jamf

Security 360 :

Rapport annuel sur les tendances de sécurité

Appareils mobiles

Sommaire

Introduction

Le rapport Security 360 de Jamf se veut une rétrospective réfléchie sur un paysage des menaces en constante évolution. Il tire ses enseignements d'incidents réels survenus au sein de notre base de clients, de découvertes faites par nos chercheurs sur les menaces, et d'observations sur les grands événements industriels du monde. Ce rapport s'intéresse principalement au paysage des menaces mobiles afin de mettre en lumière les risques auxquels les organisations sont confrontées dans ce domaine.

Nous examinons la diversité des vecteurs d'attaque mobilisés par les attaquants utilisent pour accéder aux systèmes et circuler dans l'infrastructure, afin de compromettre les données ou de causer des dommages. Les pirates informatiques exploitent les vulnérabilités des appareils et des logiciels et introduisent du code malveillant dans les applications et les communications web. Mais surtout, ils menacent les utilisateurs, le maillon faible des défenses de chaque organisation.

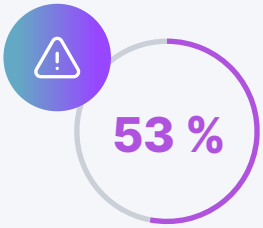
En complément de cette analyse des tendances des menaces, le rapport partage les perspectives et les éclairages du RSSI de Jamf à l'intention des responsables de la sécurité et des professionnels de l'informatique chargés de protéger les parcs mobiles.

Méthodologie de recherche

Pour comprendre et quantifier l'impact réel des tendances de sécurité identifiées dans ce rapport, nous avons examiné un groupe échantillon anonyme de plus de 1,7 million d'appareils iOS et Android au sein de notre base de clients. Nous avons mené notre analyse à la fin de l'année 2025 en revisitant la période des 12 mois précédents et en couvrant plusieurs pays du monde.

Dans le souci de respecter la vie privée des utilisateurs et les normes de sécurité les plus strictes concernant la collecte et le traitement des données, les métadonnées analysées dans cette recherche proviennent de journaux agrégés dépourvus d'informations permettant d'identifier des personnes ou des organisations.

Principales conclusions



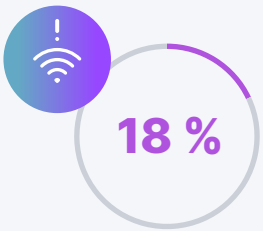
Proportion d'organisations dont au moins un des appareils est équipé d'un système d'exploitation gravement obsolète.

Un système d'exploitation obsolète est synonyme de vulnérabilités non corrigées et exploitables. L'automatisation et l'application systématique des mises à jour contribuent grandement à la protection de vos appareils.

1 sur 850

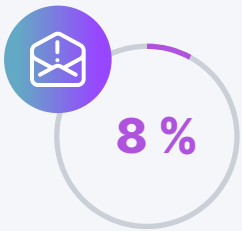
Nombre d'appareils jailbreakés utilisés dans un contexte professionnel

Jamf a détecté ces appareils ; des règles d'accès contextuelles les ont empêchés d'accéder aux ressources de l'entreprise.



Proportion d'organisations dont les employés se connectent à des points d'accès à risque.

Les points d'accès à risque ouvrent la porte aux menaces ciblant l'infrastructure, à commencer par les hotspots malveillants et attaques de type « adversaire du milieu », en particulier si les appareils ne sont pas configurés pour faire face à ce risque.



Proportion des appareils dont l'utilisateur a cliqué sur un lien d'hameçonnage.

Les attaques par hameçonnage restent une tactique populaire pour compromettre les comptes ; les tendances évoluent peu d'une année sur l'autre. Leurs effets peuvent être dévastateurs en l'absence de protections adéquates.

Les vulnérabilités « zéro clic » et les attaques du navigateur

restent aussi populaires qu'efficaces

De nouvelles vulnérabilités émergent sans cesse dans les systèmes d'exploitation et les logiciels ; elles sont la clé qui permet aux attaquants de récolter des informations sensibles par le biais de nombreuses familles de logiciels espions. Ce rapport rappelle à quel point il est important de réduire stratégiquement les risques sur vos appareils mobiles.

Principales tendances en entreprise

Les appareils mobiles sont essentiels à la productivité des employés, partout où ils travaillent. Leur sécurisation dépend de la façon des modalités de gestion, des usages qui en sont fait… et des menaces auxquelles ils sont confrontés.

Chaque jour, votre organisation fait tout son possible pour réduire sa surface d'attaque. Vous mettez en place des règles et des contrôles, vous ajoutez les meilleurs logiciels de sécurité à votre infrastructure, mais les pirates font sans cesse évoluer leurs tactiques.

Votre surface d'attaque est constituée de nombreux éléments. Dans ce rapport, nous abordons les risques majeurs les plus difficiles à contrôler par les organisations et les plus couramment exploités par les pirates, et nous proposons des pistes pour éviter des conséquences désastreuses.

1. Les vulnérabilités des logiciels et des appareils font partie de la vie des entreprises.

Malgré tout le soin apporté au développement des systèmes d'exploitation de vos appareils mobiles, la perfection n'existe pas. En 2025, plus de 48 000 CVE ont été publiées. Ce sont autant de vulnérabilités à reconnaître et à traiter.

Les développeurs le savent, et c'est pour cette raison qu'ils publient des correctifs de sécurité. C'est d'ailleurs là que vos équipes ont un rôle à jouer. Appliquez-vous ces correctifs ? Tenez-vous les systèmes d'exploitation à jour ? Respectez-vous les bonnes pratiques de sécurité ? La configuration de vos appareils a une grande importance.

Les pirates exploitent les failles ; la surface d'attaque augmente.

2. Les applications mobiles peuvent être une bénédiction comme un fléau.

Les applications sont indispensables pour le travail mobile. Votre entreprise déploie peut-être des dizaines ou des centaines d'applications sur l'ensemble de votre parc. Chaque application présente des risques propres. Les logiciels malveillants mobiles sont relativement rares, mais les attaques ciblant la confidentialité, la chaîne d'approvisionnement ou le traitement des données constituent toujours un risque concret.

Vos applications doivent également rester à jour, parce que leurs développeurs corrigent leurs vulnérabilités. Si la gestion du cycle de vie des applications est cruciale, il est tout aussi important de trouver le juste équilibre entre sécurité et confidentialité pour vos employés.

Les applications multiplient les risques, la surface d'attaque augmente.

3. Les risques liés aux réseaux et au Web menacent même les appareils les plus sûrs.

La protection de vos données est un enjeu vital, au repos comme en transit. Pour la mettre en œuvre, vous devez comprendre votre infrastructure réseau et le comportement des utilisateurs. Les employés se connectent souvent à des points d'accès non protégés qui peuvent être la cible d'attaques de type « Adversaire du milieu » (AitM). Sans une configuration adéquate, vos données peuvent être exposées.

L'hameçonnage reste une menace de premier plan, comme bien d'autres risques liés au Web. Les attaquants imitent un large éventail de sites populaires : divertissement, affaires, services publics, finances… toutes les catégories sont concernées. Ces sites contrefaits font des victimes tous les jours, d'autant plus que l'IA générative améliore considérablement l'efficacité des techniques employées.

Les erreurs des utilisateurs et les réseaux externes sont autant de points d'entrée incontrôlés ; la surface d'attaque s'agrandit encore.

4. Les risques se multiplient et les menaces sont de plus en plus sophistiquées.

Les vulnérabilités des appareils, les applications, l'infrastructure réseau et le comportement des utilisateurs sont autant de failles potentielles dans votre cyber-bouclier. Plus la surface d'attaque est grande, plus il est difficile de la couvrir, et ces trois types de risques sont souvent exploités dans le cadre d'attaques ciblées.

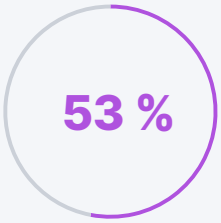
La prolifération de ces risques expose en effet les systèmes aux menaces persistantes avancées (APT) et aux logiciels espions. En 2025, Jamf Threat Labs a pu observer que les attaques de type « zéro clic » et « un clic » étaient toujours aussi exploitées. Les cadres dirigeants, les personnalités politiques, les militants et les journalistes ont été particulièrement visés.

Nous avons enquêté sur plusieurs attaques « zéro clic » et « un clic » particulièrement perverses en 2025. Ces attaques ont pour but d'exfiltrer des renseignements sensibles et exploitent plusieurs composants d'un appareil. Dans la suite de ce rapport, nous reviendrons sur ces études.

Vulnérabilités des appareils

Les systèmes d'exploitation mobiles fournissent une base plus ou moins sécurisée.

La base de code qui sous-tend l'OS de votre appareil est vaste et complexe. Et comme les êtres humains sont faillibles, elle contient inévitablement des vulnérabilités. Mais les humains sont aussi intelligents, et les pirates sont toujours à la recherche de failles à exploiter.



des **organisations** ont au moins un appareil avec un système d'exploitation gravement obsolète

Qu'est-ce qu'une CVE ?

Le programme CVE (vulnérabilités et expositions communes) entretient une base de données des vulnérabilités découvertes par la communauté de la cybersécurité. Chaque CVE identifie le logiciel ou la bibliothèque concernés, précise le degré de gravité et propose des méthodes d'exploitation possibles.

Revenons sur deux exemples marquants de 2025, dont des preuves d'exploitation ont été observées en environnement réel. Ces CVE ont été corrigées dans la version 18.4.1 d'iOS.

CVE-2025-31200

Score de gravité : 9,8 (critique)

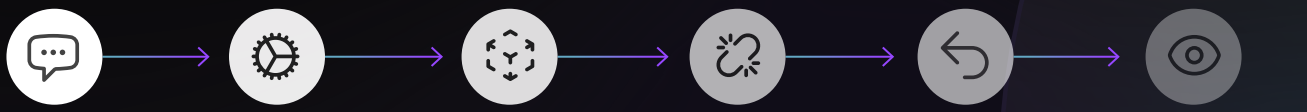
Le traitement d'un flux audio dans un fichier multimédia malveillant peut entraîner l'exécution de code.

CVE-2025-31201

Score de gravité : 9,8 (critique)

Un attaquant disposant de capacités arbitraires de lecture et d'écriture peut être parvenir à contourner l'authentification des pointeurs.

Les attaquants peuvent enchaîner les vulnérabilités de ce type pour dérober vos données et déployer des logiciels espions. Imaginez le scénario suivant (simplifié à l'extrême) :



1. Une cible de premier plan reçoit un message soigneusement élaboré contenant un fichier audio malveillant.
2. Sans interaction humaine, l'appareil mobile traite le message audio pour créer un aperçu.
3. La corruption de la mémoire qui intervient pendant le traitement fournit une capacité de lecture/écriture arbitraire.
4. Le contournement de l'authentification des pointeurs permet aux pirates de falsifier des pointeurs de code valides.
5. L'attaquant redirige l'exécution du code vers une charge utile malveillante.
6. Une fois l'appareil compromis, la surveillance commence.

Qu'est-ce que cela signifie ?

- **Il s'agit d'une attaque ciblée « zéro clic » :** l'utilisateur n'a pas besoin de cliquer sur quoi que ce soit pour que son appareil soit compromis. Les utilisateurs ciblés sont généralement des personnes très en vue, comme des journalistes, des personnalités politiques ou des cadres.
- **Les vulnérabilités s'accumulent :** les attaquants cherchent sans cesse de nouvelles exploitations, et ils savent les trouver.
- **Les correctifs sont indispensables :** ces vulnérabilités ont été corrigées dans la version 18.4.1 d'iOS. Si vos appareils ne sont pas à jour, vos données ne sont pas protégées.

Nous espérons que cela vous aura rappelé l'importance de tenir les appareils à jour. Mais ce qui est facile à dire n'est pas toujours facile à faire. Plusieurs raisons peuvent inciter un utilisateur à éviter de mettre à jour son appareil :

- Il ne souhaite pas utiliser les nouvelles fonctionnalités ou la nouvelle interface
- Une application qu'il utilise n'est pas compatible avec la nouvelle version du système d'exploitation
- Ses workflows vont être perturbés, ou les ressources ne le permettent pas

Comme nous l'avons démontré, les logiciels obsolètes sont extrêmement répandus, et tenir un parc à jour relève du défi. En imposant des délais de mise à jour et des versions minimales pour le système d'exploitation, vous protégerez votre parc d'appareils contre de graves vulnérabilités, comme celles que Jamf Threat Labs a analysées en 2025.

Les attaquants misent sur ces vulnérabilités pour implémenter des tactiques de type « zéro clic », reposant notamment sur l'analyse d'images et de fichiers audio, mais aussi des attaques en un clic dans le navigateur. Malgré les correctifs de sécurité et les efforts des fournisseurs, ils parviennent toujours à identifier de nouvelles vulnérabilités pour élaborer des techniques d'attaque, d'où l'importance d'un processus de mise à jour rigoureux. Voici un aperçu des vulnérabilités les plus importantes en 2025.

Vulnérabilités notables ciblant iOS, 2025

CVE-2025-24201 | Gravité : 10.0 (critique)	CVE-2025-43300 | Gravité : 10.0 (critique)	CVE-2025-31201 | Gravité : 9.8 (critique)
DESCRIPTION :		
Un contenu web malveillant peut s'extraire de la sandbox de contenu web.	Le traitement d'un fichier image malveillant peut entraîner une corruption de la mémoire.	Un attaquant disposant de capacités arbitraires de lecture et d'écriture peut parvenir à contourner l'authentification des pointeurs.
IMPACT :		
Cette vulnérabilité permet l'écriture de données hors limites après la fin ou avant le début du tampon prévu. Elle peut entraîner une corruption de la mémoire ou permettre à un pirate de modifier les données pour exécuter du code inattendu.	Cette vulnérabilité permet également l'écriture de données hors limites après la fin ou avant le début du tampon prévu.	Cette vulnérabilité inclut des contrôles d'accès inappropriés et permet un accès non autorisé à des composants sensibles pour la sécurité. Par conséquent, des pirates peuvent lire la mémoire, la modifier et exécuter du code non autorisé.
SYSTÈME D'EXPLOITATION CORRIGÉ :		
iOS 18.3.2 et iPadOS 18.3.2	iOS 18.6.2 et iPadOS 18.6.2	iOS 18.4.1 et iPadOS 18.4.1

Le tableau suivant présente d'autres vulnérabilités pour lesquelles nous avons des preuves d'exploitation en 2025.

iOS

VERSION D'IOS CORRIGÉE	DATE	SCORE DE LA VULNÉRABILITÉ	COMPOSANT
18.3.1	Févr. 2025	CVE-2025-24200 Score CVSS : 6.1 | Gravité : moyenne	Accessibilité
18.3.1	Févr. 2025	CVE-2025-43200 Score CVSS : 4.2 | Gravité : moyenne	Messages
18.4.1	Avr. 2025	CVE-2025-31200 Score CVSS : 9.8 | Gravité : critique	CoreAudio
26.2	Déc. 2025	CVE-2025-43529 Score CVSS : 8.8 | Gravité : élevée	WebKit
26.2	Déc. 2025	CVE-2025-14174 Score CVSS : 8.8 | Gravité : élevée	WebKit

Principales vulnérabilités touchant Android, 2025

CVE-2025-10585 | Gravité : 9.8 (critique)	CVE-2025-48543 | Gravité : 8.8 (élevée)	CVE-2024-53104 | Gravité : 7.8 (élevée)
DESCRIPTION :		
Une confusion de type dans V8 dans Google Chrome pouvait permettre à un attaquant distant d'exploiter une corruption de heap via une page HTML.	Il est possible d'échapper à la sandbox de Chrome en divers points pour attaquer le system_server d'Android grâce à une exploitation « user after free ». Cette tactique peut conduire à une escalade locale des privilèges sans qu'aucune autre autorisation d'exécution ne soit nécessaire. L'exploitation se fait sans interaction de l'utilisateur.	média : uvcvideo – Ignorer l'analyse des images de type UVC_VS_UNDEFINED dans uvc_parse_format. Ce procédé peut conduire à des écritures hors limites puisque les images de ce type ne sont pas prises en compte lors du calcul de la taille du tampon dans uvc_parse_streaming.
IMPACT :		
Un pointeur est déclaré sous un certain type, puis accède =à une ressource d'un type incompatible. Cela peut entraîner des réécritures de la mémoire, des pannes, voire une exécution de code.	L'utilisation de la mémoire libérée précédemment peut corrompre des données valides. Des pirates pourraient parvenir à exécuter un code arbitraire en introduisant des données malveillantes avant que la mémoire ne soit consolidée.	L'écriture de données hors limites, après la fin ou avant le début du tampon prévu, peut entraîner une corruption de la mémoire ou permettre à un attaquant de modifier les données pour exécuter du code inattendu.
SYSTÈME D'EXPLOITATION CORRIGÉ :		
Chrome 140.0.7339.155	Android 13, 14, 15, 16	Noyau Linux upstream, février 2025

Android

VERSION CORRIGÉE D'ANDROID	DATE	SCORE DE LA VULNÉRABILITÉ	COMPOSANT
12, 12L, 13, 14, 15	Mars 2025	CVE-2024-43093 Score CVSS : 7.3 | Gravité : élevée	Framework
Bulletin de sécurité*	Mars 2025	CVE-2024-50302 Score CVSS : 5.5 | Gravité : moyenne	Noyau
Bulletin de sécurité	Sept. 2025	CVE-2025-38352 Score CVSS : 7.4 | Gravité : élevée	Noyau

*Android ne publie pas de versions du système d'exploitation pour les mises à jour du noyau. Pour plus d'informations, consultez le bulletin de sécurité Android correspondant.

Chrome

VERSION DE CHROME CORRIGÉE	DATE	SCORE DE LA VULNÉRABILITÉ
136.0.7103.125	Mai 2025	CVE-2025-4664 Score CVSS : 4.3 | Gravité : moyenne
137.0.7151.72	Juin 2025	CVE-2025-5419 Score CVSS : 8.8 | Gravité : élevée
138.0.7204.63	Juin 2025	CVE-2025-6554 Score CVSS : 8.1 | Gravité : élevée
138.0.7204.157	Juillet 2025	CVE-2025-6558 Score CVSS : 8.8 | Gravité : élevée
142.0.7444.175*	Déc. 2025	CVE-2025-13223 Score CVSS : 8.8 | Gravité : élevée
143.0.7499.109	Déc. 2025	CVE-2025-14174 Score CVSS : 8.8 | Gravité : élevée

*La version indiquée est celle de Chrome for Desktop.

La configuration de vos appareils a une grande importance.

Les systèmes d'exploitation mobiles modernes offrent un large éventail de fonctionnalités, dont certaines étaient encore inimaginables il y a seulement cinq ans. Et comme on dit, un grand pouvoir implique...

Comme nous l'espérons, vous inscrivez vos appareils dans une solution de gestion des appareils mobiles (MDM) pour qu'ils soient correctement configurés. Les appareils doivent concilier convivialité et productivité, sécurité et confidentialité des utilisateurs. Difficile, dans ces conditions, de trouver la bonne configuration.

Bien que cela puisse varier en fonction du profil de risque et du secteur d'activité de votre organisation, certaines fonctions et configurations standard présentent un risque élevé et doivent donc faire l'objet de restrictions :

- Les appareils jailbreakés contournent les restrictions de sécurité d'Apple et permettent à l'utilisateur d'apporter des modifications pouvant rendre son appareil dangereux ou instable. Chaque appareil jailbreaké constitue une porte dérobée potentielle pour des pirates désireux de s'introduire dans votre système.
- Les boutiques d'applications alternatives permettent aux utilisateurs d'installer des logiciels en dehors de l'App Store ou de Google Play. Ces places de marché ne sont pas soumises aux mêmes exigences de sécurité et de confidentialité : le risque qu'une application soit malveillante ou problématique est donc plus élevé.

MALGRÉ CES RISQUES, JAMF THREAT LABS A DÉCOUVERT QUE :

1 sur 850
la proportion d'appareils professionnels jailbreakés

2 %
des organisations avaient des appareils connectés à des boutiques d'applications alternatives.

Le point de vue de notre RSSI

L'approche holistique détaillée ci-dessous permet d'atténuer les menaces les plus courantes ciblant les appareils mobiles : logiciels espions, applications malveillantes et correctifs manquants. Toutes sont susceptibles d'exposer les données sensibles de l'entreprise à l'insu de l'utilisateur.

- **Veillez à ce que tous les appareils mobiles soient inscrits dans la solution MDM**, qu'ils utilisent les versions approuvées du système d'exploitation, qu'ils soient tenus à jour et qu'ils respectent les normes de sécurité de base. Tout appareil non conforme doit être automatiquement isolé des ressources de l'entreprise jusqu'à ce qu'il ait été corrigé. Il est indispensable de mettre en place un cadre solide pour gérer les appareils et leurs utilisateurs et arrêter les logiciels malveillants avant qu'ils ne se diffusent dans votre infrastructure.
- **Mettez en œuvre une sécurité basée sur des agents** afin de détecter le jailbreaking, les comportements malveillants et les menaces touchant le système d'exploitation. Veillez à ce que les données de télémétrie soient transmises à votre SIEM pour que votre SOC ait une visibilité sur les menaces qui ciblent le parc mobile au même titre que le reste de votre environnement.
- **Activez le filtrage DNS et une protection contre l'hameçonnage** couvrant toutes les applications sur tous les appareils, sans s'arrêter à la messagerie. Il s'agit notamment de détecter les réseaux Wi-Fi malveillants et les attaques de l'adversaire du milieu.

Risques liés aux applications

Les applications mobiles sont indispensables aux tâches professionnelles quotidiennes de vos employés. Combien d'applications mobiles votre organisation déploie-t-elle ? Ces applications, qu'elles soient commerciales ou développées en interne, sont une voie d'accès à vos données sensibles.

<1 %

des organisations sont touchées par des logiciels malveillants mobiles.

Les logiciels malveillants pour mobile sont rares. Ils existent, mais leur prévalence n'a rien à avoir avec celle des malwares qui ciblent les ordinateurs. Cela s'explique en grande partie par l'architecture moderne des principaux systèmes d'exploitation mobiles ; le sandboxing et les boutiques d'applications contrôlées réduisent le risque que des contenus malveillants atteignent l'appareil.

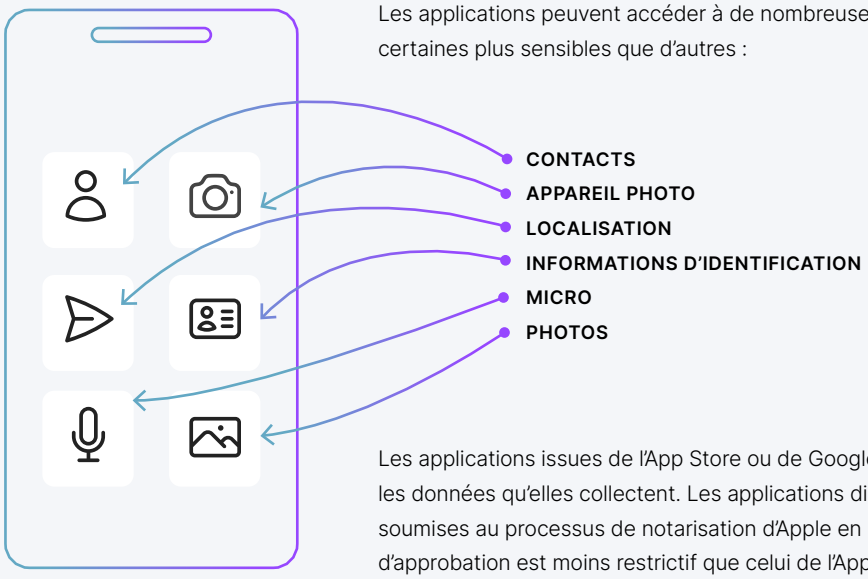
Gardez toutefois en tête que les applications élargissent votre surface d'attaque. Demandez-vous :

- **Comment les applications gèrent le stockage et la circulation des données**
- **Quelles données sont collectées par les applications, et selon quelles règles de confidentialité**
- **Sur quelles bibliothèques repose le code de l'application, pour comprendre les implications relatives à la chaîne d'approvisionnement**

Les acteurs malveillants exploitent les vulnérabilités des applications pour introduire des menaces persistantes avancées et des logiciels espions. Il est donc dans votre intérêt de bien comprendre vos applications. Rappelons également que la façon dont les applications gèrent le transfert des données sur les réseaux peut présenter des risques ; nous y reviendrons plus tard.

Les règles de confidentialité des applications dictent le traitement des données.

Les applications peuvent accéder à de nombreuses parties de votre appareil, certaines plus sensibles que d'autres :



Les applications issues de l'App Store ou de Google Play sont tenues d'indiquer à l'utilisateur toutes les données qu'elles collectent. Les applications distribuées et issues de boutiques alternatives sont soumises au processus de notarisation d'Apple en matière de sécurité et d'intégrité, mais le processus d'approbation est moins restrictif que celui de l'App Store officiel.

Il est difficile de trouver un équilibre entre sécurité et confidentialité.

Que vos employés utilisent un appareil d'entreprise ou le leur, la sécurité et la confidentialité deviennent des priorités absolues dès lors que vous autorisez l'accès aux ressources et aux données de votre organisation. La sécurité, parce que vous devez protéger vos données. Et la confidentialité, parce qu'il faut protéger l'utilisateur.

Ce savant dosage n'a rien d'évident. Par exemple :

- Certaines règles de votre **système de prévention des pertes de données** peuvent porter atteinte à la confidentialité.
- **Limiter les possibilités d'un appareil** au nom de la sécurité peut nuire à la productivité.
- Des **règles inadaptées** peuvent ouvrir la porte au shadow IT, une pratique consistant à télécharger des applications non approuvées pour certaines fonctions professionnelles.

Pour lutter contre ces problèmes, votre organisation peut :

- Imposer l'inscription à une **solution MDM** pour accéder aux ressources de l'entreprise
- Séparer les données personnelles de celles de l'entreprise à l'aide de conteneurs ou de partitions renforcées sur les appareils en BYOD afin d'appliquer les règles de prévention des pertes de données. De cette façon, l'accès aux données personnelles est impossible aux systèmes de l'entreprise, et la confidentialité des utilisateurs est préservée.
- Envoyer le trafic réseau de l'entreprise via des tunnels chiffrés pour garantir la confidentialité et l'intégrité des données.
- Sensibiliser les utilisateurs aux bonnes pratiques et aux règles de sécurité

Supplément : analyse de la sécurité des applications

Jamf s'est associé à NowSecure pour procéder à une analyse approfondie des risques liés aux applications mobiles, en particulier celles qui sont couramment déployées en entreprise. Nous avons analysé 135 des applications mobiles professionnelles et personnelles les plus populaires et répandues en utilisant la norme OWASP comme base d'évaluation des risques.

Toutes les applications analysées étaient dans leur version la plus récente au 31 décembre 2025, afin de refléter l'exposition réelle des entreprises.

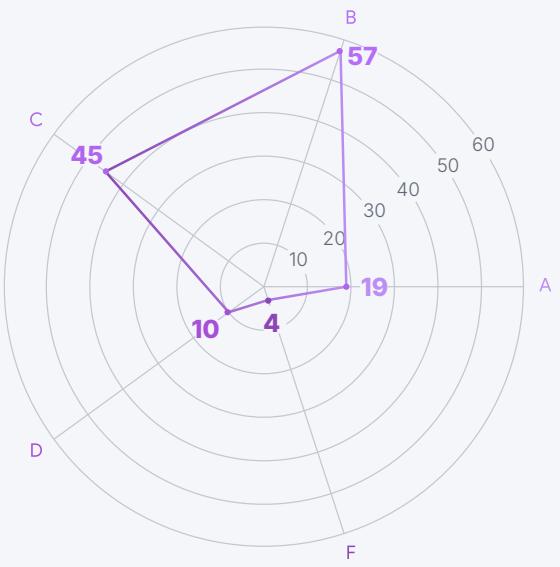
NowSecure aide les organisations à se protéger des vulnérabilités des applications mobiles et des fuites de données afin d'éviter les incidents de sécurité, de confidentialité et de conformité. En analysant en permanence les applications mobiles internes et tierces, puis en intégrant les résultats aux workflows de sécurité, d'informatique et de risque, NowSecure donne aux équipes la visibilité, les preuves et la gouvernance nécessaires pour gérer le risque mobile à grande échelle.

En savoir plus sur NowSecure.

Score de sécurité de l'application

NowSecure fournit un score de sécurité des applis mobiles allant de zéro à 100 (plus il est élevé, mieux c'est) et un score de risque de **A** à **F** (**A** = risque minime, **F** = risque substantiel). Ces scores reposent sur des tests automatisés qui évaluent les vulnérabilités, les fuites de données, les pratiques de codage non sécurisées, les faiblesses du chiffrement et les failles réseau.

SCORES DE SÉCURITÉ DES APPLICATIONS POPULAIRES

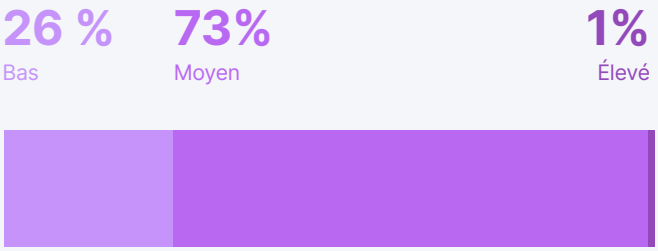


A — **F**

risque minimal — risque important

Environ **86 %** des 135 applications analysées comportaient des failles de sécurité connues, et elles n'étaient que **14 %** à présenter un risque minimal. Autrement dit, le risque est présent dans les applications professionnelles et personnelles les plus utilisées au quotidien, même avec les versions les plus récentes.

RÉPARTITION DES VULNÉRABILITÉS



Sur l'ensemble des vulnérabilités relevées dans l'analyse, la plupart affichent une gravité moyenne. Comme nous le verrons plus loin, le nombre de vulnérabilités est supérieur au nombre d'applications analysées, ce qui signifie que plusieurs applications présentent plus d'une vulnérabilité.

Évaluation des vulnérabilités des applications

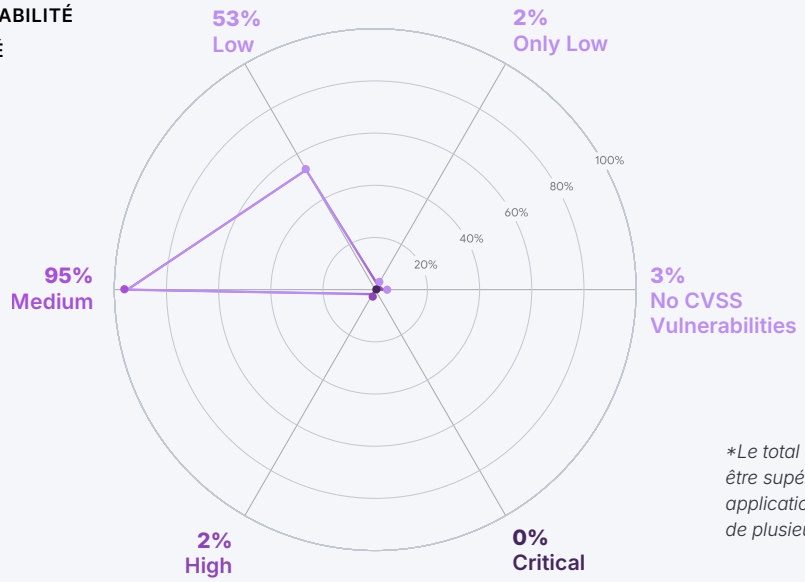
Il est important d'évaluer les implications en termes de risques que de multiples vulnérabilités peuvent avoir sur une même application. Au moment de l'évaluation, **95 %** des 135 applications contenaient au moins une vulnérabilité de gravité moyenne, et **2 %** de l'échantillon présentaient des vulnérabilités de gravité élevée en faisant des cibles potentielles pour des attaques.

Si les fabricants de logiciels sont tenus de corriger les vulnérabilités de leurs applications, il incombe aux entreprises de connaître leur exposition aux risques et de veiller à appliquer les mises à jour en temps voulu. Les recommandations concernant la cadence des correctifs varient. La CISA, par exemple, recommande de corriger les vulnérabilités de gravité critique dans les 15 jours suivant leur détection, et les vulnérabilités de gravité élevée dans les 30 jours. Dans tous les cas, ces données soulignent que toutes les organisations doivent mettre en place des programmes de mise à jour rigoureux.

Comme nous l'avons indiqué, NowSecure a évalué les versions les plus récentes des applications. Pourtant, la plupart d'entre elles présentaient des vulnérabilités. La gestion des risques liés aux applications demande une surveillance et des interventions constantes.

Mais elle n'a rien d'impossible si vous pouvez :

1. Identifier les vulnérabilités et les problèmes de confidentialité à tout moment
2. Hiérarchiser la remédiation en fonction de l'impact sur l'entreprise
3. Faire appliquer les règles grâce à des contrôles de gestion des appareils mobiles
4. Surveiller le comportement des applications tierces au fil du temps

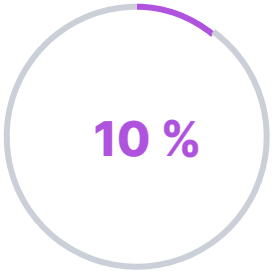


**Le total des pourcentages peut être supérieur à 100 %, car certaines applications contiennent des vulnérabilités de plusieurs niveaux de gravité.*

Chaîne d'approvisionnement

Les applications mobiles s'appuient souvent sur des SDK et des bibliothèques de tiers qui présentent des risques cachés.

Même si votre application a des règles acceptables en termes de collecte de données et de confidentialité, elle peut utiliser des kits de développement logiciel (SDK) ou des bibliothèques tierces qui présentent des failles critiques.
Parce que les entreprises sont tenues responsables en cas d'exposition des données et de manquement à la conformité, elles doivent avoir une visibilité sur les risques liés à la chaîne d'approvisionnement des logiciels.



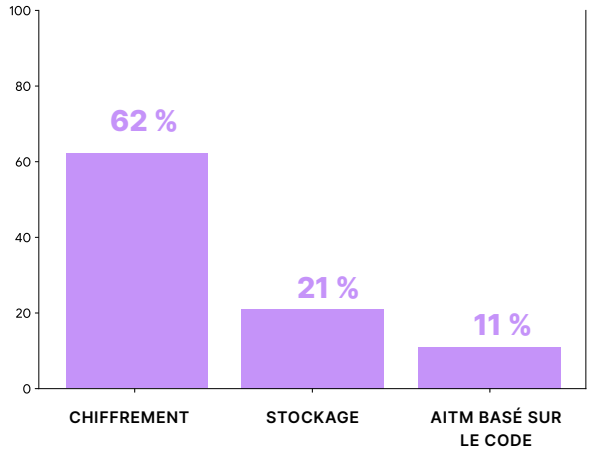
des **applications** utilisaient
des bibliothèques vulnérables

Sécurité des données

Les données peuvent s'extraire des applications de différentes manières.

- **Problèmes de chiffrement :** il est difficile pour les développeurs d'applications de sécuriser les données, de protéger les communications et de vérifier l'identité des utilisateurs. Beaucoup utilisent pour cela des bibliothèques tierces. Sur l'ensemble des applications analysées, NowSecure a identifié deux bibliothèques vulnérables connues : OpenSSL et libpng.
- **Stockage non sécurisé :** la façon dont les données sont gérées au repos est déterminante pour la confidentialité, l'intégrité et la disponibilité de vos données. Des protections faibles au niveau du stockage peuvent augmenter le risque d'exfiltration des données.
- **Risques d'attaques AitM :** la manière dont les applications traitent les données en transit est tout aussi importante. Si les communications ne sont pas correctement chiffrées, par exemple, un pirate peut intercepter ou manipuler des informations sensibles en transit.
- **Accès aux données :** mes applications mobiles ont accès au cloud et aux données de l'entreprise, particulièrement recherchées par les acteurs malveillants. Une perte de données est une perte de données, quelle que soit son origine.

TYPES DE VULNÉRABILITÉS



Utilisation de l'IA

L'IA, et en particulier l'IA générative, reste un sujet brûlant dans l'actualité. Dans un rapport de janvier 2026, Deloitte indique que l'accès des travailleurs à une IA approuvée a augmenté de 50 % en un an. Aujourd'hui, 60 % des employés utilisent des outils d'IA au travail.

Et cela se comprend : les IA basées sur l'appareil et dans le cloud offrent une foule de fonctionnalités pratiques. Les applications mobiles sont d'ailleurs de plus en plus nombreuses à intégrer les deux :

- **IA sur l'appareil :** les LLM permettent aux applications d'effectuer des tâches de traitement du langage naturel (génération de texte, frappe prédictive, etc.), tandis que les modèles d'apprentissage automatique sont utilisés pour la reconnaissance d'images, la détection d'objets en temps réel, la lecture de codes-barres et la réalité augmentée.
- **IA basée sur le cloud :** elle est capable de réaliser diverses tâches avancées en s'appuyant sur une infrastructure externe pour le traitement et le calcul.

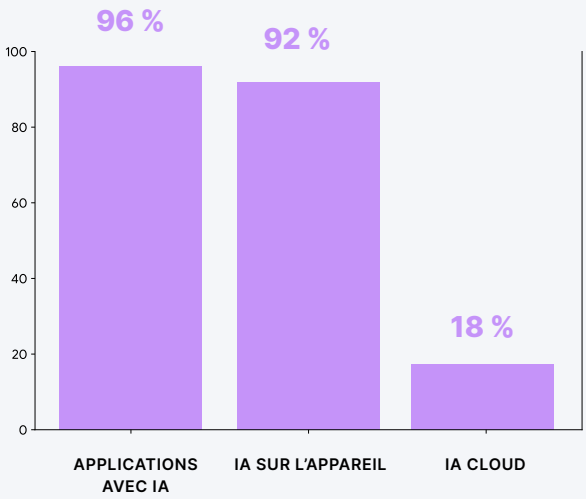
Les utilisateurs et les organisations adoptent rapidement l'IA générative, mais les risques évoluent aussi vite que la technologie.

Considérez les risques :

- Le « shadow AI » désigne l'accès à des outils d'IA qui ne sont ni approuvés ni encadrés. Les utilisateurs peuvent en effet inclure des **données sensibles de l'entreprise** et enfreindre les règles de sécurité. Comme l'IA cloud repose sur une infrastructure externe, votre organisation n'a pas forcément de visibilité sur les **risques** et l'**exposition des données**.
- Les utilisateurs peuvent utiliser des agents d'IA pour **effectuer des actions autonomes** hors du cadre des contrôles prévus.

Et un grand nombre d'applications courantes utilisent l'IA, souvent sans transparence pour l'entreprise.

PRÉSENCE DE L'IA DANS LES APPLICATIONS



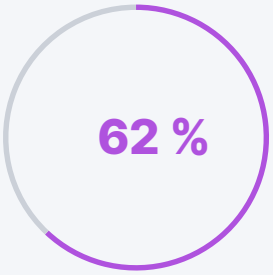
Confidentialité

Nos appareils mobiles nous accompagnent partout. Ils contiennent une multitude d'informations sur notre vie personnelle et professionnelle : photos, contacts, données sensibles, documents financiers, informations exclusives, etc.

Pour cette raison, les utilisateurs et les employeurs accordent une grande importance à confidentialité, d'autant que des lois imposent la protection de la vie privée.

Pourtant, nos applications ne sont pas toujours à la hauteur de ces exigences, que ce soit dû à l'intention du développeur ou à sa négligence. Certaines applications demandent des autorisations dangereuses qui collectent des données sensibles :

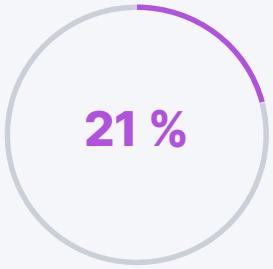
- Localisation de l'appareil
- Micro
- Appareil photo
- Contacts



des **applications** demandaient des autorisations dangereuses

Une fois qu'une application a demandé l'accès à des informations, comment les traite-t-elle ? Certaines données sont nécessaires au fonctionnement de l'application. D'autres, moins. Certaines fonctionnalités peuvent dégrader la confidentialité et la protection de la vie privée :

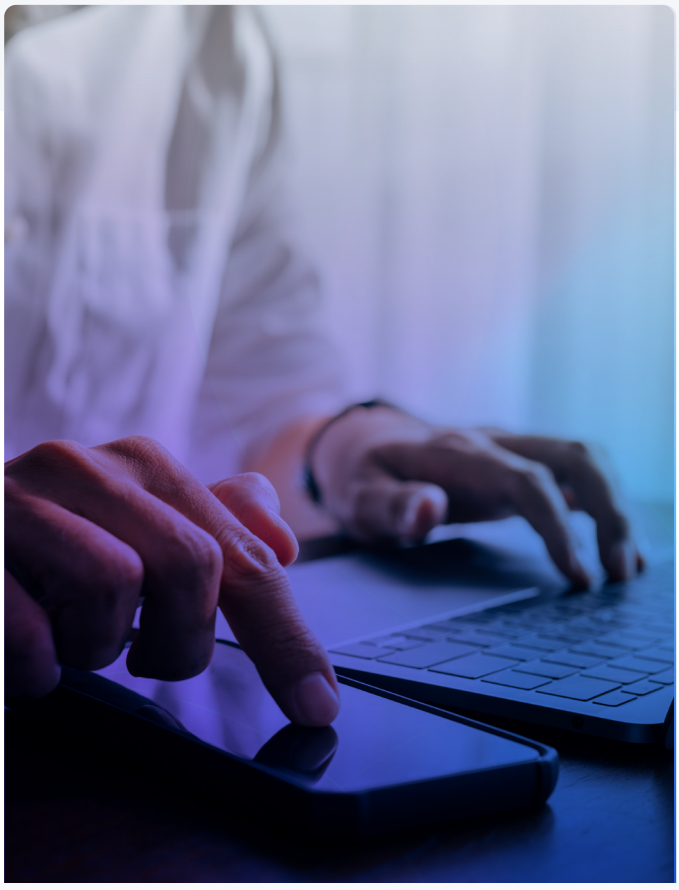
- Suivi et profilage
- Partage des données avec des tiers
- Collecte de contacts/publicité ciblée



des **applications** présentaient des comportements portant atteinte à la confidentialité

Le point de vue de notre RSSI

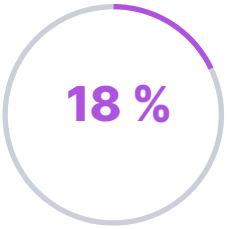
Les applications mobiles sont une porte d'entrée vers les données sensibles de l'entreprise. Pour gérer ce risque, les entreprises doivent contrôler les applications installées sur les appareils, protéger les données lorsqu'elles circulent sur les réseaux et acquérir une visibilité sur les vulnérabilités des applications dans l'ensemble du parc d'appareils. Dans le cas des appareils personnels utilisés au travail (BYOD), tout repose sur la séparation. Les données de l'entreprise doivent être protégées et isolées des informations personnelles. On obtient ainsi une approche équilibrée qui permet aux équipes de sécurité d'appliquer les contrôles dont elles ont besoin, sans empiéter, sur la vie privée des employés dont les données personnelles restent inaccessibles.



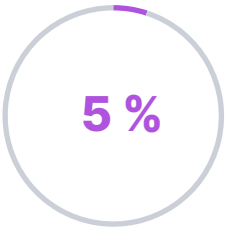
Risques liés au réseau et au Web

Tout comme le soleil se lève chaque matin, les pirates exploiteront toujours le maillon le plus faible de notre sécurité, à savoir le facteur humain. Grâce à l'IA générative, ils élaborent des attaques de plus en plus efficaces et convaincantes. Les utilisateurs cliquent sur des liens d'hameçonnage, se connectent à des réseaux Wi-Fi et à des points d'accès à risque, et oublient les bonnes pratiques de cybersécurité.

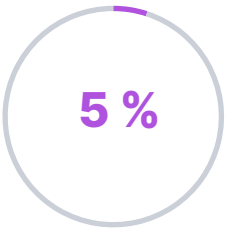
Les vulnérabilités ne se trouvent pas toujours au niveau de l'appareil ; même avec une sécurité parfaite et une configuration conforme, un mobile reste vulnérable à l'interception des données en transit. Les réseaux sont des vecteurs d'exploitation courants. Les manifestations sont variées :



des **organisations** ont des utilisateurs qui se connectent à des points d'accès à risque



des **organisations** ont des utilisateurs victimes d'attaques AitM basées sur l'infrastructure



des **organisations ont des** appareils touchés par le cryptominage pirate

Infrastructure de réseau

Vous pouvez contrôler la configuration de votre propre réseau, mais pas celle de tous les réseaux tiers (réseaux cellulaires inclus) auxquels vos utilisateurs se connectent lorsqu'ils sont hors des locaux. Vous avez sans doute mis en place l'accès conditionnel, la segmentation du réseau et des règles d'accès réseau « zero trust » (ZTNA).

Si ce n'est pas le cas, vos données sont en danger. Si un utilisateur se connecte à un réseau Wi-Fi public non sécurisé (avec un chiffrement faible ou une authentification inexistante), un pirate peut dérober ses cookies de session en contournant la validation des certificats et d'autres techniques de protection.

Les protocoles web régissent la façon dont les appareils, les navigateurs et les serveurs échangent des informations. Ils constituent un rouage essentiel de la sécurité des données. Les attaquants peuvent réduire ces protocoles à des versions plus anciennes et moins sûres, ce qui facilite le déchiffrement et le vol de données en transit. Votre organisation se retrouve ainsi exposée à des attaques de type « adversaire du milieu » (AitM).

Ces attaques AitM exploitent les vulnérabilités de l'infrastructure du réseau, plutôt que les failles du code d'un système d'exploitation ou d'une application.

Risques web

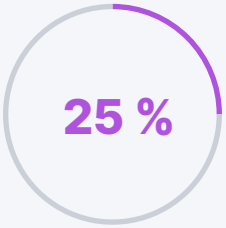
Même avec une connexion sécurisée, la navigation sur Internet n'est pas exempte de risque. Les appareils n'ont pas besoin d'être compromis pour présenter des problèmes. Les liens, les contenus publicitaires et les sites malveillants peuvent être le point de départ d'opérations de cryptominage pirate et de collecte d'identifiants par hameçonnage. Le cryptominage pirate consiste à exploiter le processeur et la mémoire d'un appareil pour miner de la cryptomonnaie. Ce détournement des ressources peut ralentir un appareil jusqu'à le rendre inutilisable.

Quant à l'hameçonnage, c'est toujours notre meilleur ennemi. Avec l'IA générative, il est plus facile que jamais d'élaborer un message de phishing convaincant. On ne peut plus compter sur les fautes de frappe et autres signes révélateurs classiques pour détecter les messages malveillants.

Les 30 marques les plus utilisées dans des campagnes d'hameçonnage

Les acteurs malveillants aiment imiter les marques populaires. Les utilisateurs sont plus enclins à cliquer sur un lien provenant d'un service qu'ils connaissent bien, et les pirates savent exploiter cette confiance. Ils ont donc tout intérêt à cibler les banques et les institutions financières, car les comptes compromis sont susceptibles de contenir à la fois de l'argent et des informations sensibles.

Notez que ces marques ne sont absolument pas en cause : les pirates utilisent leur réputation pour attirer des utilisateurs peu méfiants.



des **organisations ont eu** un utilisateur victime d'un lien d'hameçonnage.

Divertissement/ réseaux	Commerce	Services d'infrastructure	Services bancaires et financiers
Netflix	Microsoft	Optus	Allegro
Facebook	Apple	AT&T	U.S. Internal Revenue Service
Steam	Adobe	Amazon	Rakuten
eBay, Inc.		DHL	Coinbase
WhatsApp		British Telcom	PayPal
		Orange	AEON Card
		Comcast	Sumitomo Mitsui Banking Corporation
		East Japan Railway Company	Navy Federal Credit Union
			Bradesco
			Bank of America Corporation
			HSBC Group
			Raiffeisen Bank
			American Express
			ING Direct

Le point de vue de notre RSSI

En plus d'appliquer des contrôles techniques, il est essentiel d'apprendre aux employés à reconnaître et à signaler les menaces de phishing et d'autres formes d'ingénierie sociale, au moyen de programmes de sensibilisation, de formations et de tests d'hameçonnage. Les tests d'hameçonnage ont tout intérêt à utiliser l'IA pour proposer des contenus adaptés aux capacités des utilisateurs et les actualiser en fonction de l'évolution et de la diversité des menaces.

Prolifération des risques : les menaces persistantes avancées

Jusqu'à présent, nous avons abordé les risques touchant :

- Les systèmes d'exploitation et la configuration des appareils
- Les applications mobiles
- Le réseau et la navigation sur le Web

Qu'il s'agisse d'une faille dans un système d'exploitation, d'une application mobile mal sécurisée ou d'une connexion accidentelle à un Wi-Fi public, il suffit d'un risque pour mettre en danger la sécurité de vos données.
Sauf si vos règles de configuration sont robustes et que vos utilisateurs sont bien formés.

Toutefois, l'accumulation de ces risques devient rapidement problématique. Les groupes de menaces avancées ciblent plusieurs vulnérabilités en même temps pour créer des exploitations sophistiquées. Si les auteurs de ces attaques avancées ont toujours fait preuve de retenue en se concentrant sur des cibles de grande valeur, leurs outils se diffusent plus largement, ce qui peut mettre en danger des citoyens ordinaires.

Il est essentiel de comprendre ces menaces avancées pour pouvoir s'en défendre. Jamf Threat Labs a évalué différents mécanismes de livraison des exploitations (dont les attaques « zéro clic » et « un-clic ») et modèles de déploiement utilisés dans le cadre d'opérations de surveillance ciblée. Ces campagnes visent à obtenir des renseignements détenus par des profils spécifiques : journalistes, dirigeants d'entreprise, personnalités politiques, activistes, etc. L'analyse s'intéresse notamment aux vulnérabilités des systèmes d'exploitation et des applications tierces, et à la réponse des fournisseurs. Voici ce que l'équipe a découvert.

Pour protéger votre organisation :
Misez sur la détection post-exploitation, la télémétrie comportementale et la surveillance basée sur les anomalies, plutôt que de vous appuyer uniquement sur le contrôle des interactions utilisateur.

Les attaques « zéro clic » restent d'actualité

Les attaques « zéro clic » contre les appareils Apple et Android restent un vecteur de menace actif en 2025, en particulier pour les journalistes et les décideurs. On a ainsi découvert une attaque ciblant des utilisateurs de WhatsApp via une vulnérabilité d'imageparsing (CVE-2025-43300).

Cette découverte est la preuve que les attaquants parviennent toujours à exécuter du code sans aucune interaction de l'utilisateur, en contournant les défenses traditionnelles basées sur la formation. Ces attaques sont généralement associées à des opérations de surveillance ciblée ou de collecte de renseignements.

L'observation régulière de vulnérabilités « zéro clic » confirme que les attaquants motivés sont toujours déterminés à investir dans le développement d'exploitations coûteuses.

Les attaques par navigateur persistent, et en particulier la distribution discrète de charges nuisibles par le biais de publicités.

Apple et Google ont publié de nombreux correctifs de sécurité pour leurs navigateurs tout au long de l'année. Chrome a reçu 250 correctifs de sécurité ; Safari en a reçu plus de 75, preuve que l'on découvre constamment des problèmes de sécurité de la mémoire qui peuvent être exploités par des contenus web élaborés.

Ces vulnérabilités sont d'autant plus séduisantes qu'elles peuvent être exploitées par le biais de JavaScript intégré à des sites web ou des publicités malveillants, une approche à faible coût pour les attaquants. Les rapports d'intelligence des menaces confirment que les fournisseurs de logiciels espions commerciaux continuent de s'appuyer sur des chaînes d'exploitation en un clic, combinant des vulnérabilités de rendu à des techniques d'évitement des sandboxes pour une compromission totale de l'appareil.

La découverte des opérations d'Intellexa démontre que ces exploitations sont activement utilisées par les organisations de renseignement et qu'elles peuvent également être diffusées sous forme d'attaques « zéro clic » via des réseaux publicitaires.

POUR PROTÉGER VOTRE ORGANISATION :
Intégrez l'inspection du trafic web et la détection des exploitations à votre infrastructure de sécurité, et appliquez rapidement les mises à jour du système d'exploitation et du navigateur dans les environnements mobiles gérés.

Les entreprises visées ripostent activement, mais la couverture défensive reste insuffisante.

En 2025, les fournisseurs de plateformes et les grandes entreprises technologiques ont redoublé d'efforts pour repousser les opérations d'espionnage ciblées, en prenant notamment des mesures juridiques, techniques et architecturales. Des actions en justice très médiatisées, telles que le litige opposant Meta au groupe NSO, montrent qu'au-delà des défenses purement techniques, la dissuasion juridique est désormais de mise.

Parallèlement, Apple continue d'investir dans des mesures d'atténuation au niveau de la plateforme, notamment avec l'extension de marquage de la mémoire (MTE) et l'amélioration du mode de verrouillage. Pourtant, des chaînes d'exploitation persistent malgré ces mesures.

Des acteurs sophistiqués continuent d'adapter leurs outils et leurs techniques pour s'adapter aux nouvelles mesures d'atténuation. Des possibilités de contournement ont ainsi récemment été présentées lors d'une conférence privée.

POUR PROTÉGER VOTRE ORGANISATION :
Complétez les protections au niveau du fournisseur par des capacités indépendantes de détection, de visibilité criminalistique et de réponse aux incidents adaptées à des scénarios d'attaque ciblés.

Logiciels espions à surveiller

Predator | Développeur : Intellexa

Predator s'appuie principalement sur des exploitations web en un clic, diffusées notamment via des liens malveillants ou du contenu publicitaire. Il s'appuie fortement sur les vulnérabilités de WebKit, comme le montrent les correctifs répétés d'Apple. Ce modèle est plus évolutif, mais il est également sensible à la latence des corrections. Predator apporte la preuve que les attaques en un clic restent viables d'un point de vue opérationnel.

Graphite | Développeur : Paragon

Graphite est une plateforme commerciale de logiciels espions liée à l'exploitation avancée d'iOS ; elle s'appuie sur une diffusion « zéro clic » et « un clic ». Avec l'exploitation d'iMessage sans clic sur des iPhone parfaitement à jour en 2025, Graphite a démontré sa capacité à compromettre des appareils sans aucune interaction de l'utilisateur. Plusieurs infections ont été attribuées à la même infrastructure d'opérateur, confirmant un ciblage coordonné et délibéré plutôt qu'une activité opportuniste. Ces observations font de Graphite un successeur opérationnel sur le marché des logiciels espions, en dépit de la pression réglementaire et juridique accrue exercée sur les fournisseurs.

Landfall | Développeur : S.O.

Inconnue jusque-là, Landfall est une famille de logiciels espions Android de qualité commerciale, utilisée dans le cadre d'une campagne d'espionnage mobile visant les appareils Samsung Galaxy. Les opérateurs ont exploité une vulnérabilité critique de type « zero day » dans la bibliothèque de traitement d'images de Samsung pour diffuser le logiciel espion via des fichiers images malveillants, sans doute distribués via des applications de messagerie telles que WhatsApp.

La campagne, active depuis mi-2024 au moins, s'est poursuivie jusqu'à ce que Samsung corrige la vulnérabilité en avril 2025. Elle a fourni aux attaquants des capacités de surveillance complètes, avec enregistrement audio, suivi de la localisation et récolte de contacts, de photos et de journaux d'appels. D'un point de vue défensif, Landfall rappelle que les opérations de logiciels espions Android « zero day » continuent d'évoluer en toute discrétion. Cette campagne rappelle l'importance vitale de la gestion proactive des correctifs, de la détection des anomalies et de la télémétrie pour l'ensemble des plateformes mobiles.

Pegasus | Développeur : NSO Group

Pegasus est une plateforme de logiciels espions iOS et Android haut de gamme identifiée dans des chaînes d'exploitation « zéro clic » et « un clic » donnant lieu à une compromission complète de l'appareil. Ciblant un petit nombre de personnalités de grande valeur, elle est optimisée dans un souci de furtivité et de persistance. En 2025, les activités de NSO ont été affectées par des restrictions à l'exportation et des poursuites en justice. L'entreprise a depuis été rachetée par un groupe d'investisseurs, mais tout laisse penser que la technologie est toujours utilisée par des services de renseignement, peut-être sous une autre marque.

Dante | Développeur : Memento Labs

Memento Labs est un fournisseur italien de technologies de surveillance et le successeur de la Hacking Team, un groupe controversé rebaptisé après son acquisition en 2019. En 2025, des outils liés à Memento Labs ont été utilisés dans le cadre d'une campagne de cyber-espionnage avancée appelée Opération ForumTroll. Une vulnérabilité « zero day » permettait d'échapper à la sandbox de Chrome (CVE-2025-2783). Selon le CEO, l'entreprise a cessé de prendre en charge les solutions pour Windows afin de se concentrer sur les plateformes mobiles. On risque donc de retrouver cette famille de logiciels malveillants et ces vulnérabilités sur les appareils Android.

Spyrtacus | Développeur : SIO

Spyrtacus est une famille de logiciels espions commerciaux de surveillance, qui ciblerait activement les appareils Android en 2025. Il a été diffusé par le biais de liens malveillants et d'ingénierie sociale au niveau de l'application. Une fois installé sur un appareil, Spyrtacus présente les caractéristiques typiques d'un logiciel espion : exfiltration de données, localisation et collecte de messages et de contacts.

Contrairement aux logiciels espions « zéro clic » tels que Pegasus ou Graphite, l'implantation de Spyrtacus nécessite généralement un certain degré d'interaction avec l'utilisateur ou d'ingénierie sociale. La présence de Spyrtacus dans des campagnes réelles nous rappelle que les logiciels espions mobiles ne misent pas tous sur une exploitation « zero day ». Au contraire, certains attaquants n'hésitent pas à combiner l'ingénierie sociale avec des frameworks de logiciels espions commerciaux pour atteindre des objectifs similaires.

Le point de vue de notre RSSI

Malgré d'importantes mesures d'atténuation au niveau de la plateforme et des initiatives de renforcement du côté des fournisseurs, les pirates de 2025 découvrent et exploitent sans cesse de nouvelles vulnérabilités critiques, en particulier
dans des composants clés que sont les navigateurs (Chrome, Safari) et les applications de messagerie. Ces composants restent des cibles attractives en raison de leur complexité, de leur exposition fréquente à des contenus non fiables et de leur rôle central dans les workflows quotidiens des utilisateurs.

La persistance d'attaques ciblées doit nous rappeler qu'aucune stratégie d'atténuation n'élimine totalement les risques, surtout face à des adversaires qui disposent de ressources importantes. Pour toutes ces raisons, une gestion rigoureuse des appareils et une application stricte des mises à jour s'imposent toujours comme les mesures défensives les plus efficaces pour les entreprises.

De ce point de vue, la gestion des appareils mobiles n'est pas une simple fonction d'appui, mais une mesure de sécurité essentielle. En effet, elle garantit l'application rapide des mises à jour de sécurité et des configurations de référence, donne une visibilité sur les appareils et réduit les fenêtres d'exposition – autant de facteurs décisifs pour limiter l'impact des vulnérabilités émergentes.

Les risques sont importants, mais pas insurmontables.

Pour faire face à ces risques, il faut bien penser l'architecture.
La sécurité des appareils repose sur plusieurs piliers :

La gestion des appareils, pour appliquer des restrictions, des configurations et des règles

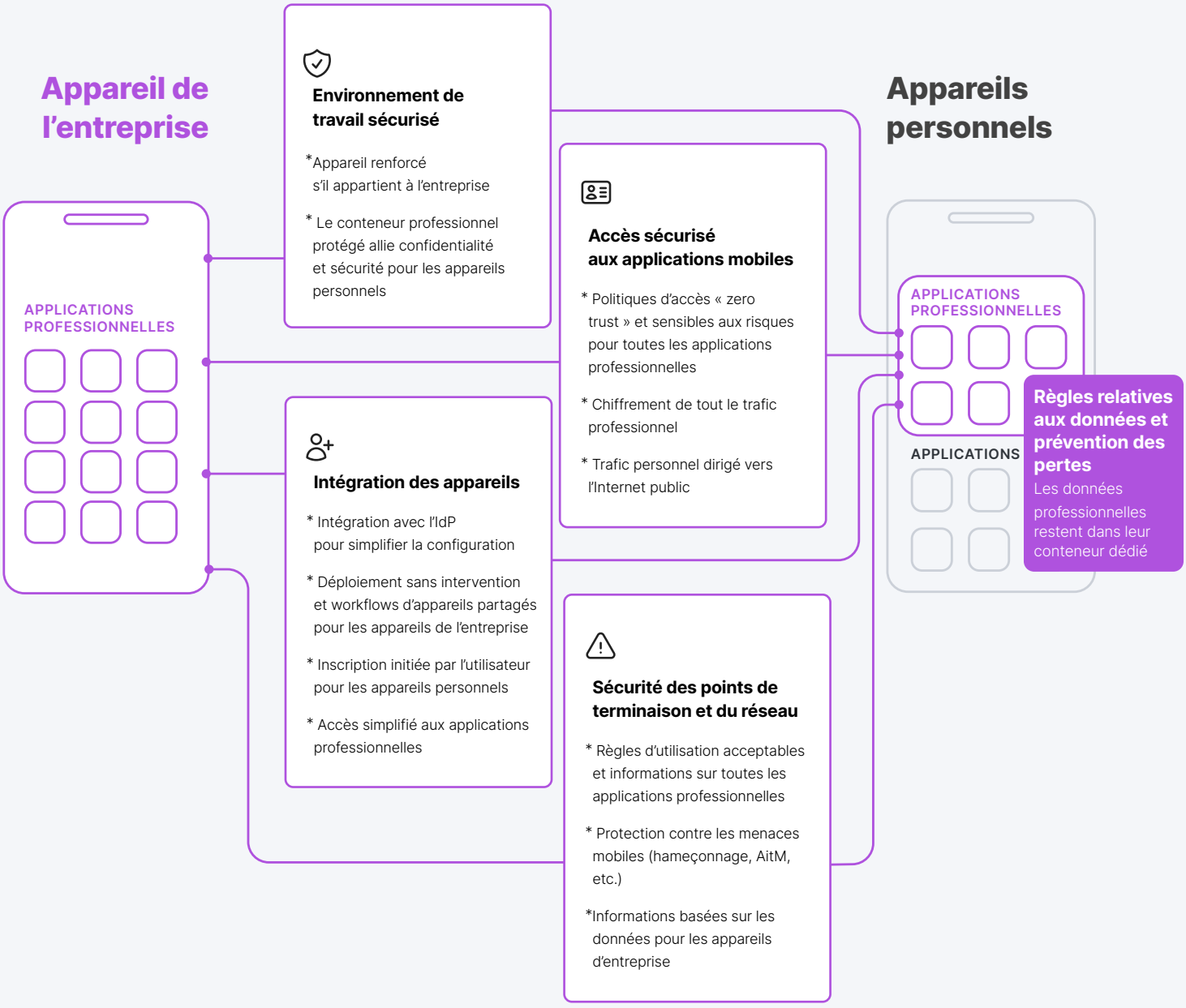
La sécurité des points de terminaison, pour surveiller l'état de santé et le comportement des appareils afin de détecter toute compromission potentielle

Un accès à distance sécurisé, pour déterminer quelles personnes et quels appareils peuvent accéder aux ressources de l'entreprise

Quand ces trois aspects sont réunis, seuls les utilisateurs autorisés et munis d'un appareil conforme peuvent accéder à vos données sensibles.

La situation peut être légèrement différente selon que **l'appareil appartient ou non à l'entreprise**.

La configuration de vos appareils peut être un risque ou un atout pour votre sécurité. En automatisant les mises à niveau, la validation des applications et l'analyse comportementale, et en appliquant des règles d'accès basées sur l'état de conformité, vous vous donnez toutes les chances de protéger vos données.



Lisez les dernières recherches de Jamf Threat Labs sur les menaces mobiles

Le logiciel espion Predator déjoue les indicateurs d'enregistrement d'iOS

FÉVRIER 2026

Grâce à une technique sophistiquée exploitant l'envoi de messages à nil avec Objective-C, le logiciel espion Predator contourne les indicateurs d'enregistrement d'iOS. Le logiciel malveillant accroche une seule méthode SpringBoard qui gère toutes les mises à jour de l'activité des capteurs, puis définit le pointeur self sur NULL. Résultat : les mises à jour de l'indicateur sont ignorées silencieusement au lieu d'être présentées à l'utilisateur. Cette approche est plus subtile que les techniques précédentes : l'appareil fonctionne normalement, mais ne donne aucune indication visuelle de la surveillance en cours, ce qui permet d'accéder discrètement à la caméra et au micro des appareils compromis.

OpenClaw : le discret assistant IA qui pourrait devenir votre plus grande menace interne

FÉVRIER 2026

OpenClaw est un cadre open source pour la création d'agents d'IA autonomes capables d'exécuter des commandes shell, d'accéder à des fichiers et d'interagir avec des applications. Comme il n'intègre pas de limites de sécurité, il introduit des risques importants pour la sécurité de l'entreprise. Le danger de ce cadre vient de son accès illimité au système, du potentiel d'exfiltration des données et de la vulnérabilité aux attaques indirectes par injection de prompt, consistant à intégrer des instructions malveillantes à du contenu commercial légitime. Des avis de sécurité récents ont démontré que des pirates pouvaient exploiter différentes failles pour obtenir un accès persistant. Les déploiements d'OpenClaw peuvent donc être considérés comme une menace interne à haut risque nécessitant des stratégies complètes de détection, de prévention et de gouvernance dans les environnements d'entreprise.

Le coupe-circuit de Predator : techniques d'anti-analyse non documentées dans les logiciels espions pour iOS

JANVIER 2026

Le logiciel espion Predator possède des capacités anti-analyse sophistiquées qui vont bien au-delà des résultats documentés jusque-là. Son système de code d'erreur, notamment, fournit aux opérateurs des informations de diagnostic précises en cas d'échec du déploiement. Le logiciel malveillant détecte le mode développeur, les outils de jailbreak, les applications de sécurité et les restrictions géographiques, et il met en œuvre un système avancé de neutralisation des défenses pour masquer les indicateurs d'enregistrement aux victimes.

Ces mécanismes fournisseurs aux opérateurs de précieuses informations en cas d'échec. Ils peuvent ainsi corriger les problèmes et adapter leur approche, preuve qu'ils sont prêts à investir des efforts considérables dans la détection et la recherche pour contourner les produits de sécurité.

Jamf Threat Labs découvre un jeu mobile qui divulgue les identifiants des joueurs

NOVEMBRE 2025

World of Warships Blitz, un jeu mobile populaire affichant plus de 10 millions de téléchargements, laissait échapper les identifiants de joueurs et des jetons de session via des connexions HTTP non chiffrées au moment de la connexion et de l'enregistrement. Les identifiants étaient dissimulés, mais la fuite permettant de réaliser des attaques par relecture des sessions, et donc de capturer et renvoyer des demandes d'authentification pour détourner des comptes. Après une divulgation responsable, le développeur a corrigé le problème dans la version 8.4.0 en coopération avec le lanceur d'alerte.

Cet incident souligne que les applications populaires peuvent, elles aussi, contenir des vulnérabilités critiques et qu'il est primordial de mettre en place des défenses de sécurité à plusieurs niveaux et de rappeler aux utilisateurs les bonnes pratiques relatives aux mots de passe.

Jamf Threat Labs découvre des applications qui font fuiter des identifiants

SEPTEMBRE 2025

Deux applications mobiles ont été surprises en train de divulguer des identifiants d'utilisateurs et des informations personnelles identifiables (PII) via des connexions HTTP non chiffrées : une application malaisienne de gestion des soins de santé avec 15 millions d'utilisateurs et l'application « Épargne » d'une société indienne de joaillerie. Parce que ces deux applications transmettent des données sensibles en clair, elles exposent leurs utilisateurs à de nombreux risques : vol d'identifiants, usurpation d'identité et accès non autorisé aux comptes, en particulier sur les réseaux publics.

Cette découverte souligne à quel point les organisations ont intérêt à sécuriser la transmission des données et à mettre en place des solutions de défense contre les menaces mobiles, comme le ZTNA et le filtrage de contenu, pour bloquer les applications à risque.

Flekst0re : évaluer la sécurité des boutiques d'applications tierces

AOÛT 2025

Les boutiques d'applications tierces pour iOS comme Flekst0re présentent de sérieux risques de sécurité, comme le montre le prototype d'une version modifiée WhatsApp capable d'enregistrer secrètement des conversations et de les transmettre à un serveur distant, avec une apparence de légitimité parfaite. Ces plateformes contournent le processus d'examen de sécurité d'Apple en resignant les applications avec des certificats d'entreprise. De plus, la fonction de source personnalisée de Flekst0re permet aux utilisateurs de télécharger des applications non vérifiées pouvant contenir des logiciels espions ou malveillants.

Les magasins tiers offrent un moyen pratique d'accéder à des applications modifiées, mais ils sapent fondamentalement les protections de sécurité d'iOS ; ils constituent ainsi un danger pour tous ceux qui utilisent des applications sensibles – services bancaires, messagerie instantanée ou e-mail.

jamf

Contactez-nous pour en savoir plus sur le paysage des menaces mobiles.