jamf

Security 360 :

Rapport annuel sur les tendances 2024

Résumé

Le rapport annuel de Jamf sur la sécurité se penche sur l'évolution du paysage des menaces en s'appuyant sur les données de clients réels, des recherches de pointe et les événements marquants du secteur. Nous proposons une évaluation réfléchie des divers vecteurs d'attaque couramment employés pour compromettre les appareils, tromper les utilisateurs et infiltrer les organisations, toujours dans le but de voler des secrets industriels et des informations personnelles. La conclusion de notre rapport apporte de nouveaux éclairages sur les bonnes pratiques du secteur et les mesures à prendre pour renforcer la posture de sécurité globale des entreprises, quelle que soit leur taille.

Introduction

Le rapport Sécurité 360 offre une large perspective sur l'évolution du paysage des menaces. En nous appuyant sur des données réelles, nous analysons les vecteurs d'attaque les plus impactants de l'année et l'adoption des bonnes pratiques de sécurité dans les organisations. Nous nous intéressons également aux applications qui innovent pour favoriser la productivité et les échanges.

Nous allons structurer notre analyse autour de quatre catégories de risques qui représentent un défi pour les organisations du monde entier :

I. Risques liés aux appareils

II. Risques liés aux applications

III. Évolution des logiciels malveillants et des attaques

IV. Risques liés au Web

À ces tendances en matière de menaces, Jamf ajoute des recommandations d'experts et des conseils que nous avons intitulés « retour aux fondamentaux ». C'est une façon pour nous d'exhorter les organisations à intégrer les bonnes pratiques de l'industrie à leurs processus de gestion des appareils, des applications et de l'infrastructure.

Voici quelques exemples de ces bonnes pratiques :

- Utiliser des produits de gestion et de sécurité intégrés pour maximiser les contrôles disponibles tout en minimisant le nombre d'agents à maintenir
- Renforcer les terminaux en suivant les recommandations de l'industrie ou les bonnes pratiques régionales
- Gérer l'exposition aux menaces en tenant à jour les systèmes d'exploitation (OS) et les applications, et en appliquant les correctifs
- Mettre en place des protections multicouches de défense en profondeur

Ce rapport regorge de conseils pensés pour aider les organisations à mieux se défendre contre les menaces connues, mais aussi à réduire la surface d'exposition, cible de techniques encore inédites. Nous nous attarderons sur l'évolution de l'ingénierie sociale pour dégager des pistes afin de protéger vos utilisateurs contre ces attaques, plus convaincantes que jamais.

Enfin, il est important de souligner que nos recherches et nos conseils s'appliquent à tous les appareils utilisés pour manipuler des données professionnelles, Apple, Microsoft et Android inclus, qu'ils appartiennent à l'entreprise ou aux employés (en BYOD).

À propos du rapport Sécurité 360

Nous voulons mieux comprendre les plus grandes tendances de sécurité qui ont un impact sur le lieu de travail moderne.

Nous devons nous intéresser à toutes les pièces du puzzle de la productivité – appareils, utilisateurs et applications – qui doivent être connectées pour permettre aux entreprises d'accomplir leur mission. Pour délivrer les éclairages de haut niveau et les statistiques présentés dans ce document, nous avons analysé les tendances de sécurité qui se manifestent chez notre clientèle. Nous avons également puisé dans les recherches originales de l'équipe Jamf Threat Labs sur les vulnérabilités des OS et des applications, dans ses explorations approfondies des attaques malveillantes et ses preuves de concept (PoC), qui couvrent quatre domaines différents :

Méthodologie de recherche

Pour comprendre et quantifier l'impact réel des tendances de sécurité identifiées dans le rapport de cette année, nous avons examiné un échantillon de 15 millions d'ordinateurs de bureau, de tablettes et de smartphones protégés par Jamf.

Nous avons mené notre analyse le quatrième trimestre de 2023, en revisitant les 12 mois écoulés et en couvrant 90 pays et de multiples plateformes : macOS, iOS/iPad, Android et Windows.

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.

Pourquoi c'est essentiel

L'objectif de cette analyse n'est pas de susciter la peur, mais bien d'informer les organisations et les utilisateurs sur les tendances actuelles de cybersécurité. Elle veut les éclairer sur les évolutions qui peuvent avoir un impact sur leur posture de sécurité et celle de leurs appareils. Elle met aussi en lumière les meilleures options dans le domaine de la sécurité des terminaux et précise comment appliquer ces mesures de protection à grande échelle, pour sécuriser tous les aspects des appareils, des utilisateurs et des données de l'entreprise.

Section I : Risques liés aux appareils

Avec la modernisation de l'informatique d'entreprise, les appareils utilisés quotidiennement par les employés deviennent de plus en plus complexes. Des capteurs intégrés détectent les informations contextuelles, des coprocesseurs déchargent les cycles de calcul les plus lourds et offrent de meilleures performances, et les possibilités de connectivité –Bluetooth, NFC, Wi-Fi, données cellulaires, etc. – sont bien plus nombreuses qu'avant.

Toutes ces nouveautés sont généralement intégrées avec les meilleures intentions du monde. Mais elles produisent un effet secondaire, d'ailleurs souvent négligé : chaque composant élargit la surface exposée aux attaques d'un adversaire.

Les appareils modernes comportent de nombreux risques. Fort heureusement, il existe des outils et des processus pour gérer ces risques efficacement.

La méthode la plus efficace est sans doute celle qui consiste à tenir à jour le système d'exploitation de chaque appareil, mais il n'est pas toujours possible de suivre le rythme de l'innovation.

On peut avoir de nombreuses raisons de retarder l'application des mises à jour logicielles : crainte des conflits, grand nombre d'agents dont il faudra la compatibilité, etc. Pourtant, si l'on ne met pas l'OS à jour, les appareils d'entreprises ont toutes les chances de comporter des vulnérabilités connues en passe d'être exploitées.

Et ces vulnérabilités ne touchent pas seulement les ordinateurs de bureau et les portables. Nous avons observé que **40 % des utilisateurs de mobiles utilisent un appareil présentant des vulnérabilités connues.** Et comme le mobile donne accès à de plus en plus d'applications d'entreprise stratégiques, ces appareils riches en données sensibles sont de plus en plus l'objet d'attaques qui pourraient être repoussées avec de meilleures pratiques.

En 2023, nous avons constaté que :

« 8 % des organisations comptaient dans leur flotte un appareil mobile ayant accès à une boutique d'applications tierce. »

« 40 % des utilisateurs de mobiles utilisent un appareil présentant des vulnérabilités connues. »

En 2023, nous avons constaté que « 8 % des organisations comptaient dans leur flotte un appareil mobile ayant accès à une boutique d'applications tierce. » Même si les intentions de l'utilisateur sont parfaitement innocentes, ces boutiques tierces regorgent d'applications souvent trompeuses qui ont un objectif clair : les inciter à exécuter des applications dont la sécurité interne a été sabotée. Dans quel but ?

Exécuter du code malveillant sur les appareils
Des fonctionnalités telles que Gatekeeper et l'API de sécurité d'entreprise devraient empêcher l'exécution de codes malveillants.

Contourner les protections de sécurité internes
C'est pourquoi il faut limiter ce qui s'exécute sur l'appareil sans contrôle approprié.

Accéder à des données d'entreprises sans autorisation
Les informations sensibles et confidentielles restent l'une des principales cibles des menaces.

Obtenir des données personnelles sans autorisation
Quand on sait que le dispositif Transparence, consentement et contrôles d'Apple, ou TCC, a pu être contourné par du code non autorisé, on comprend que la sécurité des terminaux implique forcément la protection de la vie privée.

Espionner les utilisateurs à leur insu
Là encore, les pirates ciblent de plus en plus les appareils mobiles parce que nous les avons sans cesse sur nous et qu'ils sont connectés en permanence. Cela leur permet d'écouter les conversations, d'intercepter les SMS et de suivre les mouvements physiques grâce au GPS.

Pivoter à partir de l'appareil infecté pour compromettre les réseaux
Ces étapes suivent l'installation de code malveillant.

Configurer pour la conformité

On définit souvent la conformité comme le respect des directives de diverses agences, comme les critères du CIS ou les standards du NIST, qui encadrent le traitement, l'utilisation et le stockage des données. Mais les organisations ont des besoins et des approches qui leur sont propres. Dans notre domaine, la conformité consiste à normaliser la configuration des appareils, la sécurité des données et les workflows des utilisateurs en les alignant sur un système qui vise à les protéger des acteurs malveillants.

Quelques enseignements à tirer des tendances de conformité des fonctions de sécurité propres à Apple :

FileVault : cette fonction de base, qui assure une protection stratégique des données de l'utilisateur en les chiffrant au sein du volume, était **« désactivée sur 36 % des appareils »** de l'échantillon de l'étude. Pourtant, cette fonction est très simple à déployer et à configurer à l'aide de votre solution MDM, qui gère aussi les clés de chiffrement.

Gatekeeper : avec un **« taux d'activation de 90 % dans l'App Store et chez les développeurs identifiés »,** Gatekeeper offre une couche de sécurité essentielle contre l'installation de logiciels malveillants. C'est une aubaine pour protéger la vie privée des utilisateurs : Apple vérifie, pour chaque application, que la collecte des données est bien conforme aux affirmations des développeurs.

Pare-feu : dans la mesure où les acteurs malveillants ciblent de plus en plus les appareils mobiles via le Web, il est alarmant de constater que la « fonctionnalité de pare-feu est désactivée sur 55 % des Macs. » Très facile à déployer à l'aide de solutions MDM, l'activation du pare-feu est une bonne pratique connue pour empêcher les appareils d'accepter les connexions provenant d'applications et de services non autorisés.

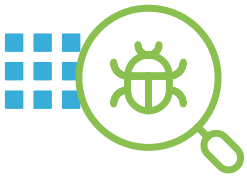
Écran de verrouillage : cette fonctionnalité fondamentale des appareils mobiles les protège contre les accès non autorisés, mais sert également de clé de déchiffrement pour toutes les données stockées localement. En 2023, « l'écran de verrouillage était désactivé sur 3 % des appareils ; dans 25 % des organisations, un utilisateur au moins ne l'avait pas activé. »

Section II : Utilisation des applications et expansion des risques

Gestion des vulnérabilités des applications

Même un appareil flambant neuf équipé du logiciel d'exploitation le plus récent peut être vulnérable s'il exécute des applications qui sont obsolètes ou comportent des bugs activement exploités par les pirates. Les organisations doivent impérativement gérer les vulnérabilités de la couche matérielle aux applications, en passant par l'OS.

Jamf a en effet observé que « 2,5 % des appareils comportaient une application vulnérable en 2023 ». Si nous devions extrapoler ce modeste pourcentage au **nombre d'appareils mobiles, estimé à 16,8 milliards dans le monde à la fin de 2023**, cela représente environ 420 millions d'appareils vulnérables dans le monde.



2,5 %

des appareils comportaient une application vulnérable

Le Conte de deux applis

Notre étude du paysage des menaces révèle que les organisations utilisent deux types d'applications fondamentalement différents. Les applications natives (sur l'appareil) utilisent les ressources de l'appareil pour exécuter du code et fournir des fonctionnalités aux utilisateurs finaux. Les applications web, en revanche, sont hébergées sur Internet, généralement dans un environnement SaaS ou un déploiement cloud privé. Elles s'appuient sur des centres de données ou des serveurs distants pour le traitement et le stockage des données.

Nos recherches montrent qu'aucun type d'application n'est épargné par les risques ;

- Les vulnérabilités doivent être gérées au sein de l'application, et la nature connectée des applications cloud les expose davantage aux manipulations à distance que celles qui résident sur un appareil.
- Et comme il est courant que plusieurs réseaux séparent un appareil d'une application distante, **la protection des données en transit** est de la plus haute importance si l'on veut gérer les risques associés aux applications cloud.
- La **protection des données au repos** est tout aussi importante pour les deux types d'applications. Même si les applications cloud sont souvent protégées par le périmètre du centre de données, les applications modernes intègrent fréquemment des logiciels open source, des substrats communs et des ressources de calcul partagées.

Les organisations dont les appareils sont gérés les connaissent mieux et les surveillent constamment. Mais qu'en est-il des appareils non gérés, et en particulier les smartphones personnels des employés ? Bien qu'il existe des différences, voici ce qui est valable pour tous les appareils, inscrits ou non :

- Il existe des vulnérabilités dans les deux cas.
- Tous deux abritent des données sensibles.
- Tous doivent être gérés.
- Tous ont besoin de règles d'accès basées sur le risque en temps réel pour atteindre l'objectif ultime : restreindre l'accès aux applications et aux données d'entreprise aux seuls utilisateurs autorisés.

Il ne reste donc qu'une seule option pour offrir à votre infrastructure une protection complète : connaître les deux types d'applications et mettre en place des protections de sécurité à plusieurs niveaux pour atténuer les risques des applications web et natives.

En mettant en œuvre un programme de gestion informatique plus intégré, qui associe les fonctions de gestion des appareils et des applications aux capacités et aux informations des outils de sécurité, les organisations peuvent créer un environnement de travail plus résilient. La clé réside dans une stratégie de sécurité en profondeur qui fournit une protection holistique à l'ensemble de votre infrastructure. Pour cela, elle doit incorporer des contrôles compensatoires pour s'adapter aux changements dans la posture de risque de l'appareil. Parallèlement, les données d'entreprise doivent être acheminées via des tunnels sécurisés distincts pour chaque demande émise par une application web.

D'autre part, une autre couche de contrôle de sécurité va associer ce qui précède à la gestion : elle va assurer la conformité à des profils de configuration renforcés, encadrer le déploiement d'applications gérées et appliquer des workflows automatisés de correction des vulnérabilités. Cette couche établit une base de référence et met en œuvre un niveau de sécurité fondamental, quel que soit le type d'appareil, le modèle de propriété ou la connexion réseau.

Applications cloud d’entreprise les plus utilisées

Microsoft

Google

Dropbox

Adobe

Box

Slack

Okta

Atlassian

Salesforce

Zoom

Gestion des vulnérabilités et des risques

Aussi séduisant soit-il, le téléchargement gratuit d’une application commerciale sur une boutique tierce s’accompagne souvent d’effets indésirables. En examinant les chiffres par plateforme, la recherche Jamf a révélé que le phénomène est deux fois plus fréquent sur Android que sur iOS.

Et bien qu’Apple renforce sans cesse la sécurité et la confidentialité dans l’ensemble de son matériel et de ses logiciels, ces résultats montrent que le constructeur n’est pas à l’abri de menaces de plus en plus ciblées.

« Le téléchargement d’applications sur des boutiques tierces est deux fois plus fréquent sur Android qu’iOS »

La sécurité des données d'entreprise et les appareils modernes

La sécurité des données se situe à l'intersection de l'équilibre entre vie professionnelle et vie privée et des technologies mobiles qui rendent possible le télétravail. Pour fonctionner, ce système doit parvenir à concilier des aspects profondément contradictoires. Prenons l'exemple d'un appareil utilisé par un professionnel de santé qui effectue des visites à domicile. Les dossiers des patients, qui sont des informations de santé protégées (PHI) et réglementées par l'HIPAA aux États-Unis, sont stockés dans l'appareil mobile du soignant, pour simplifier son travail en déplacement – c'est le premier des deux aspects. D'autre part, il est très facile pour un acteur malveillant de voler ce même appareil, ainsi que les données qu'il renferme – c'est le deuxième aspect, à l'opposé du premier. En d'autres termes, plus l'appareil est facile à transporter pour l'utilisateur, plus il peut facilement tomber entre les mains d'une personne non autorisée.

Plus de facilité = plus de risque.

Les appareils modernes ne sont pas nécessairement fournis par l'entreprise. Pour plusieurs raisons, dont la disponibilité des équipements, le coût des licences logicielles, les programmes de choix et la facilité d'utilisation, on utilise au travail un éventail d'appareils et d'applications appartenant aux employés ou à l'entreprise. Les organisations qui adoptent des normes modernes pour l'informatique et la sécurité ont un impératif : seuls les utilisateurs autorisés munis d'appareils vérifiés et conformes aux exigences de l'organisation doivent pouvoir accéder aux ressources et aux applications sensibles.

On comprend alors pourquoi l'une des grandes tendances concernant la sécurité des données des entreprises s'articule autour de deux domaines de risque :

- L'utilisation professionnelle des appareils personnels (BYOD)
- Le Shadow IT

Dans les deux cas, les appareils concernés peuvent être de tout type et de plateformes diverses, mais l'objectif est le même : l'utilisateur cherche à être productif en choisissant son matériel et ses logiciels. L'autonomie des utilisateurs est un aspect essentiel de la productivité. Néanmoins, ce manque de standardisation a de lourdes conséquences : la multiplicité des outils logiciels et des services, qui présentent tous des facteurs de risque différents, nuit gravement à la sécurité des données. Par exemple, les navigateurs web – comme Google Chrome, Microsoft Edge et Mozilla Firefox – remplissent une fonction essentielle : ils affichent les sites web qui permettent aux utilisateurs de faire des recherches et de travailler à tout instant de la journée. Mais multipliez le nombre de navigateurs par le nombre de versions en circulation, et pensez à la quantité de vulnérabilités et expositions communes (CVE) liées à chaque version. Vous obtenez un nombre incalculable de vulnérabilités potentiellement présentes sur les innombrables appareils utilisés pour accéder aux ressources des entreprises et des établissements scolaires du monde entier.

Le shadow IT, ou informatique fantôme, est depuis longtemps une épine dans le pied des entreprises. Les utilisateurs contournent les protections de sécurité pour installer des applications par des voies officieuses, ou utilisent des outils cloud qui n'ont pas été vérifiés ni approuvés. D'après nos recherches, Onion Browser et Tor figurent parmi les principales applications installées officieusement sur les appareils d'entreprise. Sur les appareils personnels, où les utilisateurs choisissent les applications qu'ils téléchargent et utilisent, les messageries liées à des réseaux sociaux figuraient dans le top 20 des applications vulnérables. En effet, les **escrocs utilisent massivement les réseaux sociaux pour cibler leurs victimes**, notamment via des offres d'emploi frauduleuses. Ces faux profils communiquent directement avec les cibles par message privé pour proposer des investissements en cryptomonnaie ou diffuser de fausses informations.

La surveillance du shadow IT fait partie intégrante de gestion de la conformité des appareils gérés par l'entreprise. Pour les appareils personnels, cette gestion a deux facettes. D'une part, les appareils doivent être configurés correctement et équipés pour le travail. Et d'autre part, les différentes règles de l'entreprise, notamment celles qui régissent la circulation des données entre les applications professionnelles et personnelles, doivent être appliquées conformément aux normes de l'organisation.

S'il faut retenir une chose, c'est que les équipes informatiques et de sécurité ont pour mission de sécuriser les ressources de l'entreprise, en limitant l'accès aux seuls utilisateurs autorisés, mais que la diversité des appareils utilisés constitue une variable qui affecte la sécurité. Les applications en libre accès, utilisables partout, y compris à l'aide d'appareils personnels dans une optique de productivité, présentent un plus grand risque. Pour compliquer encore les choses, certains employés, désireux de se faciliter la vie, contournent les règles de l'entreprise.

Prenons un exemple : si le réseau de l'entreprise bloque l'accès à un service de stockage cloud A, afin de contrôler le stockage des données professionnelles, mais qu'un employé utilise son appareil personnel pour placer des données sensibles dans un service de stockage cloud B, il a enfreint la règle et mis les données en danger.

Face à cela, la bonne pratique consiste à mettre en œuvre des règles qui associent l'authentification des utilisateurs, l'évaluation des appareils et la sécurisation de la connexion. Il s'agit de combler le fossé entre la gestion, l'identité et la sécurité en superposant les protections dans une stratégie de défense en profondeur. Les appareils, les utilisateurs et les données seront sécurisés et encadrés à chaque niveau, indépendamment du type d'appareil, de la localisation physique, du modèle de propriété, de l'OS ou du type de connexion au réseau.

Section III : Analyse des logiciels malveillants et évolution des attaques

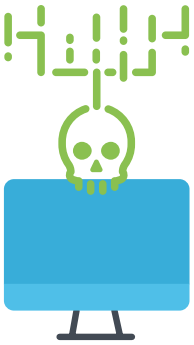
Dans cette section, nous explorons en détail les logiciels malveillants qui ont le plus d'impact sur les organisations et leur prévalence en 2023. Nous allons voir comment ont évolué les attaques affectant les deux plateformes, et comment certains pirates ciblent les vulnérabilités de l'OS pour tromper les utilisateurs et leur donner un faux sentiment de sécurité.

Menaces macOS

Si certains utilisateurs préfèrent ignorer les risques auxquels ils sont confrontés en ligne, les organisations savent que l'utilisation intensive des applications professionnelles fait d'eux une cible de choix.

Le saviez-vous ?

« 57 % des utilisateurs Mac pensent ou hésitent à infirmer que « les logiciels malveillants n'existent pas sur macOS ». Selon les résultats d'une enquête **rapportés par The Hacker News**, « un utilisateur Mac sur trois pense que ses données n'intéressent pas les cybercriminels » en 2023.



21

nouvelles familles de logiciels malveillants sur Mac

Le mythe selon lequel Mac ne peut pas être infecté par un virus a la vie dure. Pourtant, l'équipe du Jamf Threat Labs suit environ 300 familles de logiciels malveillants pour macOS, dont 21 sont apparues en 2023 !

Voici le détail complet des nouvelles instances de logiciels malveillants Mac étudiées et recensées en 2023, sur la base de nos observations :

Catégorie de logiciels malveillants	% de l'ensemble des logiciels malveillants sur Mac
Logiciels publicitaires	36,77
PUA	35,24
Troyens	17,96
Exploitations	4,40
Rançongiciels	2,00
Outils de téléchargement	0,92
Outils de piratage	0.67
Mineurs de cryptomonnaie	0,64
Certificat	0,64
Dropper	0,56
Outil d'extraction d'informations	0.25
Logiciels espions	0,23
Logiciels malveillants	0,20
Enregistreurs de frappe	0,04
Réseau	0,026
Virus	0,01
Faux antivirus	0,01
Hyperlien	0,01

Les différentes catégories sont classées par ordre décroissant de prévalence sur Mac. Soulignons toutefois quelques données intéressantes au sujet de certaines de nos découvertes, en commençant par les PUA (applications potentiellement indésirables). Cette catégorie est difficile à quantifier : elle englobe des applications bénignes et installées sciemment par l'utilisateur, mais aussi des logiciels installés à l'insu de l'utilisateur. Les utilisateurs doivent donc rester vigilants pour détecter toute opération imprévue sur leur Mac.

Au cours de l'année écoulée, ce sont les familles de Troyens qui ont été les plus nombreuses. Cela illustre la grande diversité du conditionnement et des modes de déploiement de ce type de code, et est sans doute le signe du nombre très élevé d'auteurs de logiciels malveillants.

Avec une prévalence de 17 %, la catégorie « Troyens » représente un risque important, car elle gagne en popularité au sein de la communauté des logiciels malveillants pour macOS. Posez-vous la question : qu'est-ce que les pirates insèrent dans les systèmes ? Pourquoi utilisent-ils cette tactique ? Les chevaux de Troie sont, par définition, des logiciels qui dissimulent du code malveillant. Cela nous rappelle une fois de plus que la gestion des vulnérabilités est indispensable, mais qu'il faut aussi :

- acquérir les applications auprès de sources légitimes
- appliquer un processus de validation (en choisissant des tiers de confiance comme l'App Store d'Apple, ou en confiant cette mission à l'équipe de sécurité de l'organisation)
- utiliser des logiciels de sécurité à jour

Atomic Stealer

Atomic Stealer, qui fait sa publicité sur Telegram, est un logiciel malveillant en tant que service qui propose une interface web aux pirates. Spécialisé dans le vol d'informations, il peut exfiltrer toute une série de données sensibles : mots de passe de comptes, données du navigateur, cookies de session et portefeuilles de cryptomonnaies. Atomic exploite notamment les fonctionnalités de dialogue AppleScript pour inciter les utilisateurs à fournir leurs identifiants. Une fois le mot de passe de l'utilisateur saisi, il dérobe d'autres données sensibles dans le trousseau de macOS. Distribué sous l'apparence d'applications légitimes telles que Tor Browser, Photoshop CC, Notion et Microsoft Office, ce logiciel malveillant a également été promu par le biais de Google Ads.

JokerSpy

Attribué au groupe APT BlueNoroff, JokerSpy a été repéré pour la première fois alors qu'il ciblait un échange de cryptomonnaies au Japon. Ce logiciel malveillant emploie diverses portes dérobées pour déployer des espions sur les systèmes compromis et utilise des outils open source pour ses opérations de reconnaissance. Écrites en Python, les portes dérobées permettent de charger des configurations dynamiques et d'exécuter des commandes, autorisant ainsi un large éventail d'opérations malveillantes. En plus d'évaluer les autorisations du système, JokerSpy est connu pour abuser les réglages de Transparence, consentement et contrôle (TCC) d'Apple. Il peut également déployer SwiftBelt, un ensemble d'outils open-source de post-exploitation sur macOS, couramment utilisé dans les exercices de red team.

KandyKorn

Ce logiciel malveillant a été découvert dans le cadre d'une attaque sophistiquée beaucoup plus vaste menée par des pirates nord-coréens contre des ingénieurs spécialisés dans la blockchain. Ils ont déployé une attaque en plusieurs phases via un faux bot sur Discord. La compromission initiale reposait sur divers scripts Python qui téléchargeaient des logiciels malveillants supplémentaires. Les scripts python servaient également de droppers pour l'étape suivante de l'attaque, consistant à établir une connexion avec un serveur C2. Un autre outil de piratage venait ensuite utiliser des techniques de persistance et d'évasion, comme le chargement de code binaire réfléchi, pour aboutir à l'exécution en mémoire du logiciel malveillant KandyKorn.

Lockbit

VXUnderground en parle comme d'un tournant, car c'est la première fois qu'un groupe majeur de ransomware cible les produits Apple. LockBit semble être un portage Apple de son homologue pour Linux, qui a fait surface pour la première fois au début de l'année 2022. Les premiers échantillons utilisaient une signature ad hoc et déclenchaient une fenêtre contextuelle de signature non valide au moment de l'exécution. Aux dernières nouvelles, LockBit n'exfiltre pas encore de données et serait encore au stade du développement actif, ce qui laisse penser que des fonctionnalités supplémentaires pourraient voir le jour. Quand il parvient à s'exécuter, ce ransomware chiffre les fichiers à l'aide de bibliothèques open-source et dépose une demande de rançon dans le système de fichiers.

NokNok

NokNok est une chaîne de logiciels malveillants APT attribuée à un acteur iranien et conçue pour la reconnaissance et le déploiement de portes dérobées sur les systèmes ciblés. Les attaquants utilisent des e-mails de phishing ciblés qui usurpent l'identité du Royal United Services Institute (RUSI). Ces messages incitent les victimes à télécharger une application VPN malveillante intitulée RUSI. Une fois installé, NokNok s'appuie sur des scripts bash pour créer des portes dérobées et recevoir des commandes du serveur. Il est capable de s'autodétruire ou d'exécuter des modules supplémentaires. Ces modules collectent des données sur les processus en cours, les informations système et les applications installées, et peuvent également assurer la persistance. Pour la transmission sécurisée des données, NokNok utilise son propre chiffrement, doublé d'un codage base64 et de segmentation.

iWebUpdate

iWebUpdate est un téléchargeur persistant conçu pour récupérer et exécuter des charges utiles quelconques à partir d'un serveur distant. Il maintient la persistance par l'intermédiaire d'un agent de lancement utilisateur nommé iwebupdate.plist. Dès son activation, il lance une opération de reconnaissance en exécutant des commandes telles que system_profiler. Il collecte des informations sur la version de l'OS et les envoie à un serveur de commande et de contrôle. Les charges utiles sont téléchargées dans un fichier temporaire à l'adresse /tmp/iwup.tmp, décompressées, puis exécutées. Le logiciel malveillant consulte le serveur toutes les heures pour recevoir des instructions supplémentaires.

ObjCShellz

ObjCShellz, une porte dérobée en Objective-C attribuée au groupe APT BlueNoroff/Lazarus, permet aux attaquants d'émettre des commandes shell sur les systèmes compromis. En établissant une connexion avec son serveur de commande et de contrôle, il permet d'exécuter des commandes shell dont les résultats sont retransmis au pirate. Ce logiciel malveillant a été identifié pour la première fois par l'équipe Jamf Threat Labs dans le cadre de la campagne RustBucket. Cette opération de BlueNoroff visait régulièrement les petites entreprises spécialisées dans les cryptomonnaies.

PureLand

Conçu pour dérober des informations, PureLand est un logiciel malveillant dissimulé dans une version piratée du jeu vidéo indépendant « PureLand ». Distribuée par e-mail, la version sabotée du jeu promet aux utilisateurs de générer des cryptomonnaies pendant qu'ils jouent. De façon assez intéressante, PureLand a été découvert en même temps que Realst Stealer, autre logiciel malveillant qui emploie une tactique d'ingénierie sociale remarquablement similaire, mais dont la charge utile finale est différente.

Realst Stealer

Realst Stealer, un logiciel malveillant basé sur Rust et axé sur le vol d'informations, cible principalement les cryptoactifs présents sur les systèmes compromis. Au cours d'une campagne bien documentée, des logiciels malveillants ont été ingénieusement intégrés à des jeux vidéo peu connus. Pour le distribuer, les pirates ont approché des joueurs en leur proposant un accès anticipé exclusif à ces jeux, présentés comme une opportunité de gagner des cryptomonnaies grâce aux NFT. En réalité, dès que l'utilisateur lance le jeu, Realst Stealer s'active, compromet le système et lance des routines de vol de cryptomonnaie.

Rustbucket

RustBucket est un cheval de Troie d'accès à distance. Les chevaux de Troie sont plus souvent axés sur l'espionnage que les gains financiers, mais on peut observer des recoupements en fonction des objectifs des pirates. Les Troyens possèdent souvent de nombreuses fonctionnalités : commandes shell à distance, enregistreurs de frappe, vol d'informations, etc.

RustBucket est exploité par le groupe APT BlueNoroff, une antenne nord-coréenne du célèbre groupe Lazarus. Ce logiciel malveillant en plusieurs étapes cible les utilisateurs via des campagnes d'ingénierie sociale complexes. Les droppers initiaux sont écrits en Objective-C, Swift et AppleScript, tandis que la charge utile finale est conçue en Rust. Dans les campagnes classiques, le logiciel malveillant prend l'apparence d'un lecteur PDF inoffensif. Les utilisateurs sont convaincus d'utiliser l'application pour ouvrir un document PDF, mais cette action déclenche une communication avec le serveur de commande et de contrôle du pirate.

WTFMiner

WTFMiner est un logiciel malveillant de cryptojacking discret qui se propage par le biais d'applications macOS piratées. On peut remonter sa trace jusqu'à un diffuseur de torrents qui incorporait déjà cet outil de minage à différentes applications macOS piratées en 2019. En se procurant des exemplaires, Jamf a suivi l'évolution de son développement sur trois générations. Chaque version employait des techniques de furtivité supplémentaires. Le logiciel achemine ses communications via le dark web pour un maximum de discrétion, prend l'apparence d'un processus légitime et se ferme lorsqu'on ouvre le moniteur d'activité. Les variantes les plus récentes n'ont même pas besoin de persister sur le disque : elles attendent que l'utilisateur lance les applications vérolées pour initier le minage.

Enfin, nos recherches ont permis de découvrir que les ransomwares, même s'ils sont loin d'être la famille la plus représentée, parviennent tout de même à se hisser dans le top 5 des nouveaux logiciels malveillants. Cela s'explique par le grand nombre d'instances identifiées dans cette catégorie. Certes, plusieurs familles de ransomwares ont été découvertes l'année dernière, à commencer par **Turtle Ransomware** et **Lockbit pour macOS**. Pour autant, Jamf Threat Labs a constaté que la plupart des échantillons étiquetés comme « ransomware » restent apparentés au ransomware EvilQuest découvert à l'origine en 2020.

Le fait est intéressant, mais beaucoup pensent que la diversité des échantillons d'EvilQuest est en réalité imputable à un bug de sandbox. Le ransomware n'est pas activement diffusé et ne l'a pas été depuis sa découverte en 2020.

Nos observations

Si l'on fait une analyse plus détaillée des nouveaux logiciels malveillants Mac observés dans les environnements de nos clients, nous obtenons le classement suivant :

Rang	Famille	% du total observé dans l'environnement	Catégorie
1	genieo	13,63	Logiciels publicitaires
2	imobie	12,25	PUA
3	générique	10,02	Logiciels publicitaires
4	multiverze	6,84	Logiciels publicitaires
5	tnt	6,19	PUA
6	ccleanmac	5,28	Logiciels publicitaires
7	mackeeper	4,55	Logiciels publicitaires
8	pirrit	4,45	Logiciels publicitaires
9	macinformer	4,37	Logiciels publicitaires
10	installcore	3,98	Logiciels publicitaires

Les menaces sur mobile

Si l'idée que les Mac sont à l'abri des logiciels malveillants persiste en dépit de la réalité, les menaces mobiles, en particulier sur iOS, sont réelles mais difficiles à quantifier avec de simples statistiques. Les professionnels de la sécurité sont confrontés à l'impact de ces menaces sur les données d'entreprise et la vie privée des utilisateurs. Nous révélerons plus loin quelques découvertes surprenantes faites par des chercheurs en sécurité en 2023, et qui mettent en évidence les détails de ces menaces mobiles.

Remarque : les pourcentages fournis dans cette section sur la base de nos observations semblent nettement inférieurs, surtout si on les compare à d'autres sections de ce rapport. Mais comme le dit le dicton, « il ne faut pas juger un livre à sa couverture » – et c'est particulièrement le cas dans le domaine de la cybersécurité :

- La population **mondiale a atteint 8 milliards en 2022**, selon les estimations des Nations Unies.
- On estime que le **nombre total d'appareils mobiles dans le monde est de 16,8 milliards en 2023** et qu'il continue d'augmenter
- Le pourcentage de la **population mondiale possédant un ordinateur portable ou de bureau à la maison** atteignait 47,1 % en 2019
- Le nombre moyen **d'appareils par personne est de 3,6 à l'échelle mondiale**.

Pourquoi toutes ces statistiques sur le nombre et les types d'appareils sont-elles essentielles pour comprendre l'impact des menaces modernes sur la sécurité mobile ? Elles apportent un contexte essentiel aux chiffres de notre recherche.

> « Une application potentiellement indésirable était installée sur moins de **1 %** des appareils et présente dans la flotte de moins de **2 %** des organisations en 2023. »

Comme nous le disions, un chiffre inférieur à 1 % n'est pas très inquiétant à première vue.

Pourtant, il l'est. Extrapolons les statistiques ci-dessus pour donner une vision précise et réelle de l'importance de ces pourcentages.

Commençons par les 16,8 milliards d'appareils mobiles actuellement utilisés dans le monde. Si l'on fait le calcul, 1 % de ce chiffre représente 168 millions d'appareils mobiles qui hébergent des logiciels malveillants. Intéressons-nous maintenant à la population mondiale. Sur les 8 milliards d'habitants, ôtons les 47,1 % qui possèdent déjà un ordinateur pour nous concentrer sur l'utilisation mobile. Cela représente une population de 4,232 milliards d'utilisateurs potentiels d'appareils mobiles. Ensuite, les choses se compliquent un peu : nous multiplions le nombre d'habitants par la moyenne mondiale de 3,6 appareils mobiles par utilisateur, pour obtenir 15,23 milliards d'appareils mobiles.

Nul besoin d'être un grand mathématicien pour comprendre qu'un écart substantiel sépare 15,2 milliards de 16,8 milliards. Mais il y a une subtilité. La moyenne mondiale fait la moyenne de toutes les régions pour établir une mesure globale. En effet, chaque région a des taux d'équipement différents. Certaines se classent en dessous de la moyenne mondiale, comme l'Amérique latine (3,1), tandis que d'autres affichent un taux d'équipement trois à quatre fois supérieur à la moyenne. C'est notamment le cas de l'Europe occidentale (9,4) et de l'Amérique du Nord (13,4). En reprenant les chiffres pour tenir compte des fluctuations régionales, voici le nombre d'appareils mobiles que nous obtenons pour chaque région évoquée :

- Amérique latine : 11 680 800 000
- Europe occidentale : 35 419 200 000
- Amérique du Nord : 50 491 200 000

Je vous promets que c'est le dernier calcul ! Voyons maintenant ce que représente 1 % d'appareils mobiles infectés si l'on extrapole sur la base des valeurs par région :

- Amérique latine : 116 808 000
- Europe occidentale : 354 192 000
- Amérique du Nord : 504 912 000

N'oubliez pas qu'il suffit qu'*un seul* appareil soit compromis pour que des acteurs malveillants réussissent à commettre une violation de données.

L'évolution des attaques

L'année 2023 a été généreuse en opportunités pour l'équipe Jamf Threat Labs, qui a découvert non pas une, mais plusieurs menaces mobiles différentes. Complexes et puissantes, toutes ciblaient des appareils iOS et leurs utilisateurs.

Les appareils mobiles ne se limitent pas à la plateforme d'Apple, bien sûr. Mais une grande part de nos recherches révèle que les acteurs de la menace ciblent de plus en plus l'écosystème Apple. Ils consacrent même des ressources techniques considérables au développement d'attaques inédites et difficiles à détecter pour compromettre les plateformes iOS/iPadOS.

Apple a pris les devants dans ce domaine en faisant de la sécurité et de la protection de la vie privée des éléments essentiels de sa philosophie de conception. Selon les recherches du constructeur sur les **menaces mobiles visant les données des consommateurs et des entreprises**, *« le nombre total de violations de données a plus que triplé entre 2013 et 2022, exposant 2,6 milliards d'enregistrements personnels au cours des deux dernières années seulement »*. Les chercheurs relèvent également que le phénomène « s'est aggravé en 2023 ».

Évolution de l'ingénierie sociale

Les menaces liées à la mobilité sont bien réelles. Chaque année voit l'apparition ou le perfectionnement d'applications et de services tiers. En 2023, notre équipe Jamf Threat Labs a d'ailleurs observé plusieurs nouvelles menaces sur iOS relevant de l'ingénierie sociale 2.0.

Découvertes concernant Pegasus

En avril, Jamf Threat Labs a publié les résultats de ses recherches approfondies sur deux appareils compromis par Pegasus. Le premier, un iPhone 12 Max Pro appartenant à un militant des droits de l'homme au Moyen-Orient s'est avéré être un trésor pour notre analyse. Il contenait en effet tout un ensemble d'indicateurs de compromission manifestement associés à Pegasus. Les résultats ont mis en évidence « des indicateurs de compromission (IoC) uniques et les preuves de campagnes d'espionnage actives ».

Au cours de l'analyse, Jamf a également découvert un nouveau IoC en explorant le système de fichiers du deuxième appareil, un iPhone 6s. Celui-ci appartenait à un journaliste européen travaillant pour une agence de presse internationale. Les recherches ont révélé que les pirates continuent de cibler les appareils plus anciens, ce qui nous doit nous rappeler une chose : ils cherchent à « exploiter la moindre vulnérabilité de l'infrastructure d'une organisation et à l'attaquer par tous les angles possibles ».

Faux mode avion

En août, Jamf Threat Labs a mis au point une technique post-exploit pour établir une persistance sur iOS 16. En modifiant l'interface utilisateur de manière à afficher les icônes attendues à l'écran tout en coupant les connexions Internet de toutes les applications, le pirate fait croire à l'utilisateur que le mode avion est activé. En réalité, il maintient un accès réseau sur l'iPhones exploité ou jailbreaké.

Pour plus de tranquillité, le mode avion apporte une couche supplémentaire de confidentialité et de conformité à certaines réglementations pendant les voyages. Mais en modifiant cette fonctionnalité pour la rendre inopérante, les pirates peuvent compromettre l'appareil de leur victime à son insu et établir une persistance en maintenant un accès non autorisé à l'appareil iOS, afin de poursuivre les étapes de leur attaque.

Faux mode de verrouillage

En décembre, l'équipe Jamf Threat Labs a créé une nouvelle technique suite à la preuve de concept que nous venons d'évoquer. Cette méthode a des conséquences plus lourdes sur la sécurité et la vie privée des utilisateurs. Ciblant le mode verrouillage d'Apple, cette technique de sabotage post-exploitation envoie tous les signaux visuels associés au mode verrouillage, sans appliquer aucune des protections qui y sont normalement associées.

On peut imaginer que les pirates implantent du code malveillant pour mettre en œuvre l'attaque décrite ici. En activant le mode verrouillage, l'utilisateur d'un appareil vulnérable – généralement une personnalité à haut risque – déclenche par inadvertance le code de l'attaquant. Tous les indicateurs visuels du mode verrouillage s'affichent, mais ils n'apportent aucune modification à la configuration de l'appareil. Ainsi, au lieu de protéger l'appareil en limitant les fonctionnalités accessibles à distance, l'iPhone est en réalité exposé, compromis et entièrement accessible aux acteurs malveillants.

Section IV : Menaces web et risques en ligne

Les attaques qui s'appuient sur la connectivité des appareils modernes appartiennent à la catégorie des menaces web. Elles visent généralement à attaquer l'utilisateur ou l'appareil via le réseau pour transmettre des signaux de commande et de contrôle ou pour exfiltrer des données. Ce terme générique décrit différents types de menaces. C'est également dans cette famille qu'on rencontre les attaques les plus vastes, les plus sophistiquées, les plus dommageables et, malheureusement pour les victimes, les plus performantes du paysage moderne des menaces.

Les menaces web constituent une part stratégique de la chaîne d'attaque sur les appareils mobiles. Elles ont en commun un point de départ très largement exposé aux utilisateurs et aux appareils. Leur nature est différente de celle des CVE présentes dans une application ou un OS, mais elles représentent un maillon contre lequel les organisations peuvent mettre en œuvre de puissants contrôles.

Il ne faut pas voir les menaces web comme une catégorie distincte des autres vecteurs de menace. Elles sont plutôt un véhicule de livraison. Ces attaques sont souvent combinées à des tactiques plus traditionnelles. Elles sont, le plus souvent, des pièces au sein d'un puzzle plus vaste qui peut souvent :

1. Fournir aux pirates les meilleures chances de succès pour un minimum d'efforts.
2. Contourner les règles et les contrôles de sécurité les plus stricts.

Concernant le premier point, nul besoin d'être grand clerc pour comprendre que la principale menace reste le phishing. Il ne faut que quelques secondes pour envoyer un lien malveillant par SMS à des centaines ou des milliers de cibles, et la probabilité que certaines d'entre elles cliquent dessus est suffisamment élevée pour que la campagne soit un succès.

Le deuxième point est, quant à lui, sans appel : tous les contrôles de sécurité du monde ne servent à rien si les utilisateurs donnent d'eux-mêmes leurs identifiants et, par conséquent, l'accès à des informations personnelles identifiables (IPI). Il n'est même pas nécessaire d'être un technicien habile ni de développer du code complexe. Il suffit de demander à votre cible de fournir ses identifiants de façon suffisamment convaincante pour compromettre un système ou un service.

Dans la suite, nous approfondissons nos recherches afin de mettre en évidence les principales menaces qui pèsent sur les appareils.

Phishing

Comme indiqué plus haut, le phishing est la principale menace, et ce pour une bonne raison : elle demande un minimum d'efforts pour un maximum de succès.

9 %
des utilisateurs avaient été abusés par une attaque de phishing.

et les attaques de phishing ont eu
50 % plus **de succès sur les appareils mobiles que sur les Mac.**

Les mauvaises nouvelles d'abord : ce chiffre est en hausse de 1 % par rapport à 2022. Cette année-là, 8 % des utilisateurs avaient été abusés par une attaque de phishing.

Une piste d'interprétation : si les organisations ont renforcé les protections et la formation en matière de sécurité des données, les utilisateurs constatent tout de même une augmentation des compromissions. Cette évolution est en phase avec la tendance des attaquants à cibler les utilisateurs de façon plus directe et agressive, notamment via les réseaux sociaux ; ils profitent notamment du fait que les employés en télétravail utilisent davantage leurs appareils personnels pour travailler. En 2023, les attaques de phishing ont eu 50 % plus de succès sur les appareils mobiles que sur les Mac. Et comme « plus de 90 % des attaques informatiques commencent par du phishing » d'après la **CISA**, on ne sera pas surpris que des acteurs malveillants ciblent l'appareil principal des utilisateurs comme tremplin pour passer des données personnelles à celles de l'entreprise.

« Le cryptojacking concerne 1 % des appareils et 9 % des organisations. »

Le secteur de la cybersécurité a observé les premières alertes de cryptojacking en 2011. Les attaques étaient modestes à l'époque, et la première véritable montée en puissance s'est manifestée en 2022, lorsque le nombre d'incidents a atteint les 140 millions, soit une **augmentation de 43 % à l'échelle mondiale** selon Statista. Cette tendance n'a fait qu'accélérer : Sonic Wall a enregistré une **augmentation de 399 % des attaques de cryptojacking, avec 332,3 millions** d'incidents au cours du seul premier semestre 2023.

Signe de l'omniprésence du cryptojacking, **nos chercheurs en sécurité de Jamf Threat Labs ont détecté la présence d'un logiciel de cryptojacking** dans des copies pirates de logiciels commerciaux pour macOS au début de l'année 2023. Comme le corroborent de multiples recherches, le cryptojacking reste une tendance dangereuse toujours privilégiée par certains acteurs malveillants. Cette menace n'est pas à prendre à la légère : elle a largement dépassé le stade du simple vol de ressources pour atteindre celui de l'opération criminelle lucrative, source de revenus durable pour certains groupes de pirates.

Trafic réseau malveillant

À ne pas confondre avec l'installation de logiciels malveillants (que nous abordons dans la suite du rapport), le trafic réseau malveillant représente une menace importante pour « 11 % des appareils » de notre échantillon. Au niveau des organisations, nous avons découvert que « 20 % d'entre elles ont été touchées par du trafic réseau malveillant. »

Voici quelques exemples de trafic réseau malveillant :

- Téléchargements de logiciels malveillants
- Commande et contrôle
- Exfiltration de données
- Escroqueries
- En détaillant plus finement ce pourcentage, nous avons vu que « les appareils mobiles sous Android et iOS représentaient respectivement 8 % et 6 % de ce total ». Quelques observations supplémentaires :
- **2 % des organisations ont été victimes d'une fuite de mot de passe** (identifiants publiés en ligne sans consentement)
- **1 % des utilisateurs se sont déjà connectés à un point d'accès à risque** (principalement des réseaux wi-fi gratuits et non sécurisés).
- **Environ 1 % ont été touchés par une attaque de l'homme du milieu (MitM)**, qui consiste pour un pirate à établir des connexions intermédiaires entre deux victimes et à relayer les communications en les modifiant ou en les collectant.

Ces pourcentages semblent trop faibles pour faire la une des journaux. Mais en les rapportant au nombre d'appareils de notre échantillon, nous pouvons avoir une meilleure idée de ce qu'il représente en réalité.

- 300 000 appareils ont été victimes d'une fuite de mot de passe
- 150 000 utilisateurs se sont connectés à un point d'accès à risque
- Un peu moins de 150 000 personnes ont été touchées par une attaque MitM

Ces chiffres représentent, au minimum, 150 000 cas potentiels de :

- **Compromission d'appareil**
  - Capture de données d'entreprise
  - Pivot visant à attaquer d'autres terminaux
  - Infiltration de réseau ou de service
  - Appareils non conformes
  - Appareils en infraction avec les réglementations locales, nationales, fédérales et/ou régionales
  - Responsabilités légales en cas d'incident
  - Exposition à des poursuites civiles ou pénales
  - Dégradation de la réputation de l'entreprise
  - Rupture de partenariat
  - Perte d'opportunités commerciales
  - Cessation d'activité

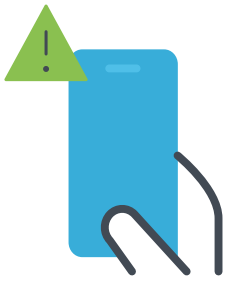
Conformité des appareils

Nous avons abordé les trois grandes tendances des menaces de cybersécurité, mais nous ne sommes pas arrivés au bout des résultats de nos recherches. Dans cette section, nous allons voir quelles configurations d'atténuation permettent de maintenir la conformité des appareils et de gérer les vulnérabilités.

Ce rapport propose des conseils fondés sur les données des résultats de nos recherches. Ils s'articulent autour de trois axes sur lesquels les équipes informatiques et de sécurité ont tout intérêt à concentrer leurs efforts. En misant sur une gestion complète et des stratégies de sécurité en profondeur, elles pourront atteindre et maintenir une conformité holistique.

Retour aux fondamentaux

Notre premier domaine d'intérêt est essentiel pour la conformité des appareils, car il pose les bases sur lesquelles s'appuient les outils et les stratégies abordés dans les autres sections. Comme son titre l'indique, ce « retour aux fondamentaux » est le moteur de votre plan de sécurité. Il vient renforcer les fonctions critiques qui constituent depuis toujours la pierre angulaire de la protection de vos terminaux.



39 %

des organisations comptaient dans leur parc au moins un appareil présentant des vulnérabilités connues.

Correctifs et mises à jour de sécurité

Jamf a constaté que 39 % des organisations comptaient dans leur parc au moins un appareil présentant des vulnérabilités connues. Les professionnels de la sécurité savent que les menaces de type « zero day » sont difficiles à identifier et plus encore à atténuer, car aucun correctif n'est encore disponible pour les neutraliser. Mais nous parlons ici des vulnérabilités connues, pour lesquelles il existe des correctifs… mais dont les appareils ne sont pas équipés.

Si le constat ci-dessus peut concerner tous les types d'appareils des organisations touchées, voici une autre statistique troublante, portant cette fois sur les appareils mobiles : **« 40 % des utilisateurs mobiles utilisant une version d'OS présentant des vulnérabilités connues ».** Il faut le voir comme une tendance majeure, car tous les acteurs – et pas seulement les organisations – sont responsables de la sécurité de leurs appareils. Ensemble, ils jouent un rôle essentiel dans l'optimisation de la posture de sécurité de la flotte grâce à des workflows itératifs dont le but est d'appliquer les mises à jour d'OS et les correctifs le plus rapidement possible.

Le report des mises à jour a deux raisons principales : la peur des conflits et le nombre d'agents à mettre à jour.

Rapid security response (RSR)

Dans un effort concerté pour lutter contre le report des mises à jour de sécurité critiques sur les plateformes macOS et iOS, Apple a introduit Rapid Security Response au début de l'année 2023. RSR uniformise la livraison de correctifs critiques pour atténuer les risques en automatisant leur téléchargement et leur installation sur les appareils pris en charge. Les appareils Apple et leurs utilisateurs sont mieux protégés contre l'introduction d'exploits connus grâce à ce dispositif qui comble le fossé entre deux versions majeures.

Projet Conformité de sécurité macOS (mSCP)

Ce projet open source, connu sous le nom de mSCP, a pour but d'aider les équipes chargées de gérer et de sécuriser les appareils Apple à appliquer des critères de sécurité en phase avec leurs objectifs de conformité. Pour répondre aux besoins de conformité spécifiques de votre organisation, mSCP propose une approche logique et systématique pour générer des configurations et des réglages. Une fois déployées, ces charges utiles vont garantir la conformité de votre flotte.

La gestion au service de la sécurité

La gestion et la sécurité entretiennent une relation symbiotique. Autrement dit, l'une ne va pas sans l'autre. La sécurité des terminaux protège les appareils contre les menaces grâce à une surveillance active. Mais sans gestion, le processus de correction demande des efforts considérables qui ne font qu'augmenter avec le nombre d'appareils et leur dispersion géographique. Inversement, les workflows de gestion ne peuvent pas automatiser la mise en conformité des appareils sans des données de télémétrie qui mettent en évidence les défauts au sein de votre flotte.

Le service RSR d'Apple est justement un outil stratégique d'application de correctifs qui s'appuie sur la gestion. C'est elle, en effet, qui fournit à l'équipe informatique le mécanisme permettant d'automatiser l'installation des correctifs RSR sur les appareils, même s'ils sont verrouillés ou que l'utilisateur n'est pas connecté.

La gestion joue enfin un autre rôle stratégique en facilitant les initiatives de conformité grâce à un contrôle actif. Les informations glanées grâce à la surveillance fournissent aux équipes informatiques et de sécurité une radiographie précise de l'état d'un terminal. Armées de cette riche télémétrie, ces équipes peuvent prendre des décisions éclairées concernant la sécurité des applications et des données. Sans ces renseignements, comment les organisations pourraient-elles connaître le statut de sécurité d'un terminal qui accède à des applications web à distance, par exemple .

Jamf Compliance Editor (JCE)

Jamf s'est appuyé sur le projet mSCP pour produire une application macOS native qui marie l'outil de conformité à nos solutions MDM. Cette application ne se contente pas de générer des assets de conformité personnalisés pour votre organisation : son interface JCE s'intègre également avec votre instance de Jamf Pro via une API sécurisée pour faciliter l'importation des nouveaux assets. Cette approche comble le fossé entre génération et déploiement pour faire gagner du temps aux administrateurs et accélérer la mise en conformité.

Défense en profondeur

Aucun outil n'est infaillible. Il n'existe pas de solution miracle qui permette d'éliminer toutes les menaces en permanence. Quoi que vous fassiez, quelque chose finira toujours par vous échapper. Mais cela ne veut pas dire que les équipes informatiques et de sécurité ne peuvent pas agir pour minimiser le risque que des menaces atteignent les ressources de l'organisation. C'est tout l'intérêt des protections multicouches : si une couche laisse passer la menace, les autres couches pourront l'intercepter avant que la situation ne se dégrade.

Plus qu'un simple assemblage de solutions, la défense en profondeur est en réalité un paradigme de sécurité qui doit guider les organisations dans l'élaboration (ou la modernisation) de leur plan de sécurité. L'objectif principal est de superposer différentes solutions, un peu comme les couches d'un gâteau. Chaque outil de sécurité, outre ses fonctions intrinsèques, agit également comme un filet de sécurité pour la couche précédente. Si une menace parvient à s'infiltrer, la couche suivante peut l'atténuer.

Trusted Access

Le paradigme de sécurité exclusif de Jamf offre un excellent exemple de combinaison de solutions : Jamf Pro (gestion), Jamf Connect (identité) et Jamf Protect (sécurité) composent une plateforme intégrée qui permet aux administrateurs de gérer l'ensemble de leur flotte de façon efficace et holistique, tout en fournissant des protections de sécurité complètes aux Mac et aux appareils mobiles iOS/iPadOS/tvOS, Android et Windows.

> « Moins de 1 % des organisations étaient en possession d'un appareil jailbreaké ou rooté en 2023. »

Ce chiffre prouve une chose : les utilisateurs sont moins nombreux à jailbreaker ou rooter les appareils utilisés dans le cadre professionnel, ce qui est une bonne nouvelle. Mais il démontre également qu'en combinant la surveillance active des appareils mobiles (sécurité), l'application dynamique des règles de sécurité propre à l'accès réseau zero-trust (identité), et l'automatisation des corrections (gestion), on obtient un excellent workflow pour empêcher les appareils non conformes de compromettre les données de votre organisation.

Les programmes de choix des employés qui misent sur le BYOD et le COPE (l'appareil appartient à l'entreprise, mais il est géré par l'utilisateur) ont de grands avantages pour la productivité des utilisateurs. Mais une gestion insuffisante – tout comme un excès de contrôle – peut avoir de nombreuses conséquences sur la sécurité des appareils et la vie privée des utilisateurs finaux. Pour parvenir au juste équilibre en matière de gestion et de sécurité, une option consiste à mettre en place des workflows à plusieurs niveaux pour les appareils personnels et ceux de l'entreprise. L'objectif : doter les deux types d'appareils d'une posture de sécurité de base.

Par exemple, les appareils fournis par l'entreprise seront automatiquement inscrits dans la solution MDM grâce au déploiement zero-touch (gestion), tandis que les appareils personnels seront inscrits par l'utilisateur avec ses identifiants (identité). Les deux types d'appareils auront des configurations similaires, mais dans le second cas, les applications et les données de l'entreprise seront stockées dans un volume professionnel, chiffré et séparé du volume personnel abritant les informations et les outils privés de l'utilisateur. D'autre part, la confidentialité du trafic professionnel sur le réseau est assurée par des microtunnels chiffrés (sécurité). Le trafic réseau personnel, quant à lui, est acheminé directement vers Internet. Enfin, la sécurité des terminaux assure le même niveau de détection et de prévention des menaces sur les appareils personnels que sur ceux de l'entreprise. Elle s'appuie sur les dernières informations d'état de l'appareil pour évaluer chaque demande d'accès aux ressources de l'entreprise. Conformément au principe zero-trust, l'accès n'est approuvé que lorsque l'appareil a été vérifié. En cas d'échec de la vérification, la demande reste rejetée et un workflow automatisé est déclenché pour corriger la configuration de l'appareil (gestion). Une fois le workflow appliqué, une nouvelle vérification est faite. C'est seulement si elle aboutit que la demande sera approuvée.

Principaux points à retenir

- Mettez en place un système de gestion pour tous vos appareils, qu'ils appartiennent à l'entreprise ou qu'ils soient en BYOD
- Utilisez des solutions de sécurité des terminaux pour bloquer les logiciels malveillants et collecter des données de télémétrie pour réaliser des analyses et détecter les menaces
- Suivez les normes de conformité
- Mettez en place une sécurité de périphérie pour couvrir les appareils qui sortent du périmètre de votre entreprise
- Sécurisez les connexions à l'aide de tunnels chiffrés pour éviter l'interception des données.
- Commencez à mettre en œuvre un programme zero-trust
- N'oubliez pas de respecter la vie privée des utilisateurs finaux.

À propos de cette étude

Nous voulions mieux comprendre les grandes tendances de sécurité qui ont un impact sur le lieu de travail moderne, et en particulier sur les appareils, les utilisateurs et les applications qui doivent être connectés pour remplir leur mission. Pour délivrer les informations et les statistiques présentées dans ce document, nous avons analysé les tendances de sécurité qui se manifestent chez notre clientèle. Nous avons également puisé dans les recherches originales de nos équipes sur les vulnérabilités des OS et des applications, et dans ses explorations approfondies de l'underground du Web. Pour comprendre l'impact réel de ces tendances de sécurité, nous avons examiné un échantillon de 15 millions d'appareils protégés par Jamf. Cet échantillon comprend des appareils iOS, macOS, iPadOS, Android et Windows, et couvre 90 pays sur une période de 12 mois. Cette analyse a été réalisée au quatrième trimestre de 2023. Les métadonnées analysées dans cette recherche proviennent de journaux agrégés dépourvus d'informations permettant d'identifier les personnes ou les organisations. L'objectif de cette analyse n'est pas de vous effrayer, mais bien de vous informer, vos utilisateurs et vous, sur les options qui s'offrent à vous. Apprenez à sécuriser au mieux tous les aspects des appareils, ainsi que les données des utilisateurs et de l'entreprise. Contactez-nous pour savoir comment mettre en place des mesures de protection et renforcer votre posture de sécurité.

Source : Jamf Threat Labs