jamf

Security 360 : Rapport annuel sur les tendances de sécurité

Appareils mobiles

Avant-propos

Dans tous les secteurs et tous les cas d'utilisation, du commerce de détail à la santé, les responsables d'activité inventent de nouveaux usages de la mobilité pour transformer les pratiques de travail et optimiser les résultats de l'organisation. De nombreux employés n'utilisent au travail que des appareils mobiles, principalement des smartphones et des tablettes. Et dans le contexte du lieu de travail moderne, les collaborateurs doivent avoir les moyens de se connecter partout, à n'importe quel moment, sur l'appareil de leur choix.

L'un des principaux moteurs de l'adoption de la mobilité a été son intégration en tant que service sur le lieu de travail. Le mobile n'est plus seulement un accessoire pratique : il constitue de plus en plus le principal point d'entrée pour accomplir une tâche. Si la mobilité n'est pas nouvelle sur le lieu de travail, elle est plus que jamais intégrée aux workflows essentiels. Sur le lieu de travail d'aujourd'hui, l'expérience numérique ne doit pas seulement être exceptionnelle, mais aussi **sécurisées** et conçues pour maximiser la productivité des employés, quel que soit l'endroit où ils choisissent de travailler.

– **Josh Stein,**
vice-président de la gestion des produits

Introduction

Le rapport « Security 360 » de Jamf est le fruit de l'analyse d'incidents réels vécus par nos clients, de recherches sur les menaces et de l'étude d'événements survenus au cours de l'année écoulée. Ce rapport explore principalement le paysage des menaces mobiles afin de mettre en lumière les risques auxquels les organisations sont confrontées.

Nous proposons une évaluation des différents vecteurs d'attaque qui sont activement utilisés pour tromper les utilisateurs, compromettre les appareils mobiles et infiltrer les organisations. Ces attaques ne se limitent pas aux vulnérabilités des appareils, c'est pourquoi notre analyse porte également sur les applications à risque, les menaces web et d'autres dangers.

Outre l'analyse des tendances dans le domaine des menaces, le rapport apporte le point de vue du CISO de Jamf, qui nous éclaire sur les priorités des responsables de la sécurité chargés de protéger leur parc mobile, leurs utilisateurs, les applications et le réseau.

Méthodologie de recherche

Pour comprendre et quantifier l'impact réel des tendances de sécurité identifiées dans ce rapport, nous avons étudié un groupe d'échantillons composé de 1,4 million d'appareils protégés par Jamf. Nous avons mené notre analyse au cours du premier trimestre 2025, en revisitant les 12 mois précédents. Elle couvre 90 pays et plusieurs plateformes : iOS, iPadOS et Android.

Dans un souci de respect de la vie privée et pour appliquer 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 les personnes ou les organisations.

Objectif de la recherche

Dans cette analyse, notre intention est de permettre aux organisations et aux utilisateurs de comprendre l'évolution des tendances actuelles de la cybersécurité, mais également de mettre en avant les mesures que peuvent prendre les organisations et les utilisateurs pour atténuer les risques. Le rapport présente également un aperçu des recherches les plus importantes menées par Jamf Threat Labs, et notamment des menaces et des vulnérabilités que l'équipe a découvertes. En informant notre public sur les dangers présents dans l'environnement, nous espérons dissiper les mythes et proposer des mesures de sauvegarde afin de protéger les utilisateurs et les données. Voici donc les bonnes pratiques courantes à mettre en œuvre :

- Mises à jour continues et rapides des systèmes d'exploitation
- Éducation et formation des utilisateurs
- Vérification des applications
- L'authentification multifacteur
- Cadres de sécurité Zero Trust
- Définition et gestion des références de conformité
- Mise en place de règles d'utilisation acceptable pour les données de l'entreprise

Nous articulons notre analyse et noter rapport selon quatre catégories de risques qui, selon nous, doivent être prioritaires pour les organisations du monde entier :

I. Phishing mobile

II. Gestion des vulnérabilités

III. Risques liés aux applications

IV. Logiciels malveillants et logiciels espions

Les analyses contenues dans ce rapport s'appuient sur les renseignements sur les menaces de Jamf. Cette vaste collection d'informations provient de recherches originales sur les menaces, de mesures d'utilisation réelles, d'analyses des actualités et de flux de données. Les renseignements sur les menaces de Jamf proviennent des recherches menées par les membres des équipes du Jamf Threat Labs et de Data Science, qui surveillent les appareils, les applications et le trafic réseau pour détecter les risques, les menaces et les vulnérabilités zero-day.

Renseignements sur les menaces Jamf

Nous avons également rédigé un rapport Security 360 axé sur les **ordinateurs Mac**, que vous pouvez consulter **ici**.

Les statistiques présentées dans ce document concernent les appareils **Apple** et **Android**.

Principales tendances dans le domaine mobile

I. Le phishing reste un défi pour les entreprises

Le phishing reste une des techniques d'attaque omniprésente, et il exerce toujours une forte influence sur le paysage des menaces. En septembre 2024, **Apple a publié un article de blog** pour donner des conseils aux utilisateurs d'iOS et les aider à « éviter les escroqueries et savoir réagir face à des e-mails, des appels téléphoniques ou d'autres messages suspects ». Quel que soit le niveau sécurité d'une plateforme ou d'un système d'exploitation, les techniques d'ingénierie sociale (dont le phishing) sont conçues pour accéder aux données de l'entreprise en passant par l'élément le moins sécurisé d'un appareil : son utilisateur.

II. Il suffit d'une vulnérabilité pour que des pirates obtiennent un accès à l'ensemble du système

C'est une réalité : des vulnérabilités apparaissent dans les logiciels (OS et applications) que nous utilisons quotidiennement. Dans sa **publication spéciale 800-124rd**, le NIST affirme que « dans un logiciel typique, les erreurs et les vulnérabilités sont présentes à une fréquence estimée à 25 erreurs environ pour 1000 lignes de code. » Les vulnérabilités et expositions communes (CVE), publiées dans la base de données nationale sur les vulnérabilités (NVD), fournissent au public des informations précieuses sur les CVE présentes dans l'environnement. Ces ressources sont vitales, mais il faut qu'un correctif soit publié pour qu'elles soient vraiment utiles à une organisation.

Apple et Google fournissent des informations essentielles en cas de découverte de vulnérabilité, en précisant notamment quelle mise à jour du système d'exploitation permet de la corriger. En début d'année par exemple, Apple a publié iOS 18.3.2 en réponse à la **CVE-2025-24201**, qui pouvait permettre à un contenu web malveillant de quitter la sandbox de contenu web. **Google a publié un bulletin de sécurité Android** corrigeant 43 vulnérabilités de sécurité, dont deux vulnérabilités zero-day critiques.

III. Les applications introduisent des risques, même sur les plateformes sécurisées

Depuis leurs débuts, l'App Store d'Apple et le Google Play Store protègent aussi bien les utilisateurs que les organisations. Les utilisateurs Apple bénéficient de garanties lorsqu'ils téléchargent une application de l'App Store, car Apple « **analyse chaque application à la recherche de logiciels malveillants et d'autres logiciels susceptibles d'avoir un impact sur la sécurité, la sûreté et la vie privée de l'utilisateur** » Quant aux utilisateurs d'Android, le Google Play Store leur propose Google Play Protect. Mais cela n'arrête pas les acteurs malveillants. Au cours des cinq dernières années, Apple a évité plus de 9 milliards de dollars de transactions potentiellement frauduleuses.La **loi sur les marchés numériques** (DMA) de l'Union européenne autorise la création de boutiques d'applications alternatives et oblige les fabricants à ouvrir leur forteresse. Les applications distribuées par les boutiques d'applications tierces ne sont pas soumises aux mêmes règles que les applications de l'Apple App Store, ce qui peut présenter des risques pour la sécurité et la vie privée des utilisateurs. L'ingénierie sociale (phishing en tête), les ransomwares, les logiciels espions et bien d'autres menaces peuvent menacer les utilisateurs qui téléchargent des applications ou utilisent des systèmes de paiement alternatifs en dehors de l'App Store d'Apple.

Du côté d'Android, en début d'année, **Google a mis en garde contre un nouveau cheval de Troie** qui avait « infecté plus de 750 applications bancaires et d'achat légitimes. » Aujourd'hui, les deux principaux magasins d'applications ont dû autoriser les utilisateurs de l'UE à sideloader des applications, ce qui a pour effet d'élargir la surface d'attaque pour les acteurs malveillants.

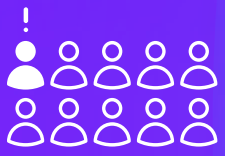
IV. Les attaques ciblées mettent les appareils mobiles en danger

Polyvalents et flexibles, les appareils mobiles permettent de travailler partout où il le faut. Il arrive souvent que de hauts responsables utilisent des appareils mobiles pour mener à bien leurs activités dans le monde entier. **Mais ces utilisateurs forment également le groupe le plus ciblé** en raison des données que contiennent leurs appareils : propriété intellectuelle, données financières, etc. Les pirates s'intéressent à ces profils prestigieux pour maximiser le rendement de leurs plans de chantage.

Au cours des douze derniers mois, nous avons découvert que :

25 %

des organisations avaient été touchées par une attaque d'ingénierie sociale



1 utilisateur sur **10**

a déjà cliqué sur un lien de phishing malveillant.

I. Phishing mobile

Le phishing est l'une des menaces les plus courantes et les plus préjudiciables qui pèsent sur les organisations d'aujourd'hui. Selon l'Agence de cybersécurité et de sécurité des infrastructures (CISA), « plus de 90 % des cyberattaques réussies **commencent par un e-mail de phishing**. »

Sur un appareil mobile, le phishing peut emprunter différents canaux. Il ne se limite plus à l'e-mail et peut prendre la forme de messages textuels (on parle alors de smishing), de messages sur les réseaux sociaux et de liens vers des sites web malveillants.

Mais pour quelle raison le phishing rencontre-t-il un tel succès sur les appareils mobiles ?

Rappelons pour commencer que **plus de 62 % des pages web consultées dans le monde** le sont sur un appareil mobile. Ces plateformes représentent donc la majorité du trafic Internet, et offrent donc aux pirates un plus grand nombre de cibles potentielles à exploiter.

Du fait de leur format compact, ils sont en revanche dotés d'écrans plus petits. Cela explique d'ailleurs leur popularité : leur taille permet de les emporter partout. C'est aussi ce qui permet aux organisations de créer des workflows mobiles dans de nombreux secteurs :

- Commerce de détail (point de vente, inventaire)
- Santé (tournées d'infirmières, équipement au chevet des patients)
- Fabrication (consignes pour les opérateurs, instructions sur l'utilisation des machines)
- Aviation (avionique de bord, appareils pour le personnel au sol)

Mais ces avantages peuvent aussi être source de distraction pour un utilisateur visé par une attaque de phishing. L'idée que les appareils mobiles sont intrinsèquement sûrs perdure, mais comme nous l'avons établi, il suffit d'un lien pour compromettre un appareil.

Les 20 marques les plus utilisées dans des campagnes de phising

Les appareils mobiles servent de support à de nouveaux workflows ; ils simplifient les échanges avec les clients et améliorent l'expérience utilisateur. Pour beaucoup d'entre nous, l'appareil mobile est un outil de travail essentiel, qu'il nous accompagne partout ou soit l'interface principale de nos tâches. La mobilité nous connecte à notre vie, au travail comme à la maison. Les pirates le savent et ils le mettent à profit.

Dans le cadre de nos recherches, nous avons constaté que certaines marques populaires reviennent régulièrement dans les attaques d'ingénierie sociale visant à tromper les utilisateurs sur mobile. Nous avons réparti ces marques en **quatre catégories** :

Nous utilisons les appareils mobiles pour une myriade de raisons : accès aux e-mails professionnels, achat d'articles ménagers, opérations bancaires personnelles. Ces usages courants et souvent nécessaires sont autant de tentations pour les acteurs malveillants, qui y voient un moyen d'accéder à nos données. Dans le tableau ci-dessous, nous présentons les vingt marques les plus utilisées en ingénierie sociale, réparties en quatre catégories.

1. Divertissement	2. Entreprise	3. Services d'infrastructure	4 Personnel
Netflix	Outlook	United States Postal Service	Amazon.com Inc
Bet365	Office365	Gazprom	Telegram
Steam	Allegro	AT&T Inc	Facebook Inc
	InterActive Corp	Orange S.A.	Chase
	Tencent	DHL	WhatsApp
		BT Group	Yahoo, Inc.

En raison de leur popularité, de leur prestige et de leur influence sur les entreprises et les particuliers, ces marques sont fréquemment exploitées par les pirates dans leurs attaques d'ingénierie sociale. En raison de la solidité de leur réputation, les utilisateurs sont plus enclins à interagir avec contenus malveillants déguisés en communications légitimes.

Si cette liste met en évidence les 20 marques les plus utilisées au cours de l'année écoulée, elle est loin d'être exhaustive. Les pirates s'adaptent constamment et les marques qu'ils imitent peuvent changer à tout moment. Ces observations soulignent surtout à qu'ils misent sur la confiance que ces marques ont su inspirer au fil des ans pour tromper et exploiter les utilisateurs.

Dans le monde moderne, nos informations personnelles sont constamment en danger. Avec la multiplication des appareils mobiles utilisés à des fins personnelles et professionnelles, le champ d'action des pirates s'élargit sans cesse. Les pirates emploient des tactiques toujours plus sophistiquées et créent des interfaces et des expériences réalistes en adoptant des styles de communication authentique pour attirer les victimes dans leur piège. Fort heureusement, les organisations peuvent mettre en place certaines mesures de protection (formation continue des employés, outils de prévention des menaces) pour protéger leurs utilisateurs et leurs données.

Sur les **12 mois de la période de l'étude**, Jamf a recensé environ **10 millions d'attaques de phishing** menées contre notre échantillon de **1,4 million d'appareils**.

Nous avons également constaté que **1,5 à 2 %** de ces attaques étaient régulièrement classées comme « **zero-day** » ; autrement dit, les pirates incitaient les utilisateurs à cliquer sur des liens malveillants menant à des destinations totalement inédites.

En identifiant et en inspectant les attaques de phishing de type zero-day, les organisations peuvent protéger les utilisateurs contre les nouveaux sites d'hameçonnage.

Le point de vue du RSSI

- **Mettre en place un programme de formation complet :** Cette initiative joue un rôle central dans notre réussite. Nous menons des campagnes de phishing sophistiquées, nous organisations des formations ludiques et proposons aux utilisateurs qui le souhaitent des formations ponctuelles. Les utilisateurs ont la possibilité de signaler les e-mails de phishing et reçoivent du feedback sur leurs signalements tout au long de l'année. Notre approche ne s'arrête pas à une simple formation annuelle.
- **Tenez-vous au courant des nouvelles tendances et tactiques :** Cela peut sembler évident, mais les pirates exploitent toutes les pistes possibles, y compris les nouvelles qui bouleversent l'actualité. Vous devez adapter votre formation et vos tactiques de blocage pour faire face à ces situations. Cela peut susciter un certain malaise chez les utilisateurs, mais la transparence est essentielle. Cette formation doit les préparer à réagir face à un pirate potentiel qui n'aura pas de compassion pour eux et cherchera souvent à susciter une réaction émotionnelle pour les faire céder.
- **Adoptez une approche à plusieurs niveaux :** Il n'existe pas de solution ou d'outil uniques pour se protéger d'une campagne de phishing ciblée. Il faut donc couvrir tous les angles. Bloquez les domaines malveillants. Mettez en place l'AMF. Adoptez une approche « Zero Trust ». Activez des règles d'ubiquité impossible. Une ou deux de ces mesures ne suffiront sans doute pas. La meilleure approche consiste à les multiplier pour éviter d'être à votre tour victime d'une attaque de phishing.

II. Gestion des vulnérabilités

On parle de vulnérabilité lorsqu'un système, une application ou un protocole présente une faiblesse ou une faille qui peut être exploitée par des pirates pour en compromettre la sécurité, l'intégrité ou la disponibilité. **Apple** et **Google** fournissent une liste des vulnérabilités connues qui ont affecté leurs systèmes d'exploitation. Cela signifie toutefois que ces vulnérabilités se retrouvent « dans la nature » jusqu'à la publication d'un correctif de sécurité par Apple ou Google. Entre le 1er janvier 2024 et le 1er avril 2025, Apple a documenté **29 mises à jour de sécurité** corrigeant des CVE associées à des versions majeures et mineures de macOS. Au cours de la même période, Android a documenté **39 vulnérabilités système** associées à une CVE dans le bulletin de sécurité Android.

Apple (via **Rapid Security Responses**) et Google (via les **correctifs de sécurité Android**) publient des correctifs de sécurité indépendants entre les mises à jour logicielles. Quel est l'intérêt de ces correctifs ? Ces mises à jour sont ponctuelles et peuvent être appliquées automatiquement sans avoir à attendre une nouvelle version.

Les **cybermenaces** modernes sont aussi créatives que complexes, et tous les utilisateurs, professionnels ou particuliers, doivent faire preuve de vigilance et mettre à jour leurs appareils. Il ne s'agit pas seulement de mettre à jour l'appareil : il faut également s'assurer que la **mise à jour** est **authentique**.

Jamf Threat Labs s'est récemment penché sur une méthode particulière utilisée au cours d'une séquence d'attaque : le maintien de la persistance. Leurs recherches ont montré comment « des pirates pourraient exploiter l'interface des réglages d'iOS, modifier les paramètres de mise à jour du système et afficher des invites et des notifications concernant la disponibilité d'une mise à jour d'iOS. »

Intéressons-nous à quelques vulnérabilités notables traitées dans des mises à jour récentes d'Appel (ce rapport a été rédigé en avril 2025) :

Correction de la CVE par Apple	Date	Score de la vulnérabilité	Impact
iOS 18.4.1 et iPadOS 18.4.1	Avril 2025	CVE-2025-31200 Score CVSS : 7,5 | Gravité : élevée	CoreAudio
iOS 18.4 et iPadOS 18.4	Avril 2025	CVE-2025-30430 Score CVSS : 9,8 | Gravité : critique	Services d'authentification
iOS 18.3 et iPadOS 18.3	Janvier 2025	CVE-2025-24085 Score CVSS : 7,8 | Gravité : élevée	CoreMedia
iOS 18.3 et iPadOS 18.3	Janvier 2025	CVE-2025-24154 Score CVSS : 9,1 | Gravité : critique	Filtre de contenu web

Versions AOSP* mises à jour	Date	Score de la vulnérabilité	Impact
13, 14, 15	Avril 2025	CVE-2025-26416 Gravité : critique	Escalade des privilèges
15	Mars 2025	CVE-2025-22403 Gravité : critique	Exécution de code à distance
15	Février 2025	CVE-2025-0096 Gravité : élevée	Escalade des privilèges
12, 12L, 13, 14, 15	Janvier 2025	CVE-2024-43771 Gravité : critique	Exécution de code à distance

* Android Open Source Project

Les vulnérabilités enregistrées sur les sites web d'Apple et d'Android nous rappellent à quel point elles sont inévitables au cours du développement d'un logiciel. Pour les professionnels de la sécurité, l'essentiel est de pouvoir visualiser ces vulnérabilités pour y remédier et préserver la sécurité de vos données.

Pour y parvenir, l'un des meilleurs moyens consiste à tenir les systèmes d'exploitation à jour, en misant sur les bons outils.

Maintenir une bonne posture de sécurité avec des systèmes d'exploitation à jour

Le meilleur moyen pour les entreprises d'atténuer les vulnérabilités et de maintenir leur organisation en conformité consiste à tenir à jour le système d'exploitation de leurs appareils. Comme on l'a vu sur la page précédente, Apple et Android mettent régulièrement à jour les OS qui présentent des vulnérabilités connues.

En entreprise, l'approche la plus courante pour tenir à jour les OS (et les applications professionnelles de leurs employés) consiste à utiliser une solution de gestion des appareils mobiles (MDM). La MDM fournit également des rapports d'inventaire détaillés qui donnent des informations sur l'OS de chaque appareil géré. Mais dans la plupart des cas, les organisations possèdent un parc d'appareils variés pour différents cas d'utilisation et profils d'utilisateurs, ayant chacun leurs propres applications. Difficile, dans ces conditions, de faire en sorte que tous les appareils du parc exécutent le système d'exploitation le plus récent. C'est même parfois infaisable, simplement parce qu'il faut tester certaines applications avant de faire la mise à niveau.

Au cours des douze derniers mois :

32 %

des organisations utilisent au moins un appareil présentant des vulnérabilités critiques (et qu'il est possible de corriger).

55,1 %

des appareils mobiles utilisés au travail utilisent un OS vulnérable

Nous avons observé que beaucoup d'organisations utilisent des appareils mobiles qui n'ont pas reçu les derniers correctifs de sécurité. D'après nos données, **4,8 %** des appareils Android présentant des vulnérabilités ont été utilisés pour accéder aux ressources d'une entreprise.

La mobilité nous permet de façonner nos méthodes de travail. Parce qu'ils permettent aussi bien de passer des appels professionnels en voiture que de créer des workflows efficaces pour les employés en contact direct avec la clientèle, les appareils mobiles repoussent les frontières du possible au travail. Mais ils restent des appareils informatiques et sont, à ce titre, vulnérables face aux acteurs malveillants. Les organisations peuvent agir pour atténuer les menaces qui pèsent sur leurs appareils mobiles en misant sur des outils qui concilient convivialité et sécurité, sur la formation des employés et sur une bonne connaissance des menaces courantes.

Le point de vue du RSSI

- **Assurez la visibilité des vulnérabilités au sein de votre organisation :**
  Avant toute chose, efforcez-vous d'obtenir autant d'informations que possible sur les vulnérabilités présentes sur les appareils des utilisateurs et dans l'infrastructure. Ces données vous permettront ensuite d'analyser l'empreinte des applications, les risques, le rayon d'impact, etc. C'est un excellent moyen de commencer à hiérarchiser vos vulnérabilités.
- **Mettez en place un solide programme de gestion des correctifs :**
  Pour revenir à la MDM, vous devez vous munir d'un outil qui vous puisse vous dire quelles sont les versions prises en charge et les versions les plus récentes des OS et des logiciels de votre environnement. Et s'il le fait en n'exerçait aucun impact ou presque sur les utilisateurs finaux, l'adoption n'en sera que plus facile.
- **Mettez en œuvre une approche d'accès basée sur le risque :**
  Si un appareil non conforme tente d'accéder aux ressources de votre entreprise, bloquez l'accès jusqu'à ce que l'utilisateur final puisse corriger la situation et remettre l'appareil en conformité, si possible de la façon la plus simple possible.

III. Risques liés aux applications

Fin novembre 2024, l'Agence de cybersécurité a publié **un rapport sur les vulnérabilités les plus couramment exploitées en 2023** (il s'agit de l'édition la plus récente). Le rapport étudie en détail les 15 CVE les plus préoccupantes, en précisant les possibilités qu'elles offrent aux acteurs malveillants. Les vulnérabilités sont présentes dans tous les systèmes d'exploitation, mais aussi dans les applications utilisées au quotidien par les travailleurs et les étudiants. Comme le mentionne le rapport, « les pirates ont exploité davantage de vulnérabilités zero-day pour compromettre les réseaux d'entreprise en 2023 qu'en 2022, ce qui leur a permis de mener des opérations contre des cibles hautement prioritaires. » L'agence de cybersécurité précise ensuite ce que les développeurs et les organisations utilisatrices peuvent faire pour atténuer ces vulnérabilités. Pour les organisations, }le rapport recommande de :

- Mettre à jour les logiciels, OS, applications et micrologiciels *dans les meilleurs délais*
- Procéder régulièrement à la découverte automatisée des actifs
- Mettre en place un processus robuste de gestion des correctifs
- Documenter des configurations de référence sécurisées
- Effectuer régulièrement des sauvegardes sécurisées des systèmes
- Tenir à jour le plan de réponse aux incidents de cybersécurité

Qu'est-ce qui fait qu'une application est « à risque » ? Voici les principales caractéristiques que recouvre cette désignation :

- Caractéristiques anormales
- Profils de code malveillants
- Permissions dangereuses
- Comportement dynamique à risque
- Profil de développeurs suspects

En obtenant une visibilité sur les versions des applications, les problèmes de sécurisation et d'autres attributs, les organisations se donnent les moyens d'enquêter activement en cas de problème et de le corriger immédiatement.

Les entreprises ont impérativement besoin de connaître l'état de santé de leurs applications. Les informations suivantes offrent de précieux indices pour identifier les applications à risque et y remédier :

- Nombre d'utilisateurs exécutant une version obsolète d'une application
- Nombre d'utilisateurs disposant d'une version spécifique d'une application donnée
- Liste des applications au chiffrement défaillant, et donc susceptibles de laisser fuiter des données sensibles sur les réseaux non protégés.
- Les applications qui demandent l'autorisation d'accéder aux données stockées dans d'autres parties de l'appareil.

Exploration d'une vulnérabilité en environnement réel
Contournement du cadre Transparence, consentement et contrôle (TCC)

Dans les systèmes d'exploitation Apple, le cadre TCC invite les utilisateurs à accepter ou refuser les demandes d'accès à des données sensibles – photos, contacts et localisation – émanant des applications. Une vulnérabilité de contournement du TCC permet de désactiver ce contrôle et d'autoriser une application à accéder à des informations privées à l'insu de l'utilisateur. Autrement dit, des pirates peuvent obtenir un accès non autorisé aux fichiers et dossiers de l'utilisateur, à ses données médicales, à son micro ou à sa caméra, entre autres, sans qu'il en soit averti.

Jamf Threat Labs a découvert la CVE-2024-44131, une vulnérabilité de contournement du TCC affectant le fournisseur de fichiers sur les appareils iOS. Apple a rapidement réagi à cette découverte en intégrant un correctif dans iOS 18.0. Les CVE telles que CVE-2024-44131 nous rappellent à quel point il est crucial de maintenir les appareils professionnels à jour.

Protections de l'App Store et tentatives de fraude

Comme nous l'avons déjà évoqué dans ce rapport, Apple a empêché plus de 9 milliards de dollars de transactions frauduleuses au cours des cinq dernières années. Pour la seule année 2024, l'entreprise a bloqué plus de 2 milliards de dollars d'opérations illégitimes. Plus précisément, en 2024, Apple a :

- Fermé plus de 146 000 comptes de développeurs en raison de problèmes de fraude
- Rejeté 139 000 inscriptions de développeurs
- Refusé plus de 43 000 applications parce qu'elles contenaient des fonctionnalités cachées ou non documentées
- Rejeté plus de 320 000 applications pour cause de plagiat, de spam ou de tentative de manipulation des utilisateurs.
- Détecté et bloqué plus de 10 000 applications illégitimes distribuées sur des boutiques pirates.

L'App Store est généralement considéré comme le moyen le plus sûr et le plus intuitif de télécharger des applications, avec les meilleures garanties de protection de la vie privée. L'App Store pour iOS utilise un système de sandbox, invite l'utilisateur à valider les demandes des applications, et n'autorise que le code signé à s'exécuter sur l'appareil. Mais comme le montrent les données, cela ne suffit pas à éliminer les attaques de pirates et la fraude. Apple s'engage à faire de l'App Store une boutique d'applications sûre et fiable, et protège ainsi les utilisateurs et les développeurs depuis son lancement en 2008. En revanche, les « applications tierces », c'est-à-dire les applications provenant d'autres boutiques, comme AltStore, ne bénéficient pas des mêmes protections.

Le point de vue du RSSI

Pour être efficace, la sécurité mobile requiert une approche à plusieurs niveaux. Votre organisation utilise sans doute le matériel le plus récent d'un fournisseur fiable, équipé du dernier système d'exploitation. Malheureusement , cela ne suffit toujours pas à protéger votre organisation et vos systèmes les plus sensibles contre les compromissions. Vous devez adopter les bonnes pratiques de sécurité dans chaque couche de votre pile technologique, et les applications en font pas exception.

- **Mettez en place un programme de vérification pour les applications mobiles sensibles de votre organisation :** Commencez par les applications critiques et vérifiez régulièrement que tout le monde utilise les versions les plus récentes et sécurisées. Développez le programme en vérifiant chaque application qui entre dans le magasin d'applications de votre entreprise.
- **Appliquez des règles qui signalent les appareils comme « non conformes »** lorsqu'ils possèdent des applications indésirables. Empêchez ces appareils à risque d'accéder à vos applications SaaS, à vos centres de données stratégiques ou à vos charges de travail distantes jusqu'à ce que les applications problématiques aient été mises à jour ou supprimées.
- **Intégrez la sécurité des applications mobiles aux programmes de formation** pour aider vos utilisateurs à jouer un rôle actif dans la sécurité. Apprenez-leur à faire les mises à jour nécessaires sur les appareils qui les accompagnent tout au long de la journée de travail.
- **Si votre organisation n'a pas besoin de boutiques d'applications alternatives**, fixez des règles qui interdisent l'accès à ces catalogues sur les appareils professionnels. Empêchez également le sideloading d'applications pour vous assurer que l'appareil n'exécute que celles qui proviennent de sources officielles.

L'équipe de Jamf Threat Labs a publié une étude démontrant comment une application de réseau social installée par sideloading pouvait inspecter les photos de l'utilisateur et les télécharger sur le serveur d'un pirate. L'application était « modifiée, mais parfaitement fonctionnelle ». L'équipe suggère plusieurs mesures claires pour améliorer la sécurité des appareils :

- Activer et examiner régulièrement le rapport de confidentialité des applications
- Faire preuve de discernement en ce qui concerne les autorisations des applications
- Éviter de stocker des informations sensibles

Télécharger uniquement des applications provenant de sources fiables (comme l'App Store).

Les applications natives et les applications web hébergées dans le cloud ne sont pas à l'abri des risques. Les applications cloud sont même davantage exposées en raison de l'étendue de la surface d'attaque. Cependant, avec les bons outils de visibilité, de contrôle et de correction, les organisations peuvent limiter la présence d'applications à risque sur le lieu de travail.

IV. Attaques ciblées et logiciels espions sophistiqués

Depuis 2021, **Apple envoie** des notifications de menace aux utilisateurs de plus de 150 pays. Adressées principalement à des personnes en vue comme des journalistes, des personnalités politiques ou des diplomates, ces notifications informent les utilisateurs qu'ils sont la cible d'attaques de logiciels espions mercenaires. Fin avril 2025, Apple « a envoyé des notifications à plusieurs personnes qui, selon l'entreprise, pourraient avoir été ciblées par un logiciel espion émanant d'un gouvernement. » Mais Apple n'est pas le seul constructeur concerné. Ces attaques ciblent tous les types de systèmes d'exploitation et d'applications. **Selon The Citizen Lab,** « un logiciel espion avait été implanté dans WhatsApp et dans d'autres applications sur l'appareil [Android] » d'un utilisateur.

Les malwares et les logiciels espions, comme ceux pour lesquels Apple envoie des alertes, comptent parmi les menaces les plus avancées qui pèsent aujourd'hui sur les organisations et les particuliers. Heureusement, il existe des outils pour protéger les utilisateurs à tous les niveaux de votre organisation.

Apple fournit des conseils pour se protéger des logiciels malveillants, dont beaucoup ont déjà été abordés dans le présent document. Plus précisément, Apple conseille de :

- Tenir à jour les appareils en installant les versions les plus récentes des logiciels, parce qu'elles incluent les derniers correctifs de sécurité
- Protéger les appareils avec un code secret
- Utiliser l'authentification à deux facteurs et un mot de passe fort pour son compte Apple
- Installer des applications à partir de l'App Store uniquement
- Utiliser des mots de passe forts et uniques en ligne
- Ne pas cliquer sur des liens ou des pièces jointes provenant d'expéditeurs inconnus.

Jamf Threat Labs : compromettre un appareil à l'insu de la victime

Jamf Threat Labs a démontré qu'il était possible de compromettre un appareil dépourvu de logiciel de sécurité à l'insu de la victime. L'équipe explique comment un pirat pourrait accéder aux e-mails, à la messagerie d'entreprise, à l'authentification à deux facteurs et à un grand nombre de données personnelles. Elle propose ensuite des pistes pour protéger les données professionnelles et personnelles :

1. Imposer des configurations sécurisées pour maintenir la conformité les appareils BYOD comme ceux de l'entreprise
2. Mettre en place la prévention et la surveillance des menaces avec des actions ciblées qui préservent la vie privée des utilisateurs finaux.
3. Forcer le chiffrement sur tous les appareils gérés.

Le point de vue du RSSI

Les logiciels malveillants ne sont pas aussi omniprésents sur les mobiles que sur les machines classiques. Mais lorsqu'on en découvre, ils utilisent bien souvent des techniques très sophistiquées pour cibler des personnes avec précision.

- **La négligence n'est plus possible** : vous ne pouvez pas partir du principe que votre organisation ne sera jamais infectée par des logiciels malveillants mobiles. L'année dernière, Apple a envoyé des avis de compromission par logiciels espions aux utilisateurs d'une centaine de pays.
- **Au minimum, désignez un responsable de la sécurité mobile**, dont la mission sera de produire des rapports réguliers sur l'intégrité du déploiement mobile de votre organisation. Consignez les incidents de vol de téléphone, de phishing ciblé, de dégradation des performances, bref, tout ce qui relève d'un comportement inhabituel. Dans l'idéal, mettez en place un flux de télémétrie pour fournir à votre centre des opérations de sécurité les données de vos outils de gestion et de sécurité des appareils. Traitez les appareils mobiles comme tous les autres terminaux.
- **Dans la mesure du possible, collectez les données des systèmes mobiles et recherchez des traces d'attaques zero-day.** Pour mener à bien ce projet, vous aurez besoin d'une expertise qui peut être interne ou sous-traitée. Dans les entreprises qui ont une équipe d'analystes de sécurité attitrée, il est essentiel d'investir dans le développement d'une expertise en forensique mobile.

Principaux points à retenir

Le phishing mobile est l'un des moyens les plus couramment employés par les pirates pour accéder à des informations sensibles. En mettant en œuvre un programme de formation, en s'informant régulièrement sur les tendances et les tactiques (notamment pour tenir à jour ce programme) et en adoptant une approche multicouche de la sécurité, les organisations peuvent établir un système de défense sans aucun angle mort.

Tous les types de logiciels présentent des vulnérabilités. Une bonne hygiène de sécurité permet d'atténuer les risques que ces vulnérabilités sont susceptibles d'introduire. C'est en mettant régulièrement à jour les systèmes d'exploitation et en désactivant les fonctionnalités inutiles (à commencer par les boutiques d'applications tierces) que les organisations peuvent assurer leur conformité aux profils de référence internes comme aux cadres externes.

Les manquements dans la gestion et l'utilisation des applications sont également source de risque. Le danger ne réside pas toujours dans l'application elle-même : il peut aussi provenir des connexions malveillantes qu'elle établit. Une boutique d'applications d'entreprise, regroupant des logiciels validés en continu (en particulier dans le cas des applications privées et personnalisées), permet de superviser plus étroitement les applications vulnérables pour appliquer rapidement les correctifs.

Les APT et les attaques de logiciels espions sont de plus en plus fréquentes. Souvent émises par des États voyous ou des groupes spécialisés, ces menaces affectent les organisations du monde entier. Elles ciblent souvent des personnes haut placées, dont l'appareil contient des données sensibles. Une stratégie de « défense en profondeur » qui traite les appareils mobiles comme tous les autres appareils permettra aux organisations de protéger efficacement leur écosystème d'appareils mobiles autant que les données auxquelles ils accèdent.

Établissez et maintenez des règles d'utilisation acceptable pour les appareils professionnels qui se connectent aux ressources de l'entreprise ou doivent se conformer aux politiques internes. Les appareils en BYOD devront faire l'objet de contrôles supplémentaires dans un souci de protection de la vie privée, à l'instar des **protections de confidentialité fournies** par Apple.

jamf

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