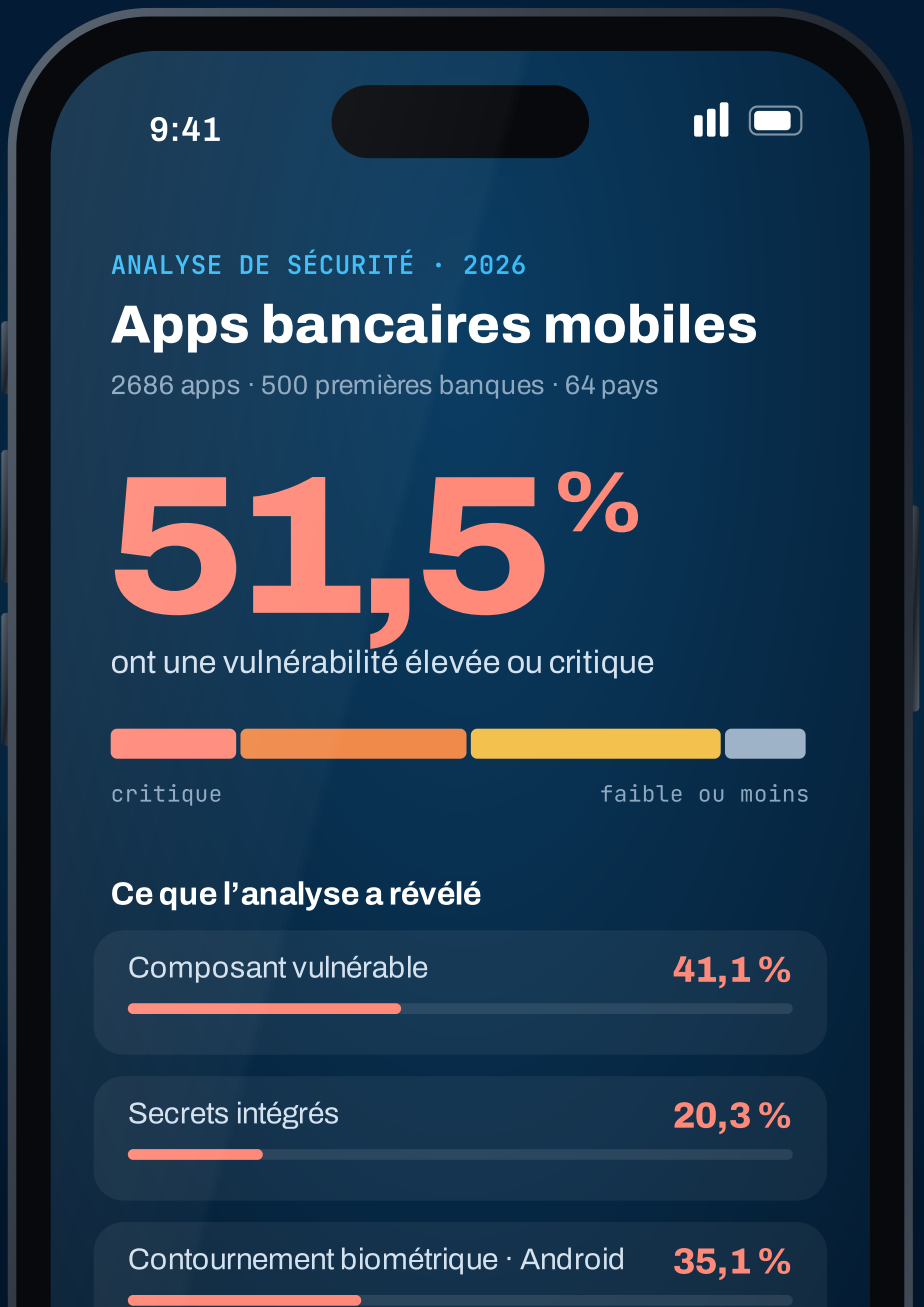
Ostorlab

Rapport 2026 Sécurité des applications bancaires mobiles

Ce que contiennent 2686 applications bancaires des 500 premières banques de 64 pays sur Android, iOS et HarmonyOS, et ce que cela implique pour la fraude.

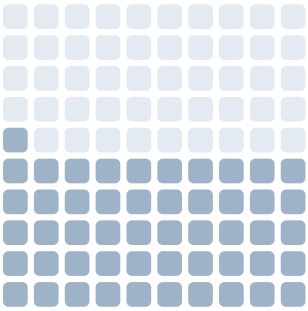


RÉSULTAT CLÉ

Les néobanques indépendantes concentrent les vulnérabilités les plus graves.

Les applications des néobanques sont plus souvent classées à risque élevé ou critique que celles des banques traditionnelles, 61,1 % contre 51,2 %, et tout l'écart vient des néobanques indépendantes. Les néobanques détenues par une banque traditionnelle ressemblent à leur maison mère.

51,2%

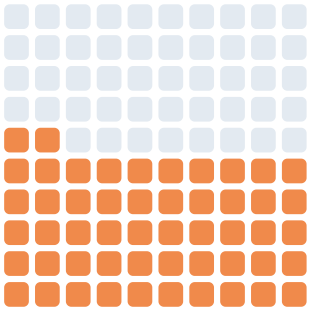


Banques traditionnelles

Banques de réseau, de détail et d'entreprise

2596 APPLICATIONS

52,5%

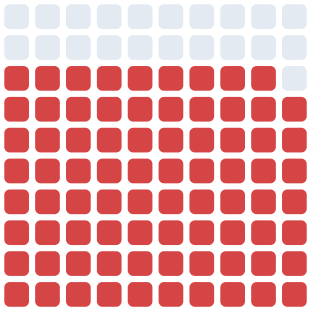


Néobanques détenues par une banque

Marques numériques d'une banque traditionnelle

61 APPLICATIONS

79,3%



Néobanques indépendantes

Banques entièrement numériques, sans maison mère traditionnelle

29 APPLICATIONS

Ce qui explique l'écart

Prise de contrôle OAuth, classée élevée ou critique

6,1 %
24,1 %

Sérialisation non sûre, classée élevée ou critique

6,4 %
17,2 %

Secret intégré hors clés d'API Google

19,8 %
48,3 %

Elles sont pourtant en tête sur les défenses modernes

API clés d'accès intégrée

4,6 %
37,9 %

Attestation d'app ou d'appareil

19,9 %
48,3 %

Biométrie liée à une clé

74,0 %
100,0 %

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

SOMMAIRE

2686 applications, onze chapitres.

Chaque ligne renvoie à sa page.

Résultat clé : les néobanques indépendantes 02

Synthèse 04

Le rapport en neuf chiffres 05

01 Méthodologie 06

2686 applications, de toutes les régions 07

Trois types de données, cinq règles pour chaque chiffre 08

02 Comment sont construites les applications bancaires 09

Les applications web hybrides concentrent le plus de risques 10

Une plateforme, de nombreuses banques 11

Souvent mises à jour, conçues pour d'anciens téléphones 12

Une nouvelle version toutes les 6 à 9 semaines 13

03 Ce que contiennent les applications 14

De l'analytique partout, des SDK antifraude dans peu d'applications 15

La banque IA n'est pas encore dans l'application 16

04 Ce qu'ont révélé les analyses 17

La moitié des applications présente une vulnérabilité grave 18

Les vulnérabilités de code et de confidentialité touchent la plupart des applications 19

Une application sur cinq embarque un secret qui devrait le rester 20

Quatre applications sur dix embarquent une vulnérabilité connue 21

Chaque plateforme a ses propres faiblesses 22

05 Authentification et paiements 23

Le code des clés d'accès est livré, les clés d'accès non 24

Le site de la banque désigne-t-il l'application ? 25

La biométrie est souvent liée à une clé, mais un tiers est contournable 26

06 Protection applicative : ce que contiennent les applications 27

Protections trouvées dans le code 28

Les SDK portent une grande partie des contrôles 29

Peu d'applications superposent leurs défenses 30

07 Au-delà de l'application 31

Domaines bancaires : prêts pour le post-quantique, peu ouverts aux signalements 32

Des étiquettes de confidentialité qui ne correspondent pas à l'application 33

Certains serveurs bancaires répondent au-delà du web 34

Une banque sur six a un incident de sécurité public recensé 35

Les règles auxquelles les banques sont soumises, et ce qu'elles affirment 36

08 Le paysage des menaces 37

Quatre banques sur dix figurent sur la liste d'un cheval de Troie 38

2026 : les attaquants retournent l'application de la banque contre elle 39

Une banque verrait-elle que son application a été remplacée ? 40

Où va l'argent 41

09 Par région, type de banque et pays 42

Aucune région ne coche toutes les cases 43

Résultats par pays 44

Les applications bancaires les plus sûres par région 45

10 Études de cas 46

CyberDakait : sept chevaux de Troie, un appel téléphonique 47

WindRelay : un prêt depuis l'application même de la victime 48

Hirudo : le cheval de Troie qui remplace votre application bancaire 49

Dans la copie, chaque contrôle peut être amené à mentir 50

La clé d'API Google devenue un identifiant d'IA 51

11 Que faire maintenant 52

Ce que les banques doivent faire en 2026 : les 10 priorités 52

A Définitions et notes sur les données 53

Les contrôles qui arrêtent la fraude moderne restent les plus rares.

Cette année, nous avons examiné 2686 applications bancaires mobiles des 500 premières banques de 64 pays. Les banques mettent souvent à jour leurs applications, et la plupart intègrent les protections de base. Celles qui comptent face aux attaques actuelles, comme les clés d'accès, l'attestation et la protection applicative à l'exécution, restent minoritaires.

La moitié des applications présente une vulnérabilité grave

51,5 % des applications ont au moins une vulnérabilité élevée ou critique selon notre analyse automatisée. Seulement 11,8 % n'ont rien au-dessus du niveau faible. Les causes les plus fréquentes sont les secrets intégrés à l'application (20,3 % hors clés d'API Google) et les composants présentant des vulnérabilités connues (41,1 %).

L'authentification forte reste émergente

Seulement 4,9 % des applications intègrent une API de clés d'accès, et 20,2 % utilisent l'attestation d'application ou d'appareil. Sur Android, 35,1 % présentent un parcours biométrique que notre scanner a pu contourner, alors que la plupart des applications qui lient la biométrie le font à une clé.

Les attaquants ciblent désormais l'application elle-même

Des applications de 192 des 500 premières banques figurent sur des listes publiques de cibles de chevaux de Troie bancaires. En 2026, des campagnes comme Hirudo et Gigabud sont allées plus loin en remplaçant ou en clonant de véritables applications bancaires sur le téléphone de la victime. Au Royaume-Uni, la banque mobile a concentré 52 % des pertes liées aux escroqueries au virement autorisé en 2025.

La protection applicative est courante par morceaux, rare dans son ensemble

Sur Android, 69,9 % des applications détectent le root, mais seulement 26,9 % embarquent un produit de protection commercial ou de plateforme. Nos données montrent ce que contiennent les applications, pas leur résistance réelle, qui nécessite des tests sur appareil.

TROIS RÉSULTATS ISSUS DES ANALYSES

51,5%



des applications ont au moins une vulnérabilité élevée ou critique

1384 applications sur 2686

35,1%



des applications Android présentent un parcours biométrique que notre scanner a pu contourner

Applications Android

4,9%



des applications intègrent une API de clés d'accès, le contrôle qui rend inutiles les mots de passe hameçonnés

Le rapport en neuf chiffres.

COMPOSANTS 01

41,1%

des applications embarquent un composant présentant une vulnérabilité connue

1103 applications sur 2686

Chapitre 04 · page 17 →

CLÉS SECRÈTES 02

20,3%

des applications intègrent des secrets tels que des clés d'API, des jetons d'accès ou des clés privées

544 applications sur 2686 ; clés d'API Google exclues

Chapitre 04 · page 17 →

ANCIENS TÉLÉPHONES 03

96%

des applications s'installent sur des versions qui ne reçoivent plus de correctifs de sécurité

Android 99 % · HarmonyOS 100 % · iOS 72 %

Chapitre 02 · page 12 →

ATTESTATION 04

20,2%

des applications utilisent l'attestation d'application ou d'appareil

525 applications sur 2602 au code lisible

Chapitre 05 · page 23 →

PROTECTION APPLICATIVE 05

26,9%

des applications Android embarquent un produit de protection à l'exécution

Produits commerciaux ou de plateforme, applications Android

Chapitre 06 · page 27 →

IA 06

2 applications

font référence à une API de grand modèle de langage ; aucune n'embarque de SDK de LLM, tandis que 28,3 % utilisent du ML embarqué

Sur 2686 applications ; les modèles de codes-barres, de texte et de visages dominent

Chapitre 03 · page 14 →

CHEVAUX DE TROIE 07

38%

des banques ont des applications sur des listes publiques de cibles de chevaux de Troie bancaires

192 des 500 premières banques ; listes publiées pour la plupart de 2021 à 2023

Chapitre 08 · page 37 →

POST-QUANTIQUE 08

71%

des hôtes web bancaires joignables négocient un TLS post-quantique

732 sur 1038 négociations TLS abouties

Chapitre 07 · page 31 →

PERTES LIÉES AUX ESCROQUERIES 09

52%

des pertes liées aux escroqueries au Royaume-Uni en 2025 sont passées par la banque mobile

301,8 M£ sur 576,4 M£ d'escroqueries au virement autorisé (UK Finance)

Chapitre 08 · page 37 →

CHAPITRE 01

01

Méthodologie

Nous avons téléchargé 2686 applications bancaires des 500 premières banques de 64 pays et soumis chacune à l'analyse de sécurité automatisée d'Ostorlab, sur Android, iOS et HarmonyOS.



À l'écran : l'échantillon par pays et par région.

2686

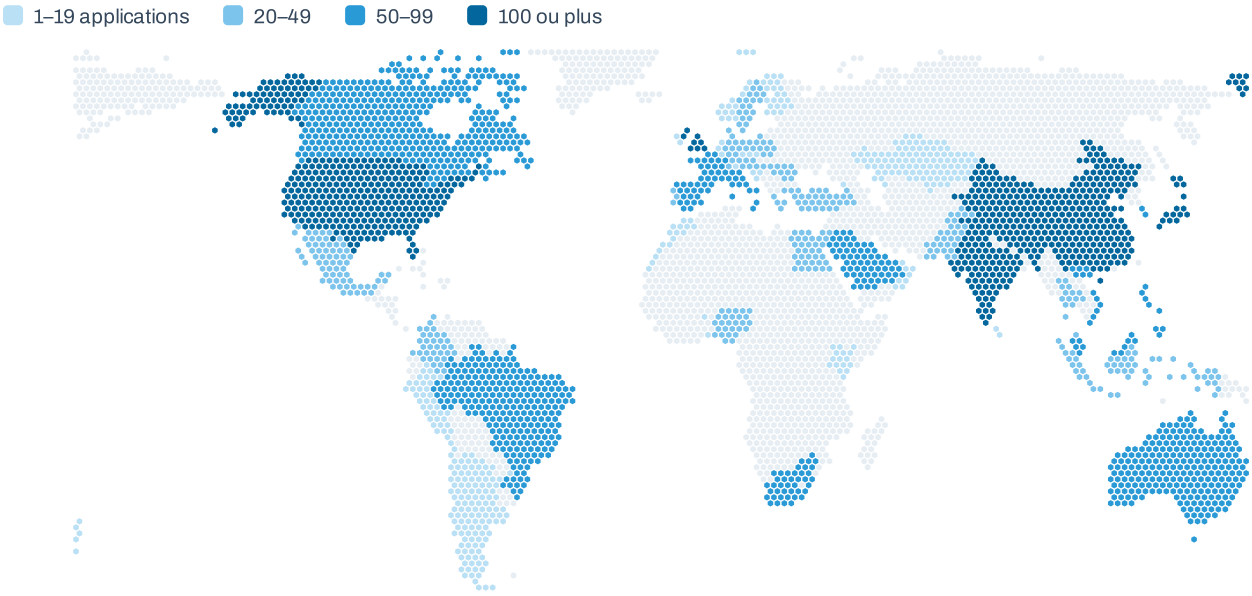
applications des 500 premières banques de 64 pays

2686 applications, de toutes les régions.

L'échantillon couvre 2686 applications des 500 premières banques, dont 29 des banques d'importance systémique mondiale, sur Android, iOS et HarmonyOS.

Des banques de 64 pays, sur tous les continents

FIG. 1,1

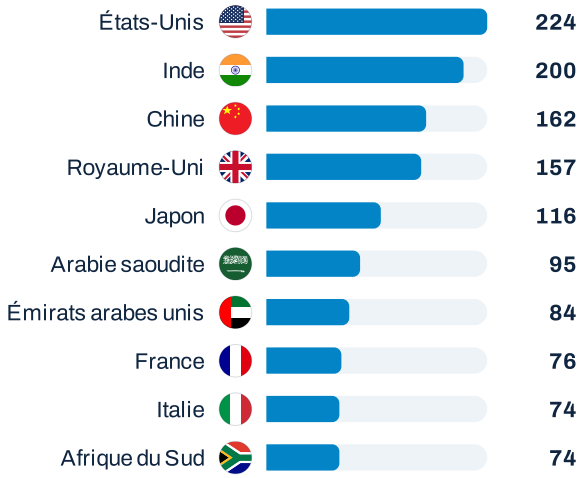


Applications analysées par pays, selon le marché d'origine de la banque. 2841 fiches ont été collectées ; 155 n'ont pas pu être téléchargées.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Les dix principaux marchés

FIG. 1,2

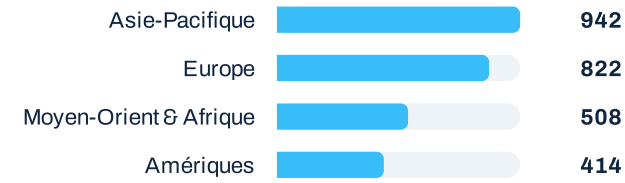


Nombre d'applications, par pays d'origine de la banque.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

L'Asie-Pacifique est la première région

FIG. 1,3



Nombre d'applications, par région d'origine de la banque.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Trois types de données, cinq règles pour chaque chiffre.

Chaque figure de ce rapport provient de l'analyse des applications par Ostorlab, et chaque chiffre suit les mêmes cinq règles, afin que graphiques, texte et légendes concordent.

Inventaire des applications

Recense ce qui compose chaque application : framework, SDK, permissions, protections et hôtes avec lesquels elle communique. Les 2686 applications.

Analyse de sécurité automatisée

Les règles du scanner d'Ostorlab détectent les vulnérabilités, évaluent leur sévérité et les rattachent à l'OWASP MASVS. Les règles diffèrent selon la plateforme. Les 2686 applications.

Signaux de contrôle

Seize vérifications des contrôles d'authentification, de paiement et de confidentialité, chacune avec l'élément de code qui l'a déclenchée. Les 2686 applications.

COMMENT LIRE CHAQUE CHIFFRE

01 **Chaque part indique son dénominateur**

Chaque pourcentage précise, dans la légende sous le graphique, les applications sur lesquelles il a été mesuré.

02 **Les règles propres à une plateforme restent sur leur plateforme**

Une règle qui n'existe que sur Android est rapportée en part des applications Android, jamais de l'ensemble des applications.

03 **Les inconnues sont comptées, pas devinées**

Le code packé ou illisible est exclu du dénominateur d'une vérification, et le nombre d'applications exclues est indiqué.

04 **Les clés d'API Google sont présentées à part**

Google prévoit leur présence dans les applications : le chiffre principal sur les secrets les exclut.

05 **Aucune banque n'est nommée**

Les éléments proviennent d'applications réelles, présentées sans le nom de la banque et avec chaque secret masqué.

Lire les chiffres

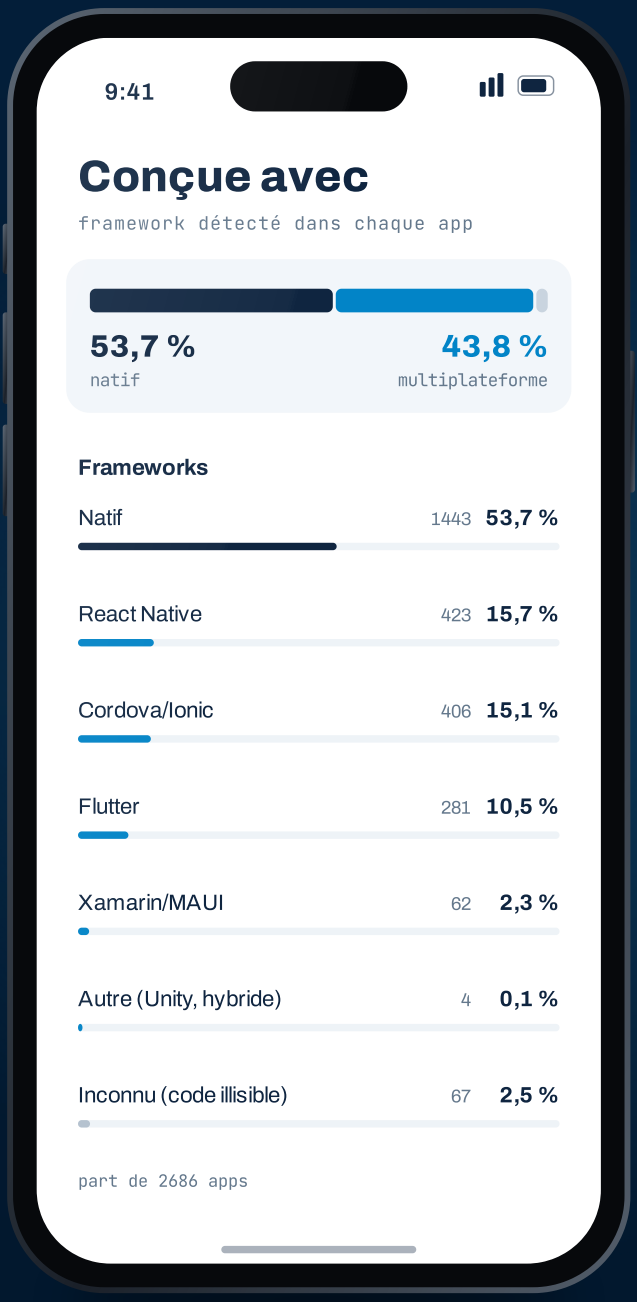
Une vulnérabilité signifie que notre scanner a fait correspondre une règle dans le paquet publié. C'est l'indice qu'un problème est présent, pas la preuve qu'il est exploitable en production. La sévérité suit les niveaux du scanner : critique, élevée, moyenne et faible. Le scanner utilise aussi deux niveaux inférieurs. « Potentiel » signale un motif qui peut être une vraie faille mais qu'une personne doit confirmer, comme une chaîne ayant la forme d'une clé. « Renforcement » signale une protection manquante. Une application reçoit la note de sa vulnérabilité critique, élevée, moyenne ou faible la plus sévère ; les vulnérabilités « potentiel » et « renforcement » ne modifient pas cette note. Lorsqu'un graphique les compte, il le précise.

CHAPITRE 02

02

Comment sont construites les applications bancaires

La plupart des banques développent encore en natif, mais quatre applications sur dix reposent désormais sur un framework multiplateforme. Ce choix se reflète dans les résultats de sécurité.



À l'écran : le framework détecté dans chaque application.

43,8%

des applications reposent sur un framework multiplateforme

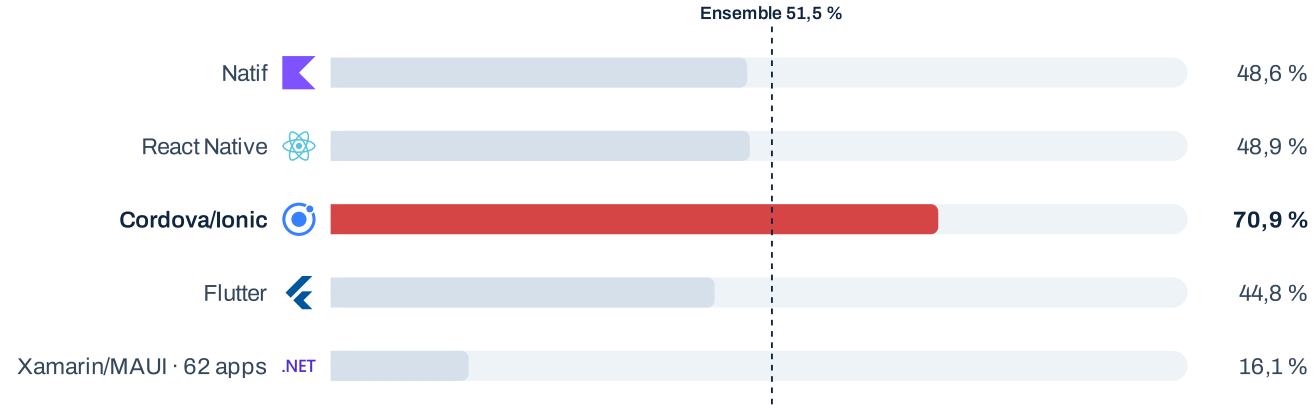
1176 applications sur 2686

Les applications web hybrides concentrent le plus de risques.

Les applications Cordova et Ionic embarquent une application web dans une coque native. Elles représentent 15,1 % de l'échantillon, et 70,9 % d'entre elles présentent une vulnérabilité élevée ou critique, contre 48,6 % des applications natives.

70,9 % des applications Cordova et Ionic présentent une vulnérabilité grave

FIG. 2,1

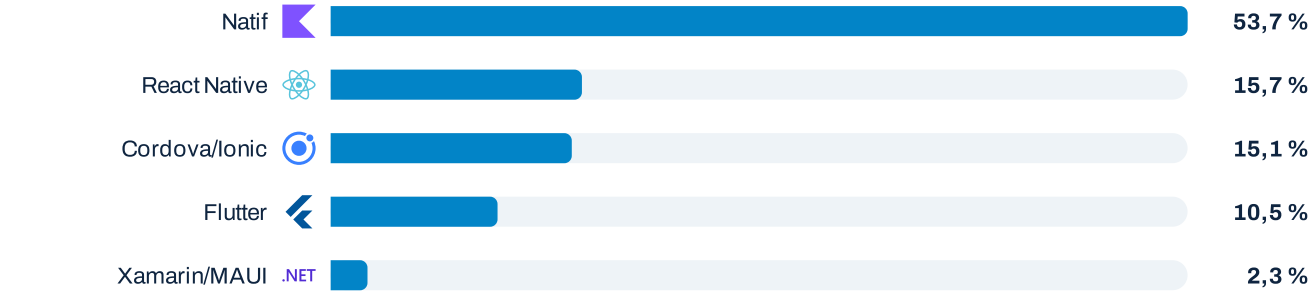


Part des applications de chaque framework avec au moins une vulnérabilité élevée ou critique. Ligne pointillée : les 2686 applications.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Le natif reste majoritaire dans les applications bancaires

FIG. 2,2



Part de 2686 applications par framework ; les 67 au code illisible ne sont pas représentées.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Les applications Cordova et Ionic sont aussi en tête pour les composants vulnérables (72,2 %), surtout des bibliothèques JavaScript obsolètes intégrées à la couche web.

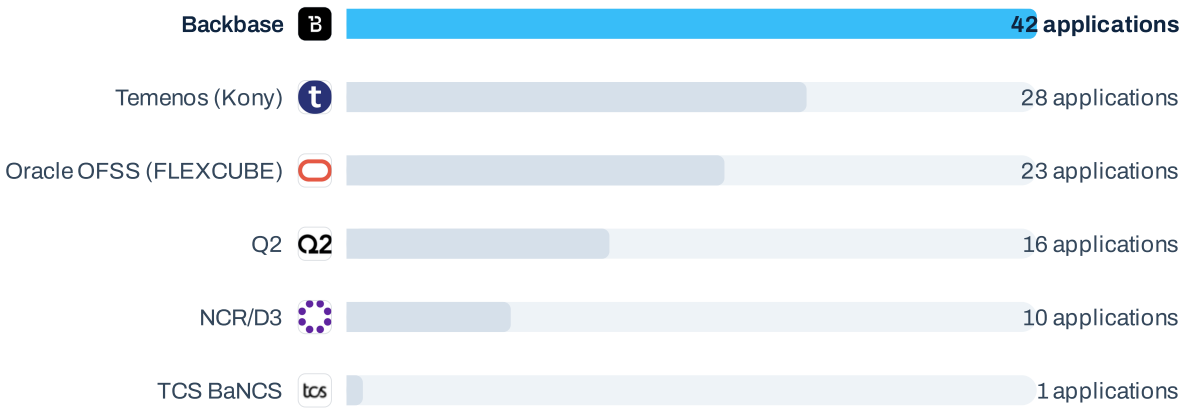
Il n'y a pas de différence nette entre les applications natives (48,6 %), React Native (48,9 %) et Flutter (44,8 %). Les applications Xamarin et MAUI s'en sortent le mieux, mais elles ne forment qu'un petit groupe de 62 applications, et ce sont elles qui intègrent le plus souvent des secrets (43,5 %).

Une plateforme, de nombreuses banques.

Beaucoup de banques n'écrivent pas leur application à partir de zéro : elles prennent la licence d'une plateforme de banque numérique et y apposent leur marque. 120 applications de l'échantillon portent la signature de code de l'une de 6 plateformes de ce type.

Backbase est la plateforme bancaire la plus détectée

FIG. 2,3



Nombre d'applications. 120 applications sur 2602 correspondent à une signature de plateforme connue. Une correspondance exige du code de plateforme reconnaissable : ces chiffres sont donc un minimum.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

> **Lorsqu'une plateforme est partagée, une seule vulnérabilité peut toucher toutes les banques qui l'utilisent.**

Pourquoi c'est important

Une faille dans le code d'une plateforme partagée est une faille dans chaque application construite dessus, et sa correction dépend de la version publiée par l'éditeur, puis de son déploiement par chaque banque. Une seule divulgation peut exposer de nombreuses banques à la fois.

Les bonnes pratiques

Demandez à l'éditeur de la plateforme une nomenclature logicielle (SBOM), les résultats de ses tests de sécurité et un délai de correction convenu. Suivez ses avis de sécurité d'aussi près que les vôtres.

Souvent mises à jour, conçues pour d'anciens téléphones.

Les banques suivent le rythme de la plateforme : 72,1 % des applications Android ciblent la dernière API Android. Mais sur toutes les plateformes, la plupart des applications s'installent encore sur des versions du système d'exploitation qui ne reçoivent plus de correctifs de sécurité.

Sur toutes les plateformes, la plupart des applications s'installent sur des versions non corrigées

FIG. 2,4



Part des applications de chaque plateforme dont la version minimale de l'OS est lisible. Une application est comptée lorsque sa version minimale déclarée est antérieure à la plus ancienne version encore corrigée (Android 14, iOS 18 ; les applications HarmonyOS déclarent une version d'Android). Cela montre ce que l'application autorise, pas ce qu'utilisent les clients.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Prendre en charge d'anciens téléphones est un choix commercial : les clients les conservent. Le risque est que l'application tourne sur un système aux failles connues et non corrigées. Seulement 0,5 % des applications Android refusent les versions non corrigées ; sur iOS, 28,5 % exigent iOS 18 ou une version ultérieure. Les banques peuvent vérifier le niveau de correctif à la connexion et limiter les opérations à haut risque sur les appareils qui ne reçoivent plus de mises à jour.

Version la plus ancienne sur laquelle chaque application peut être installée

FIG. 2,5

Android et HarmonyOS · version d'Android

	Android	HarmonyOS
4 ou antérieure	0,8 %	4,0 %
5	4,4 %	12,8 %
6	5,3 %	7,8 %
7	17,4 %	24,3 %
8	19,5 %	19,5 %
9	13,1 %	13,0 %
10	16,5 %	12,4 %
11	7,0 %	3,4 %
12	12,8 %	2,9 %
13	2,7 %	0,0 %
14 ou ultérieure	0,5 %	0,0 %

iOS · version d'iOS

	iOS
11 ou antérieure	1,8 %
12	2,1 %
13	5,0 %
14	6,5 %
15	27,0 %
16	23,1 %
17	5,9 %
18 ou ultérieure	28,5 %

Part des applications de chaque plateforme selon la plus ancienne version sur laquelle elles s'installent. Une barre correspond exactement à cette version ; une telle application s'installe aussi sur toutes les versions plus récentes. Android 14 et iOS 18 sont les plus anciennes versions encore corrigées.

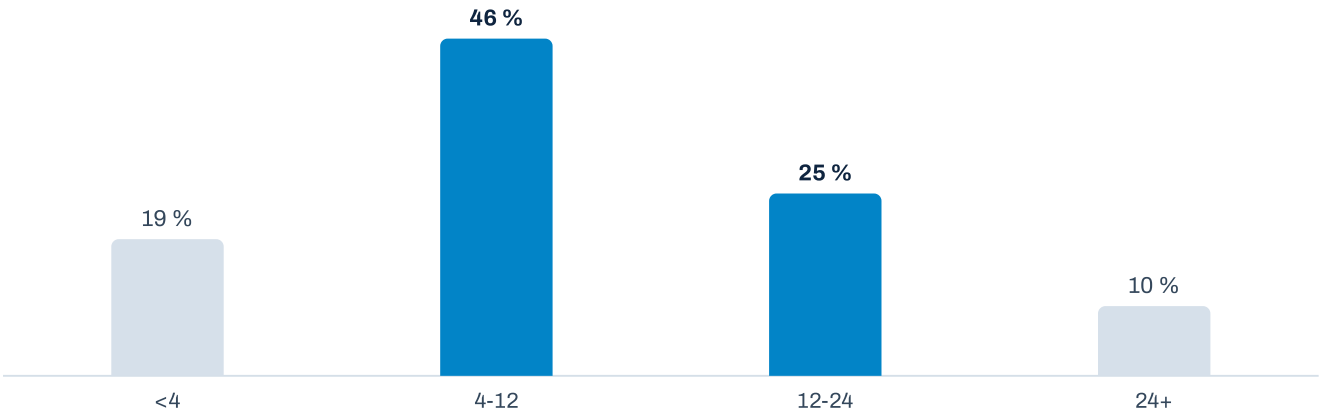
SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Une nouvelle version toutes les 6 à 9 semaines.

L'application Android médiane publie au moins 8,9 versions par an (reconstituées à partir des avis Google Play) et l'application iOS médiane 6,0 (historique des versions de l'App Store). Le store HarmonyOS n'indique que la version actuelle : HarmonyOS n'a donc pas pu être mesuré. Des publications fréquentes sont un atout : c'est ainsi que les correctifs des vulnérabilités décrites dans ce rapport parviennent aux clients.

La plupart des applications publient entre 4 et 24 versions par an

FIG. 2,6



Part des applications Android dont l'historique des versions a été reconstitué à partir des avis Google Play, par nombre de versions par an ; médiane 8,9, une borne inférieure, car les versions sans avis échappent au décompte. iOS : médiane 6,0, d'après l'historique des versions de l'App Store.

SOURCE Fiches et avis Google Play et App Store, collectés pour ce rapport.

75,1 %
des applications Android dotées d'une date de mise à jour sur Google Play ont été mises à jour au cours des 90 derniers jours

6,8 %
n'ont pas été mises à jour depuis un an

3,8 Md
installations Google Play cumulées pour les applications Android, au minimum

Taille

La taille médiane de téléchargement est de 68 Mo sur Android, 38 Mo sur iOS et 129 Mo sur HarmonyOS. La moitié des bibliothèques natives de ces applications proviennent de SDK tiers connus, et seulement 4 % peuvent être rattachées à la banque elle-même. Le code tiers fait l'objet du chapitre suivant.

Publications rapides, composants anciens

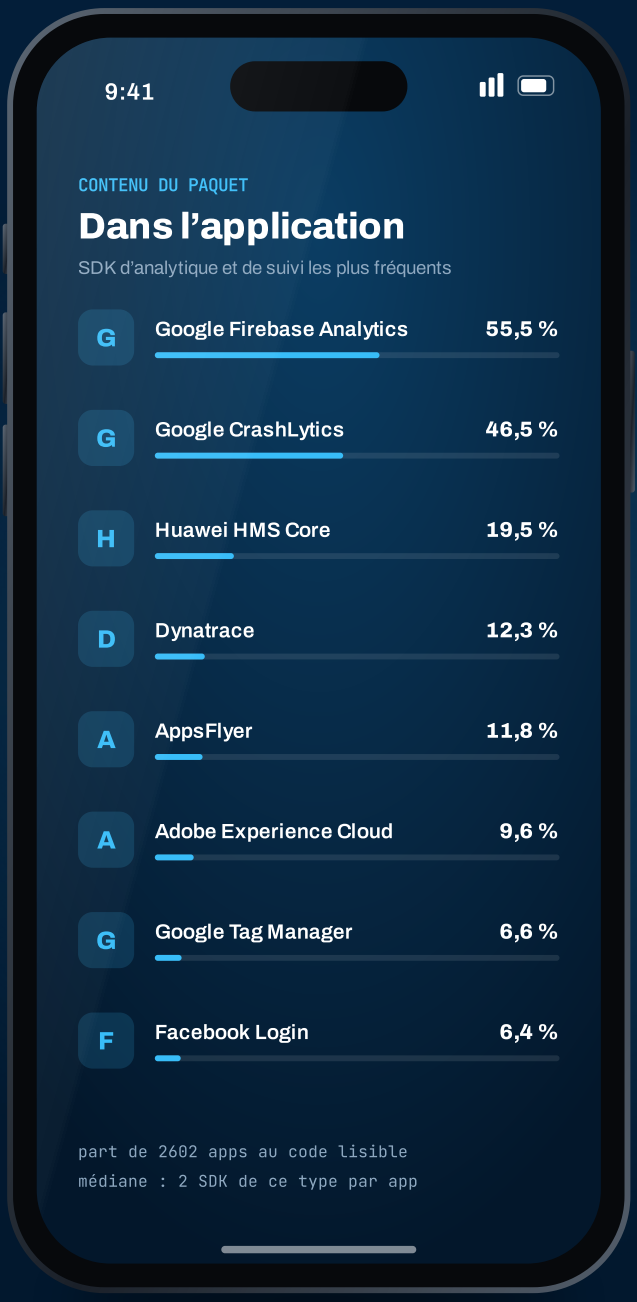
Publier souvent ne maintient pas chaque élément à jour. Comme le montre le chapitre 4, 41,1 % des applications embarquent encore un composant présentant une vulnérabilité connue.

CHAPITRE 03

03

Ce que contiennent les applications

Une application bancaire est surtout faite du code des autres : analytique, rapports de plantage, détection de fraude, cartographie, scanners. Chaque SDK apporte ses propres flux de données et ses propres vulnérabilités.



À l'écran : les SDK d'analytique et de suivi les plus fréquents.

80,6%

des applications au code lisible embarquent au moins un SDK d'analytique ou de suivi

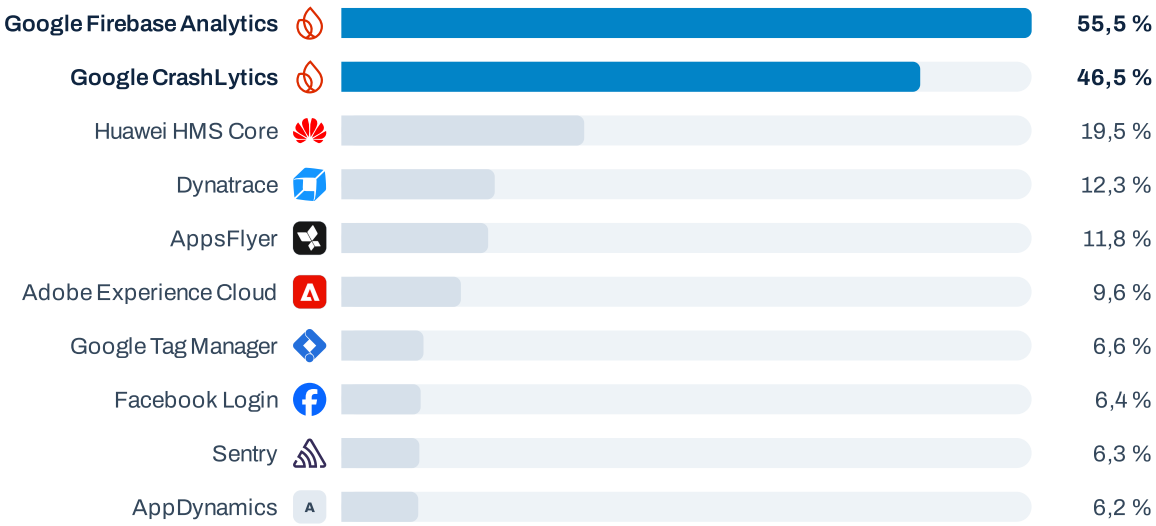
2096 applications sur 2602

De l’analytique partout, des SDK antifraude dans peu d’applications.

Firebase Analytics de Google est présent dans 55,5 % des applications. Les SDK dédiés à la fraude et au risque appareil, que les banques utilisent pour repérer en temps réel les prises de contrôle de compte, n’apparaissent que dans 12,1 %.

Firebase Analytics et Crashlytics de Google dominent les traceurs

FIG. 3,1

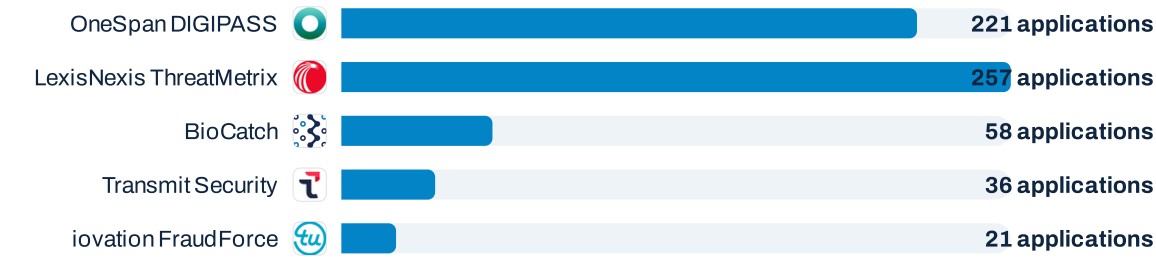


Part de 2602 applications au code lisible. Signatures de traceurs issues de la base Exodus Privacy. Huawei HMS Core est présent dans 64 % des applications HarmonyOS ; il couvre les services Huawei de notifications push, de localisation et d’analytique.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Les SDK de sécurité spécialisés touchent peu d’applications

FIG. 3,2



Nombre d’applications. SDK d’authentification : 9,3 % des applications. SDK de fraude et de risque appareil : 12,1 %.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

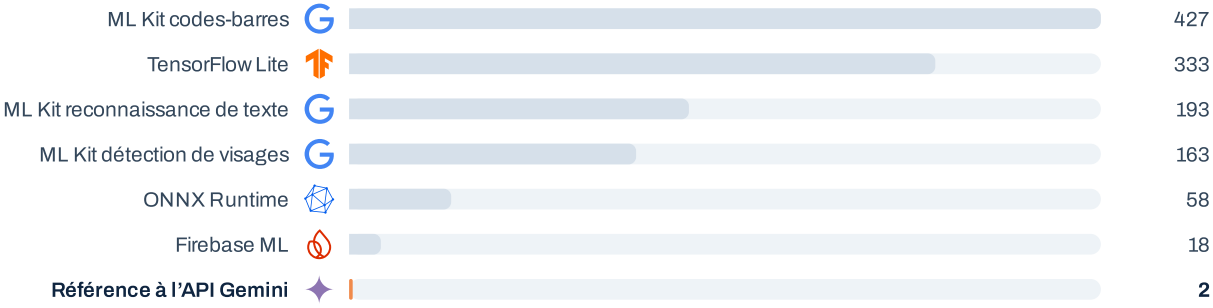
Les SDK spécialisés se concentrent dans les applications iOS : 35,3 % des applications iOS embarquent un SDK de fraude ou de risque appareil, contre 8,8 % sur Android. Plusieurs éditeurs servent de nombreuses banques : leur sécurité compte donc bien au-delà d’une seule application.

La banque IA n’est pas encore dans l’application.

28,3 % des applications embarquent de l’apprentissage automatique sur l’appareil, presque entièrement pour lire des codes-barres, des documents et des visages. Aucune application n’embarque de SDK de grand modèle de langage : 2 applications sur 2686 font référence à une API de LLM, et nous n’avons trouvé aucune clé de fournisseur d’IA intégrée dans une application.

Le ML embarqué lit codes-barres, texte et visages

FIG. 3,3

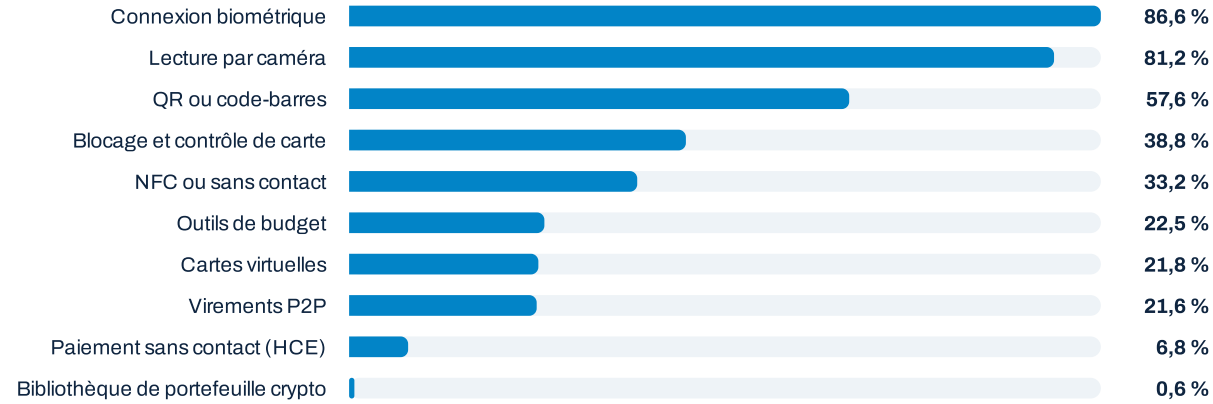


Nombre d’applications. Référence à l’API Gemini : l’application mentionne le point de terminaison de l’API Gemini ; aucune application n’embarque de SDK de LLM. Les fonctions de LLM peuvent tourner entièrement sur les serveurs de la banque et n’apparaîtraient alors pas dans l’application.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

La connexion biométrique et la lecture par caméra sont quasi universelles

FIG. 3,4



Part de 2686 applications. Détection à partir du code, des ressources et des permissions ; une fonction présente dans le code peut être désactivée. Bibliothèque de portefeuille crypto/monnaie numérique : comptée lorsque le code de l’application embarque une bibliothèque de portefeuille ou de blockchain ; cela ne montre pas que l’application propose le trading de cryptomonnaies.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Les applications dotées d’un SDK de chatbot ou d’assistant virtuel intègrent plus souvent des secrets

FIG. 3,5



Part des applications avec au moins un secret intégré hors clés d’API Google. Un SDK de chatbot est une bibliothèque de chatbot ou d’assistant virtuel fournie par un éditeur, comme Dialogflow, Kore.ai, Kasisto ou Watson Assistant, et non un grand modèle de langage ; seules 2 applications mentionnent l’API Gemini, et aucune n’embarque de SDK de chatbot. Les grandes banques en utilisent plus souvent et embarquent davantage de SDK : c’est une corrélation, pas une causalité.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

CHAPITRE 04

04

Ce qu'ont révélé les analyses

L'analyse automatisée d'Ostorlab a trouvé au moins une vulnérabilité élevée ou critique dans la moitié des applications. Les secrets intégrés et les composants obsolètes arrivent en tête, suivis de problèmes propres à chaque plateforme.



À l'écran : le rapport d'analyse d'une application réelle de l'échantillon.

18,4%

des applications ont au moins une vulnérabilité critique

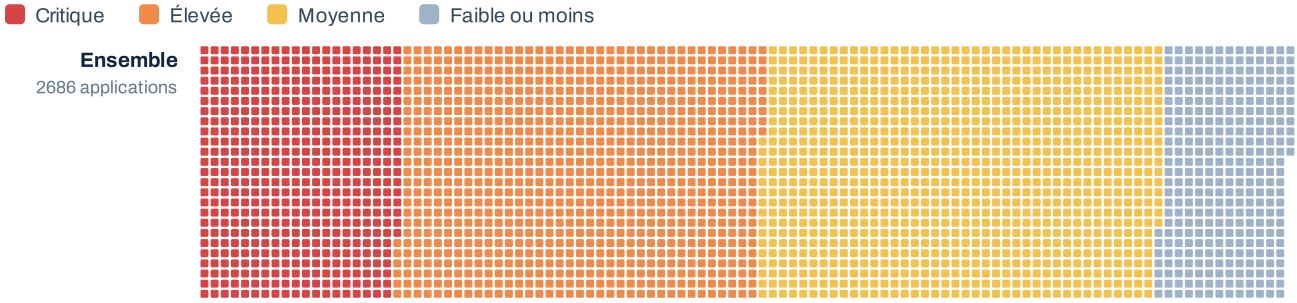
494 applications sur 2686

La moitié des applications présente une vulnérabilité grave.

Chaque application reçoit la note de sa vulnérabilité la plus sévère. Sur Android, 54,2 % ont au moins une vulnérabilité élevée ou critique ; sur iOS, 36,2 %. Les applications HarmonyOS ont le plus de vulnérabilités critiques, à 31,6 %, en raison de composants obsolètes.

Chacune des 2686 applications, selon sa vulnérabilité la plus sévère

FIG. 4,1

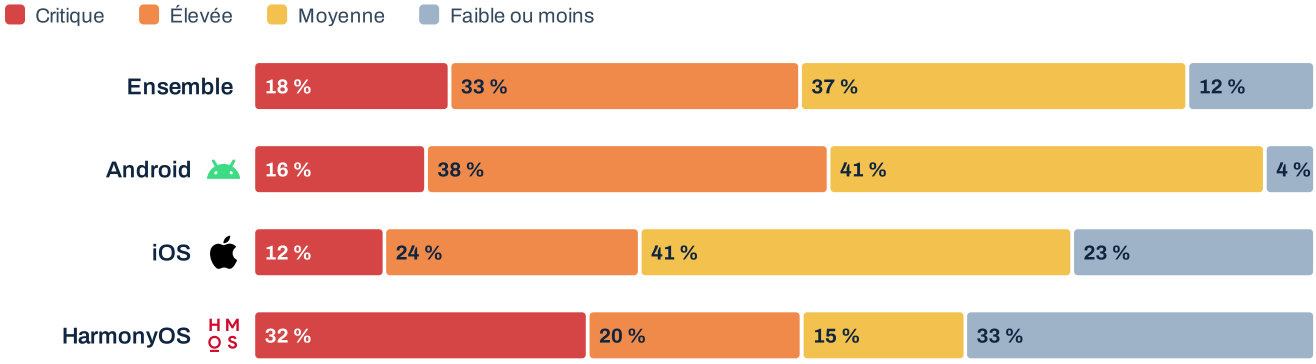


Un carré par application, trié par sévérité. « Faible ou moins » inclut les applications dont la pire vulnérabilité est faible, « potentiel » ou « renforcement », et celles sans aucune vulnérabilité.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Les applications HarmonyOS ont le plus de vulnérabilités critiques

FIG. 4,2



Part des applications selon leur vulnérabilité la plus sévère. Les 2686 applications. « Faible ou moins » inclut les applications dont la pire vulnérabilité est faible, « potentiel » ou « renforcement », et celles sans aucune vulnérabilité. La part plus forte de « faible ou moins » sur iOS et HarmonyOS reflète en partie le nombre réduit de règles du scanner sur ces plateformes.

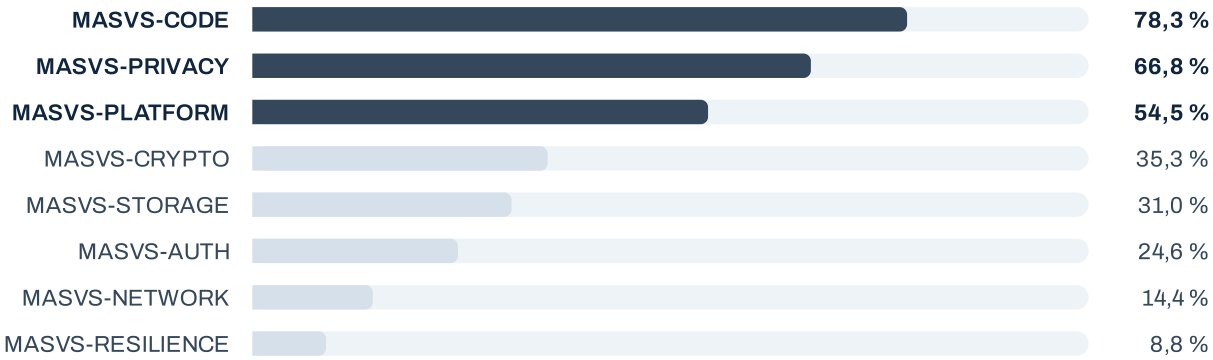
SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Les vulnérabilités de code et de confidentialité touchent la plupart des applications.

La plupart des vulnérabilités se rattachent à un groupe de contrôles de l'OWASP MASVS, le standard du secteur pour la sécurité des applications mobiles. En comptant les vulnérabilités critiques, élevées, moyennes et faibles, les vulnérabilités de code apparaissent dans 78,3 % des applications et celles de confidentialité dans 66,8 %. Les applications iOS et HarmonyOS ne présentent aucune vulnérabilité de cryptographie ou d'authentification, ce qui fait baisser ces groupes.

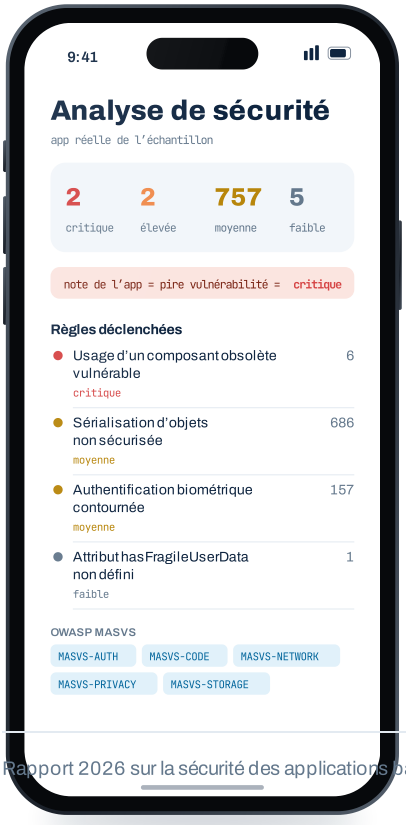
Part des applications avec une vulnérabilité dans chaque groupe de contrôles de l'OWASP MASVS

FIG. 4,3



Part de 2686 applications avec au moins une vulnérabilité critique, élevée, moyenne ou faible dans chaque groupe. Les vulnérabilités « potentiel » et « renforcement » sont exclues. 15 % des vulnérabilités Android ne se rattachent à aucun groupe.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.



UNE APPLICATION, TELLE QUE LE SCANNER LA PRÉSENTE

766 vulnérabilités, une seule note

Cette application Android de l'échantillon présente 2 vulnérabilités critiques, 2 élevées, 757 moyennes et 5 faibles. Comme toutes les applications de ce rapport, elle reçoit la note de sa pire vulnérabilité : **critique**.

Une règle peut se déclencher de nombreuses fois dans une même application. Le nombre de vulnérabilités moyennes est élevé car une seule règle de sérialisation a correspondu à des centaines d'appels ; cela reste un seul problème à corriger.

Le scanner a aussi signalé 98 éléments « potentiel » et 2 éléments « renforcement ». « Potentiel » signale un motif qui peut être une vraie faille mais qu'une personne doit confirmer ; « renforcement » signale une protection manquante. Aucun des deux ne modifie la note de l'application.

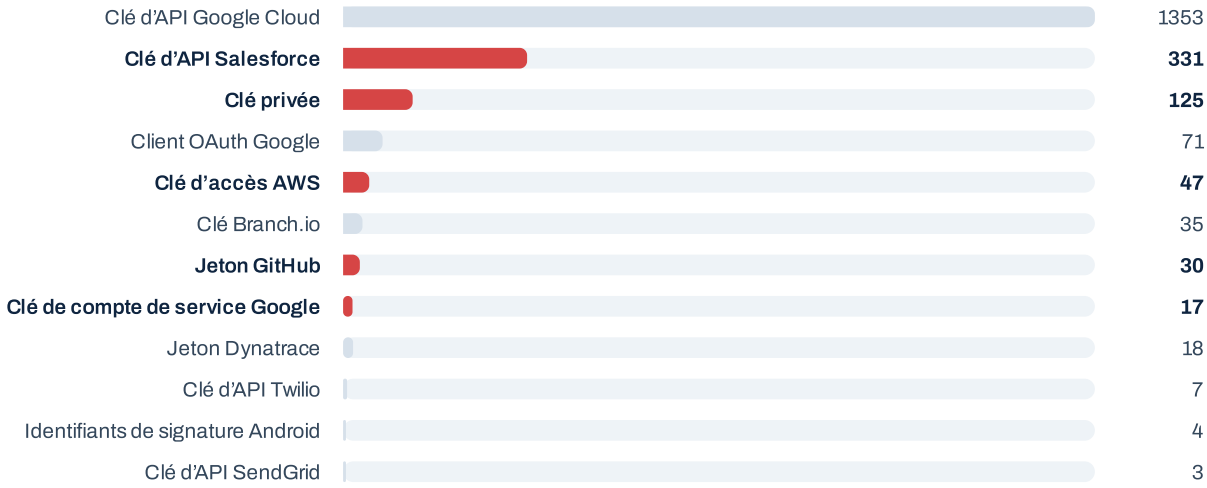
MASVS-AUTH-2 MASVS-CODE-1 MASVS-CODE-3 MASVS-CODE-4 MASVS-NETWORK-1 MASVS-PRIVACY-1 MASVS-PRIVACY-3 MASVS-PRIVACY-4 MASVS-STORAGE-1 MASVS-STORAGE-2

Une application sur cinq embarque un secret qui devrait le rester.

59,8 % des applications contiennent au moins un secret dans un format reconnaissable. La plupart sont des clés d'API Google, que Google conçoit pour être livrées dans les applications : elles identifient un projet pour des services comme Maps et Firebase, et sont protégées par des restrictions définies dans le projet cloud (signature de l'application, API autorisées), non par le secret. Nous n'avons pas vérifié si les clés sont restreintes. Hors clés Google, 20,3 % des applications livrent encore des clés privées, des clés cloud et des jetons d'accès (Android 18 %, iOS 21 %, HarmonyOS 28 %).

Après les clés d'API Google, les clés Salesforce et les clés privées dominent

FIG. 4,4



Nombre d'applications dans lesquelles les règles du scanner sur les secrets ont signalé chaque type ; une application peut en contenir plusieurs. Une recherche dans l'ensemble du paquet, une méthode différente, trouve une clé d'API Google dans 80 % des applications Android, 71 % des applications HarmonyOS et 31 % des applications iOS (page 51).

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.



Analyse réelle d'une application de l'échantillon ; valeurs masquées

> **N'importe qui peut télécharger une application bancaire et lire ce qu'elle contient.**

LE PAQUET D'UNE APPLICATION

Cette application Android embarque 4 types de secrets candidats, dont une clé d'API Google, un DSN Sentry, une adresse de base de données Firebase et des jetons signés. Chacun est lisible par toute personne qui télécharge l'application.

Une clé d'API Google peut obtenir de nouveaux accès après la publication de l'application : voir l'étude de cas page 51.

Les bonnes pratiques

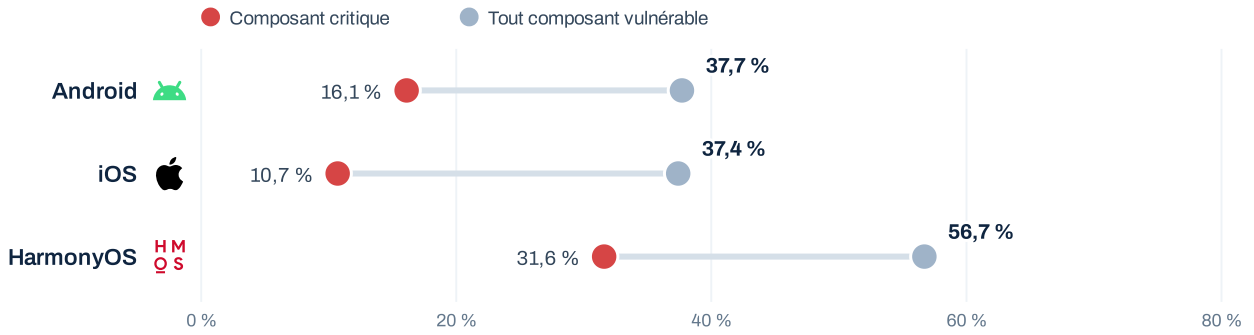
Conservez les secrets sur le serveur et délivrez à l'application des jetons à courte durée de vie. Lorsqu'une clé doit être livrée, comme pour Google Maps, restreignez-la à la signature de l'application et aux API nécessaires, puis surveillez son utilisation.

Quatre applications sur dix embarquent une vulnérabilité connue.

41,1 % des applications incluent un composant tiers présentant une vulnérabilité publiée, et 18,2 % un composant dont la vulnérabilité est classée critique. Les applications HarmonyOS sont les plus touchées.

Les applications HarmonyOS embarquent le plus de composants vulnérables

FIG. 4,5

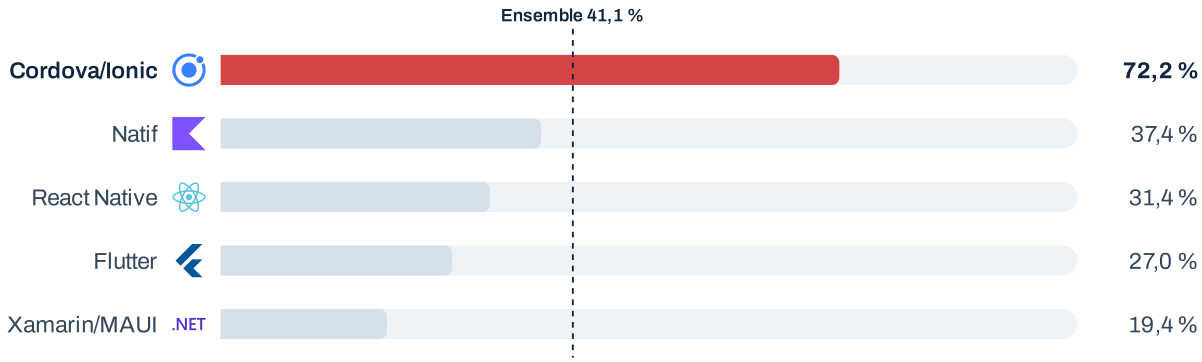


Part des applications sur chaque plateforme. L'étiquette indique la part avec un composant vulnérable, quel qu'il soit.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

72,2 % des applications Cordova et Ionic embarquent un composant vulnérable

FIG. 4,6



Part des applications de chaque framework. Ligne pointillée : les 2686 applications.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Pourquoi le problème persiste

Les composants sont entraînés par d'autres composants. Une banque peut mettre à jour son propre code chaque mois et livrer quand même une bibliothèque vieille de plusieurs années au sein d'un SDK qu'elle ne contrôle pas.

Les bonnes pratiques

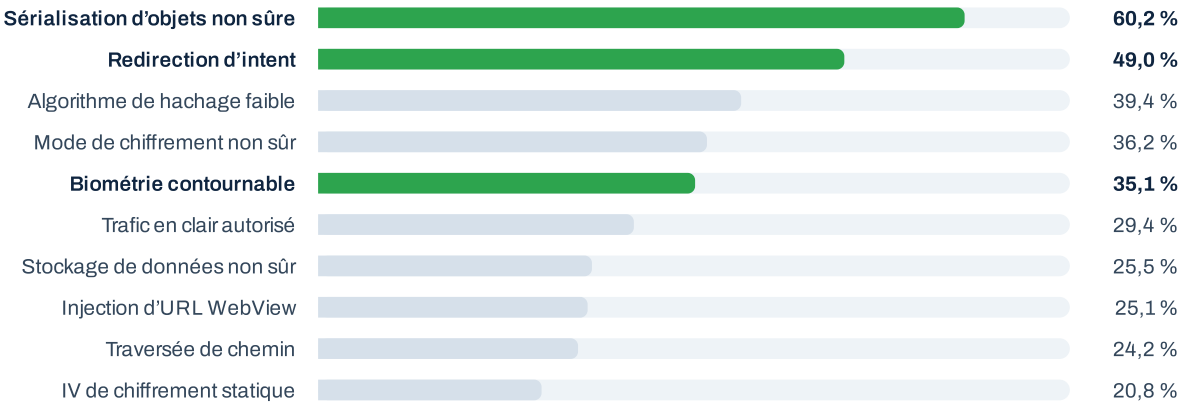
Tenez une nomenclature logicielle (SBOM) pour chaque version, suivez les avis de sécurité qui la concernent et fixez un délai de correction pour les composants critiques. Exigez la même chose des éditeurs de SDK.

Chaque plateforme a ses propres faiblesses.

De nombreuses règles d'analyse n'existent que pour une seule plateforme : nous comparons donc les applications au sein d'une même plateforme. Sur Android, les problèmes au niveau du code dominent. Sur iOS, les principaux problèmes relèvent de la configuration. Sur HarmonyOS, les composants anciens et le code web arrivent en tête.

Android : la sérialisation et la redirection d'intents en tête

FIG. 4,7

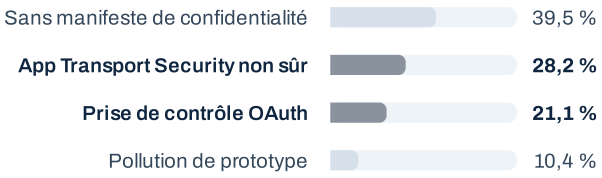


Part des applications Android. Règles propres à Android.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

iOS : les problèmes de configuration en tête

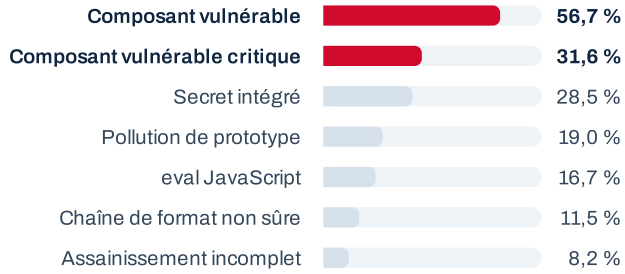
FIG. 4,8



Part des applications iOS. Les liens universels empêchent la prise de contrôle OAuth, dans laquelle une autre application s'approprie la redirection de connexion.

HarmonyOS : les composants anciens et le code web en tête

FIG. 4,9



Part des applications HarmonyOS.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

CHAPITRE 05

05

Authentification et paiements

Les clés d'accès, l'attestation et la biométrie liée à une clé rendent les mots de passe volés et les applications falsifiées bien moins utiles. Elles se diffusent, lentement.



À l'écran : illustration d'une invite de clé d'accès, pas une application réelle.

4,9%

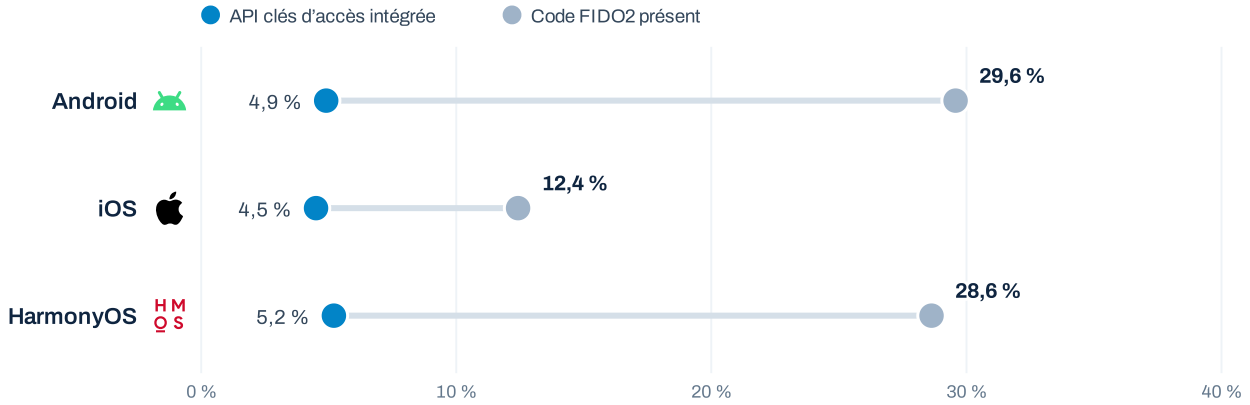
des applications intègrent une API de clés d'accès

Le code des clés d'accès est livré, les clés d'accès non.

Près d'un tiers des applications Android contiennent du code FIDO2 ou WebAuthn, mais seulement 4,9 % appellent une API de clés d'accès. Sur iOS, c'est le cas de 4,5 %. Ce code peut arriver au sein d'autres bibliothèques sans que la fonction soit activée.

Le code FIDO2 est courant, les API de clés d'accès sont rares

FIG. 5,1



Part des applications sur chaque plateforme. API de clés d'accès intégrée : l'application appelle Credential Manager, l'API FIDO2 de Google ou les API de clés d'accès d'Apple.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

79,8 % des applications n'utilisent aucune attestation

FIG. 5,2

	Forte	Faible seule	Aucune
Android	16,0 %	2,8 %	81,2 %
Forte : Play Integrity · Faible : SafetyNet seul (obsolète)			
iOS	3,6 %	17,2 %	79,2 %
Forte : App Attest · Faible : DeviceCheck, sans App Attest confirmé			
HarmonyOS	20,9 %	4,5 %	74,5 %
Forte : Play Integrity 13,4 %, HMS Safety Detect 7,5 % · Faible : SafetyNet seul (obsolète)			

Part des applications au code lisible sur chaque plateforme. Forte : le serveur de la banque peut vérifier l'application et l'appareil. Faible seule : une vérification plus ancienne ou limitée à l'appareil, sans vérification forte à côté. App Attest et DeviceCheck sont des services d'Apple ; Play Integrity et SafetyNet sont ceux de Google ; HMS Safety Detect est celui de Huawei.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

L'attestation permet au serveur de la banque de vérifier qu'une requête provient de son application authentique sur un appareil authentique. C'est la principale défense contre les applications reconditionnées comme Hirudo, et pourtant 79,8 % des applications ne l'utilisent pas. L'application ne permet pas de voir si les serveurs appliquent le résultat.

Le site de la banque désigne-t-il l'application ?

Les clés d'accès et les liens d'application ne fonctionnent que si le site web de la banque désigne l'application. Nous avons lu le fichier d'association public de chaque banque et vérifié s'il mentionne l'application.

Peu de sites bancaires désignent leur application pour les identifiants enregistrés et les clés d'accès

FIG. 5,3



Part des applications sur chaque plateforme dont le site web de la banque autorise l'application à partager les identifiants enregistrés et les clés d'accès. Lu dans les fichiers apple-app-site-association et assetlinks.json des domaines bancaires.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

16 %

des applications iOS appartiennent à une banque dont le fichier mentionne aussi des identifiants d'applications de test

92

des 226 domaines bancaires dotés d'un fichier d'association Apple mentionnent des identifiants d'applications hors production

88

des 217 domaines bancaires dotés d'un fichier Android asset links mentionnent des packages hors production



Le fichier d'une banque, tel que notre vérification l'a lu

LE FICHIER D'ASSOCIATION D'UNE BANQUE

Le fichier de la banque désigne son application iOS pour les liens universels : les liens vers le site de la banque ouvrent donc l'application. Il ne la désigne pas pour les identifiants web : l'application ne peut donc pas proposer les clés d'accès de la banque. Il mentionne aussi 4 identifiants d'applications de test à côté de l'application de production.

Une question d'hygiène, pas une vulnérabilité

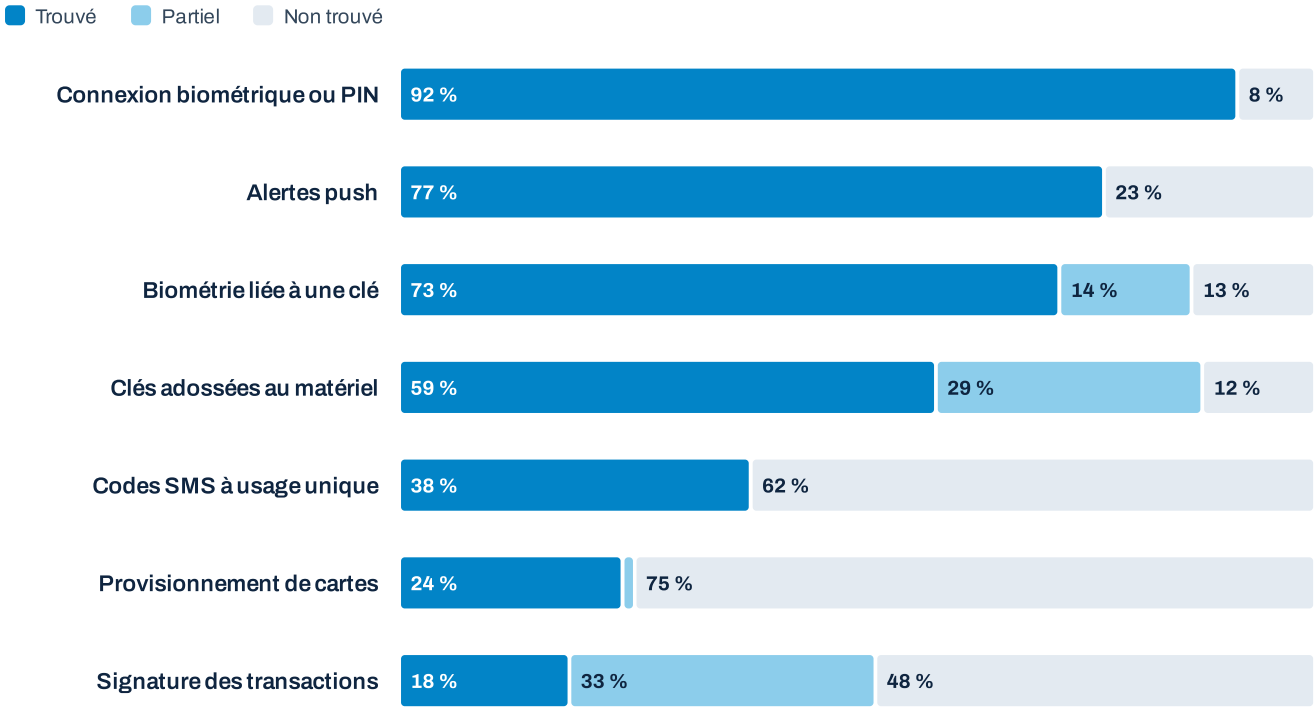
Seules les applications signées par la banque peuvent utiliser ces entrées. Mais un fichier de production qui mentionne des versions de test révèle à tous les identifiants de build internes de la banque, et maintient les liens et les identifiants fonctionnels pour des versions que les clients ne devraient jamais utiliser. Le manque le plus important reste l'entrée absente : sans elle, une application ne peut pas proposer de clés d'accès du tout.

La biométrie est souvent liée à une clé, mais un tiers est contournable.

Lorsque nous avons pu déterminer comment une application Android utilise la biométrie, 73,2 % lient la vérification à une clé cryptographique, et 11,4 % la traitent comme une simple réponse oui/non qu'un logiciel malveillant peut falsifier. Notre scanner a aussi trouvé un parcours biométrique contournable dans 35,1 % des applications Android. Par ailleurs, un tiers des applications Android et la plupart des applications iOS prennent en charge les codes à usage unique par SMS, cible des attaques par SIM swapping.

Comment les applications connectent les utilisateurs et valident les paiements

FIG. 5,4



Part de 2686 applications, toutes plateformes confondues. Trouvé : éléments de code nets. Partiel : une partie seulement des éléments. L'attestation et les SDK antifraude sont traités pages 24 et 15.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Biométrie contournable

Un parcours contournable peut coexister, dans une même application, avec une biométrie liée à une clé utilisée ailleurs. Chaque action sensible devrait passer par le parcours lié à la clé, afin qu'un « oui » falsifié ne déverrouille rien.

Codes SMS et SIM swapping

Dans une attaque par SIM swapping, un fraudeur convainc l'opérateur mobile de transférer le numéro de la victime vers une carte SIM qu'il contrôle. Chaque code à usage unique envoyé par SMS parvient alors à l'attaquant, et non au client. Les codes liés à l'appareil et à la transaction ne transitent pas par SMS.

CHAPITRE 06

06

Protection applicative : ce que contiennent les applications

La protection applicative à l'exécution détecte les téléphones rootés, les débogueurs, les outils de hooking et les copies falsifiées de l'application. Nous avons recherché ces protections dans le code de chaque application, sur les trois plateformes.



À l'écran : illustration d'une application protégée sur un téléphone rooté.

26,9%

des applications Android embarquent un produit de protection applicative commercial ou de plateforme

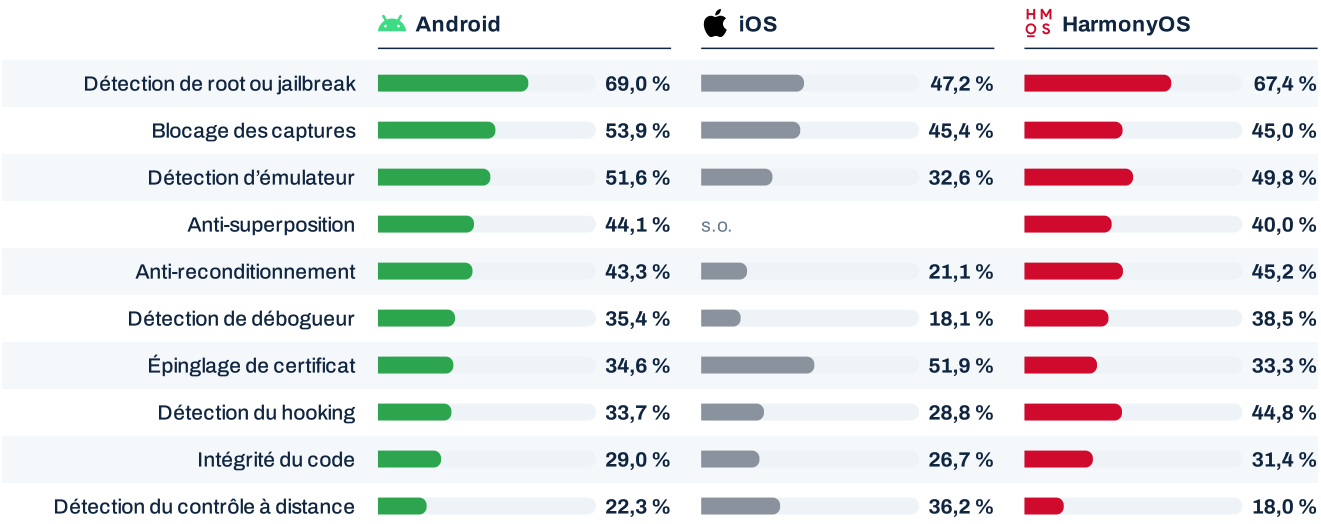
Applications Android

Protections trouvées dans le code.

Sur toutes les plateformes, la plupart des applications vérifient au moins si le téléphone est rooté ou jailbreaké. Bien moins nombreuses sont celles qui détectent les outils de hooking, la falsification ou le contrôle à distance : 22,3 % des applications Android et 36,2 % des applications iOS contiennent du code détectant le partage d'écran ou le contrôle à distance, que les chevaux de Troie utilisent pour frauder depuis le téléphone même de la victime.

La détection du root est courante, celle du hooking et du contrôle à distance ne l'est pas

FIG. 6,1



Part des applications dont la vérification est appelée depuis le code propre de la banque ou un code non attribué, sur chaque plateforme. Tri selon la part Android. s.o. : la protection anti-superposition ne s'applique pas sur iOS, où aucune application ne peut s'afficher par-dessus une autre.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

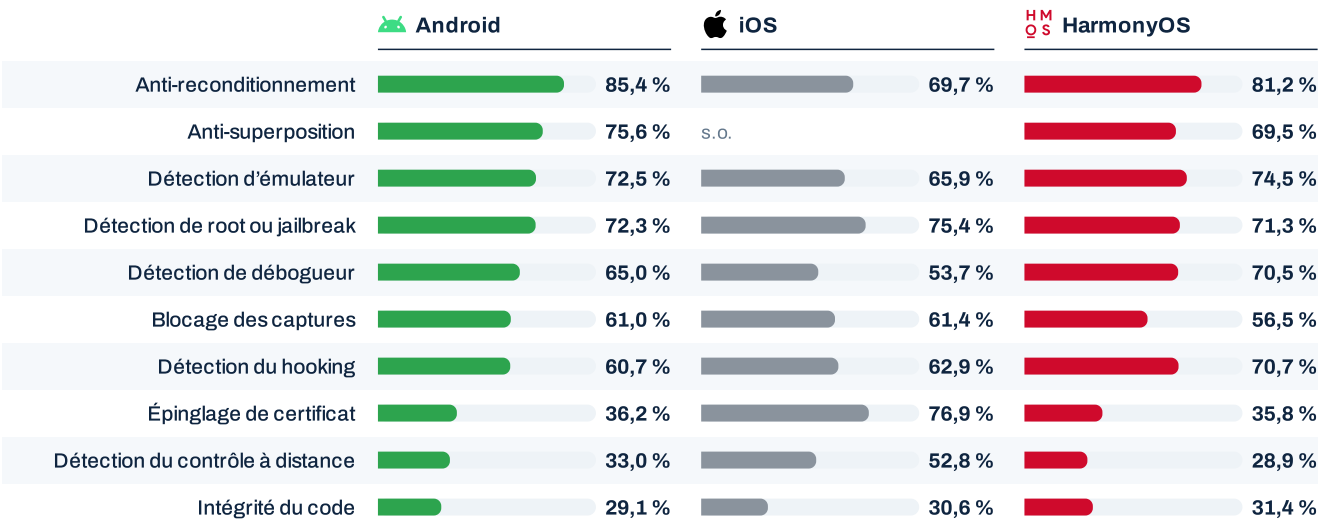
Présente ne veut pas dire efficace

Ces résultats montrent qu'une protection existe dans l'application. Ils ne montrent pas qu'elle résiste à un attaquant qui la connaît. Le vérifier nécessite des appareils réels et est prévu pour une prochaine édition. Considérez ces chiffres comme un plafond de protection.

Les SDK portent une grande partie des contrôles.

En comptant les contrôles présents dans un SDK intégré en plus du code propre de la banque, 85,4 % des applications Android comportent des contrôles anti-reconditionnement, mais seulement 33 % une détection du contrôle à distance, le contrôle qui compte le plus face aux chevaux de Troie d'accès à distance.

Les contrôles anti-reconditionnement sont répandus ; les contrôles d'intégrité du code sont rares sur toutes les plateformes FIG. 6,2



Part des applications de chaque plateforme. Trouvé : le contrôle est dans l'application, dans le code propre de la banque ou dans un SDK intégré. s.o. : les attaques par superposition ne s'appliquent pas sur iOS. Un contrôle présent dans un SDK ne protège l'application que si la banque l'active.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Peu d'applications superposent leurs défenses.

La protection applicative fonctionne mieux en couches, afin que le contournement d'un contrôle ne désactive pas les autres. L'application Android médiane présente des éléments nets pour 4 des 10 protections recherchées ; 10,7 % en présentent 8 ou plus.

Les 10 protections recherchées

01 **Détection du root**
Repère un téléphone rooté, où les données de l'application sont exposées.

02 **Détection d'émulateur**
Repère que l'application tourne dans un émulateur et non sur un vrai téléphone.

03 **Détection de débogueur**
Repère un débogueur attaché à l'application en cours d'exécution.

04 **Détection du hooking**
Repère des outils comme Frida qui modifient l'application pendant son exécution.

05 **Anti-reconditionnement**
Repère une copie modifiée de l'application, signée par un tiers.

06 **Intégrité du code**
Vérifie que le code de l'application n'a pas été modifié.

07 **Épinglage de certificat**
N'accepte que le certificat du serveur de la banque.

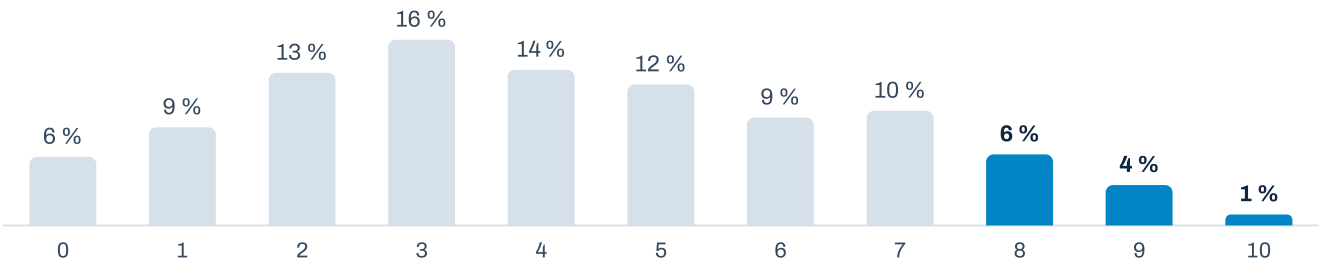
08 **Anti-superposition**
Empêche une autre application d'afficher un faux écran par-dessus l'application bancaire.

09 **Blocage des captures**
Empêche les captures et l'enregistrement des écrans sensibles.

10 **Détection du contrôle à distance**
Repère le partage d'écran ou un outil d'accès à distance.

L'application Android médiane présente 4 protections sur 10

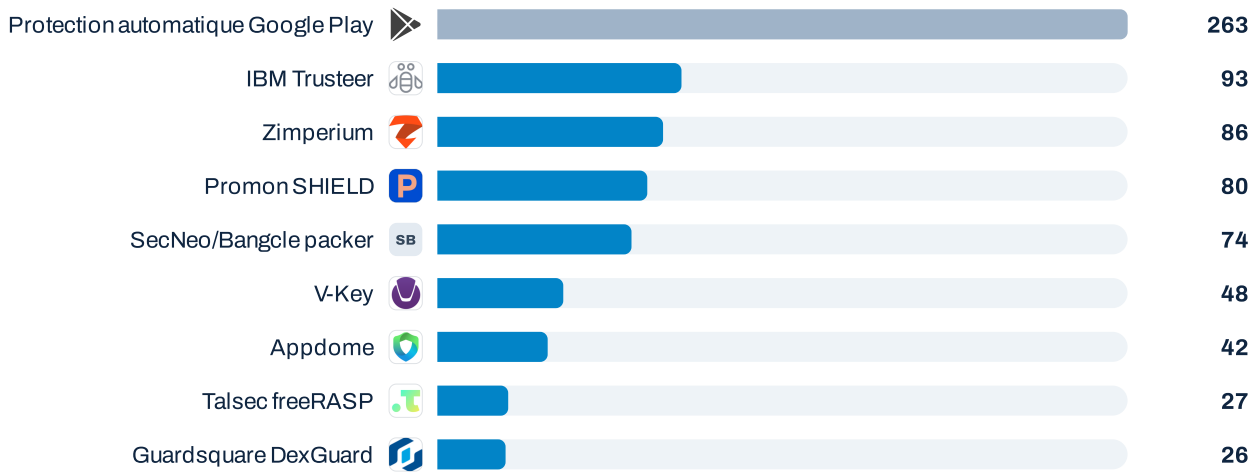
FIG. 6,3



Part des applications Android selon le nombre de protections avec des éléments nets, sur 10. En surbrillance : 8 ou plus.

La protection automatique de Google Play est la plus répandue

FIG. 6,4



Nombre d'applications utilisant chaque produit, toutes plateformes. La protection automatique de Google Play (pairip) est appliquée par le store, et non choisie dans le code.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

CHAPITRE 07

07

Au-delà de l'application

Une application n'est digne de confiance que si les domaines, les serveurs et l'établissement qui la sous-tendent le sont aussi. Nous avons vérifié les domaines web et de messagerie des banques, les serveurs avec lesquels les applications communiquent, les étiquettes de confidentialité, les incidents publics recensés et les règles auxquelles chaque banque est soumise.



À l'écran : une étiquette type et les incohérences que notre analyse a le plus souvent relevées.

67%

des applications Android ont une étiquette de confidentialité Google Play qui contredit leurs propres permissions ou SDK

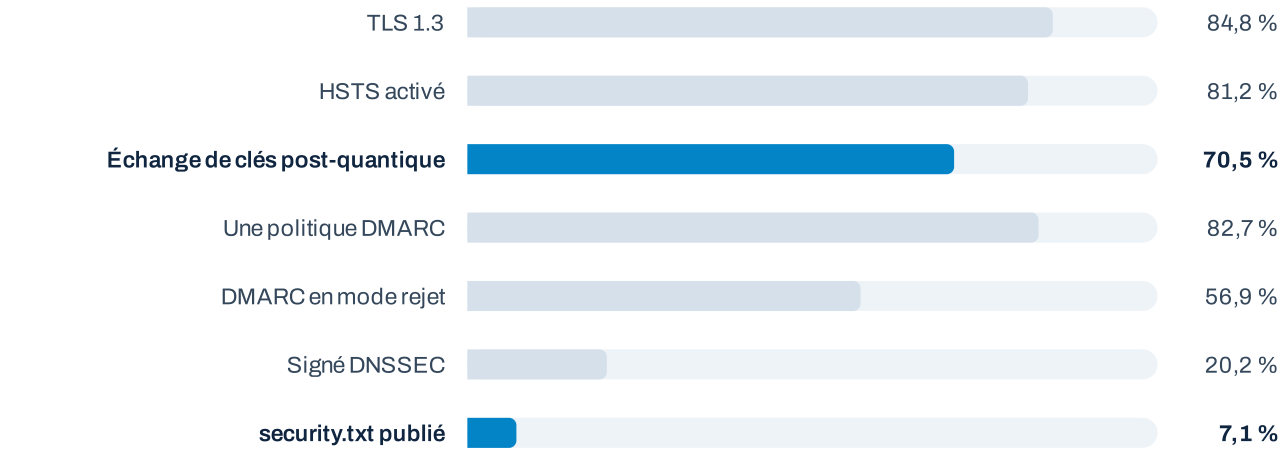
Applications Android dotées d'une étiquette de confidentialité Google Play

Domaines bancaires : prêts pour le post-quantique, peu ouverts aux signalements.

70,5 % des hôtes web bancaires joints négocient déjà un échange de clés post-quantique. L'hygiène de base est à la traîne : seulement 7,1 % des domaines publient un fichier security.txt indiquant aux chercheurs où signaler une faille.

Le TLS post-quantique devance security.txt

FIG. 7,1

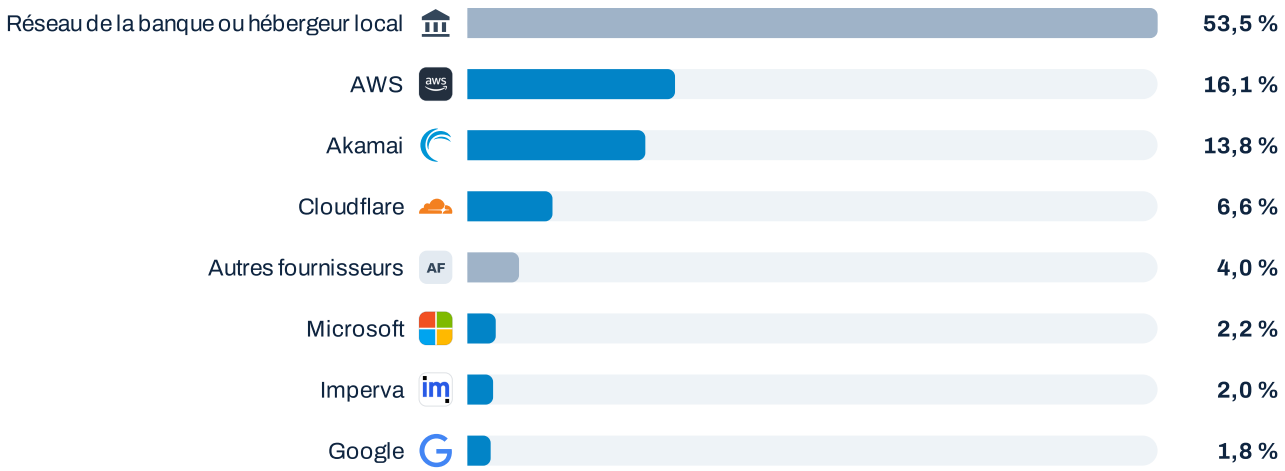


TLS et HSTS : part de 1140 hôtes web joignables. Post-quantique : 1038 négociations abouties. Contrôles DNS : 1252 domaines.

SOURCE Négociations TLS réalisées par Ostorlab et enregistrements DNS publics des domaines des banques.

La plupart des backends tournent sur le réseau propre de la banque ; AWS domine parmi les clouds

FIG. 7,2



Part de 5101 adresses IP de backend appartenant aux banques, référencées par les applications sur les trois plateformes et résolues via le DNS public.

SOURCE Hôtes référencés dans les applications, résolus via le DNS public ; registres de propriété des adresses IP.

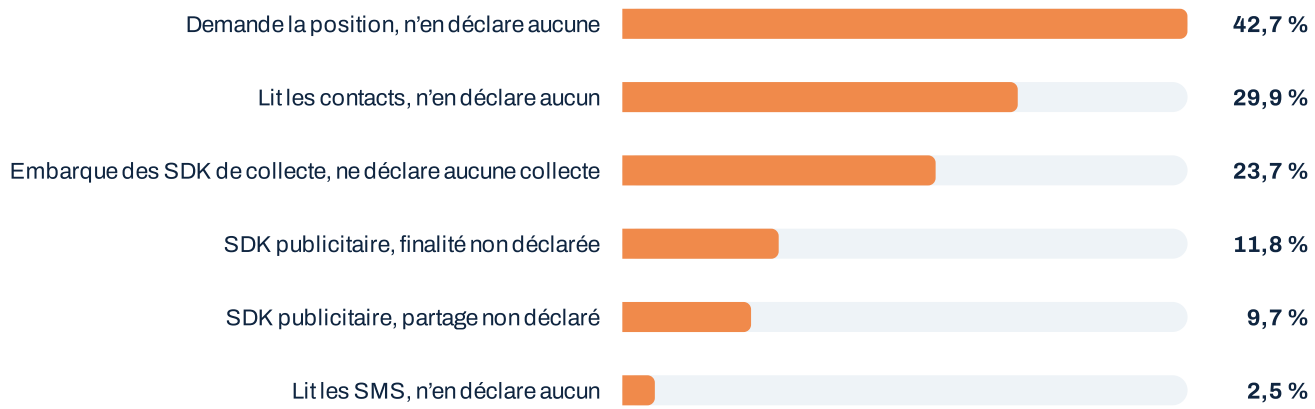
AWS, Akamai, Cloudflare et Microsoft hébergent 38,7 % des adresses de backend. Une panne ou une compromission chez l'un d'eux touche de nombreuses banques à la fois. Le règlement DORA de l'UE demande précisément aux banques d'en tenir compte avant de signer, notamment lorsqu'il s'agit de « la conclusion d'un contrat avec un prestataire tiers de services TIC dont les services ne sont pas facilement substituables » (règlement (UE) 2022/2554, article 29, paragraphe 1).

Des étiquettes de confidentialité qui ne correspondent pas à l'application.

Les stores demandent aux développeurs de déclarer les données que collecte leur application. Pour 67 % des applications bancaires Android, cette déclaration contredit ce que montrent les permissions ou les SDK de l'application.

La position non déclarée est l'incohérence d'étiquette la plus fréquente

FIG. 7,3



Part des applications Android dotées d'une étiquette « Sécurité des données » Google Play. Une application peut présenter plusieurs incohérences.

SOURCE Étiquettes « Sécurité des données » de Google Play, comparées aux permissions et aux SDK des applications.

Pourquoi c'est important

Une permission dans le manifeste ne prouve pas que l'application l'utilise : certaines incohérences relèvent de manifestes trop prudents. Mais les régulateurs lisent les étiquettes comme des engagements. Une étiquette qui minimise la collecte constitue un risque de conformité et trompe les clients qui comparent les applications.

Étiquettes iOS

Parmi les applications bancaires iOS dotées d'une étiquette de confidentialité, 19 % déclarent des données utilisées pour suivre les utilisateurs dans les applications d'autres entreprises, le plus souvent des identifiants et des données d'utilisation.

Certains serveurs bancaires répondent au-delà du web.

Sur les 5101 adresses de serveurs appartenant aux banques vers lesquelles pointent les applications, 4113 figurent dans des données publiques d'observation d'Internet. 251 d'entre elles répondent sur des ports autres que ceux du web et des CDN, chez 113 banques, et 79 exécutent un logiciel dont la version correspond à une vulnérabilité connue.

251

IP bancaires avec des ports ouverts au-delà des ports web et CDN, chez 113 banques

79

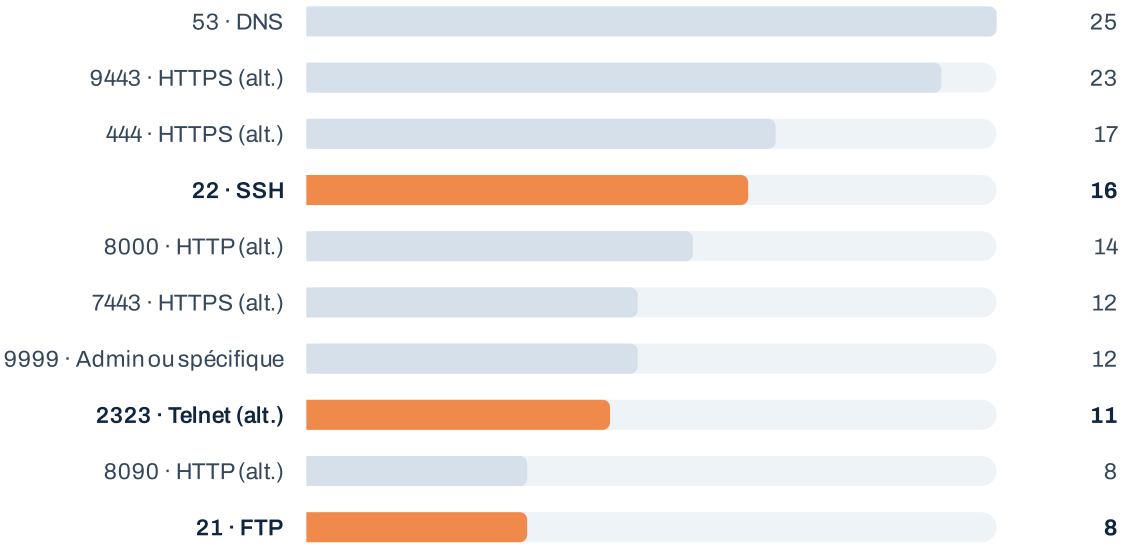
IP bancaires avec des CVE déduites des versions logicielles, chez 74 banques

25

IP bancaires exécutant un produit en fin de vie

Les ports DNS et HTTPS alternatifs dominent parmi les ports ouverts supplémentaires

FIG. 7,4



Nombre d'IP appartenant aux banques qui répondent sur chaque port, sur 4113 indexées par Shodan InternetDB. Les ports 80 et 443 et les ports de proxy CDN sont exclus ; 151 IP qui répondent sur plus de 40 ports, signe typique de pare-feu et de tarpits, ne sont pas comptées.

SOURCE Shodan InternetDB, index passif ; aucune requête n'a été envoyée à un serveur bancaire.

Nous n'avons analysé aucun serveur bancaire

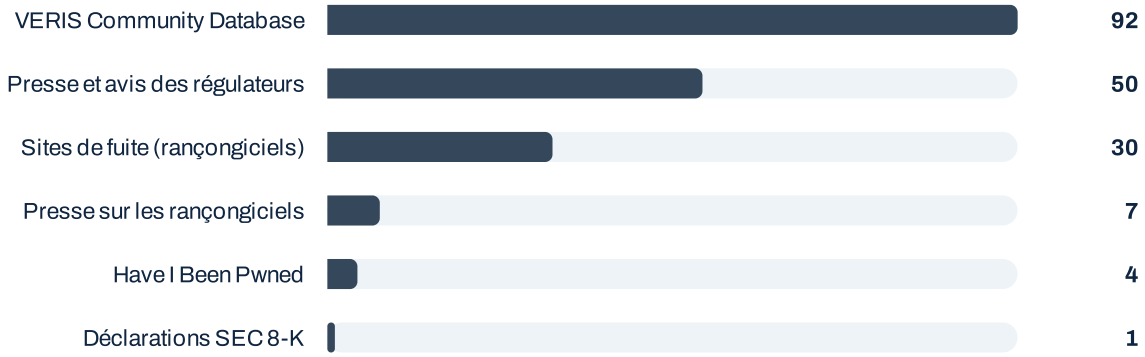
Les ports ouverts et les versions logicielles proviennent de données publiques d'observation d'Internet (Shodan InternetDB) : aucun système bancaire n'a été sollicité. Les 988 autres adresses ne figurent pas dans ces données : leur état est inconnu, elles ne sont pas forcément fermées. Les CVE sont rapprochées à partir de la version logicielle observée : chacune est une piste que la banque doit confirmer.

Une banque sur six a un incident de sécurité public recensé.

Dans les bases de données d'incidents, les sites de fuite de rançongiciels, les avis des régulateurs et les déclarations à la SEC, nous avons trouvé au moins un incident public recensé pour 83 des 500 premières banques (16,6 %). 55 d'entre elles ont un incident datant de 2020 ou après.

La plupart des incidents recensés proviennent de la base VERIS

FIG. 7,5



Nombre d'incidents recensés pour les 500 premières banques ; une banque peut en avoir plusieurs. Chaque correspondance a été vérifiée manuellement. Les recherches dans la presse et les avis des régulateurs ne couvrent que les 29 G-SIB.

SOURCE VCDB, Have I Been Pwned, ransomware.live, déclarations SEC 8-K, presse et avis des régulateurs.

Ce qu'est un incident recensé

Un incident recensé est un incident signalé publiquement : une attaque, un initié abusant de ses accès, une erreur ayant exposé des données ou la revendication d'un groupe de rançongiciel. Il ne s'agit pas d'une vulnérabilité de l'application de la banque, et beaucoup d'incidents sont anciens : la base VERIS remonte à plus de dix ans.

Les CVE qui nomment une banque

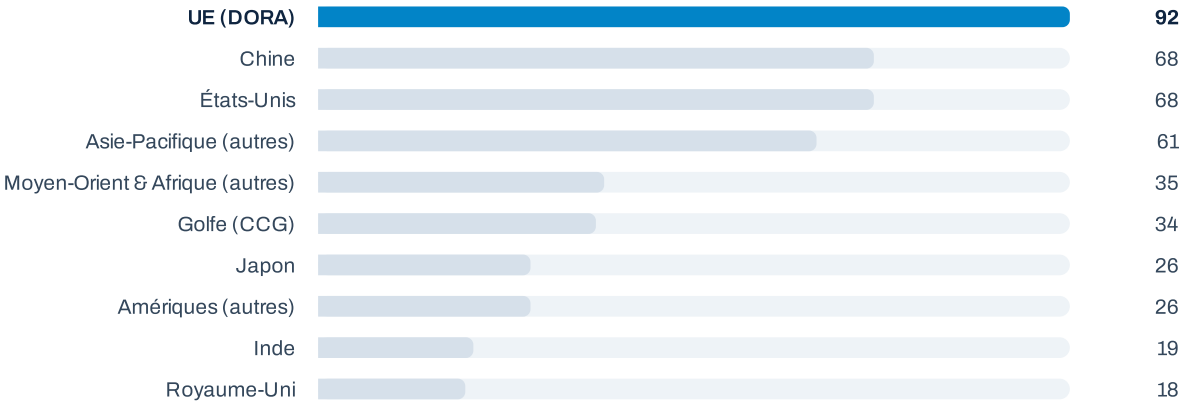
51 CVE publiées correspondent à la marque de 37 banques, dont 14 depuis 2025. La plupart concernent d'anciennes versions d'applications mobiles, et la correspondance par marque inclut des faux positifs : nous les traitons donc comme des pistes plutôt que comme des vulnérabilités avérées.

Les règles auxquelles les banques sont soumises, et ce qu'elles affirment.

Chaque banque de l'échantillon relève d'un régime national ou régional de gestion du risque lié aux TIC. 95 des 500 premières banques sont soumises au règlement européen sur la résilience opérationnelle numérique (DORA), applicable depuis janvier 2025, qui fait de dépendances comme les hébergeurs de la page 32 une responsabilité de la direction.

Le règlement DORA de l'UE couvre le plus grand groupe de banques

FIG. 7,6



Nombre des 500 premières banques, selon le régime de leur pays d'origine. Les dix plus grands groupes sont représentés ; 40 autres banques relèvent de groupes plus petits.

SOURCE Registres des régulateurs et marchés d'origine des banques.

332

des 500 premières banques sont émettrices Apple Pay

44

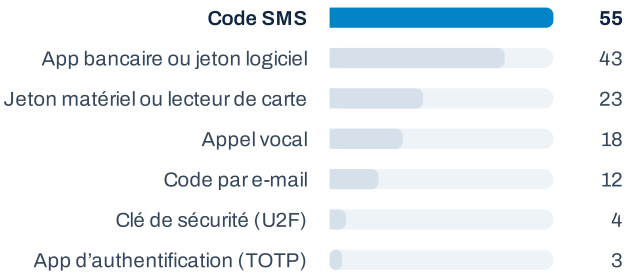
banques déclarent sur leur site web détenir une certification, le plus souvent ISO 27001

19

banques ont un programme public de divulgation des vulnérabilités, dont 5 avec un bug bounty

Le SMS est le second facteur le plus mis en avant

FIG. 7,7



Nombre des 73 banques dont le site web décrit les méthodes de connexion ; une banque peut en indiquer plusieurs. 8 mettent en avant les clés d'accès.

SOURCE Sites web des banques et liste 2fa.directory.

Des déclarations, pas des certificats

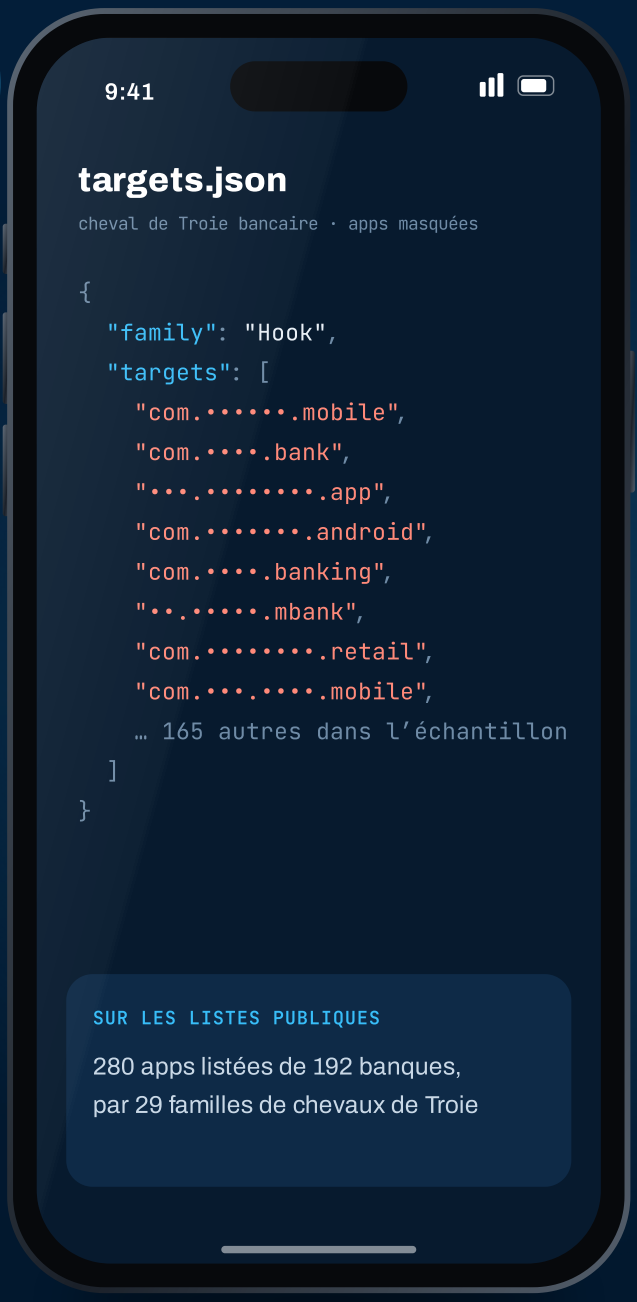
Les certifications sont ce qu'affirme le site web de la banque, et non des certificats vérifiés. 62 banques publient un fichier security.txt sur au moins un domaine, et 19 mentionnent un programme de divulgation. Le SMS reste le second facteur le plus mis en avant, alors même que des régulateurs comme la banque centrale des Émirats arabes unis suppriment progressivement les codes à usage unique par SMS.

CHAPITRE 08

08

Le paysage des menaces

Les chevaux de Troie bancaires tiennent des listes des applications qu'ils attaquent. Les kits d'hameçonnage copient les pages de connexion des banques. Au cours de l'année écoulée, des attaquants ont aussi remplacé de véritables applications bancaires par des copies modifiées.



À l'écran : la structure d'une liste de cibles publiée, noms d'applications masqués.

15%

des applications Android analysées figurent sur au moins une liste publique de cibles de chevaux de Troie bancaires

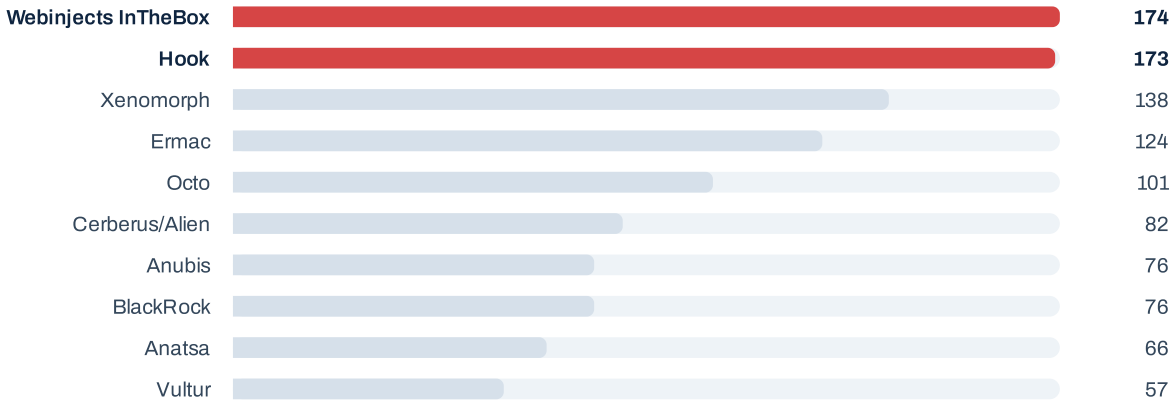
Applications Android

Quatre banques sur dix figurent sur la liste d'un cheval de Troie.

Des chercheurs publient les listes de cibles trouvées dans les chevaux de Troie bancaires. En les rapprochant des applications Android de notre échantillon, 280 applications de 192 banques (38,4 %) sont citées par au moins l'une des 29 familles.

Hook et InTheBox ciblent le plus d'applications de l'échantillon

FIG. 8,1



Nombre d'applications de notre échantillon figurant sur les listes de cibles publiées de chaque famille : 47 listes, publiées pour la plupart de 2021 à 2023 par ThreatFabric, Cleafy, Zimperium et d'autres. Android uniquement, car les listes citent des packages Android.

SOURCE Listes de cibles de chevaux de Troie bancaires publiées (ThreatFabric, Cleafy, Zimperium et d'autres), 2021–2023.

L'Europe et les Amériques attirent 93 % des hôtes d'hameçonnage et les neuf banques les plus ciblées

FIG. 8,2

54 %
Europe
5 des 9 banques les plus ciblées

39 %
Amériques
4 des 9 banques les plus ciblées

5 %
Asie-Pacifique
aucune des 9 banques les plus ciblées

1 %
Moyen-Orient & Afrique
aucune des 9 banques les plus ciblées



Couleur : part de chaque région dans les hôtes d'hameçonnage actifs qui citent une banque. Repères : nombre des neuf banques les plus ciblées basées dans ce pays ; ensemble, ces neuf banques attirent 57 % de tous les hôtes. Gris : hors échantillon. Les banques ne sont pas nommées.

SOURCE PhishTank, OpenPhish, Phishing.Database et URLhaus.

2026 : les attaquants retournent l'application de la banque contre elle.

Pendant dix ans, les chevaux de Troie bancaires ont affiché de faux écrans par-dessus la véritable application. Les campagnes de l'année écoulée vont plus loin : elles modifient, clonent ou remplacent l'application authentique, de sorte que le code même de la banque finit par travailler pour l'attaquant.

DEPUIS 2016

Superposition

Afficher par-dessus

Un cheval de Troie affiche un faux écran de connexion ou de paiement par-dessus la véritable application et lit ce que saisit le client.

POURQUOI ÇA MARCHE

L'application authentique n'est pas modifiée ; le cheval de Troie n'a besoin que de l'autorisation d'accessibilité.

CE QUI L'ARRÊTE

Protection anti-superposition, contrôle des services d'accessibilité

GOLDFACTORY, 2025

Altération

Modifier l'application

L'attaquant prend l'application authentique, y injecte du code de hooking et la signe à nouveau : les écrans mêmes de la banque exécutent alors le code de l'attaquant.

POURQUOI ÇA MARCHE

La copie a l'apparence et le comportement de la véritable application, y compris ses contrôles d'intégrité, que le hook désactive.

CE QUI L'ARRÊTE

Vérification de la signature avec la clé de la banque, attestation côté serveur

GIGABUD, 2026

Clonage

Exécuter une seconde copie

L'attaquant exécute l'application authentique dans un profil professionnel caché ou un espace virtuel qu'il contrôle.

POURQUOI ÇA MARCHE

Les outils antifraude voient la véritable application sur un appareil connu : la session paraît normale.

CE QUI L'ARRÊTE

Détection des profils professionnels et des espaces virtuels, liaison à l'appareil

HIRUDO, 2026

Remplacement

Substituer l'application

Un dropper désinstalle l'application authentique et installe une copie modifiée portant le même nom, la même icône et le même numéro de version.

POURQUOI ÇA MARCHE

Le client ne voit aucun changement. Seule la clé de signature diffère, et seul le serveur de la banque peut la vérifier.

CE QUI L'ARRÊTE

Une attestation côté serveur qui vérifie la clé de signature

Comment se déroule une substitution d'application, étape par étape

1. Une fausse mise à jour

La victime installe un dropper depuis un lien ou une fausse page de store.

2. La vraie application disparaît

Le dropper désinstalle l'application bancaire authentique.

3. Une copie revient

Il installe une copie modifiée : même nom, même icône et même version, mais une clé de signature différente.

4. Les identifiants fuient

La copie capture les mots de passe et les codes à usage unique tout en paraissant normale.

5. Le serveur tranche

Seule l'attestation sur le serveur de la banque peut distinguer la copie de l'application authentique.

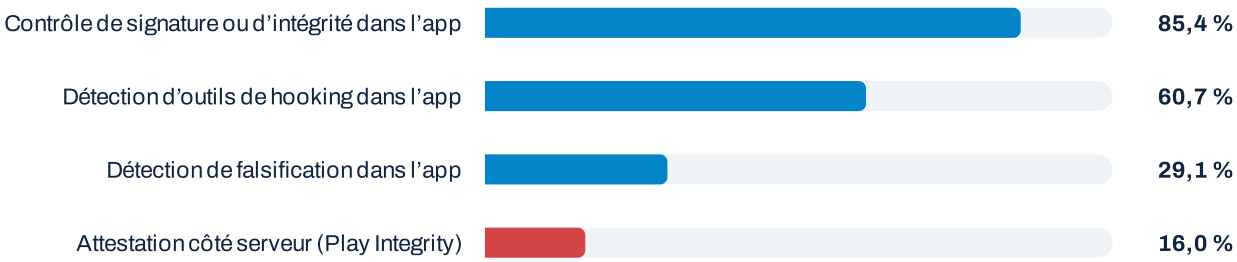
SOURCE Group-IB (GoldFactory, Gigabud), ThreatFabric (Hirudo) ; analyse Ostorlab.

Une banque verrait-elle que son application a été remplacée ?

Une copie modifiée peut désactiver n'importe quel contrôle exécuté sur le téléphone. Le serveur peut faire mieux : il peut refuser les requêtes qui ne portent pas une preuve récente, signée par Google ou Apple, que l'application est bien la version authentique de la banque. Seulement 16 % des applications Android contiennent le code nécessaire pour demander cette preuve, et nous ne pouvons pas voir si leurs serveurs l'exigent.

Les contrôles dans l'application sont courants ; les contrôles côté serveur sont rares

FIG. 8,3



Part des applications Android. Dans l'application : trouvé dans le code propre de la banque ou dans un SDK intégré. Attestation côté serveur : l'application contient le code permettant de demander la preuve ; l'application ne permet pas de voir si le serveur l'exige, et un appareil authentique mais compromis peut tout de même passer la vérification.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Les 2026 campagnes

Date	Campagne	Type	Ce qui s'est passé	Signalé par
Déc. 2025	**GoldFactory**	Altération	Des applications bancaires authentiques en Thaïlande, au Vietnam et en Indonésie, injectées de code de hooking qui contourne leurs contrôles d'intégrité : 27 applications modifiées, plus de 11 000 infections signalées.	Group-IB
Févr.–juil. 2026	**Gigabud**	Clonage	Applications bancaires exécutées dans un profil professionnel Android pour échapper à la détection de fraude ; environ 1469 appareils compromis signalés.	Group-IB
Mai 2026	**Test en laboratoire**	Altération	58 % des applications bancaires testées sur huit marchés ont pu être reconditionnées.	Promon
2026	**Familles à superposition**	Superposition	34 familles de logiciels malveillants bancaires actives ciblant 1243 marques financières dans 90 pays.	Zimperium
Août–oct. 2026	**Hirudo**	Remplacement	Un dropper substitue à une véritable application bancaire indonésienne une copie modifiée signée avec une clé de test publique ; huit applications de sept banques disposaient de remplaçantes toutes prêtes. Étude de cas, page 49.	ThreatFabric

Que faire

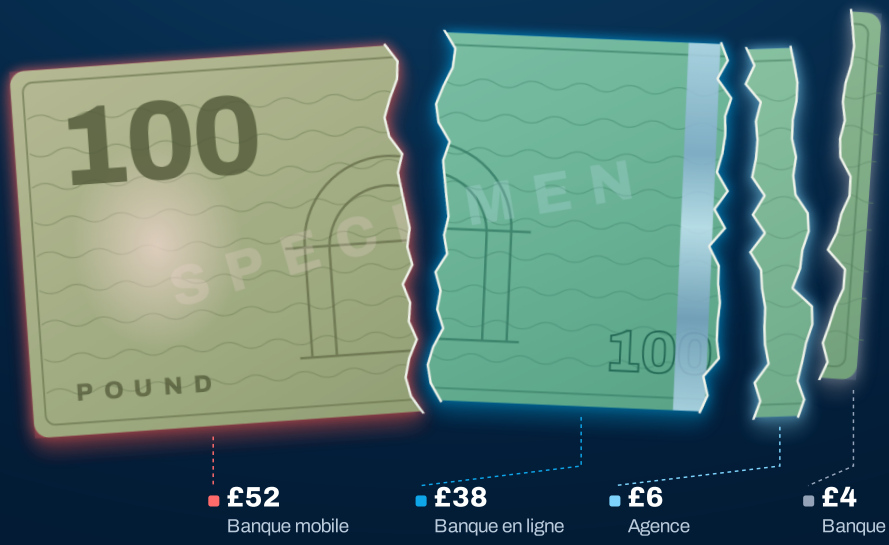
Considérez tout contrôle exécuté sur le téléphone comme un simple ralentisseur. Laissez le serveur décider : exigez l'attestation pour la connexion et les paiements, rejetez les requêtes provenant d'applications signées avec une autre clé que celle de la banque, et liez la session du client à l'appareil sur lequel elle a commencé.

Où va l'argent.

Les données publiées sur la fraude sont lacunaires : sur 101 marchés examinés, 83 publient un chiffre comparable. Là où les données existent, elles vont dans le même sens : la fraude s'est déplacée vers les paiements que le client est amené par la ruse à effectuer, et vers le téléphone.

FIG. 8.4

Sur 100 £ perdues dans des escroqueries au Royaume-Uni, 52 £ sont sorties via une application de banque mobile



576,4 M£
perdus dans des escroqueries au virement autorisé au Royaume-Uni en 2025

79 %
des paiements frauduleux, en nombre, ont été effectués via la banque mobile

88 %
des pertes signalées ont été remboursées au titre de la règle britannique de remboursement

Un billet de 100 £ déchiré selon le canal par lequel le paiement frauduleux a été effectué ; chaque morceau est aussi large que la part de son canal dans la valeur perdue. Dans les escroqueries au virement autorisé (APP), le client est amené par la ruse à envoyer l'argent. Les pertes autorisées ont augmenté de 19 % sur l'année, tandis que les pertes non autorisées ont baissé de 5 %.

Source : UK Finance, Annual Fraud Report 2026 ; UK Payment Systems Regulator

Europe

En 2024, 74 % de la valeur des virements frauduleux dans l'UE provenait de la manipulation du payeur pour qu'il autorise le paiement. La fraude à la carte est 13 fois plus fréquente, en valeur, lorsque la carte n'est pas présente. Source : rapport de la BCE et de l'ABE sur la fraude aux paiements, données 2024.

Le remboursement fonctionne

Depuis que le remboursement est devenu obligatoire au Royaume-Uni en octobre 2024, les banques ont restitué 88 % de la valeur des pertes signalées liées aux escroqueries APP au cours des 18 mois suivants. La responsabilité se déplace vers les banques, ce qui accroît la valeur des contrôles qui stoppent les escroqueries dans l'application. Source : UK Payment Systems Regulator.

Contexte, pas causalité

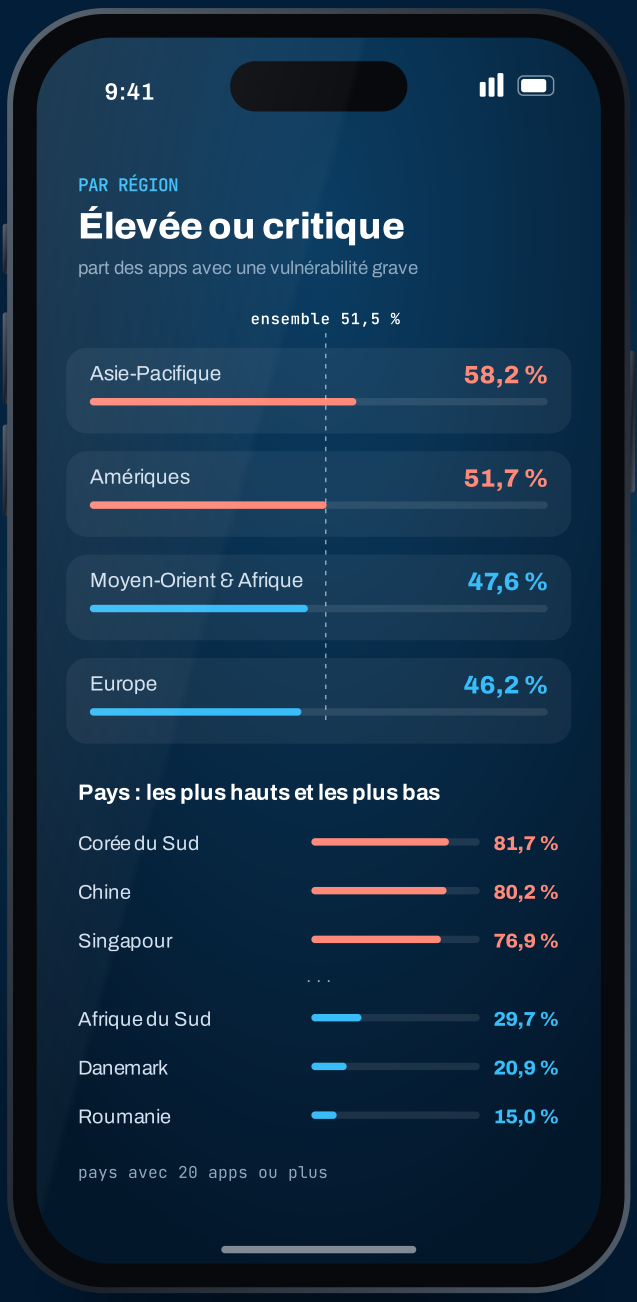
Ces statistiques décrivent la fraude sur chaque marché. Elles ne montrent pas que les faiblesses applicatives décrites dans ce rapport ont causé ces pertes.

CHAPITRE 09

09

Par région, type de banque et pays

Les résultats varient davantage selon le pays que selon la plateforme. Certains marchés sont en tête pour la protection applicative, d'autres pour l'attestation, et aucun ne domine sur tous les plans.



À l'écran : applications avec une vulnérabilité élevée ou critique, par région et par pays.

64

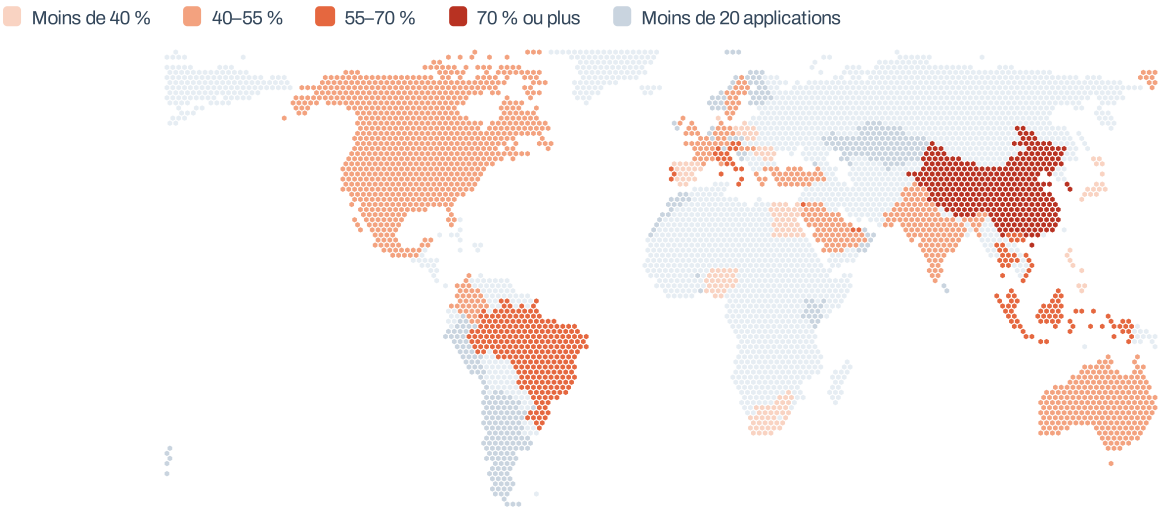
pays dans l'échantillon, des États-Unis et de la Chine au Togo et au Liechtenstein

Aucune région ne coche toutes les cases.

Les applications d'Asie-Pacifique cumulent le plus de vulnérabilités graves et le plus de protection applicative. Les applications européennes ont le moins de vulnérabilités élevées ou critiques. Les applications des Amériques sont en tête pour les clés d'accès, à 9,9 %.

Les vulnérabilités graves varient fortement d'un pays à l'autre

FIG. 9,1



Part des applications de chaque pays, pour les 40 pays comptant au moins 20 applications ; en gris : pays de l'échantillon comptant moins de 20 applications.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Aucune région ni aucun type de banque n'est en tête sur tous les indicateurs

FIG. 9,2

Groupe	Applications	Élevée ou critique	Composant vulnérable	Secrets intégrés	Produit de protection	Attestation	API clés d'accès
Asie-Pacifique	942	58,2 %	46,3 %	24,5 %	33,7 %	20,0 %	2,8 %
Europe	822	46,2 %	40,0 %	15,7 %	21,3 %	16,9 %	4,7 %
Moyen-Orient & Afrique	508	47,6 %	39,0 %	23,0 %	19,9 %	19,9 %	4,3 %
Amériques	414	51,7 %	33,8 %	16,2 %	29,5 %	23,4 %	9,9 %
Par type de banque							
Traditionnelle	2596	51,2 %	40,9 %	19,8 %	26,4 %	19,3 %	4,4 %
Néobanque détenue par une banque	61	52,5 %	47,5 %	24,6 %	37,7 %	16,4 %	4,9 %
Néobanque indépendante	29	**79,3 %**	44,8 %	**48,3 %**	24,1 %	**48,3 %**	**37,9 %**
Ensemble	*2686*	*51,5 %*	*41,1 %*	*20,2 %*	*26,6 %*	*19,6 %*	*4,8 %*

Part des applications de chaque groupe. Les néobanques indépendantes ont bien plus souvent une vulnérabilité élevée ou critique que les autres applications (79,3 % contre 51,2 % ; test exact de Fisher, p = 0,002), tandis que les néobanques détenues par une banque ressemblent au reste. Les néobanques indépendantes sont aussi en tête pour l'attestation et les API de clés d'accès. Elles ne représentent que 29 applications, dont un tiers provient d'une seule banque : l'ampleur de l'écart est donc indicative. Cellules colorées comme sur la page suivante. Les secrets intégrés excluent les clés d'API Google. Seules les règles multiplateformes sont comparées, car la répartition des plateformes diffère selon la région.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Résultats par pays.

Les 18 pays comptant le plus d'applications dans l'échantillon. Chaque cellule est colorée selon son écart au-dessus de la part de l'ensemble des applications : rouge pour un risque, bleu pour une défense. Les cellules non colorées sont égales ou inférieures à cette part.

Chaque pays a son propre profil de risques et de défenses

FIG. 9,3

Au-dessus de la part globale : Risque +5 pts +12 +20 Défense +5 pts +12 +20

Pays	Applications	Élevée ou critique	Composant vulnérable	Secrets intégrés	Produit de protection	Attestation	API clés d'accès
États-Unis	224	52,2 %	35,3 %	12,9 %	33,9 %	28,1 %	12,9 %
Inde	200	50,0 %	30,5 %	21,0 %	**43,0 %**	**32,5 %**	0,5 %
Chine	162	**80,2 %**	**77,8 %**	**43,8 %**	**51,9 %**	15,4 %	5,6 %
Royaume-Uni	157	47,1 %	**57,3 %**	31,2 %	**43,9 %**	18,5 %	14,0 %
Japon	116	38,8 %	33,6 %	13,8 %	6,9 %	4,3 %	3,4 %
Arabie saoudite	95	47,4 %	32,6 %	31,6 %	17,9 %	13,7 %	6,3 %
Émirats arabes unis	84	**64,3 %**	**59,5 %**	25,0 %	23,8 %	28,6 %	0,0 %
France	76	43,4 %	35,5 %	3,9 %	21,1 %	9,2 %	0,0 %
Italie	74	58,1 %	**58,1 %**	21,6 %	5,4 %	29,7 %	2,7 %
Afrique du Sud	74	29,7 %	17,6 %	**37,8 %**	20,3 %	**54,1 %**	9,5 %
Malaisie	71	57,7 %	42,3 %	25,4 %	31,0 %	25,4 %	1,4 %
Espagne	69	37,7 %	24,6 %	8,7 %	**42,0 %**	27,5 %	7,2 %
Brésil	66	60,6 %	31,8 %	22,7 %	27,3 %	21,2 %	10,6 %
Australie	63	54,0 %	33,3 %	19,0 %	4,8 %	23,8 %	3,2 %
Corée du Sud	60	**81,7 %**	**71,7 %**	21,7 %	3,3 %	3,3 %	0,0 %
Vietnam	56	**64,3 %**	51,8 %	**33,9 %**	**41,1 %**	25,0 %	3,6 %
Qatar	55	41,8 %	40,0 %	21,8 %	10,9 %	25,5 %	0,0 %
Canada	50	48,0 %	26,0 %	14,0 %	12,0 %	14,0 %	4,0 %
Ensemble	*2686*	*51,5 %*	*41,1 %*	*20,2 %*	*26,6 %*	*19,6 %*	*4,8 %*

Part des applications de chaque pays. Coloration : 5, 12 et 20 points de pourcentage ou plus au-dessus de la part globale. Les applications de la Chine incluent de nombreuses applications HarmonyOS, qui relèvent ses chiffres de composants vulnérables et de vulnérabilités critiques.

SOURCE Analyse de sécurité automatisée de 2686 applications bancaires par Ostorlab.

Les applications bancaires les plus sûres par région.

Trois banques par région dont les applications présentent des faiblesses moins nombreuses et moins graves que celles de leurs pairs, par ordre alphabétique. Aucun score n'est indiqué.

Amérique du Nord

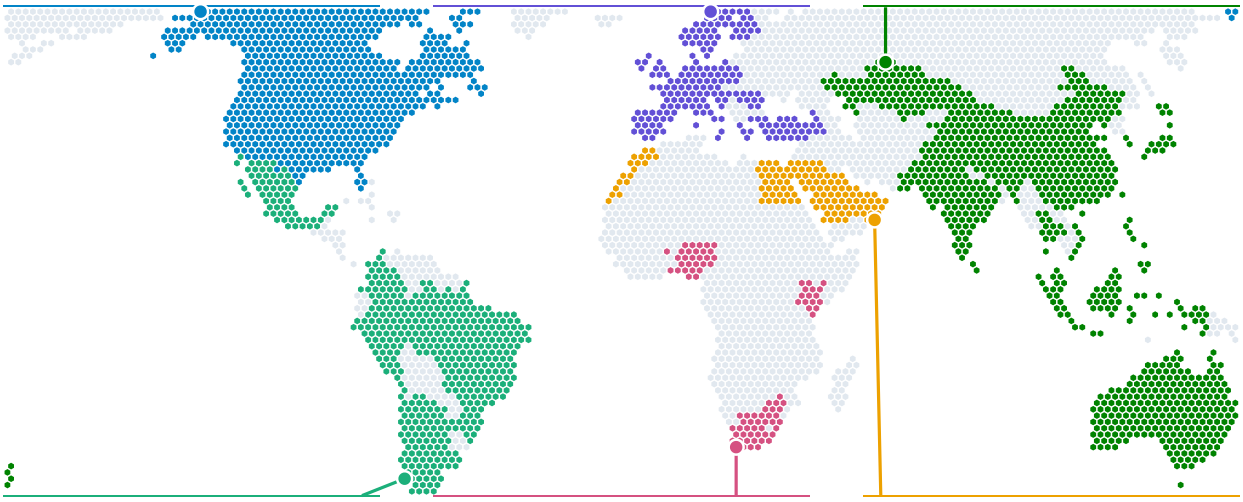
- **Scotiabank** — Canada
- **WaFD Bank** — États-Unis
- **Zions Bancorporation** — États-Unis

Europe

- **Ibercaja** — Espagne
- **Komerční banka** — Tchéquie
- **TSB** — Royaume-Uni

Asie-Pacifique

- **Bandhan Bank** — Inde
- **HBL** — Pakistan
- **RCBC** — Philippines



Amérique latine

- **Banorte** — Mexique
- **BCP** — Pérou
- **Itaú** — Brésil

Afrique subsaharienne

- **Absa** — Afrique du Sud
- **Co-Operative Bank of Kenya** — Kenya
- **Rand Merchant Bank** — Afrique du Sud

Moyen-Orient & Afrique du Nord

- **Gulf Bank** — Koweït
- **Qatar Islamic Bank** — Qatar
- **Saudi Investment Bank** — Arabie saoudite

Couleur : pays dont les banques ont été comparées, une couleur par région Gris : non comparés

Comment les banques ont été comparées

Ce sont les banques qui sont comparées, pas des applications isolées. Chaque application analysée reçoit une valeur tirée de sa note d'analyse (70 %) et des défenses et faiblesses trouvées dans son code (30 %), puis est classée parmi les applications de son propre store. Le score applicatif d'une banque est la moyenne de toutes ses applications analysées, ramenée vers le milieu lorsqu'elle en a peu.

L'historique de sécurité compte

Le score applicatif est ensuite abaissé pour chaque incident de sécurité de la banque signalé publiquement au cours des trois dernières années : davantage pour un incident grave, moins pour un incident mineur. Les escroqueries visant les clients ne comptent pas. Un historique vide signifie que rien n'a été trouvé, pas que rien ne s'est produit.

Ce que signifie un classement

Les trois banques les mieux classées de chaque région, parmi celles ayant au moins deux applications analysées. Être classée signifie présenter des vulnérabilités moins nombreuses et moins graves que ses pairs. Cela ne signifie pas que les applications en sont exemptes.

SOURCE Notes d'analyse Ostorlab et contrôles de sécurité des applications des 500 premières banques ; rapports d'incidents publics. Les logos sont les icônes des sites web des banques et des marques de leurs propriétaires, présentés uniquement à des fins d'identification.

CHAPITRE 10

10

Études de cas

Quatre attaques publiques de 2026, chacune mise en regard de ce que notre analyse a trouvé dans les applications ciblées. Elles vont d'une fausse application installée pendant un appel téléphonique au remplacement de l'application authentique, jusqu'à une clé cloud qui gagne de nouveaux pouvoirs après la publication de l'application.



À l'écran : les quatre cas et la page où commence chacun d'eux.

4

attaques publiques de 2026, chacune mise en regard de ce que notre analyse a trouvé dans les applications ciblées

ÉTUDE DE CAS 1 SUR 4 · LA FAUSSE APPLICATION

CyberDakait : sept chevaux de Troie, un appel téléphonique.

Sept familles de chevaux de Troie Android visant les clients de banques indiennes. Le logiciel malveillant est banal. Ce qui le rend efficace, c'est l'appel qui précède : un escroc se faisant passer pour la banque convainc la victime de l'installer.

7
familles de chevaux de Troie dans le groupe

17 960+
appareils infectés, comptés à partir des serveurs mêmes des opérateurs

7,6 M
SMS interceptés sur les téléphones des victimes

Publié par Group-IB le 28 octobre 2026

Le déroulement de l'attaque

1

L'appel

Un correspondant se faisant passer pour la banque propose un « plan de protection de carte de crédit » ou une récompense.

Indiquer aux clients que la banque n'envoie jamais d'application pendant un appel

2

Le lien

La victime reçoit un fichier d'application se faisant passer pour l'une de 11 banques indiennes ou l'un de 2 programmes gouvernementaux.

3

La fausse mise à jour

Un écran de « mise à jour » imitant Google Play fait installer l'application et accorder ses permissions.

4

La superposition

Une copie des écrans de la banque demande les données de carte, les identifiants et le code PIN.

5

Le SMS

Le cheval de Troie lit les SMS reçus et transmet les codes à usage unique aux opérateurs.

Lier les codes à l'appareil et à la transaction, plutôt que de simples SMS

6

Le vol

Avec les identifiants et les codes, les opérateurs vident les comptes. Les pertes signalées dépassent 30 500 $.

CE QU'A RÉVÉLÉ NOTRE ANALYSE

Protection anti-superposition dans l'app **75,6 %**

Prise en charge des codes SMS à usage unique **33,7 %**

Part des applications Android. La protection anti-superposition ne protège que l'application authentique : une fausse application envoyée pendant un appel ne l'exécute jamais. L'attaque réussit lorsque la banque accepte un code SMS comme preuve d'identité.

CE QUI L'AURAIT ARRÊTÉE

- Indiquer aux clients, dans l'application et sur tous les canaux, que la banque n'envoie jamais d'application et n'en demande jamais l'installation pendant un appel.
- Remplacer les codes SMS par des validations liées à l'appareil et à la transaction.
- Mettre en attente pour vérification les nouveaux appareils et les nouveaux bénéficiaires qui apparaissent pendant un appel.

Group-IB, *False Protection, Emptied Accounts: The Seven Android Trojan Families Targeting Indian Banking Apps*, 28 octobre 2026.
Aucune banque n'est nommée : Group-IB ne nomme pas les banques usurpées.

ÉTUDE DE CAS 2 SUR 4 · L'APPLICATION DÉTOURNÉE

WindRelay : un prêt contracté depuis l'application bancaire même de la victime.

Deux outils utilisés conjointement en Europe centrale : SpyNote, un cheval de Troie d'accès à distance qui livre à l'opérateur le téléphone de la victime, et WindRelay, qui relaie par NFC la carte de paiement de la victime vers un téléphone détenu par une mule.

2
outils combinés : un cheval de Troie d'accès à distance et un relais NFC

3
pays ciblés : Tchéquie, Slovaquie et Slovénie

23
échantillons collectés de novembre 2025 à juillet 2026

Publié par Group-IB le 12 août 2026

Le déroulement de l'attaque

1

L'appel

Un opérateur de vishing contacte la victime en se faisant passer pour la banque ou un autre tiers de confiance.

2

L'installation

La victime installe une application ; chaque build de SpyNote porte le nom de la victime.

3

Le passage de la carte

L'application de relais fait tenir la carte de la victime contre le téléphone et saisir le code PIN, puis transmet le tout à une mule.

4

Les espèces

La mule paie ou retire des espèces avec la carte relayée.

5

La prise de contrôle

Via SpyNote, l'opérateur pilote le téléphone et ouvre l'application bancaire authentique.

Détecter le partage ou la prise de contrôle à distance de l'écran

6

Le prêt

Dans au moins un cas, les opérateurs ont contracté un prêt au nom de la victime depuis cette application.

Des contrôles renforcés côté serveur pour les prêts, les bénéficiaires et les plafonds

CE QU'A RÉVÉLÉ NOTRE ANALYSE

Détection du contrôle à distance dans l'app **33,0 %**

Attestation côté serveur (Play Integrity) **16,0 %**

Part des applications Android. La prise de contrôle a lieu dans la véritable application, sur le véritable appareil de la victime : la liaison à l'appareil et les contrôles de SIM sont donc satisfaits. Seule l'application peut voir que son écran est piloté depuis l'extérieur.

CE QUI L'AURAIT ARRÊTÉE

- Détecter le partage d'écran et le contrôle à distance, et transmettre le signal au moteur de risque de la banque.
- Exiger une nouvelle validation liée à une clé pour les prêts, les nouveaux bénéficiaires et les hausses de plafond.
- Traiter un passage de carte suivi d'une demande de code PIN dans une application comme un schéma de fraude.

Group-IB, *WindRelay and SpyNote: an NFC and RAT combination in fraud*, 12 août 2026.
Aucune banque n'est nommée : Group-IB ne nomme pas les banques concernées.

ÉTUDE DE CAS 3 SUR 4 · L'APPLICATION REMPLACÉE

Hirudo : le cheval de Troie qui remplace votre application bancaire.

Un cheval de Troie bancaire Android qui ne se contente pas d'afficher de faux écrans. Il désinstalle la véritable application et installe une copie modifiée dont les hooks cachés fournissent de fausses réponses aux propres contrôles de sécurité de l'application.

42
applications financières dans la liste de cibles d'Hirudo

8
applications bancaires de 7 banques indonésiennes disposant d'une copie modifiée toute prête

1
ligne de code ajoutée à chaque copie pour charger le moteur de hooking

Publié par ThreatFabric le 14 octobre 2026

Le déroulement de l'attaque

1

L'appât

Une application fonctionnelle de shopping, de mini-séries, de football ou de vidéos pour adultes.

2

La fausse mise à jour

L'appât installe le cheval de Troie, qui demande l'accès à l'Accessibilité et aux notifications.

3

Les secrets

De faux écrans de paiement, de banque et de portefeuille collectent codes PIN et mots de passe ; un faux écran de schéma livre le code de déverrouillage.

4

La cible

Le cheval de Troie repère l'une des huit applications bancaires ciblées et vérifie son certificat de signature.

5

La substitution

Une fausse invite de mise à jour ouvre le programme de désinstallation, puis le cheval de Troie installe lui-même la copie modifiée.

6

La prise de contrôle

La copie s'exécute avec de faux signaux de sécurité pendant que l'opérateur regarde l'écran en direct.

Vérifier le verdict Play Integrity sur le serveur pour chaque action protégée

Dans l'application modifiée

La copie conserve le nom et le numéro de version d'origine, mais elle est signée avec une clé de test Android publique : c'est pourquoi l'application authentique doit d'abord être supprimée. Une ligne ajoutée charge un moteur de hooking qui ne s'active que si un fichier écrit par le cheval de Troie existe.

Accès à distance et collecte

Visualisation de l'écran et sessions caméra en direct, analyse des SMS sur 90 jours, et cibles d'identifiants en Chine, en Inde, au Mexique, au Maroc et en Thaïlande. Un serveur d'opérateur non sécurisé contenait des milliers d'identifiants volés et de profils financiers.

ThreatFabric, *Hirudo: from fake updates to patched banking apps*, 14 octobre 2026.

BleepingComputer, *Hirudo Android malware replaces banking apps to evade security checks*, 14 octobre 2026.

Aucune banque n'est nommée : ThreatFabric ne nomme pas les banques indonésiennes. Ce qu'a révélé notre analyse : page suivante.

Dans la copie, chaque contrôle peut être amené à mentir.

Hirudo exécute les contrôles de la banque dans un processus contrôlé par l'attaquant, et y répond lui-même. 61 % à 85,4 % des applications bancaires Android comportent les contrôles intégrés qu'il falsifie.

LA QUESTION QUE POSE L'APPLICATION	CE QUE RÉPOND HIRUDO	APPLICATIONS ANDROID QUI LA POSENT
Certificat de signature « Est-ce la clé de signature de la banque ? » →	FAUSSE RÉPONSE D'HIRUDO Renvoie le certificat authentique et masque la signature par clé de test.	Contrôle de signature ou anti-reconditionnement **85,4 %**
Services d'accessibilité « Une autre application contrôle-t-elle l'écran ? » →	FAUSSE RÉPONSE D'HIRUDO Renvoie une liste vide, masquant le service de contrôle du cheval de Troie.	Protection contre la superposition ou l'abus d'accessibilité **75,6 %**
Blocage des captures « Cet écran peut-il être enregistré ? » →	FAUSSE RÉPONSE D'HIRUDO Supprime l'indicateur, pour que les écrans bancaires puissent être vus et enregistrés à distance.	Protection contre les captures d'écran **61,0 %**
Attestation de clé matérielle « La clé est-elle dans un matériel sécurisé ? » →	FAUSSE RÉPONSE D'HIRUDO Répond avec une keybox matérielle divulguée dont Google a révoqué les certificats.	Non compté : impossible à distinguer des autres appels d'attestation
Play Integrity « Est-ce l'application authentique sur un téléphone authentique ? » →	FAUSSE RÉPONSE D'HIRUDO Envoie la requête au serveur de l'attaquant, qui renvoie un verdict favorable que l'application accepte.	Appel Play Integrity **16,0 %**

Hooks : ThreatFabric. Parts : applications Android dont le contrôle figure dans le code propre de la banque ou dans un SDK intégré ; Play Integrity : applications au code lisible. Un contrôle présent n'est pas pour autant un contrôle qui résiste à un hook.

Ce qui tient encore : les réponses que le serveur de la banque vérifie de son côté

- Vérifier Play Integrity sur le serveur, en liant le verdict à la session et à l'action protégée.
- Vérifier les certificats d'attestation de clé par rapport à la liste de révocation de Google.
- Maintenir des contrôles de risque transactionnel sur le serveur à la connexion, à la récupération d'identifiants, à l'ajout de bénéficiaires et à la validation des paiements.
- Intégrer les signaux d'accessibilité et de capture d'écran au scoring de risque plutôt que de les utiliser comme des blocages isolés.

Sources : ThreatFabric (hooks) ; analyse Ostorlab (applications).

ÉTUDE DE CAS 4 SUR 4 · LA CLÉ QUI FUIT

La clé d'API Google devenue un identifiant d'IA.

Google a longtemps expliqué aux développeurs que ses clés d'API, les chaînes commençant par `AIza`, ne sont pas des secrets : elles identifient un projet pour Maps ou Firebase et sont destinées à être livrées dans les applications. Mais ce à quoi une clé donne accès est défini dans le projet cloud, souvent par une autre équipe, bien après la publication de l'application.

2863
clés d'API Google actives avec accès à Gemini trouvées dans des données web publiques

32
clés actives avec accès à Gemini dans 22 applications Android populaires

82 314 $
facture Gemini signalée par une victime d'une clé détournée

Publié par Truffle Security en février 2026 et par CloudSEK en avril 2026

Comment une clé inoffensive devient un identifiant d'IA

1

La clé est livrée

L'application contient une clé d'API Google pour Maps ou Firebase, comme le permet la documentation de Google.

Restreindre chaque clé livrée aux API et à la signature d'application qui en ont besoin

2

Gemini est activé

Une autre équipe active la Generative Language API dans le même projet cloud.

Placer les API d'IA dans un projet dont les clés ne sont jamais livrées sur un appareil

3

La clé obtient l'accès à l'IA

Toutes les clés existantes du projet peuvent désormais appeler Gemini. Rien ne change dans l'application.

4

L'abus

Un attaquant extrait la clé de l'application, lit les fichiers envoyés à Gemini et fait grimper la facture : une victime s'est vu facturer 82 314 $.

CE QU'A RÉVÉLÉ NOTRE ANALYSE

Applications Android	80,3 %
Applications iOS	30,6 %
Applications HarmonyOS	71,4 %

Part des applications avec au moins une clé d'API Google n'importe où dans le paquet ; 72,5 % de l'ensemble des applications. Les clés n'ont pas été testées : la plupart sont probablement limitées à Maps ou Firebase, et l'équipe applicative ne peut pas le savoir à partir de la clé.

CE QUI L'AURAIT ARRÊTÉE

- Restreindre chaque clé aux API nécessaires et au certificat de signature de l'application.
- Placer Gemini et les autres API d'IA dans un projet cloud distinct.
- Renouveler toute clé déjà livrée dans une application avant d'activer une nouvelle API.

Truffle Security, *Google API keys weren't secrets, but then Gemini changed the rules*, 25 février 2026.
CloudSEK, *Hardcoded Google API keys in top Android apps now expose Gemini AI*, 7 avril 2026.
Aucune banque n'est nommée : aucune des deux sources ne nomme les établissements financiers dont les clés ont été exposées.

Ce que les banques doivent faire en 2026 : les 10 priorités.

Dix actions, chacune liée à un résultat de ce rapport et à un groupe de contrôles de l'OWASP MASVS, classées selon leur effet direct sur la réduction de la fraude.

01 Vérifier l'application sur le serveur

Utiliser Play Integrity et App Attest, vérifier le verdict sur le serveur et rejeter les requêtes en échec. C'est la seule défense qu'une application modifiée ou substituée ne peut pas désactiver.

79,8 % des applications n'utilisent aucune attestation

MASVS-RESILIENCE

02 Lier chaque action sensible à une clé

Faire passer les connexions et les validations de paiement par une biométrie liée à une clé adossée au matériel, jamais par une simple vérification oui/non.

35,1 % des applications Android ont une biométrie contournable

MASVS-AUTH MASVS-CRYPTO

03 Proposer les clés d'accès

Ajouter la connexion par clé d'accès et publier les fichiers asset links et associated domains correspondants, afin qu'un mot de passe hameçonné ne suffise plus.

4,9 % intègrent une API de clés d'accès

MASVS-AUTH

04 Retirer les secrets de l'application

Déplacer les clés privées, les clés cloud et les jetons de service vers le serveur et délivrer des jetons à courte durée de vie. Restreindre les clés qui doivent être livrées à la signature de votre application et aux API nécessaires.

20,3 % intègrent des secrets hors clés d'API Google

MASVS-STORAGE MASVS-CRYPTO

05 Verrouiller la redirection de connexion

Renvoyer les connexions via des liens universels et des app links que seule votre application peut revendiquer, jamais via des schémas d'URL personnalisés qu'une autre application peut enregistrer.

21,1 % des applications iOS permettent une prise de contrôle de compte OAuth

MASVS-PLATFORM MASVS-AUTH

06 Détecter le contrôle à distance et les superpositions

Combiner la détection du root, du hooking, de la falsification, des superpositions et du partage d'écran, activer les contrôles que vos SDK embarquent déjà et les tester sur des appareils réels.

33 % des applications Android détectent le contrôle à distance

MASVS-RESILIENCE

07 Savoir ce que vous livrez

Tenir une nomenclature logicielle (SBOM) pour chaque version, SDK et plateformes d'éditeurs compris, et corriger les composants critiques dans un délai fixé.

41,1 % embarquent un composant vulnérable

MASVS-CODE

08 Chiffrer chaque connexion

Désactiver le trafic en clair, épingler les certificats de vos propres API et limiter les WebViews à vos propres pages.

29,4 % des applications Android autorisent le trafic en clair

MASVS-NETWORK MASVS-PLATFORM

09 Surveiller les anciens appareils

Vérifier le niveau de correctif du système d'exploitation à la connexion et limiter les opérations à haut risque sur les appareils qui ne reçoivent plus de mises à jour.

99,5 % des applications Android tournent sur un Android non corrigé

MASVS-CODE

10 Fiabiliser les étiquettes et les contacts

Aligner les étiquettes de confidentialité des stores sur ce que fait réellement l'application, et publier un fichier security.txt pour que les chercheurs puissent vous joindre.

7,1 % des domaines bancaires publient un security.txt

MASVS-PRIVACY

Définitions et notes sur les données.

Échantillon

L'étude couvre les applications mobiles des 500 premières banques. 2841 fiches d'applications ont été collectées et 2686 ont été téléchargées et analysées, sur Android, iOS et HarmonyOS. Les pays et régions correspondent au marché d'origine de la banque.

Sévérité

La sévérité d'une application est celle de sa vulnérabilité critique, élevée, moyenne ou faible la plus sévère. Les niveaux « potentiel » (un motif qu'une personne doit confirmer) et « renforcement » (une protection manquante) ne modifient pas cette note ; un graphique qui les compte le précise. « Élevée ou critique » signifie au moins une vulnérabilité de l'un de ces niveaux ; « faible ou moins » signifie aucune vulnérabilité critique, élevée ou moyenne.

Règles propres à une plateforme

Les règles de contournement biométrique, de redirection d'intent, de sérialisation, de cryptographie, de trafic en clair et de stockage ne s'appliquent qu'à Android ; les règles App Transport Security et de manifeste de confidentialité ne s'appliquent qu'à iOS. Leurs parts ont pour dénominateur les applications de la plateforme concernée.

Valeurs inconnues

Lorsque le code d'une application est packé ou illisible, les vérifications renvoient « inconnu ». Ces applications sont exclues du dénominateur de la vérification concernée, et leur nombre est indiqué à côté du chiffre. Les graphiques de protection applicative présentent « inconnu » comme un segment à part.

Secrets intégrés

Secrets dans un format reconnu, comme des clés d'API, des jetons d'accès ou des clés privées. Les clés d'API Google Cloud sont présentées séparément. La validité des clés n'a pas été testée.

Clés d'accès et attestation

« API de clés d'accès intégrée » signifie que l'application appelle Android Credential Manager, l'API FIDO2 de Google ou les API de clés d'accès AuthenticationServices d'Apple. Les classes FIDO2 embarquées par d'autres bibliothèques ne comptent pas. L'attestation désigne Play Integrity, SafetyNet, HMS Safety Detect, App Attest ou DeviceCheck.

Protection applicative

Protections trouvées dans le code ou dans des produits intégrés, sur les trois plateformes. Sur iOS, la détection du jailbreak remplace celle du root et la protection anti-superposition ne s'applique pas. La présence n'a pas été testée sur appareil.

Versions d'OS non corrigées

Android et HarmonyOS : en dessous du niveau d'API 34 (Android 14), sans correctifs de l'Android Security Bulletin depuis mars 2026. iOS : en dessous d'iOS 18, la plus ancienne version majeure qu'Apple corrige encore entièrement.

Données côté banque

L'exposition des backends et les CVE proviennent de l'index passif InternetDB de Shodan et sont déduites des versions, sans test. Les incidents recensés proviennent de VCDB, Have I Been Pwned, ransomware.live, des déclarations SEC 8-K et, pour les G-SIB, de la presse et des régulateurs ; chaque correspondance a été vérifiée manuellement. Les certifications sont des déclarations des sites web.

Données externes

Les contrôles web et de messagerie couvrent 1252 domaines bancaires. La prise en charge du post-quantique a été lue dans les négociations TLS enregistrées. Les listes de cibles de chevaux de Troie proviennent de 47 listes publiées. Les hôtes d'hameçonnage proviennent d'un instantané unique de quatre flux publics. Les étiquettes de confidentialité proviennent de Google Play et de l'App Store. Pour les 142 sites web bancaires que nous n'avons pas pu ouvrir, nous avons lu la copie d'archive publique la plus récente (Internet Archive) datant de 2025 ou après ; les copies archivées peuvent être plus anciennes que le site en ligne.

Statistiques de fraude

536 chiffres publiés par des régulateurs, des banques centrales et des organismes professionnels, chacun conservé avec sa période et sa population. Ils décrivent la fraude sur chaque marché, et non les pertes causées par les faiblesses décrites dans ce rapport.

Études de cas

Synthèses de recherches publiques, créditées sur chaque page. Les chiffres d'analyse présentés à côté sont les nôtres.

Ostorlab

Rapport **2026** sur la sécurité des applications bancaires mobiles

Version 3 · 12 novembre 2026