

► ŘEŠENÍ KASPERSKY FRAUD PREVENTION SDK FOR MOBILE

Kaspersky Fraud Prevention SDK for Mobile je komplexní řešení určené k ochraně aplikací mobilního bankovnínictví spuštěných v operačním systému Android, iOS a Windows Phone. Spojuje v sobě špičkové technologie zabezpečení IT společnosti Kaspersky Lab a chrání data zákazníků, zabezpečuje komunikaci s bankou a zajišťuje, aby v mobilních zařízeních používaných k obsluze online bankovnínictví nečíhaly žádné hrozby.

Řešení Kaspersky Fraud Prevention SDK for Mobile je velice flexibilní a umožňuje bance plynule převést služby zákazníkům do mobilních zařízení a současně jim nabídnout ochranu před podvody.

Řešení Kaspersky Fraud Prevention SDK obsahuje pět klíčových funkčních oblastí zaměřených na prevenci převzetí účtu, zanesení malwaru a dalších útoků, ještě než mohou způsobit škody.

SKENOVÁNÍ A ODEBRÁNÍ MALWARU

Pro bankovní operace je nezbytně nutné čisté, bezpečné zařízení. Dokonce ještě před načtením bankovní aplikace se řešení Kaspersky Fraud Prevention SDK přesvědčí, zda pracovní prostředí neobsahuje malware a zranitelná místa, která by mohla vést ke snížení zabezpečení.

HROZBY

- Malware infikující zařízení ještě před načtením bankovní aplikace nebo následně

OCHRANA

- Kompletní skenování malwaru a zranitelných míst vyhledá před instalací hlavní aplikace případné hrozby a umožní jejich odstranění. Pokud uživatel odmítne odstranit zjištěný škodlivý kód, doporučí se blokáce bankovní aplikace.
- Antivirová komponenta ochrání zařízení v reálném čase a může provést skenování na vyžádání u jakéhokoli nainstalovaného softwaru.

DETEKCE RIZIK

Pro zajištění bezpečného pracovního prostředí ještě před otevřením bankovní aplikace zkontroluje řešení Kaspersky Fraud Prevention SDK veškerá rizika související se zařízením a jeho internetovým připojením.

HROZBY

- Zařízení, kde došlo k rootingu nebo jailbreakingu, a přítomnost neoficiálních či zastaralých verzí firmwaru, které obsahují neopravená zranitelná místa
- Nedůvěryhodné sítě Wi-Fi
- Aplikace, které jsou nebo by mohly být škodlivé

OCHRANA

- Zkontroluje speciální komponenty na eskalovaná uživatelská oprávnění a ověří, zda je veškerý spuštěný firmware opravdu aktuální
- Analýza bezpečnosti sítě Wi-Fi ověří, zda je uživatel připojen k důvěryhodné síti Wi-Fi
- Detekce rizik upozorní bankovní aplikaci na přítomnost veškerých nebezpečných nebo podezřelých aplikací. Aplikace může varovat uživatele a pomoci jim odstranit podezřelý software. Pokud je podezřelý program posouzen jako „vysoce rizikový“, může být bankovní aplikace zablokována, dokud se nebezpečí ze zařízení neodstraní.
- Technologie Device Fingerprinting („otisky prstů zařízení“) umožňuje bankovní aplikaci analyzovat klíčové informace o zařízení (IMEI, IMSI, polohu, telefonní číslo apod.) v rámci vlastních systémů proti podvodům.

OCHRANA MOBILNÍCH PROHLÍŽEČŮ

Většina online bankovních operací vyžaduje přístup k internetu. A to znamená, že potřebují mechanismy, jež mohou zabezpečit výměnu dat mezi zařízením uživatele a systémem online bankovníctví.

HROZBY

- Phishing a nedůvěryhodné weby
- Falšování serveru DNS – útok typu „prostředník“, který přesměruje datový provoz na server útočníka
- Narušení a úprava informací mezi mobilním zařízením a infrastrukturou využívající padělané certifikáty nebo nedůvěryhodné kanály Wi-Fi

OCHRANA

- Komponenty filtrování adres URL a webu kontrolují pověst zdroje podle cloudové databáze. Webová antivirová komponenta kontroluje, zda webová stránka neobsahuje škodlivý kód. Jsou zablokovány zdroje, jež nejsou bezpečné, a uživatel obdrží upozornění.
- Aplikace DNS Checker ověří, zda se doména shoduje s důvěryhodnou IP adresou banky. Pokud je zjištěn nesoulad, relace bankovníctví je ihned ukončena a uživatel obdrží upozornění na problém.
- Komponenta pro ověření platnosti certifikátu zjistí, zda je připojený server autentický. Kontrolují se připojení Wi-Fi a ověřuje se, zda jsou šifrovaná.

OCHRANA DAT A ZPRÁV SMS

Všechny online bankovní systémy musejí se svými uživateli sdílet důležité informace. Tyto údaje mohou být ohrožené, když se odesílají z banky uživateli nebo od uživatele do banky. Řešení Kaspersky Fraud Prevention SDK nabízí ochranu pro oba tyto případy.

HROZBY

- Spyware, který zaznamenává stisknutí kláves a přenáší tyto informace počítačovým zločincům, přičemž může potenciálně umožnit přístup k přihlašovacím údajům
- Narušení a falšování zpráv SMS mezi bankou a klientem, což počítačovým zločincům umožňuje přístup k citlivým informacím nebo nabízí možnost zmanipulovat transakci
- Škodlivé aplikace, jež mohou přistupovat k důležitým údajům v zařízení uživatele

OCHRANA

- Zabezpečená klávesnice a pole pro vstup slouží k ochraně zadávání citlivých údajů
- Zabezpečení SMS rozpozná a přeruší veškeré zprávy z banky. Zprávy lze odstranit z příchozí pošty a bezpečně uložit jinde
- Bezpečné uložení poskytuje chráněný prostor pro uložení citlivých údajů

SEBEOBRANA

Integrované funkce zajišťují, aby malware nemohl narušit práci řešení Kaspersky Fraud Prevention SDK.

HROZBY

- Pokusy o odstranění řešení zabezpečení IT ze zařízení, což by vedlo ke zranitelnosti zařízení vůči útoku
- Úpravy binárního kódu nebo zdrojů aplikace založené na sadě nástrojů pro vývoj softwaru (SDK)
- Zastaralé antivirové databáze, které vystavují zařízení nebezpečí útoku malwaru, který byl odhalen po poslední aktualizaci

OCHRANA

- Řešení Kaspersky Fraud Prevention SDK obsahuje mechanismus zabraňující malwaru v blokování technologií ochrany
- Existuje pět klíčů k prevenci úprav:
 - Použití digitálního certifikátu aplikace založené na sadě nástrojů pro vývoj softwaru (SDK) a spuštění kontroly integrity
 - Opětovné spuštění aplikace, pokud se zastavila
 - Ochrana hlavní aplikace v reálném čase
 - Detekce metod zanesení infekce
 - Vypnutí režimu ladění
- Nástroj pro aktualizaci obnovuje antivirové komponenty nejméně jednou za 24 hodin a zajišťuje, aby byly před použitím aplikace bankovníctví aktuální

Společnost Kaspersky Lab také nabízí kompletní podporu během procesu zavádění. Náš profesionální tým služeb je k dispozici a poradí, jak nejlépe zavést řešení Kaspersky Fraud Prevention SDK, přičemž se postará, aby byla instalace rychlá a bezproblémová.