TECHNICAL BRIEF

The Rise of Malicious Apps in Asia Elicits New Recommendations from the Monetary Authority of Singapore

Authorities in Singapore are sounding the alarm in response to a 65.5% spike in scam cases, amounting to losses totalling $334.5 million (US$245.7M) in the first half of 2023. Of particular concern, consumers are being lured to download malicious Android apps from third- party sites, outside official app stores like Google Play, ultimately leading to account takeover (ATO) and fraudulent transactions. Malicious apps, especially banking trojans, are a growing problem across Asia.

To mitigate the impact of these attacks, the Monetary Authority of Singapore's (MAS) Cyber Security Advisory Panel, issued a press release on, "Ways to Tackle Mobile Malware Scams and Generative AI Risks for the Financial Sector." It includes security recommendations, which are being interpreted as a bellwether of regulatory requirements to come in the near future.

In this Technical Brief, we'll cover the types of scams that are targeting Singaporeans, explain the new MAS security proposals and present a cybersecurity solution that meets or exceeds MAS recommendations out of the box. Transmit Security's AI-driven identity-security platform gives financial institutions automated protection against mobile malware, generative AI (GenAI) threats and other tricks, like fake login overlays that collect customer credentials.

What's driving the uptick in malicious apps?

Scammers are enticing victims to download malware-infected apps with discounts or promotions, often on social media or third-party sites. Disguised as legitimate-looking apps, consumers fall for attractive deals.

Once installed, attackers use the app to remotely access the victim's device and steal data. The payload often includes a keylogger that abuses accessibility permissions to record input, including usernames and passwords. Later, bad actors login and take over accounts to run fraudulent transactions. Using malicious apps, attackers have even siphoned money from victims' social security savings in Singapore's Central Provident Fund.

These scams are more evasive, fast and damaging as they leverage the most advanced technologies to trick customers. The tools and tactics they're using include:

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

GenAI phishing: The same tools are making it easier for fraudsters to create polished phishing emails and spoofed websites, tricking more users to download their malicious apps.

Deepfakes: To enhance the illusion of legitimacy, scammers are using GenAI to create video and voice deepfakes, luring more victims to fall for their schemes. They're also using AI-powered chatbots or virtual assistants for social engineering attacks, impersonating customer service reps, for example. In doing so, they manipulate victims into sharing personal information, passwords or financial details, leading to fraud. Deepfakes are also used in call centers where voice cloning tools are able to deceive voice authentication systems.

Remote access trojans (RATs): Threat actors use RATs, such as CypherRAT and SpyNote, to gain access to the victim's operating system, screen and keystrokes. They're often disguised as legitimate apps, selling discounted low-cost items, like seafood or mooncakes. On the payment page, users may be prompted to choose their bank and log in to their account, effectively stealing their credentials, including multi-factor authentication (MFA).

Some RATs with broader spying capabilities take control of infected devices and bypass detections with obfuscations and quick install features. After installation, they prompt the victim to enable accessibility services, which gives them deep access to the device's functionalities and user data. Threat researchers say half a million new malware apps are being generated daily.

Banking trojans: Advanced malware, like Xenomorph, Escobar, Anubis, BankBot and others, enable fraudsters to take control of devices and bank accounts. Sold on the dark web, these trojans are customizable so that fraudsters can tailor them to look like any legitimate app. Among their many tricks, they overlay fake (but real-looking) login forms on the screen. Unwitting customers enter their credentials and one-time passcodes (OTPs), which are sent directly to the cybercriminals.

Overlays exploit Android's Accessibility Services to intercept and transmit login data. This is why some banks in Singapore are asking customers with side-loaded apps to turn off their accessibility permissions or uninstall the risky app. It's worth noting that Xenomporph, once installed, cannot be uninstalled; it adds itself as a device admin and prevents its removal.

New security recommendations from MAS

To mitigate these threats and sustain trust in digital banking services, MAS has issued four high-level security recommendations:

1. **Multi-pronged security -** To address the challenges of malicious mobile malware and GenAI threats, MAS recommends a holistic cybersecurity approach. This involves a comprehensive strategy to tackle banking scams that begin with side-loaded mobile apps. In doing so, MAS advises close collaboration with tech providers to block the installation of harmful apps.
2. **Phishing-resistant credentials -** Banks can strengthen the customer login for mobile banking and payment systems through advanced MFA. This includes the use of passwordless MFA, passkeys and other methods that eliminate the use of passwords.
3. **GenAI data leaks and manipulation -** It's vital to increase the awareness of both GenAI advantages and dangers. As financial institutions (FIs) integrate GenAI into their systems and operations, they must guard against data leaks, data poisoning and manipulation. This calls for security measures that include proper data management protocols.
4. **GenAI cybersecurity -** Utilizing AI to boost cybersecurity includes the application of AI-driven tools for security monitoring, proactive threat detection and advanced cyberattack simulations to enhance the overall defense.

Preventing account fraud with Transmit Security

Transmit Security offers a holistic identity-security platform with true passwordless authentication, passkeys and other strong forms of MFA, anti-malware, fraud detection and journey-time orchestration powered by machine learning (ML), AI and GenAI. As a complete, multi-pronged solution, it detects and blocks malicious apps, fraud, bots, phishing and deep fakes created with GenAI — no matter how realistic they appear.

With a unified out-of-the-box solution, banks in Singapore can prevent fraud and prepare to meet future MAS mandates — with minimal cost and effort. Plus, Transmit Security helps FIs avoid consumer backlash over privacy concerns. Here's how it prevents each of the tactics fueling the rise of scams:

Detects and stops malicious apps: Transmit Security leverages signature files plus AI and ML to protect against ever-evolving malware and malicious apps. We've developed more robust AI models with GenAI, able to analyze event clusters and respond quickly to today's highly deceptive variants and zero-day malware. This leading-edge platform also detects infected app behavior that's indicative of malware, including banking trojans, like Xenomorph. In addition, our risk engine spots login overlays to prevent fraud before it can start.

Prevents GenAI tactics: Transmit Security detects deceptive scams based on behaviors and activity, so it doesn't matter how professional the ads, social posts or reviews look. Our real-time detection engine spots risk, trust, fraud, bots and aberrant behavior with multi-method detection:

- **AI-driven fraud prevention:** Runs in the background at all times, leveraging hundreds of detection mechanisms, including advanced behavioral biometrics, 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 behavior, devices, location and other parameters.
- **Immediate detection of new attack patterns:** ML and AI spot new or evolving attacks by evaluating signals within the full context of your mobile application flows and threat data. In parallel, our developers continually add new detection mechanisms and tune algorithms.
- **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, giving FIs immunity to slick phishing emails and websites created with GenAI. Instead of spotting inconsistencies or typos, our phishing detection examines the digital trail. The domain, IP address, redirects, distribution methods plus the devices and behaviors all provide clues. With real-time analysis, our risk engine blocks phishing sites and URL redirects the very moment a customer clicks on a spoofed version of your website.
- **Phishing-resistant authentication:** Transmit Security supports and secures passkeys in addition to offering our best-in-class passwordless MFA. Any user who has a device that supports passkeys or fingerprint and face ID can be prompted to use them.

  Customers who use our true passwordless MFA achieve the highest level of 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.

Looks past deepfakes — under the hood: Transmit Security uses AI to detect social engineering chat bots, adversarial attacks and other AI-based fraud tactics. With our intelligent platform, banks can prevent fraud by calling on the broad range of capabilities.

- **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 mousing and typing more slowly than usual, it could indicate they are being guided by a fraudster, in which case, our security measures disrupt the behavior and probe for answers. Depending on responses and your organization's risk tolerance and user flows, our orchestration engine may trigger an authentication or verification challenge, end the session or allow them to proceed.
- **Passwordless MFA and passkeys** with extra protection for passkey vulnerabilities shield against all types of scams, including those that start with deepfakes.

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.

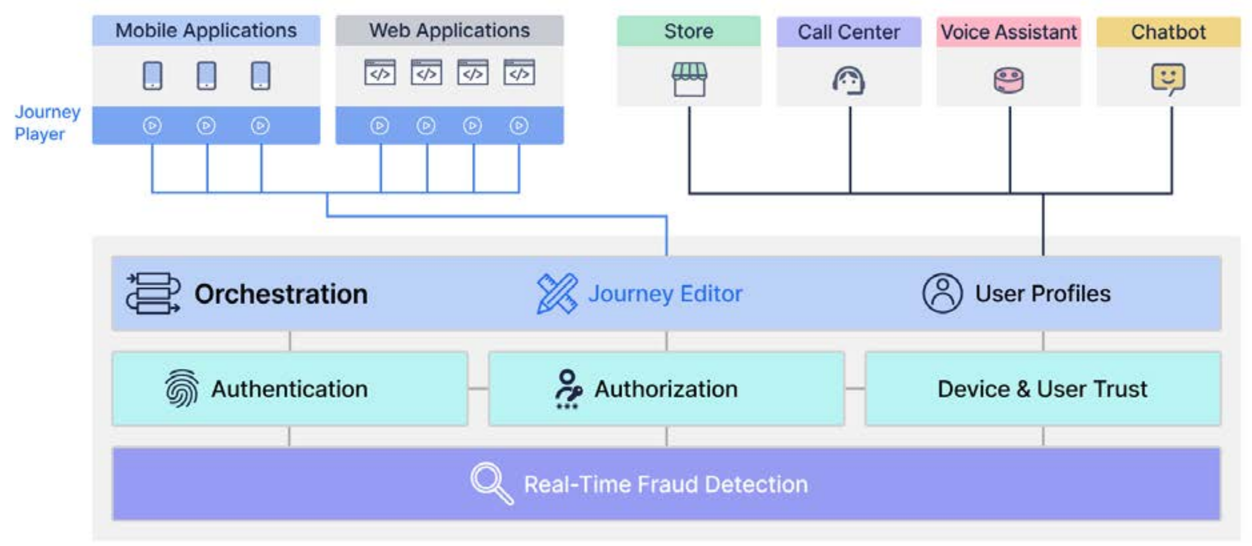
- **Attack simulator:** We've developed a cutting-edge attack simulator to help fraud teams visualize how different attack patterns appear on the Transmit Security Platform. You can experiment with mock data or simulate real-life attacks to train and prepare teams on:
  - How new, emerging threats might affect your applications and services
  - The impact of different attack types (bots, malware, spoofed devices or emulators)
  - How to resolve different attacks by developing approaches for investigating them
  - Ways in which an attack may impact different moments in the user journey (e.g., login, registration and transaction).
- **AI-powered identity analytics:** Leveraging the power of GenAI, we've integrated conversational analytics into our platform. Much like ChatGPT, you can ask questions to receive instant answers about your fraud data, users and their security posture. With the ability to view all risk/trust events, you can quickly adapt and tune rules to improve security and UX. This tool also creates charts or graphs on demand. Simply ask for the type of visual you need to gain insights about your apps, users, risk scores, attack types and more.
- **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 and UX.

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.

Transmit Security's Consolidated Solution



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