La securité à 360°

Le rapport annuel de Jamf sur la sécurité, basé sur des données, examine les menaces et leur impact sur les entreprises du monde entier. Découvrez des conseils pratiques sur la façon de configurer les outils professionnels pour garantir une connectivité rapide et sûre à tous les utilisateurs en 2022.

Chiffres clés

Le pourcentage d'entreprises ayant subi une installation de logiciels malveillants sur un appareil à distance en a doublé, passant **de 3 % en 2020 à 6 % en 2021**.

En 2021, 39 % des entreprises ont autorisé les appareils présentant des vulnérabilités connues du système d'exploitation à fonctionner dans un environnement de production sans restriction des privilèges ou de l'accès aux données, contre **28 % en 2020**.

7 % des appareils professionnels ont continué à accéder aux services de stockage dans le cloud après avoir été compromis **en 2021**.

Au cours de l'année **2021**, le nombre d'appareils se connectant chaque semaine à des hotspots à risque par semaine a doublé, passant **de 0,5 % à 1 %**.

Un utilisateur sur dix est victime d'attaques de phishing sur des appareils à distance.

Introduction

À l'aube de la pandémie mondiale, les organisations ont été confrontées à la tâche exténuante d'assurer la continuité de l'activité tout en assurant la transition vers un environnement de travail hybride ou entièrement à distance au pied levé. Deux ans plus tard, le paysage professionnel a largement adopté les technologies d'accès à distance et les logiciels basés sur le Cloud pour autoriser les employés à travailler de pratiquement n'importe où et à accéder aux données de l'entreprise à tout moment, sur n'importe quel appareil. Mais quel a été l'impact de cette évolution sur la sécurité des entreprises dans le monde ?

Chaque année, nous analysons les menaces qui pèsent sur les appareils utilisés sur le lieu de travail moderne. La répartition des employés a évolué, tout comme notre perspective sur le paysage des menaces.

Cette année, le rapport examine cinq tendances clés en matière de sécurité ayant un impact réel sur les entreprises dont les utilisateurs se connectent à distance à une multitude d'applications hébergées dans des centres de données privés et publics via une variété de dispositifs et de plateformes portables.

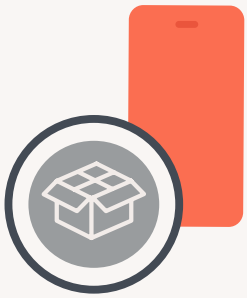
En 2021, 6 % des entreprises ont subi une installation de logiciels malveillants sur un appareil à distance, contre **3 % en 2020.**

Tendance 1 - Adapter la stratégie de sécurité à la réalité du télétravail

L'évolution vers des employés en télétravail plus permanents s'accompagne d'un changement dans la manière d'assurer la sécurité. Au lieu des solutions traditionnelles sur site qui se concentrent sur la protection des actifs au sein du bureau et du réseau de l'entreprise, les entreprises se sont efforcées de décentraliser et de distribuer leurs services de sécurité aux terminaux qui produisent et consomment des données et aux applications Cloud qui stockent et utilisent les données. Il en résulte une sécurité des terminaux plus performante et plus autonome, ainsi qu'une sécurité des applications plus résiliente et plus robuste.

Les technologies d'accès à distance qui relient les terminaux distants et distribués et les applications distribuées hébergées dans le cloud peuvent être adoptées pour autoriser ou refuser intelligemment l'accès par appareil et par application.

Une partie de ce processus consiste à déterminer quels indicateurs de risque doivent déclencher une décision de refus d'accès aux applications d'entreprise. Les indicateurs de risque et de compromission



Moins de 1 % des entreprises disposaient d'un appareil jailbreaké ou raciné en **2021**.

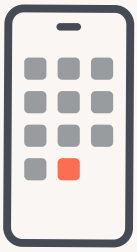
Les deux données ci-dessus indiquent que les utilisateurs manipulent beaucoup moins leurs appareils qu'auparavant et que les pirates multiplient les attaques contre les appareils des entreprises.

sont subjectifs. Si une organisation a une tolérance élevée au risque, elle peut exiger que des indicateurs de compromission des appareils soient présents avant de refuser une connexion à une application d'entreprise. Bien que les indicateurs de compromission soient subjectifs, les indicateurs standard de compromission des appareils de Jamf Threat Labs sont les suivants : (1) l'installation de logiciels malveillants et (2) un appareil Jailbreaké ou enraciné. D'après les données de Jamf Threat Labs, les appareils compromis sont plutôt rares, mais ils ont quand même un impact réel sur les utilisateurs et les entreprises. Les entreprises ayant une faible tolérance au risque pourraient vouloir refuser l'accès en présence de tout indicateur de vulnérabilité ou de compromission. Bien que les indicateurs de vulnérabilité soient également subjectifs, les indicateurs standard de dispositif vulnérable de Jamf Threat Labs comprennent : (1) un système d'exploitation vulnérable, (2) la présence d'une application indésirable, (3) la présence d'une boutique d'applications tierces, et (4) d'autres violations de la conformité des appareils et des erreurs de configuration. Ces indicateurs de risque étaient également présents au sein de nos données en 2021.

En 2021, 39 % des entreprises utilisaient régulièrement un système d'exploitation présentant une vulnérabilité de sécurité connue, contre **28 % en 2020**.

Au cours de l'année 2021, le nombre d'entreprises ayant une application potentiellement indésirable installée dans leur parc informatique a plus que doublé, passant **de 5 % à 11 %**.

Il s'agit de toute application dont la malveillance n'est pas avérée, mais qui risque d'introduire des menaces dans l'environnement en permettant à l'utilisateur de contourner les règles ou d'introduire du contenu inapproprié (par exemple, via des réseaux publicitaires malveillants).

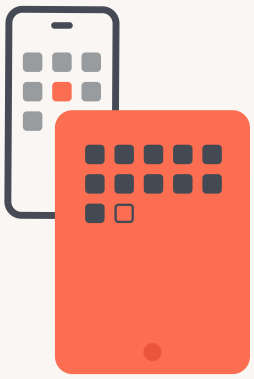


Au cours de l'année 2021, le nombre d'appareils sur lesquels était installé un App Store tiers est passé **de 1 % à 4 %**.

En 2021, 5% des appareils, soit 20% des organisations, ont été impactés par une configuration d'appareil à risque.

Si le pourcentage d'appareils compromis ou vulnérables est faible, il est alarmant de voir combien de ces appareils accèdent à des ressources sensibles.

En 2021, 7 % des appareils compromis ont accédé à des services de stockage dans le cloud (tels que OneDrive, Google Drive et DropBox) et **25 %** à des services d'e-mail (tels que Gmail et Outlook). Ces chiffres passent respectivement à **9 % et 48 %** si l'on inclut les indicateurs d'appareils vulnérables ci-dessus.



9 % des appareils compromis ont accédé à un CRM (comme Salesforce et Microsoft Dynamics) et **34 %** à des services de conférence (comme Zoom, Skype et Microsoft Teams) en **2021**. Ces chiffres passent respectivement à **15 % et 64 %** si l'on inclut les indicateurs de vulnérabilité des appareils ci-dessus.

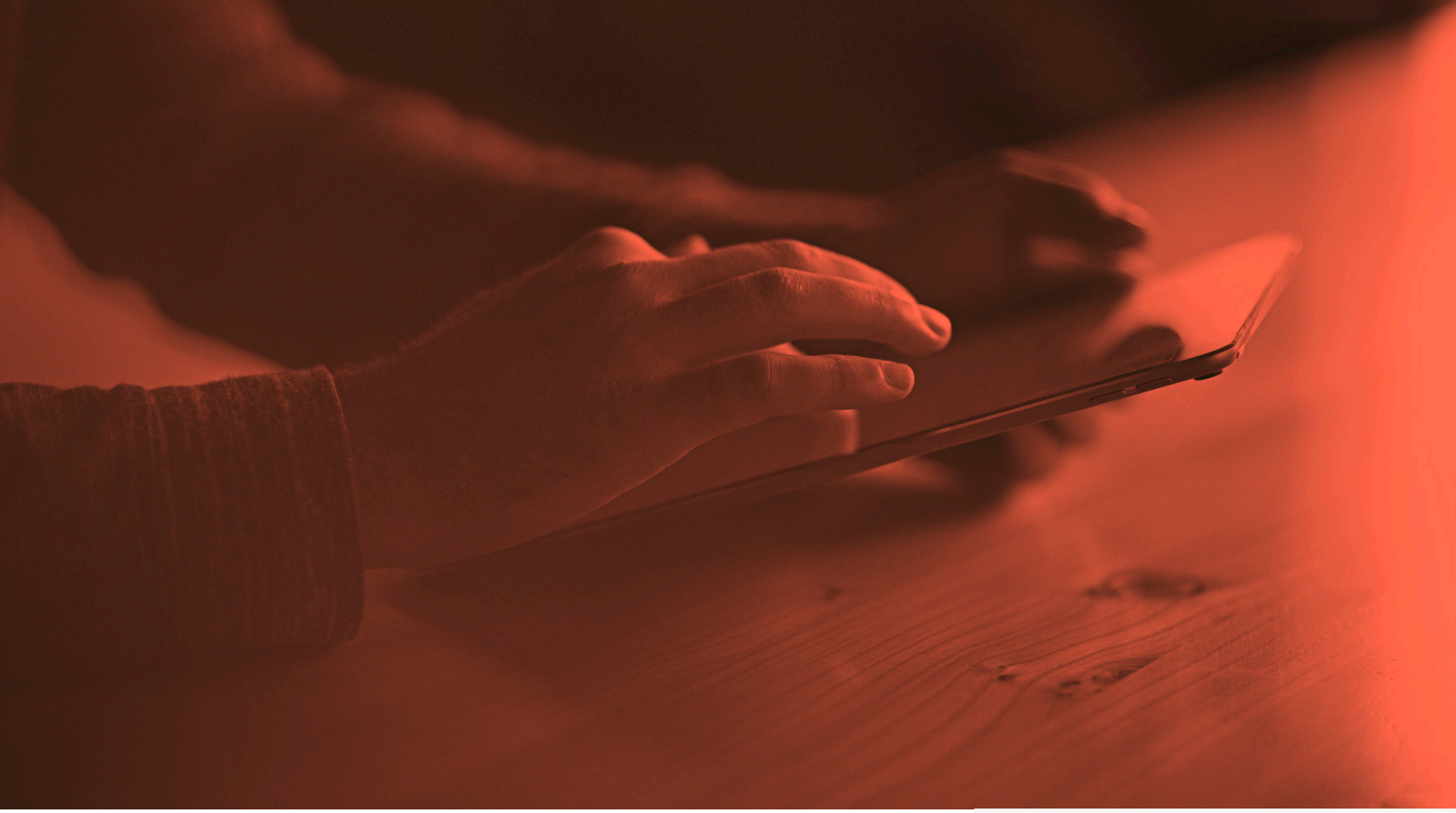
Mais il ne sert à rien de définir une politique de sécurité pour le télétravail sur la base des données ci-dessus si vous ne disposez pas des outils nécessaires pour évaluer les risques et appliquer les décisions d'accès en temps réel. Les technologies d'accès à distance traditionnelles, telles que les VPN, ne suffiront certainement pas.

L'adoption mondiale de la technologie VPN utilisée pour chiffrer le trafic sur des lignes de communication non sécurisées a augmenté en 2020, bien que le passage aux applications Cloud ait vu cette croissance diminuer en 2021, avec 43% des utilisateurs admettant que "je sais ce que c'est, mais je n'en utilise pas", dans le cadre d'une enquête menée par security.org.

Pas mal pour une technologie de sécurité qui a été développée il y a plus de vingt-cinq ans. Et si l'utilisation d'un VPN est préférable à l'absence totale de protection, les limites du VPN, combinées au fait que l'informatique a beaucoup évolué ces deux dernières années, ont donné naissance à des approches plus modernes de l'accès à distance, telles que l'accès réseaux de Zero Trust, ou ZTNA.

Il s'agit d'un ensemble de technologies de sécurité qui offrent une protection dynamique pour répondre aux besoins des nouvelles technologies de réseau telles que le Wi-Fi et le cellulaire, brisant ainsi les nombreuses hypothèses sur lesquelles reposait le VPN. Cette technologie tire son nom du fait qu'elle ne fait jamais confiance de manière inhérente à un utilisateur ou à un appareil, contrairement au VPN. Au lieu de cela, ZTNA n'autorise les connexions aux applications et aux services qu'après avoir vérifié que l'appareil et l'utilisateur sont autorisés à accéder aux services demandés et répondent aux exigences minimales de "santé" pour le faire en toute sécurité.

ZTNA a été conçu en tenant compte des réseaux et des workflows modernes en s'intégrant aux fournisseurs d'identité Cloud pour tirer parti des autorisations basées sur les droits d'accès explicites des utilisateurs. Les solutions ZTNA respectueuses de la vie privée atténuent les risques et protègent les données, tout en étant suffisamment souples pour que les applications et les données personnelles restent privées, ce qui préserve la confidentialité des utilisateurs. En outre, les utilisateurs autorisés ne peuvent se connecter qu'aux applications auxquelles ils sont autorisés à accéder, ce qui empêche les pirates qui compromettent un seul utilisateur d'accéder à toutes les applications du catalogue.



Tendance 2 - Les auteurs de menaces ont modifié leurs outils et leurs campagnes pour tirer parti des appareils sur lesquels les utilisateurs choisissent de travailler.

À mesure que les organisations adoptent de nouvelles technologies pour sécuriser leurs communications et maintenir la continuité de leurs activités face à des processus en constante évolution, les acteurs de la menace s'emploient à mettre à jour les méthodes et les cibles de leurs attaques pour améliorer leur efficacité.

Les catégories d'attaques restent les mêmes, mais, plus précisément, la manière dont elles sont exécutées par les pirates a été améliorée pour tenir compte du fait que les utilisateurs sortent désormais des limites du bureau traditionnel et travaillent sur des appareils plus conviviaux, tels que des smartphones, des tablettes et des ordinateurs portables, et qu'ils choisissent de plus en plus souvent des appareils Apple. Selon une enquête récente, près de 90 % des employés seraient prêts à accepter une baisse de salaire pour utiliser la plateforme qu'ils préfèrent, tandis que 62 % d'entre eux choisissent Apple quand ils le peuvent.

Si les infections confirmées par des logiciels malveillants restent faibles, le trafic de logiciels malveillants sur les réseaux est plus répandu. Le trafic réseau malveillant fait référence aux indicateurs de compromission

36 % des organisations ont rencontré des indicateurs de trafic réseau malveillant sur un appareil à distance en **2021**.

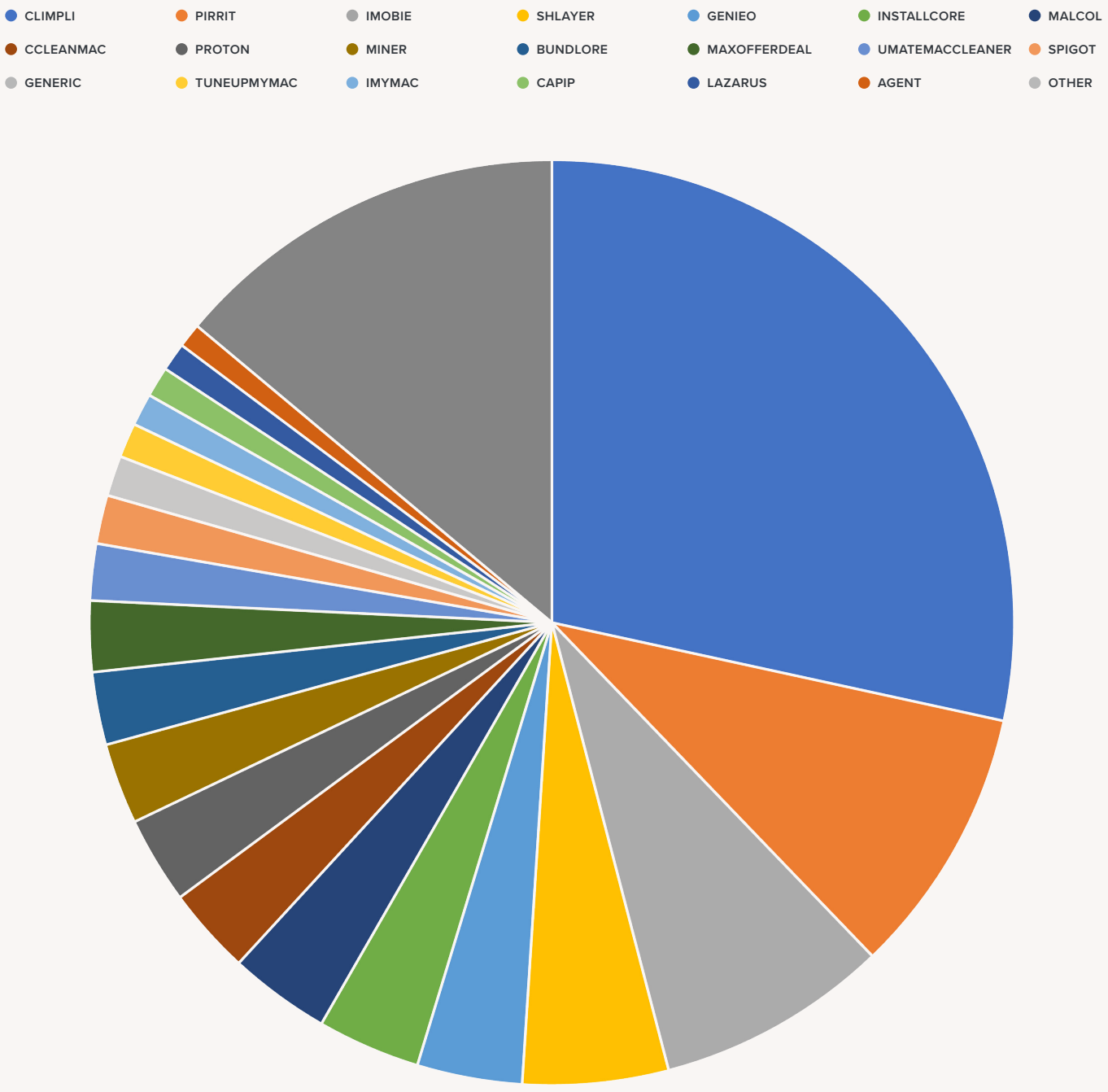
(IoC) basés sur le réseau qui peuvent être observés dans les schémas de communication entre l'appareil et les serveurs Internet ; ces signaux peuvent inclure l'exfiltration de données ou des connexions à des serveurs de commande et de contrôle ou à des sites connus pour héberger des logiciels malveillants. Le trafic réseau malveillant n'est généralement observé que dans les environnements de production et ne peut être identifié par une simple évaluation du code statique. C'est pourquoi la surveillance de cet indicateur est si importante, au-delà des contrôles de sécurité officiels de l'App Store.

Les logiciels malveillants pour Mac deviennent un problème. En 2021, Jamf Threat Labs a annoncé la découverte d'une nouvelle variante du **malware Shlayer**, qui autorisait un pirate à contourner les technologies de sécurité Gatekeeper, Notarization et File Quarantine dans macOS. L'exploit permet d'exécuter des logiciels non approuvés sur Mac et est distribué via des sites web compromis ou des résultats de moteurs de recherche empoisonnés.

Toujours en 2021, Jamf Threat Labs a découvert un contournement TCC de type "zero-day" dans le malware XCSSET, qui permettait à un pirate de contourner les protections TCC d'Apple qui protègent la vie privée des utilisateurs. En tirant parti d'une application installée avec les autorisations appropriées, le pirate peut s'appuyer sur cette application donatrice pour créer une application malveillante à exécuter sur les appareils des victimes, sans demander l'autorisation de l'utilisateur pour accéder ou utiliser les fonctionnalités matérielles, comme l'appareil photo ou le microphone, par exemple.

De nombreuses personnes ne réalisent pas que des logiciels malveillants affectent les appareils Mac modernes. **Le graphique ci-dessous représente la part des familles de malwares pour Mac qui ont tenté de compromettre les appareils protégés par Jamf en 2021**. Les cinq premières sont Climpli, Pirrit, Imobie, Shlayer et Genieo.

Part des familles de logiciels malveillants Mac détectées en 2021



L'essor du télétravail a donné lieu à des menaces de sécurité ciblant non seulement les appareils et les applications, mais aussi les utilisateurs eux-mêmes, de manière plus agressive. Les acteurs de la menace ont orienté leurs campagnes de phishing vers les applications cloud modernes utilisées pour le travail, telles que les applications Office 365 et Google Workplace (anciennement G Suite). À l'heure où les entreprises s'efforcent de déplacer leurs actifs vers le cloud, il s'agit d'une préoccupation majeure. Un seul faux pas de la part d'un employé victime d'une attaque de phishing intelligente (par exemple, lui demandant de confirmer ses identifiants de connexion à Box) peut permettre à un acteur malveillant d'accéder aux actifs de l'entreprise stockés sur ces types d'applications Cloud populaires.

Selon l'étude de Jamf : ***Les tendances du phishing en 2021***, qui a été publiée au quatrième trimestre de 2021, les trois principales marques utilisées dans les attaques de phishing qui ont réussi à inciter les utilisateurs à se séparer de leurs données sensibles en 2021 sont Apple, PayPal et Amazon, qui comptent respectivement pour 43 %, 27 % et 9 % de ces attaques. Ces attaques ont touché des appareils de plusieurs systèmes d'exploitation et pas seulement des appareils Apple, bien que la marque Apple soit la plus utilisée dans les attaques. Il convient de noter que ces marques n'ont rien fait de mal, elles sont simplement utilisées par les pirates en raison de leur nom reconnaissable.

L'espace mobile est également touché par une augmentation significative des attaques de smishing, ou hameçonnage par SMS, qui consistent à envoyer aux utilisateurs des SMS/textos malveillants provenant d'une fausse identité dans le but de compromettre des comptes par usurpation d'identité.

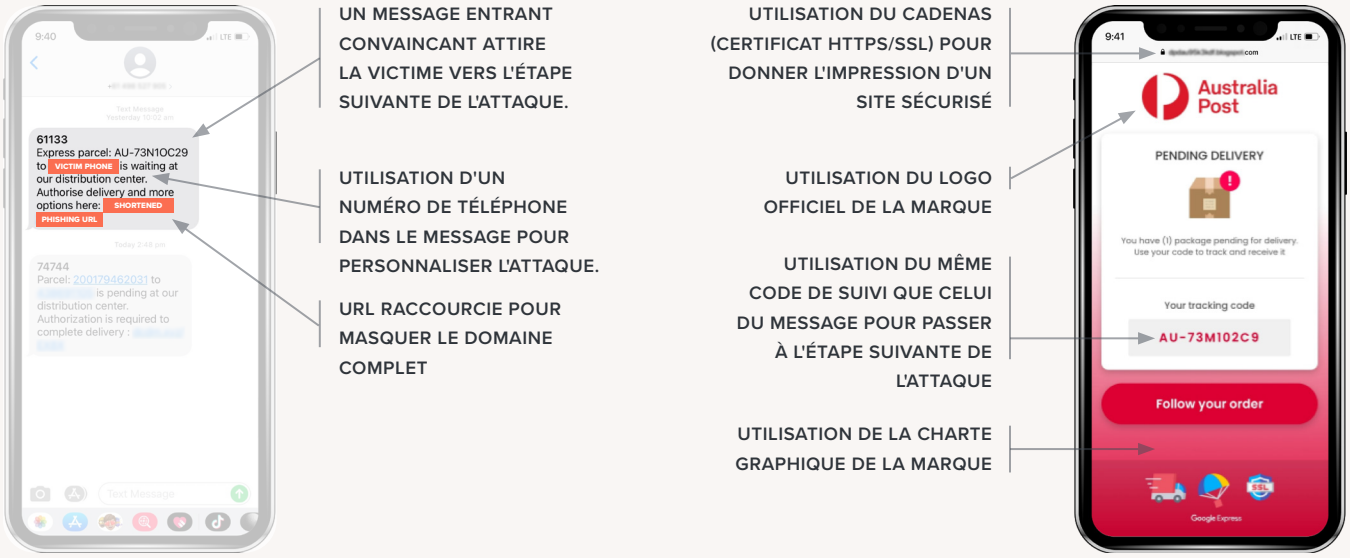
Les attaques se concentrent sur l'e-mail, les services bancaires, les réseaux sociaux et tentent même de tromper les utilisateurs en leur faisant divulguer des codes d'authentification à deux facteurs légitimes reçus de services réels afin d'étendre leur portée dans des

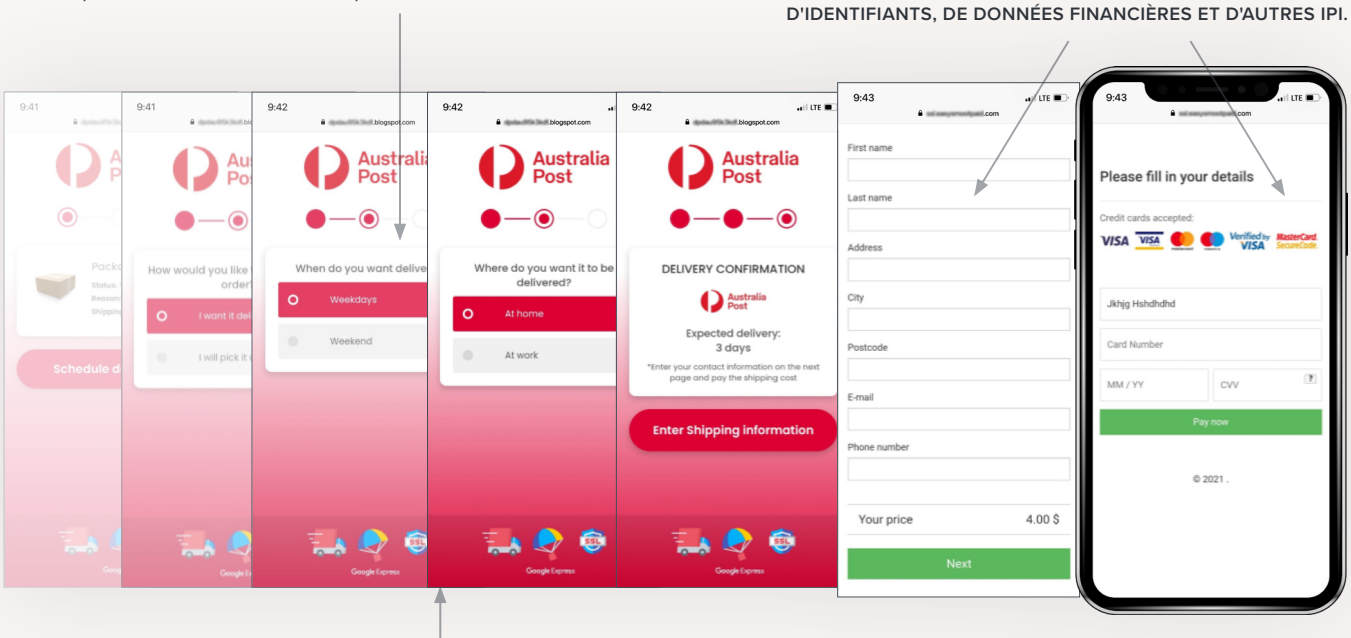
Phishing Trends Report 2021

Les 10 principales marques utilisées dans les campagnes de phishing en 2021

1. **Apple**
2. **PayPal**
3. **Amazon**
4. **Chase**
5. **Facebook**
6. **Google**
7. **Twitter**
8. **Netflix**
9. **Microsoft**
10. **Wells Fargo**

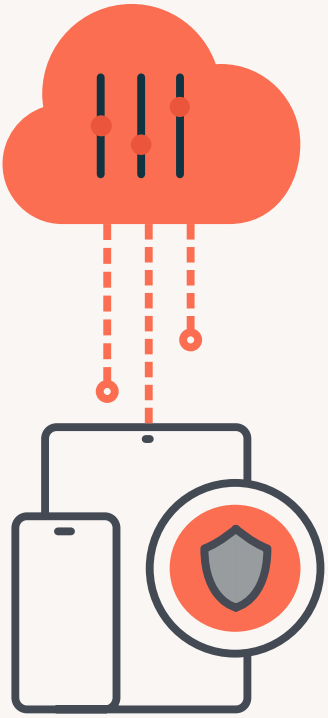
domaines sécurisés par la technologie d'authentification multifacteurs. Les utilisateurs sont probablement plus sensibles au phishing sur les appareils mobiles en raison de la taille réduite des écrans, des barres d'URL cachées, de la confiance inhérente dans l'appareil et les applications, ainsi que de la nature précipitée et distraite de l'utilisation mobile. Selon les données de Jamf Threat Labs, 1 utilisateur sur 10 est victime d'attaques de phishing sur mobile. Jamf Threat Labs a enquêté sur une campagne de phishing mobile lorsque de nombreux SMS suspects ont été identifiés, utilisant des tactiques similaires et cherchant à obtenir les mêmes informations personnelles sensibles des utilisateurs. Les messages avaient pour thème la livraison de colis et utilisaient la marque bien connue Australia Post (Australia Post est l'équivalent de USPS aux États-Unis ou de Royal Mail au Royaume-Uni, et les victimes potentielles sont donc toutes les personnes qui vivent en Australie et reçoivent du courrier). Il s'agit d'une attaque opportuniste, compte tenu du fait que les gens comptaient beaucoup sur la livraison à domicile pendant les confinements stricts et répétés du COVID-19 en Australie. Comme les autres grandes marques utilisées dans les attaques de phishing, Australia Post n'a rien fait de mal, la marque est simplement utilisée par les pirates en raison de son nom reconnaissable.





Tendance 3 - Il est primordial de trouver un équilibre entre les besoins de sécurité et le respect de la vie privée des utilisateurs

On estime qu'en 2022, le nombre d'utilisateurs ayant accès à la technologie mobile sera de 7,26 milliards, soit environ 89,76 % de la population mondiale, selon les prévisions d'Ericsson et du groupe Radicati. Grâce à l'accès à de multiples réseaux de communication pour une connectivité ultra-rapide, à un matériel multi-cœur et à une autonomie prolongée, il n'est pas étonnant que de plus en plus d'utilisateurs se servent d'appareils mobiles pour effectuer des tâches professionnelles en plus de leurs tâches personnelles.



Les entreprises misent également sur cette tendance en prenant en charge de nombreuses formes de propriété des appareils, notamment BYOD (Bring Your Own Device), CYOD (Choose Your Own Device), COPE (Corporate owned, Personally Enabled) et COBO (Corporate Owned, Business Only), afin de répondre aux besoins de l'entreprise et de ses utilisateurs, qu'il s'agisse de réduire les coûts, de favoriser la productivité ou de donner le choix aux employés.

Cependant, alors que les équipes informatiques et de sécurité se préoccupent des processus et workflows liés à la sécurité, les utilisateurs

finaux se soucient de leur confidentialité et de leur autonomie. Plus précisément, quelle part de leur utilisation en ligne est visible pour les employeurs, et comment l'utilisation de leurs appareils sera-t-elle influencée par les outils de sécurité et de gestion. Si la sécurité est primordiale, l'importance de la vie privée ne peut être sous-estimée, surtout lorsque les utilisateurs disposent d'appareils de l'entreprise (ou qu'ils soumettent leurs propres appareils personnels). La question qui se pose est la suivante : le droit à la vie privée éclipse-t-il les préoccupations en matière de sécurité ou les exigences du processus de sécurité prennent-elles le pas sur les préoccupations en matière de vie privée ?

La réponse n'est pas aussi claire, car elle dépend beaucoup de l'environnement et d'autres facteurs atténuants, tels que les exigences réglementaires et la personne qui conserve la propriété finale du matériel lui-même. Cela dit, Apple mène la charge en fournissant des frameworks pour les applications qui fonctionnent sur ses appareils afin de protéger le droit à la vie privée des utilisateurs. Apple a récemment introduit de nouveaux contrôles de confidentialité dans macOS Mojave qui obligent les utilisateurs à activer manuellement l'accès aux caméras et aux microphones, aux informations de localisation et aux connexions réseau, etc., de sorte que les apps et les services qui utilisent ces fonctions s'installeront désormais avec un accès désactivé par défaut pour protéger les utilisateurs finaux contre toute surveillance non autorisée.

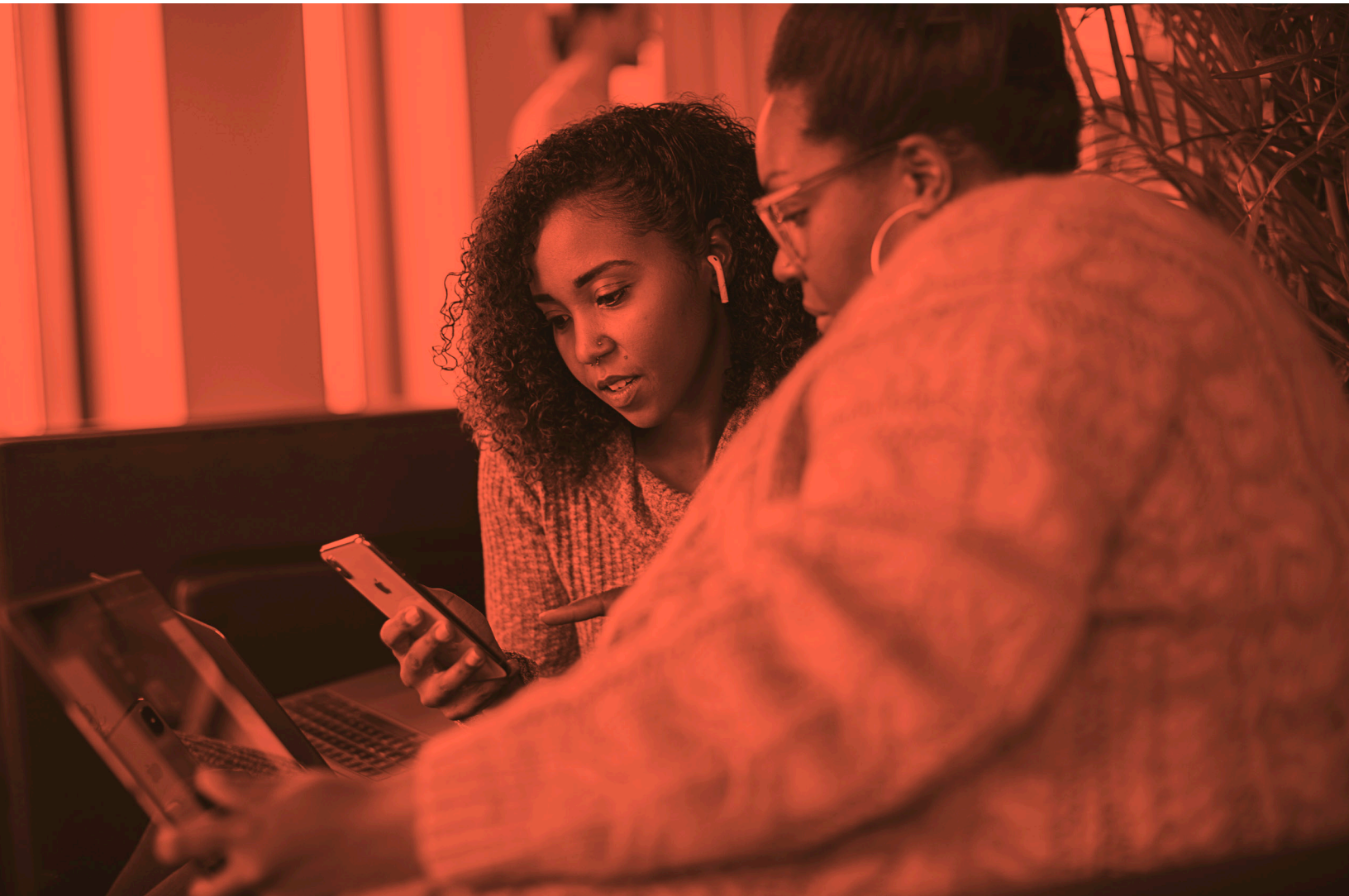
Les solutions de gestion des appareils et de sécurité intrusives ne sont pas les seuls problèmes de confidentialité auxquels sont confrontés les utilisateurs. Les développeurs d'applications peuvent également empiéter sur la confidentialité des utilisateurs, en particulier lorsque les apps sont gratuites, car il est probable qu'ils monétisent les données des utilisateurs.

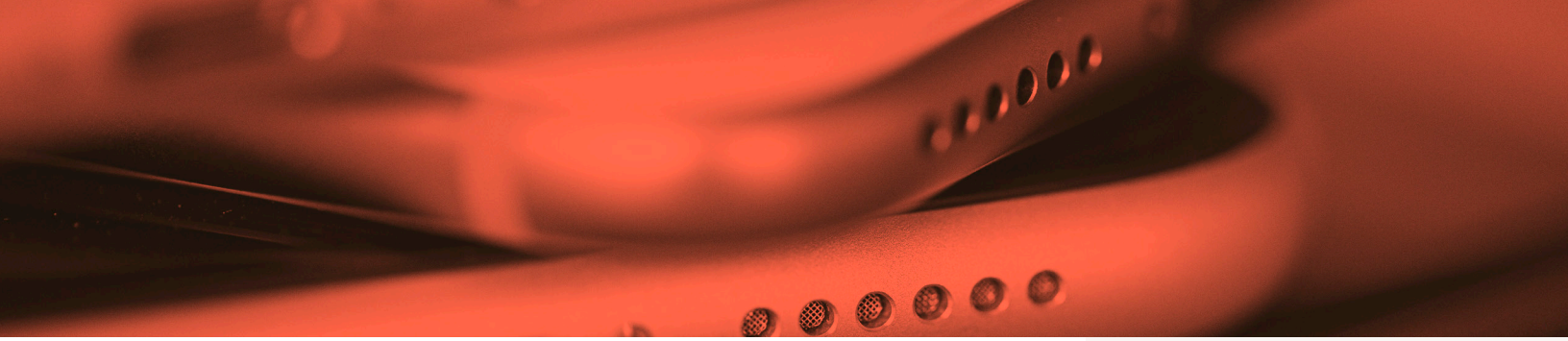
Selon l'étude de Jamf **An Analysis of iOS App Permissions**, qui a été publiée (en anglais) au deuxième trimestre 2021, l'autorisation la plus couramment demandée est l'accès à la photothèque avec 66 % des apps iOS incluses dans notre étude demandant cet accès, suivi par l'appareil photo (60 %), la localisation (58 %) et le microphone (34 %). En outre, de nombreuses catégories d'applications suspectes ont demandé un accès dont elles n'avaient pas besoin. Par exemple, il est logique que la majorité (62 %) des apps de navigation demandent l'accès à votre localisation, mais pourquoi près de la moitié d'entre elles (48 %) demandent également l'accès à votre appareil photo ? Il en va de même pour les 83 % d'apps d'achat qui demandent l'accès à votre appareil photo. C'est logique pour la lecture des codes QR, mais pourquoi tant d'applications (87 %) demandent-elles aussi l'accès à votre photothèque ? Il est utile de réfléchir à ce dont une app a réellement besoin pour fonctionner avant d'appuyer sur "accepter".

Mais que se passe-t-il une fois l'accès accordé ? Que peut-on faire alors pour freiner l'exploitation des données personnelles ? C'est là qu'interviennent le framework App Tracking Transparency d'Apple et la politique d'Identifiant publicitaire de Google, qui protègent le partage non autorisé des informations de confidentialité collectées à partir des capteurs et des technologies intégrés aux appareils mobiles. Ces deux solutions obligent les développeurs à les utiliser lors de la conception de leurs applications et leurs services, ce qui permet à l'utilisateur d'exercer un contrôle direct sur les données relatives à la vie privée.

De plus, les solutions de gestion des appareils telles que Jamf Pro respectent ces exigences, permettant au service informatique de désigner les applications de l'entreprise, ce qui permet non seulement de les déployer mais aussi de les gérer en toute sécurité, sans pouvoir accéder ou interagir avec les applications personnelles - ni avec leurs données - contenues dans les appareils personnels qui font partie d'un modèle BYOD ou les appareils appartenant à l'entreprise qui font partie d'un modèle CYOD/COPE.

En trouvant un équilibre entre la sécurisation des applications et des données, ainsi que de l'appareil lui-même, mais en permettant aux utilisateurs de contrôler en fin de compte les données privées associées à leurs applications personnelles et à l'utilisation de l'appareil, les entreprises peuvent protéger au mieux les données propriétaires qui sont à la fois sensibles par nature et confidentielles, tout en maintenant une approche "non interventionniste" des données personnelles de l'utilisateur, permettant aux utilisateurs finaux de contrôler le niveau d'accès à ces données, améliorant ainsi les protections globales de la vie privée en place.





Tendance 4 - Les utilisateurs finaux constituent toujours la principale menace pour la sécurité des données.

Une prémisse de base concernant la sécurité reste vraie par-dessus tout : quels que soient les types de contrôles de sécurité en place, leur configuration pour surveiller, détecter et atténuer les risques de manière agressive, et malgré le niveau d'automatisation pour prévenir et remédier aux problèmes liés à la sécurité, tout peut être annulé par un utilisateur à son insu.

Il ne s'agit pas d'une crainte, d'une incertitude ou d'un doute, mais d'une vérité bien réelle concernant le niveau de protection mis en place pour sécuriser les réseaux d'entreprise, avec souvent peu ou pas de considération pour la formation des utilisateurs. C'est pourquoi les acteurs malveillants continuent de prospérer en ciblant ces "fruits mûrs" dans leurs tentatives d'obtenir des données sensibles par le biais de campagnes de phishing et de logiciels malveillants/indésirables pour finalement pénétrer dans les réseaux d'entreprise.

Selon un dicton, la sécurité est la responsabilité de tous. En effet, les équipes informatiques et de sécurité peuvent disposer des compétences et des outils nécessaires pour mettre en œuvre des contrôles et corriger les menaces, mais tous les utilisateurs, quel que soit leur rôle au sein de l'organisation, doivent veiller à ce que les pratiques de sécurité restent efficaces. Il est inquiétant de constater que certaines mesures de sécurité essentielles sont encore négligées. Selon les données de Jamf Threat Labs, l'écran de verrouillage de 2 % des appareils utilisés dans le cadre professionnel sera désactivé en 2021, contre 3 % en 2020. Cela représente une menace importante en cas de perte ou de vol d'un appareil d'entreprise.

Selon l'Internet Crime Report2020 du FBI, publié en 2021, les trois principaux délits signalés par les victimes sont (1) les escroqueries de phishing, (1) les escroqueries par non-paiement/non-livraison et (3) l'extorsion. Également mis en évidence dans ce rapport : les attaques de phishing (y compris le vishing, le smishing et le pharming), ont impacté 241 342 victimes en 2020, contre 114 702 en 2019, avec des pertes ajustées de plus de 54 milliards de dollars. De plus, le phishing a impacté plus de deux fois plus de personnes que le deuxième délit le plus important : le non-paiement/non-livraison.

2 % des appareils utilisés pour le travail avaient l'écran de verrouillage désactivé en **2021**, contre **3 % en 2020**.

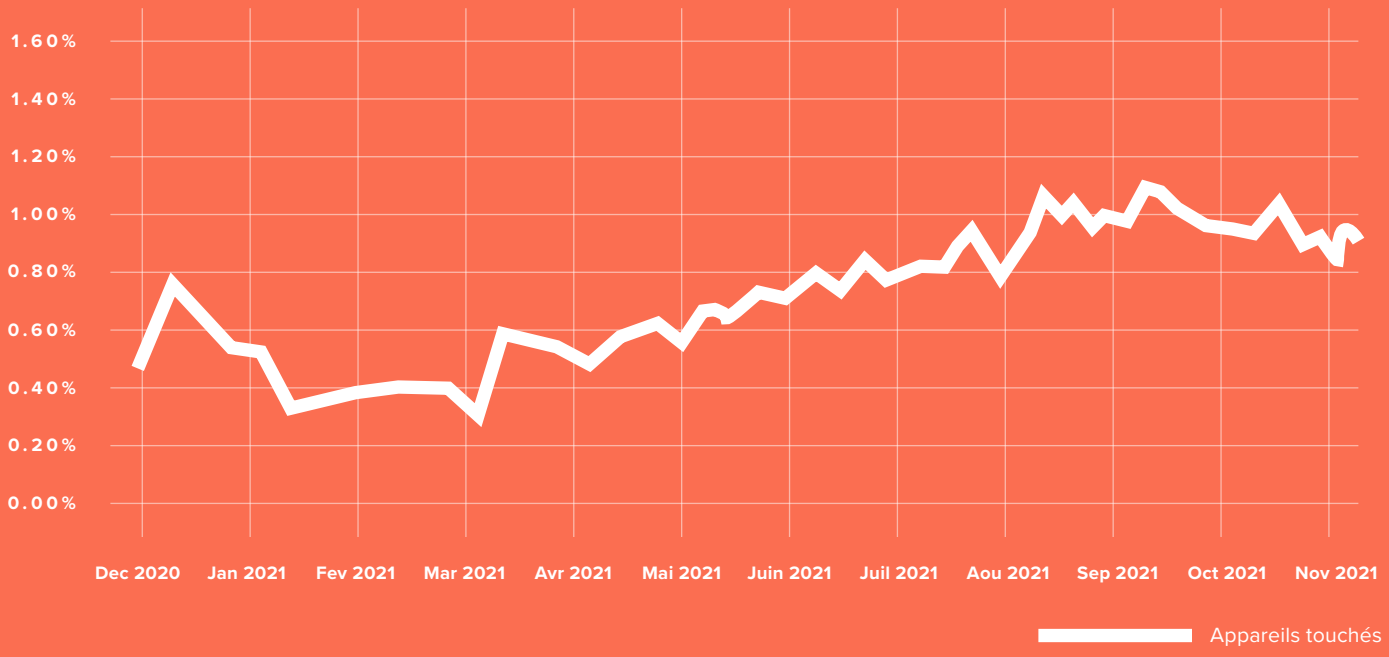
D'après nos données, **un tiers (29 %)** des organisations ont eu au moins un utilisateur victime d'une attaque de phishing **en 2021**.

Les conséquences du phishing pour les consommateurs sont déjà assez graves, mais si l'on considère l'impact sur les entreprises, c'est terrible. Selon le rapport 2021 de Verizon sur les enquêtes relatives aux violations de données, 36 % des violations de données sont dues au phishing, soit 11 % de plus que l'année précédente. Les utilisateurs peuvent également se connecter à des hotspots à risque lors de leurs déplacements.

La commodité du Wi-Fi gratuit à l'aéroport ou dans un café est souvent trop séduisante pour les employés qui ne pensent pas forcément à l'impact potentiel d'une attaque dans laquelle un acteur malveillant utilise une connexion Wi-Fi pour intercepter silencieusement un transfert de données, connue sous le nom d'attaque Man-in-the-Middle (MitM). Mais ce ne sont pas les seuls risques présents sur le Wi-Fi. Il existe un certain nombre d'indicateurs d'un hotspot à risque qui pourraient mettre les données en danger, notamment la présence d'un certificat racine tiers suspect qui pourrait compromettre l'authenticité des connexions SSL fiables en permettant l'interception des communications chiffrées.

Au cours de l'année 2021, le nombre d'appareils se connectant par semaine des hotspots à risque a doublé, passant **de 0,5% à 1 %**, peut-être en raison de l'augmentation des voyages et des déplacements domicile-travail due à l'assouplissement des restrictions liées à la pandémie.

Appareils se connectant à des hotspots à risque par semaine



Investir dans des programmes de formation à la sensibilisation à la sécurité pour les acteurs de l'entreprise est un élément important de la stratégie de sécurité d'une entreprise et ne doit pas être négligé. Il s'agit d'une formation continue et polyvalente pour les utilisateurs finaux, qui couvre une variété de meilleures pratiques et informe les utilisateurs sur les menaces les plus récentes qui sont les plus susceptibles de les affecter. Ills seront ainsi en mesure de mieux identifier les nouvelles attaques et évolutives et de prendre des mesures proactives pour améliorer leur hygiène de sécurité, non seulement au travail, mais aussi dans leur vie privée.

Tendance 5 - La gestion des risques liés aux applications devient de plus en plus complexe

Les applications sont le moteur de l'informatique. La connectivité à Internet étant le moteur de l'utilisation des applications, les applications et services basés sur le Cloud offrent aux utilisateurs une multitude d'options pour rester productifs et profiter des temps morts en dehors des heures de travail, le tout à partir du même appareil. Mais la croissance des logiciels malveillants, combinée à un développement médiocre et à des attaques de la chaîne d'approvisionnement, peut placer des applications potentiellement indésirables et malveillantes sur des appareils qui peuvent exposer des données, divulguer des informations sensibles et/ou compromettre l'appareil, et l'entreprise par la suite.

Il n'est pas illégal de pirater des appareils pour supprimer leur sécurité interne et permettre la modification de certaines fonctionnalités. L'accès à des App Stores tiers qui vendent des apps douteuses dont l'exploitation est normalement interdite dans les App Stores officiels d'Apple et de Google n'est pas non plus illégal, mais ces activités peuvent conduire à l'installation d'apps "piratées" illégales qui ne disposent pas de la licence du développeur.
Le risque de sécurité inhérent au sideloading est similaire à celui du jailbreaking, les deux pouvant conduire à l'installation d'applications risquées susceptibles d'infecter les appareils avec des logiciels malveillants, d'espionner les utilisateurs, de voler ou de divulguer des informations personnelles identifiables, d'inonder leur appareil de publicités ou de le bloquer purement et simplement, voire pire. Selon les données de Jamf Threat Labs, moins de 1 % des organisations disposaient d'un ou de plusieurs appareils jailbreakés ou racinés dans leur parc informatique en 2021 et 5 % des organisations avaient un ou plusieurs appareils ayant installé une application tierce en 2021.

Le code interne de ces versions d'applications non officielles ou obtenues illégalement n'est pas examiné ni analysé pour détecter les menaces de sécurité, comme le sont les applications des App Store officiels. Cela signifie qu'une application se présentant comme une alternative de navigateur sécurisée peut en fait être un logiciel malveillant.

Lorsqu'elles sélectionnent des apps pour un usage professionnel approuvé, les équipes informatiques doivent s'assurer qu'elles sont correctement approuvées pour être utilisées avec l'infrastructure de l'entreprise et elles doivent effectuer un contrôle continu et dynamique des applications qui va au-delà des simples examens statiques du code. Cela permettra de détecter les problèmes qui surviennent lorsque l'application est connectée à l'internet pendant son utilisation, tels que un chiffrement faible ou inexistant, des réseaux de diffusion de publicités connus pour diffuser des malwares, ou des "fonctionnalités" inconnues ou non annoncées qui créent effectivement une situation de cheval de Troie dans laquelle une app est utilisée pour une fonction, mais permet secrètement à une autre fonction de fonctionner en arrière-plan.

Moins de 1 % des organisations disposaient d'un ou plusieurs appareils jailbreakés ou racinés dans leur parc informatique en **2021**.

En 2021, 5 % des organisations ont vu un ou plusieurs appareils installer une app tierce.

Une autre préoccupation importante liée à la sécurité des apps est celle des attaques de type "pipeline" ou celles qui cherchent à compromettre le canal de distribution ou d'approvisionnement comme moyen de compromettre indirectement tous les appareils qui dépendent de l'application ou du service compromis. Bien que cette forme d'attaque soit difficile à identifier puisqu'elle vise généralement le fabricant ou le développeur de l'application elle-même, elle a généralement un impact plus profond et des effets plus durables sur les entreprises qui en sont victimes, comme l'explique un rapport de CNN sur l'attaque de SolarWinds qui a compromis un logiciel commercial utilisé pour gérer les équipements de réseau en décembre 2020 et qui touche encore les organisations aujourd'hui. Il y a des choses que les entreprises peuvent faire pour s'isoler de ce type d'exposition autant que possible.

Nous recommandons de déployer les applications et les services uniquement à partir de développeurs connus en utilisant les App Stores officiels pour votre écosystème d'appareils. Tester les applications dans des environnements de non-production permet aux équipes informatiques et de sécurité d'évaluer le fonctionnement de l'application ou du service, ce qui leur permet d'apporter les ajustements nécessaires avant le déploiement final. Pour les organisations qui développent des applications en interne, assurez-vous que votre infrastructure de développement est sécurisée et que l'accès est limité aux seules personnes qui en ont besoin, comme les programmeurs, et réduisez le nombre d'apps exécutées dans ces bancs d'essai au strict nécessaire pour développer l'app. Le respect des pratiques de développement d'applications sécurisées, le contrôle régulier des applications à l'échelle du parc informatique et la mise à jour des environnements permettront d'atténuer bon nombre des facteurs qui permettent aux malwares d'infiltrer les sites de développement et à minimiser la probabilité qu'un tiers compromette le workflow de développement, ce qui entraînerait le déploiement d'applications compromises en production.

Recommendations

Malgré une tentative de définition de normes informatiques d'entreprise qui dure depuis des décennies, de nombreuses entreprises ont atteint un point où l'absence de normalisation est la norme. Selon l'enquête Verizon MSI 2021 (en anglais), près d'un quart (24 %) des personnes interrogées ont déclaré que leur organisation avait sacrifié la sécurité des appareils mobiles pour faciliter leur réponse aux restrictions mises en place en raison de la pandémie. Quel système d'exploitation votre entreprise utilise-t-il ? Tous les systèmes d'exploitation. Quel type d'utilisateurs autorisez-vous à accéder à vos applications ? Tous les utilisateurs. De quels endroits les utilisateurs sont-ils autorisés à travailler ? Tous. Les solutions d'accès sécurisé à distance doivent être suffisamment flexibles et agiles pour permettre, et non bloquer, la productivité. Nous vous recommandons d'utiliser cette liste de contrôle pour développer une stratégie de sécurité moderne fournie par le Cloud afin de répondre aux besoins des environnements informatiques hybrides d'aujourd'hui.

Définir les exigences en fonction des nouveaux cas d'utilisation créés par le travail à distance

Que voulez-vous permettre aux employés de faire sur leurs appareils - accéder aux e-mails ou aux bases de données sensibles ? Segmentez les données pour que l'accès soit granulaire.

- Évaluez vos cas d'utilisation et définissez les exigences pour vos employés en télétravail.
- Les exigences ci-dessus détermineront votre modèle de propriété des appareils : quels types d'appareils prendrez-vous en charge, qui les possède et comment sont-ils gérés ?
- Donnez la priorité aux besoins des utilisateurs finaux pour garantir l'adoption des outils de sécurité - choisissez des solutions qui ne les ralentiront pas, qui ne les gêneront pas et qui sont adaptées à l'écosystème des appareils qu'ils utilisent.

Fournir une connectivité rapide et sécurisée

- En ce qui concerne la connectivité et les applications Cloud, déterminez ce que vous devez savoir sur les utilisateurs, les appareils, les réseaux et les apps avant de leur accorder l'accès aux ressources d'entreprise.
- Limitez les utilisateurs aux seuls outils professionnels dont ils ont besoin, cela évite que les comptes privilégiés soient exploités pour attaquer un grand nombre de systèmes.
- Adoptez un accès conditionnel continu pour évaluer les règles en temps réel.

Définir et appliquer une règle d'utilisation acceptable.

- Passez en revue vos politiques d'utilisation acceptable existantes et assurez-vous que tous les types de terminaux sont pris en compte.
- Mettez en œuvre une politique d'utilisation acceptable pour chaque sous-ensemble approprié d'appareils afin de contrôler le Shadow IT, l'utilisation indésirable et de garantir la conformité réglementaire.

Déployer une solution de gestion suffisamment souple pour s'adapter à tous les modèles de propriété des appareils

- Déployez une solution de gestion qui vous permettra d'approvisionner les appareils en ressources d'entreprise, de configurer les comptes et la connectivité, et de procéder à des contrôles de sécurité et de conformité continus sans sur-gestion et sans empiéter sur la vie privée des utilisateurs.
- Automatisez la correction des appareils jugés non conformes ou dans un état de vulnérabilité ou de compromission afin de les remettre en conformité.

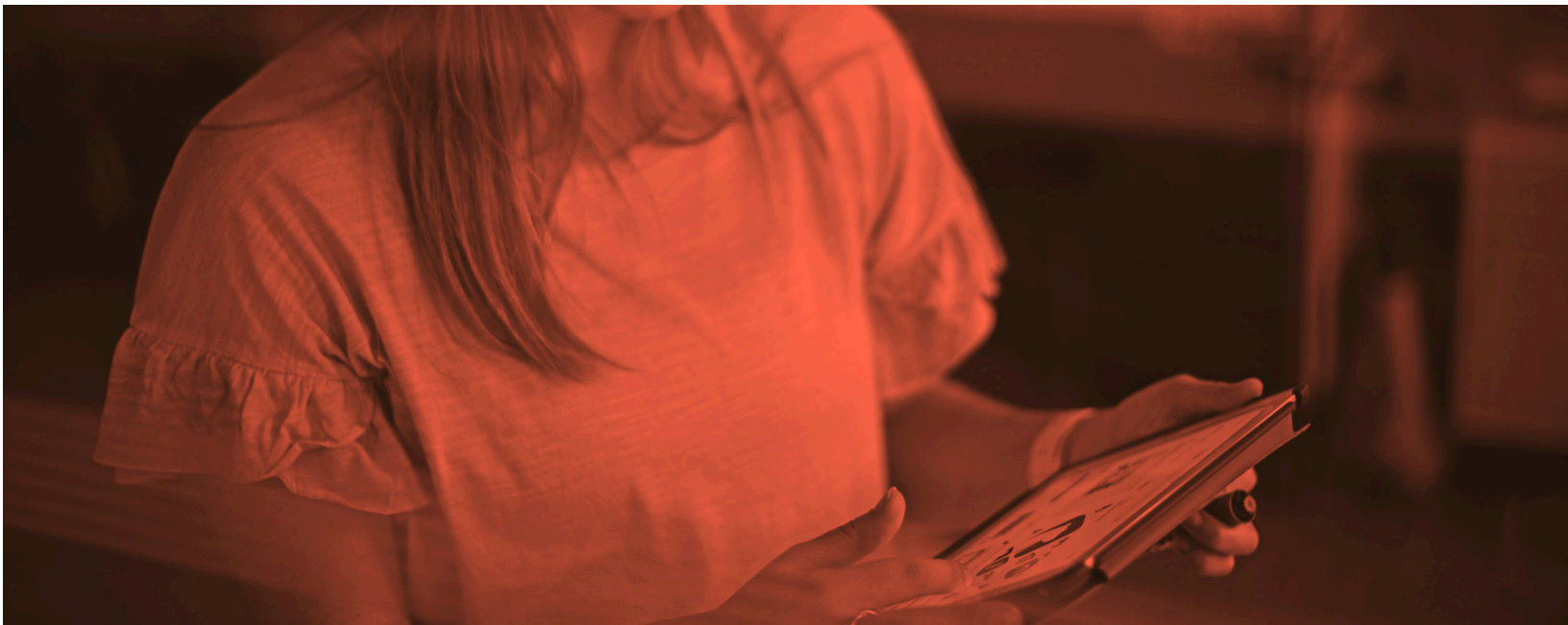
Élargir les règles de gestion des accès afin d'intégrer l'état de risque des appareils

Mettez en œuvre une solution IAM (Identity and Access Management) conviviale pour l'authentification aux applications d'entreprise sur tous les appareils, y compris les appareils mobiles.

- Intégrez des évaluations des risques liés aux appareils dans vos politiques de gestion des accès afin de vous assurer que le niveau de risque des appareils est pris en compte.
- Veillez à ce que le niveau de risque soit évalué en permanence pendant toute la durée d'une session.

Déployer la protection des terminaux sur tous les appareils, une solution de sécurité basée sur le Cloud est particulièrement importante pour se protéger contre le large éventail de cybermenaces et de risques d'utilisation, y compris les attaques de type « zéro-day »

- Assurez-vous que votre solution de sécurité est dotée d'une forte capacité de détection des terminaux avec des capacités sur les appareils, complétées par des mesures préventives basées sur le réseau pour stopper les attaques avant qu'elles n'atteignent un appareil.



- Assurez-vous que votre solution de sécurité peut faire face aux cybermenaces externes (telles que le phishing, les attaques de type "man-in-the-middle" et les malwares) et aux risques liés au comportement d'utilisation (apps chargées en parallèle, etc.).
- Pour tous les outils de sécurité, veillez à ce que les configurations appropriées soient faites pour traiter les vecteurs de menace qui conviennent à votre entreprise tout en respectant la vie privée de vos utilisateurs finaux.
- Évaluez les capacités de machine learning de la solution de sécurité pour comprendre comment le moteur de menaces identifie et protège contre les menaces nouvelles et inconnues (heuristique/analyse comportementale).

Revoir régulièrement cette liste et envisager les changements à apporter en fonction des éléments suivants

- Les changements de taille et de composition de l'entreprise, par exemple les fusions ou les acquisitions.
- Les nouvelles réglementations qui affectent la manière dont vous traitez les données.
- Une évolution de la stratégie informatique.
- Les menaces que vous avez constatées sur les employés.
- Un achat de nouveaux équipements et mise hors service d'appareils en fin de cycle de vie.
- De nouvelles applications dont les employés ont besoin pour accomplir leur travail.
- Modification des frameworks des systèmes d'exploitation qui régissent la facilité de gestion, le déploiement et la confidentialité des données.

À propos de cette recherche

Nous voulions mieux comprendre les plus grandes tendances en matière de sécurité qui émergent dans le nouveau monde du travail hybride. Les informations et statistiques trouvées dans ce document sont le résultat de notre analyse des tendances de sécurité au sein d'un échantillon de 500 000 appareils protégés par Jamf, couvrant iOS, macOS, iPadOS, Android et Windows, dans 90 pays, sur une période de 12 mois. Cette analyse a été réalisée au quatrième trimestre de 2021. Les métadonnées analysées dans cette recherche proviennent de journaux agrégés qui ne contiennent pas d'informations permettant d'identifier les personnes ou les organisations. L'objectif de cette analyse n'est pas de susciter la peur, mais plutôt de vous informer, vous et vos utilisateurs, des options disponibles et de la meilleure façon de sécuriser tous les aspects des données des appareils, des utilisateurs et des organisations. Contactez-nous pour savoir comment vous pouvez mettre en place des mesures de protection et améliorer votre posture de sécurité.