced malware, like Xenomorph, posing as 50 different apps on the Google Play store, enabled fraudsters to steal credentials, skim OTPs, control devices and take over bank accounts. Another notable example, SpyNote can record audio and phone calls, which could be used to make voice deepfakes. These trojans, sold on the dark web, can be customized to look like any app.

Among their many tricks, trojans overlay fake login forms on the screen by exploiting accessibility services. Unwitting customers enter their credentials and one-time passcodes (OTPs), which are sent directly to the criminals. Most commonly used in mobile banking, fintech, eWallets, and cryptocurrency apps, this tactic has prompted some FIs to ask customers to turn off accessibility permissions or uninstall apps. But it's worth noting, not all trojans can be uninstalled.

New security recommendations

To mitigate the impact of malicious mobile apps, the Monetary Authority of Singapore's Cyber Security Advisory Panel, issued a press release on, "Ways to Tackle Mobile Malware Scams and Generative AI Risks for the Financial Sector."

Singapore's security recommendations are being interpreted as a bellwether of regulatory requirements to come for global banks. They're advising:

1. **Multi-pronged security:** A holistic cybersecurity approach
2. **Phishing-resistant credentials:** Passwordless, passkeys & password-free MFA
3. **Protocols for GenAI use:** Guidelines to prevent GenAI data leaks and manipulation
4. **GenAI cybersecurity:** Proactive threat detection and cyberattack simulations

How Transmit Security stops mobile malware

Transmit Security provides a holistic, AI-driven identity-security platform with advanced anti-malware, real-time fraud detection and phishing-resistant authentication. Journey-time orchestration pulls it all together, leveraging machine learning (ML), AI and GenAI to optimize detection and automate decisioning.

A single solution detects and stops malicious mobile apps, fraud, bots and phishing, no matter how legitimate they appear on the surface. Leading-edge detection methods, like behavioral biometrics, identify infected app behavior indicative of trojans like Xenomorph and Gigabud RAT. The risk engine also spots login overlays and other injection operations that insert malicious code, alter data or hijack app functions without the user's knowledge.

Not only will you prevent today's rapidly-evolving threats, but you'll also be ready to meet future compliance mandates with minimal cost and effort, using Transmit Security's broad range of advanced capabilities:

AI-powered security: As a market leader in AI innovation, Transmit Security has developed more robust detection models, able to analyze event clusters and respond more quickly to new variants and zero-day malware. ML and AI spot highly deceptive attacks by evaluating signals within the full context of your application flows and threat data. To enhance detection, we continually add new detection mechanisms and tune algorithms.

In parallel, Transmit Security has developed robust GenAI models to analyze security events, detect evasive threats and improve analytics. Our conversational AI tool delivers instant answers (in text or graphs) for insights about your fraud data.

Signature-based malware detection: The Transmit Security detection engine is continuously updated with new anti-malware signatures to give you immediate protection. Our malware detection methods are based on multiple unique identifiers and patterns to strengthen accuracy:

- **Known package names:** Identifies threats based on known malware signatures.
- **Creation or manipulation of OS-level files:** Discerns if an app modifies or creates new files at the operating system level — a strong indicator of malware.
- **Changes to environmental runtime parameters:** Monitors for unexpected or unauthorized changes in system runtime configurations, which suggests malware is attempting to execute malicious code or hide its presence.
- **Detection of ADB/Root (Frida/Magisk):** Detects the illegitimate use of tools for device manipulation and rooting, such as Android Debug Bridge (ADB), Frida and Magisk, which indicate the device has been compromised or is under the control of an attacker.

Behavioral-based malware detection: Since trojans and other threats can take over mid session after a successful login with MFA, it's essential to continually analyze behaviors and activities in comparison to known customer patterns. Robust behavioral biometrics detects highly deceptive malware based on micro-anomalies, such as latency in touch interactions, which can indicate remote control of a device.

Attack surface detection: Context-aware security understands and monitors the attack surface for a more proactive defense that stops attacks before they do harm. Transmit Security actively looks for the abuse of accessibility services, login overlays and SMS OTP harvesting as follows:

- **Accessibility service detection:** Our risk engine uses behavioral biometrics to detect and block anomalies in the usage of accessibility services in real time. It's essential since malware exploits accessibility features to control or change application behavior and input field data, harvest data and move between screens. The legitimate use of accessibility features is determined and allowed, depending on the typical use patterns by the customer and app.
- **Overlay detection:** Transmit Security detects the appearance of an overlay screen in real time to block credential harvesting and input capture attacks.
- **Detection of side-loaded apps:** Our real-time risk assessments detect side-loaded apps with the potential to harvest SMS OTPs. It does this by monitoring for system events related to SMS reception. A malicious app could use a receiver to get notified whenever an SMS OTP is received on the device. It also looks for services that run background, scan for and extract OTPs without the user's knowledge.

Multi-method detection: Going beyond behavioral biometrics, our real-time detection engine, running in the background at all times, analyzes risk, trust, fraud, bots and behavior. It uses hundreds of detection mechanisms, including device fingerprinting, bot detection, application and network evaluation, authentication analysis, reputation services, fraud ring blacklists and more. Risk signals are compared against the specific individual's typical devices, behavior, location and more.

Orchestration: Our powerful orchestration engine correlates fraud detection data and authentication across channels. Holistic analysis delivers highly accurate recommendations to Allow, Challenge or Deny, reducing false positives/negatives by 90% when compared to competing solutions. Journey-time orchestration then triggers the appropriate user flow to either mitigate risk or optimize the customer experience at run time.

Blocks GenAI phishing: Transmit Security delivers both immediate and proactive phishing prevention to protect customers and your brand. It's achieved as part of our multi-pronged approach:

- **Real-time anti-phishing:** Our risk engine stops phishing at its origin, making it immune to slick phishing campaigns created with GenAI. It examines the digital trail, including the domain, IP address, redirects, distribution methods plus the devices and behaviors. Real-time detection blocks phishing sites and URL redirects the very moment a customer clicks on a spoofed version of your website.
- **Phishing-resistant authentication:** Transmit Security delivers true passwordless MFA while supporting and securing passkeys. Any user who has a device that supports passkeys or fingerprint and face ID can be prompted to use them.

  Customers who use our best-in-class passwordless MFA achieve the highest assurance — without ever using a password. This is unique for 3 reasons:

  1. **Multi-device support -** Unlike other solutions, Transmit Security let's customers register on a FIDO-enabled device and transfer trust to more devices without using passwords.
  2. **Omnichannel -** One implementation supports all channels, solving a limitation of FIDO. Plus, customers only register one time to move across all apps, channels or devices.
  3. **Broader support -** Unlike passkeys, our passwordless MFA enables you to authenticate users on any biometric-enabled device across all major ecosystems.

  Passkeys are also phishing-resistant, and our platform not only supports them but secures them as well. We've created an added security layer to prevent passkey leakage, ensuring a deliberate transfer of trust, so passkeys only sync across devices and ecosystems when desired.
- **Social engineering detection:** Multi-method detection powered by ML and AI spot user anomalies, including signs of manipulation or authorized push payment (APP) fraud. For example, if the customer is initiating a money transfer while mousing and typing more slowly than usual, it may indicate they are being guided by a fraudster. Our security measures can disrupt the activity and probe for answers. If warranted, it can trigger an authentication or identity verification challenge or end the session.

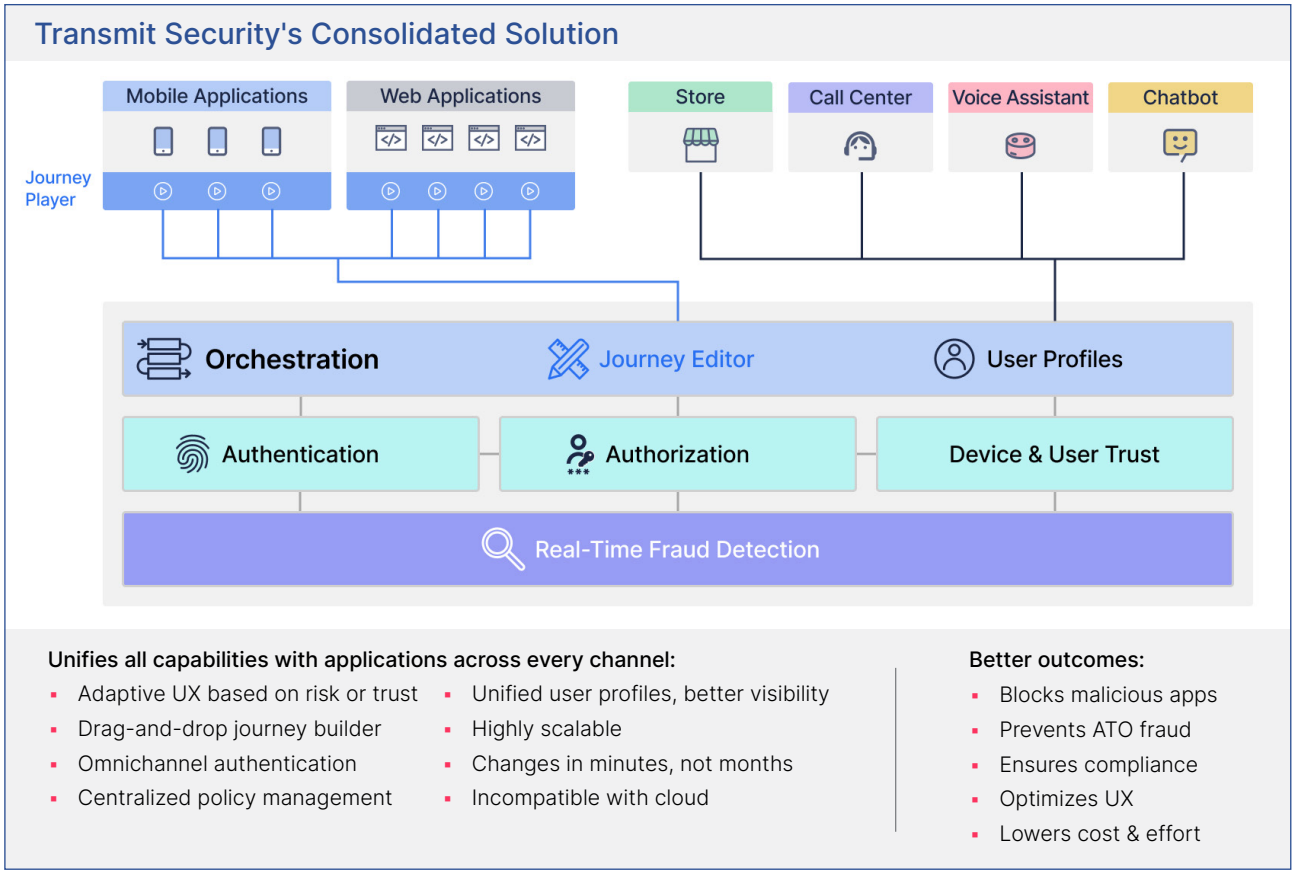
Simplifies fraud ops: With a single, comprehensive identity-security solution Transmit Security removes identity stack complexity and lowers operational costs all while closing the security gaps that plague fraud teams.

- **Attack simulator:** We've developed a cutting-edge attack simulator to help fraud teams visualize how different attack patterns appear on the Transmit Security Platform. You can experiment with mock data or simulate real-life attacks to train and prepare teams on:
  - How new, emerging threats might affect your applications and services
  - The impact of different attack types (ex: bots, malware, devices emulators)
  - How to resolve different attacks by developing new approaches
  - Ways in which an attack may impact different moments in the user journey
- **GenAI-powered identity analytics:** Leveraging the power of GenAI, we've integrated conversational analytics into our platform. Much like ChatGPT, you can get instant answers about your fraud data, users and their security posture to quickly adapt and tune rules. It also creates charts or graphs on demand to provide insights that will help you improve security and UX.
- **Visibility and control:** A single, centrally-managed admin portal provides visibility of each users' authenticators, devices, behaviors, risk scores and apps. A dynamic user store consolidates user profiles across brands and channels, giving admins a single source of truth as well as graphical displays of real-time data, attack patterns and trends.
- **Plug-and-play architecture:** Developer-friendly APIs and SDKs eliminate the need for integrations — no coding required. There's also minimal effort to create identity journeys with a drag-and-drop journey builder plus out-of-the-box user flows and scenarios. You can alter the flow as needed without making any code changes to your app. You have full control over your brand experience with a customizable UI.

Out-of-the box privacy compliance: Transmit Security ensures data privacy at all times. As a cybersecurity company with expertise in data protection, we've built the most secure platform to protect PII. We also maintain those protections to evolve quickly as regulations change, making it effortless for organizations to keep up with privacy mandates.

Full platform synergies

All capabilities within the Transmit Security Platform benefit from instant access to unified user profiles along with risk scores, threat intelligence and other security data. Holistic, contextual analysis strengthens behavioral biometrics, device fingerprinting and other capabilities — all managed via one console.



Unifies all capabilities with applications across every channel:

- Adaptive UX based on risk or trust
- Drag-and-drop journey builder
- Omnichannel authentication
- Centralized policy management
- Unified user profiles, better visibility
- Highly scalable
- Changes in minutes, not months
- Incompatible with cloud

Better outcomes:

- Blocks malicious apps
- Prevents ATO fraud
- Ensures compliance
- Optimizes UX
- Lowers cost & effort

Discover how Transmit Security stops fraud and rewards customers with secure and easy access to all that your business offers.

Book a meeting