ThreatMark

Mobile Banking Fraud

Защитите ваши мобильные каналы обслуживания уникальным решением от компании ThreatMark

В наши дни уже большинство операций выполняется через мобильные устройства. Удобство мобильных устройств резко усложнило их защиту, мошенничество становится все более интеллектуальным, используя все время меняющиеся векторы специфичных для мобильных устройств и кросс-канальных атак.

Наше решение обеспечивает уникальную многоуровневую защиту мобильных каналов, комбинируя **глубокое профилирование пользователей** с мощным **механизмом обнаружения угроз**.

Обнаружение угроз:

Разработанный нами небольшой компонент Anti-Fraud встраивается в мобильное приложение и защищает ваших пользователей от таких видов атак, как перехват mTAN, считывание экранной клавиатуры и SMS, банковские троян, кросс-канальные атаки и кража личности мобильного пользователя.

Проверки безопасности, обнаруживающие джейлбрейк/рутованность устройства, использование ненадёжных сетей, вредоносные приложения или инструменты, позволят выявить приложения, функционирующие в ненадёжной среде. Применяя индивидуальные политики безопасности, можно гибко настраивать обработку транзакций и операций, инициируемых с таких устройств.

Мошенники также пытаются взломать банковские системы безопасности, декомпилируя банковские приложения с целью установить неавторизованное соединение между клиентом и сервером. Наше решение обнаруживает поддельные приложения, атаки и попытки взлома с использованием скриптов, тем самым защищая банковские приложения.

Если какое-либо приложение содержит вредоносный или подозрительный код, запросило у операционной системы потенциально опасные права, это будет выявлено в реальном времени. Неизвестные потенциальные угрозы отправляются на дальнейший анализ в наш Центр обеспечения безопасности, позволяя вам быстро реагировать даже на атаки нулевого дня.

Верификация личности:

Поведение каждого пользователя, взаимодействующего с мобильным устройством и мобильным приложением, находится под постоянным мониторингом системы и сравнивается с накопленными знаниями о более раннем поведении пользователя с использованием методов машинного обучения. Если сильно изменяются скорость набора текста, экранные жесты, пути навигации внутри приложении или другие наблюдаемые параметры пользователя, на сервер подается сигнал о потенциальном взломе аккаунта или перехвате управления. Для каждого устройства также создается цифровой отпечаток, который сравнивается с нашей анонимизированной базой устройств, используемых мошенниками и добропорядочными пользователями.