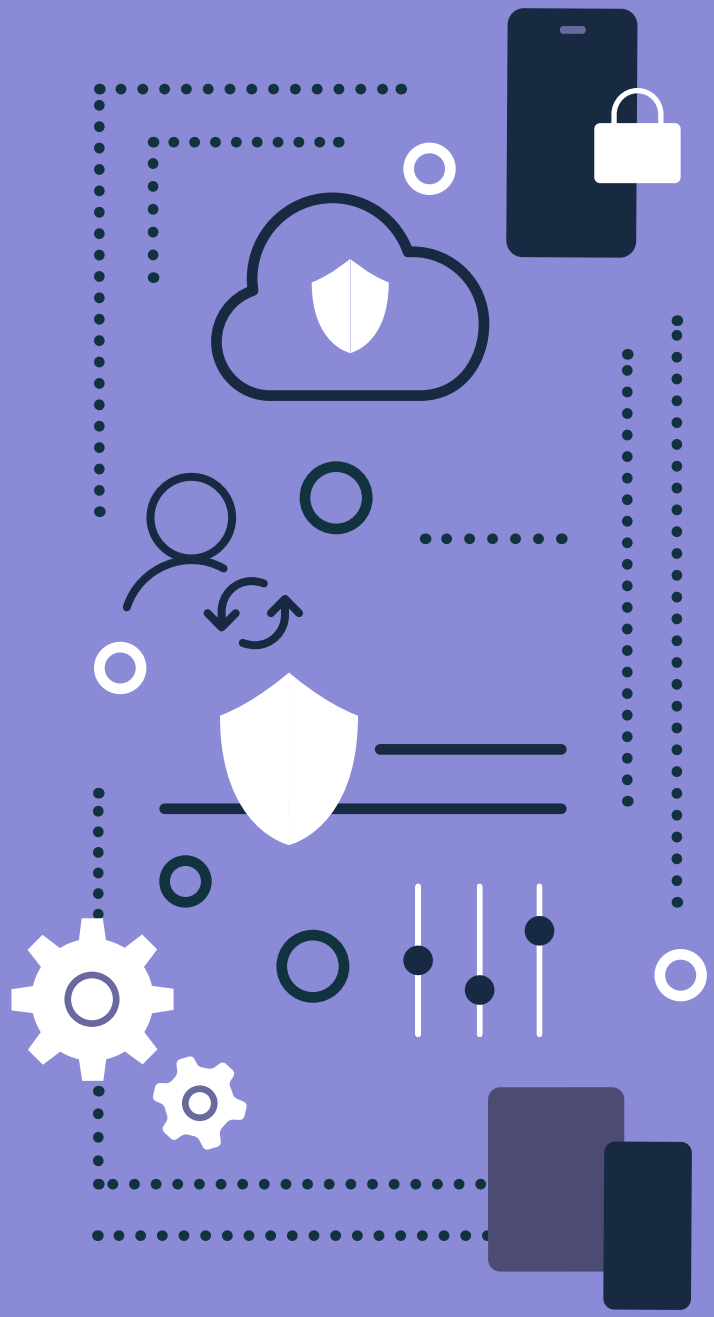


jamf

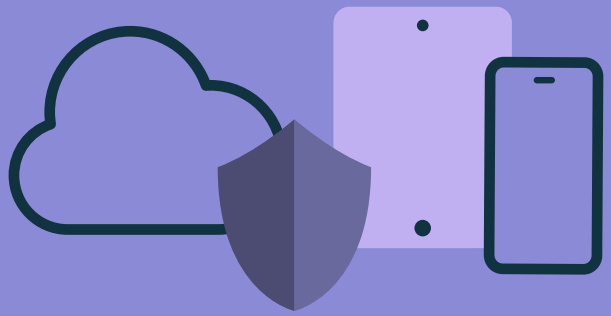
Le guide essentiel des

antivirus pour Mac

LES LOGICIELS MALVEILLANTS QUI CIBLENT LES MAC SONT UN ENJEU MAJEUR À L'HEURE OÙ LES ENTREPRISES ÉLARGISSENT LEUR FLOTTE APPLE.

Dans l'ensemble, Apple s'en sort bien, étant donné que les détections spécifiques aux logiciels malveillants semblent avoir ralenti par rapport à d'autres types de logiciels malveillants plus ciblés. Et ce alors que les détections sont en hausse sur toutes les plates-formes informatiques.

Les organisations ont adopté le télétravail et les pratiques hybrides, et le paysage technologique a radicalement changé. En réponse, les auteurs de logiciels malveillants et d'attaques s'adaptent en modifiant la portée et l'ampleur de leurs outils. En utilisant plusieurs types d'attaques à la fois, les pirates redoublent de complexité. De plus, un recours accru à l'automatisation permet d'étendre les cibles pour inclure les outils de collaboration dont les utilisateurs ont besoin pour rester productifs.



DANS CE GUIDE, NOUS ALLONS :

- Définir les antivirus (AV) axés Mac
- Montrer comment les logiciels malveillants affectent de plus en plus les utilisateurs Mac
- Expliquer pourquoi il est essentiel de comprendre ces tendances pour sécuriser les données privées
- Voir comment Jamf peut aider à protéger vos Mac

ANTIVIRUS AXÉS MAC

L'antivirus est un outils essentiel pour fournir une sécurité de base à la plupart des appareils d'une organisation. Apple inclut un mécanisme antivirus de base dans macOS avec XProtect, Gatekeeper et MRT. Malheureusement, ces outils ne sont pas mis à jour régulièrement et les organisations n'ont pas de visibilité sur leurs opérations. Elles ont besoin de capacités antivirus plus sophistiquées pour prévenir et mettre en quarantaine les logiciels malveillants Mac. Et cela va bien au-delà de ce que les solutions axées Windows peuvent fournir.
Elles ne peuvent pas se permettre d'attendre que des problèmes de logiciels malveillants, de logiciels publicitaires ou d'autres logiciels indésirables surviennent.

Elles doivent implémenter un antivirus qui identifie et résout efficacement les attaques spécifiques aux Mac, sans perdre des ressources précieuses à rechercher des menaces conçues pour Windows. Des capacités d'antivirus efficaces, rentables et complètes sont essentielles autant pour la sécurité que pour l'expérience des utilisateurs.

Les infractions au respect de la vie privée sont innombrables d'après un rapport de Kaspersky Labs, qui cite en particulier la transmission des coordonnées GPS, la capture de messages déchiffrés et la surveillance des appels téléphoniques.

UN PAYSAGE DE MENACES EN CONSTANTE ÉVOLUTION

Toujours plus nombreuses, les campagnes de phishing tirent parti des crises contemporaines et se nourrissant des craintes et des inquiétudes des individus, en particulier face aux diverses pénuries qui frappent l'économie mondiale. Les escroqueries liées à l'assistance informatique, en particulier, se multiplient.

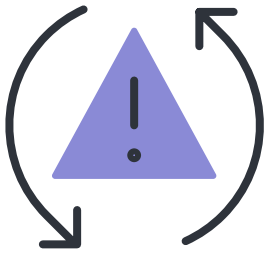
VOL DE DONNÉES EN LIGNE

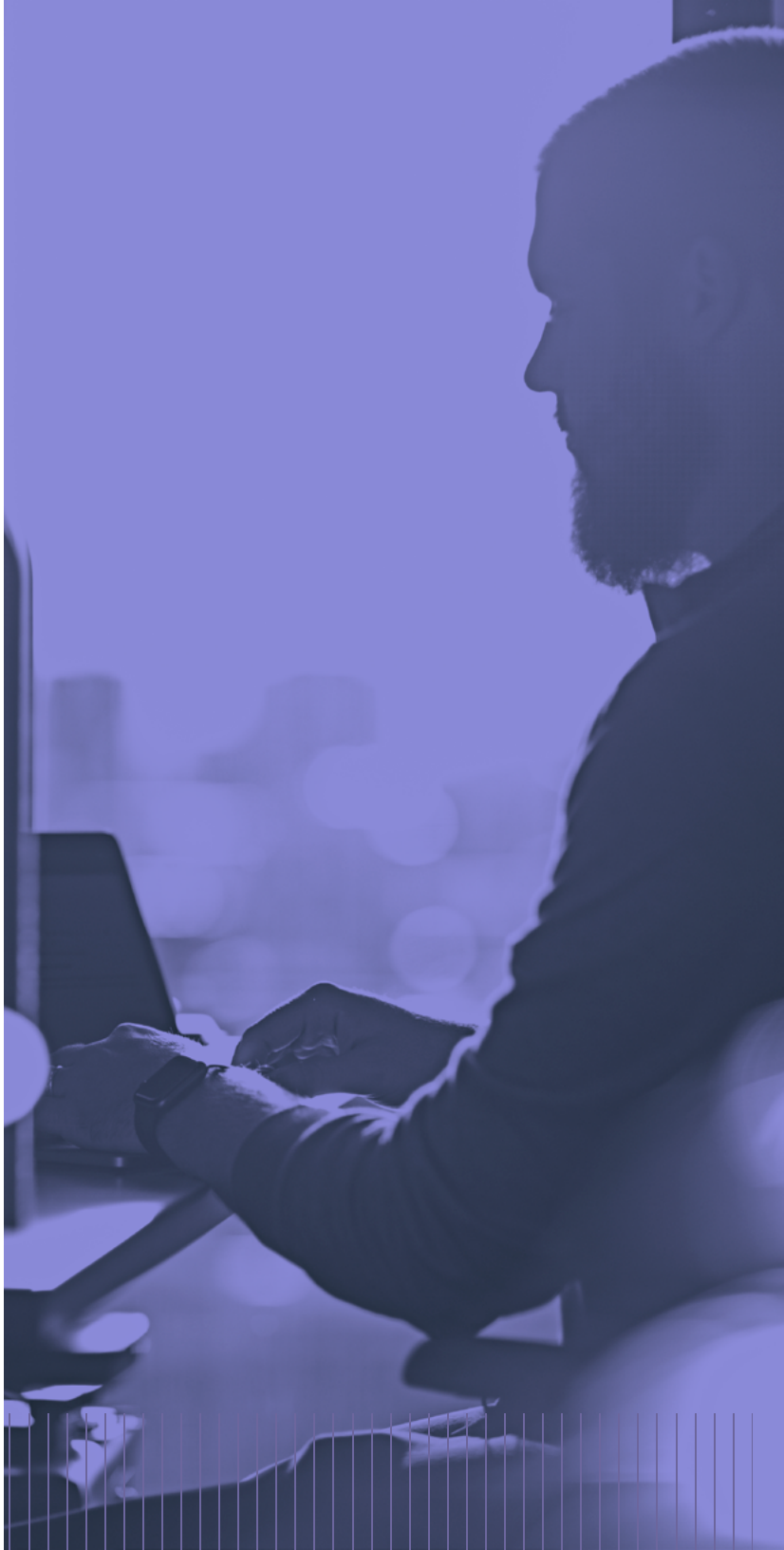
Divers logiciels malveillants – publicitaires, espions et traqueurs – sont mis à profit pour obtenir et exfiltrer des données sur les utilisateurs. Les logiciels de traque, ou de « creeping » en ligne, exploitent toutes sortes de données d'identification personnelle en temps réel.

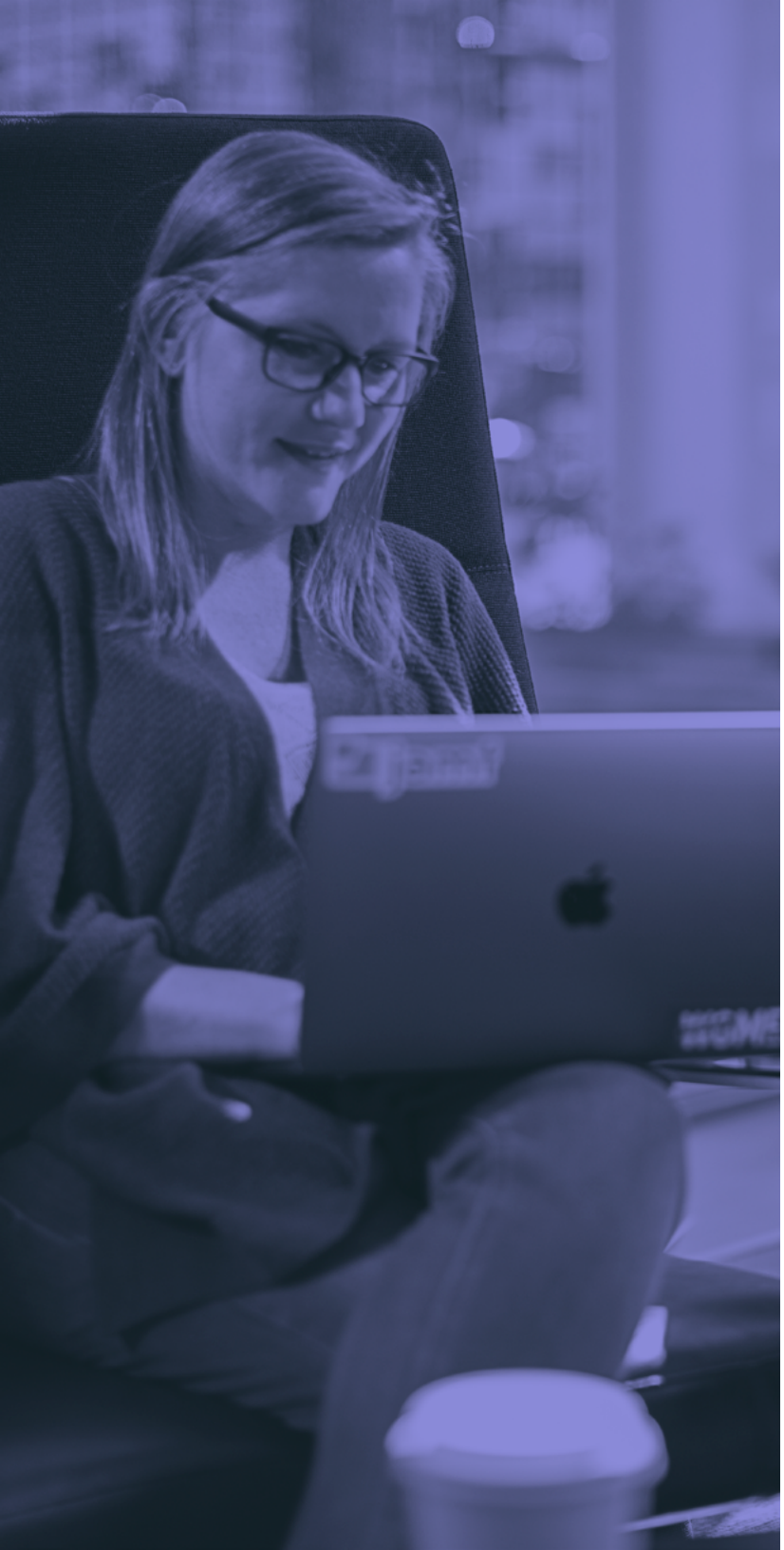
ON JOUE AUX ÉCHECS, PAS AUX DAMES

Les auteurs de menaces sont rarement pressés, ce qui veut dire que les campagnes d'attaques peuvent durer aussi longtemps que nécessaire. Elles ne se cantonnent pas à l'infiltration d'un logiciel malveillant unique sur un appareil : bon nombre d'entre elles essayent d'obtenir un accès et d'exploiter des tremplins existants. Les pirates ont ainsi le temps d'adapter et affiner leur stratégie d'attaque ou leurs outils, et de rassembler autant d'informations qu'ils le souhaitent. Cela leur permet, en bout de ligne, d'incorporer des logiciels malveillants plus profondément dans les systèmes ciblés.

Il s'agit d'un cercle vicieux où chaque élément impacte et alimente directement le suivant.







ANTIVIRUS POUR MAC : UN ÉTAT DES LIEUX

La croissance des logiciels malveillants poursuit sa tendance à la hausse, avec un total de 1 227 048 144 logiciels malveillants identifiés en 2022 par AV-Test.org – en incluant les applications potentiellement indésirables (PUA). La bonne nouvelle pour les utilisateurs Mac ? La ventilation par OS a révélé que seuls 220 des logiciels malveillants identifiés ciblaient macOS !

Ce tournant s'explique par plusieurs facteurs :

- Le nombre croissant d'appareils Apple dans les entreprises
- Le fait que les employés optent pour des produits Apple quand leur entreprise leur donne le choix (ou utilisent leurs appareils Apple personnels)
- La transition mondiale vers le télétravail et les pratiques hybrides, qui a effacé les frontières entre le bureau et le domicile

NE VOUS RÉJOUISSEZ PAS TROP VITE

Les particuliers verront certainement ce chiffre d'un bon œil, mais les données télémétriques recueillies par diverses sources indiquent que les appareils utilisés dans l'espace personnel restent les cibles de programmes potentiellement indésirables, notamment des logiciels publicitaires.

La problématique est totalement différente de celle qu'on observe du côté des établissements d'enseignement. Chez les particuliers utilisateurs de Mac, les programmes indésirables et les logiciels publicitaires tentent d'accéder à des informations d'identification personnelle. Et la diffusion de publicités malveillantes, le traçage des données privées et les applications douteuses prétendant nettoyer votre Mac peuvent avoir des conséquences dramatiques.

PANACHÉS DE LOGICIELS MALVEILLANTS

Si le dernier rançongiciel ciblant Mac connu a été détecté il y a plusieurs années, en 2020 EvilQuest (également appelé ThiefQuest) est apparu sur le devant de la scène. Ce logiciel malveillant a toutes les caractéristiques d'un rançongiciel, mais il cache son jeu : les avertissements de chiffrement et les demandes de rançon ne sont qu'un subterfuge pour masquer un vol persistant et ciblé de données personnelles et professionnelles.

Les logiciels malveillants de ce type peuvent évoluer au fil du temps, tout comme les logiciels normaux : ils acquièrent des fonctionnalités supplémentaires qui causent plus de dommages, et se font plus discrets afin d'échapper à la détection. Ils peuvent même se mettre à jour eux-mêmes pour évoluer après avoir infecté un appareil. EvilQuest a toutes les caractéristiques d'une histoire sans fin.

LES VIEUX SINGES PEUVENT APPRENDRE À FAIRE DES GRIMACES

Dans la catégorie « casse-pieds pour l'instant », les logiciels malveillants de type publicitaire évoluent également. Les dernières versions d'Apple macOS s'efforcent de vérifier les signatures des applications avant de permettre leur lancement. Certains auteurs de logiciels malveillants se sont donc donné beaucoup de mal pour obtenir un accès aux données précieuses de votre système et de monétiser les publicités que vous voyez sur le Web.

Une attaque de ce type consiste, par exemple, à dupliquer l'application Safari et à la modifier en installant des extensions non autorisées pour traquer les utilisateurs. Citons encore l'utilisation de profils de configuration (les mêmes que ceux qui sont utilisés par les administrateurs informatiques pour gérer les réglages des appareils), que des utilisateurs abusés installent sur leurs appareils et qui accordent aux pirates les accès dont ils ont besoin pour réaliser d'autres attaques.

Les logiciels publicitaires sont considérés comme moins dangereux alors qu'ils peuvent avoir un impact démultiplié. En effet, ils sont le type de logiciel malveillant le plus courant sous macOS et ils affichent les formes d'innovation les plus avancées dans leur mode d'infection des systèmes (sans parler de la possibilité de plus en plus courante d'envoyer des charges utiles néfastes à distance).

NE TRAVAILLEZ PAS PLUS, MAIS MIEUX

Il n'y a malheureusement pas de solution unique pour résoudre les menaces grandissantes auxquelles nous sommes confrontés. L'un des points à retenir est le fait que les menaces ne proviennent pas du même endroit à chaque fois. Les pirates changent de tactiques de plus en plus souvent et ciblent les appareils et les services qui produiront les meilleurs résultats. Les données disponibles confirment que les pirates ne semblent pas près de s'arrêter.

Qu'est-ce que cela signifie pour tous ceux qui dépendent des ordinateurs pour vivre et travailler ? La sécurité doit être configurée pour défendre, dévier, prévenir ou remédier à toutes les menaces. La vigilance est indispensable à la sécurité. Il faut également former les utilisateurs pour qu'ils apprennent à identifier les types de menaces les plus courants, tels que les tentatives de phishing, ou éviter d'installer des logiciels inconnus.

Le service informatique et les équipes de sécurité doivent faire preuve de vigilance pour renforcer et préserver la position de sécurité de l'organisation. Des logiciels de détection peuvent localiser les menaces en fonction de signatures connues. Des systèmes heuristiques peuvent aussi réaliser des analyses comportementales afin de détecter des menaces inconnues avant qu'elles ne surviennent.

Ces outils fournissent les informations nécessaires pour comprendre d'où proviennent les menaces ciblant votre organisation et comment mieux s'en défendre.

Une réponse rapide et l'automatisation permettent de réagir promptement face aux menaces détectées et de corriger les problèmes sans délai – un facteur vital pour la réussite de l'organisation. Ces deux éléments aident à minimiser la surface d'attaque et à gérer les risques plus efficacement, tout en renforçant la stratégie de défense en profondeur.

Après tout, lorsque nous utilisons des Mac, c'est pour arriver à un résultat ; pas pour passer en revue des milliers de lignes de code à la recherche de bogues avant de lancer une application. Nous le savons, Apple fait tout pour simplifier l'expérience de ses utilisateurs pour libérer leur créativité. Alors, pourquoi les logiciels de sécurité ne suivraient-ils pas cette voie ?

INTÉGRATION + ASSISTANCE JAMF

Jamf Protect prévient les logiciels malveillants et remédie aux comportements dangereux grâce à une détection basée sur les signatures, et des analyses comportementales sur Mac. Munis des informations granulaires descendantes sur les appareils, les services informatiques et de sécurité peuvent voir ce qui affecte la performance des appareils du point de vue de la sécurité. Par ailleurs, avec Jamf Pro, la mise en place d'une gestion des correctifs et d'une correction centralisées permet de résoudre quasiment tous les problèmes de sécurité. Jamf Connect vient compléter ce tiercé de haute sécurité. La solution de Jamf Connect pour la gestion des identités et des accès utilise des services d'identité basés sur le cloud pour sécuriser l'accès aux appareils et aux ressources.

Une stratégie de défense en profondeur qui combine les outils intégrés d'Apple avec la puissance de Jamf vous aidera à maintenir une sécurité Mac efficace. Ces outils s'intègrent facilement, sans affecter l'expérience des utilisateurs finaux, et offrent des informations et des analyses pertinentes sur les appareils. Cette stratégie sur plusieurs niveaux permet aux services informatiques de prendre les meilleures décisions pour la protection de leurs appareils et des données des utilisateurs.

Jamf, la référence pour la gestion et la sécurisation d'Apple, propose les produits et les solutions qui vous aideront à mettre en œuvre la stratégie de sécurité la plus adaptée à votre organisation et à vos utilisateurs.

Nous appelons cette approche Trusted Access. **Explorez-la.**

MAIS NE NOUS CROYEZ PAS SUR PAROLE,

mettez les antivirus et la protection des terminaux à l'épreuve.

Pour protéger votre flotte de Mac contre les menaces de sécurité grandissantes et les logiciels malveillants connus, mais aussi pour remédier aux comportements dangereux, faites l'essai gratuitement ou contactez votre revendeur Apple.

Demandez un essai gratuit

ou contactez votre revendeur Apple lorsque vous voudrez renforcer votre sécurité.

Rendez-vous sur jamf.com/fr pour en savoir plus sur Jamf Protect et la protection des terminaux Mac.