Antivirus pour Mac dans l'enseignement supérieur

jamf

L'état des logiciels malveillants pour les appareils Apple est devenu un sujet de plus en plus important à mesure que l'écosystème Apple s'implante dans l'enseignement supérieur.

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.

Des menaces graves classées comme des logiciels malveillants, tels que les rootkits et les rançongiciels, sont en chute par rapport aux années précédentes. De grands botnets ont également été réduits à néant, malgré plusieurs attaques très médiatisées l'année dernière. Cela est probablement attribuable à une évolution de l'utilisation des appareils et de leur emplacement.

La crise sanitaire mondiale est le principal catalyseur de cette transition, qui voit les environnements de réseaux d'entreprises, accessibles localement par des millions d'utilisateurs, abandonnés au profit du travail à domicile.

En d'autres termes, le paysage a considérablement 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 cet e-book, nous allons :

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

Antivirus pour Mac

L'antivirus (AV) est un incontournable pour fournir une sécurité de base à la plupart des appareils institutionnels. 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. Les institutions 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.

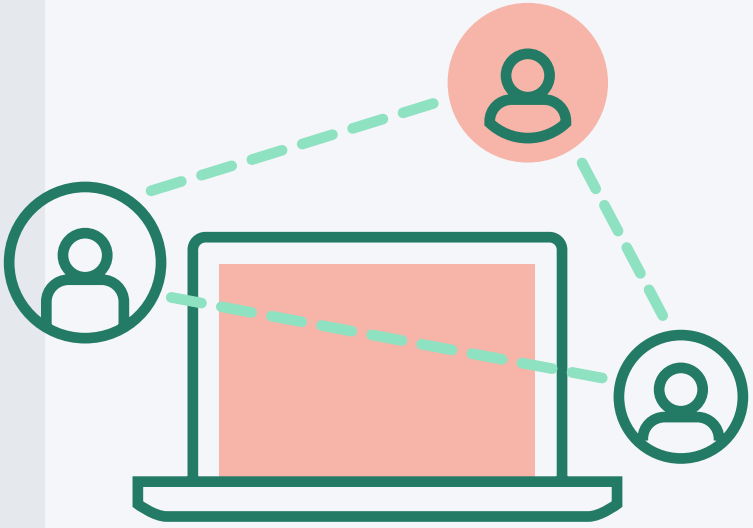
Elles doivent implémenter un antivirus qui identifie et résout efficacement les attaques spécifiques aux Mac, sans perdre des ressources précieuses à rechercher des menaces conçues pour Windows. Des capacités d'antivirus efficaces, rentables et complètes sont essentielles autant pour la sécurité que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

Un paysage de menaces en constante évolution

On note une augmentation significative des campagnes de phishing depuis le début de la crise sanitaire. Elles sont alimentées par l'inquiétude des individus, en particulier lorsqu'il s'agit de marchandises en quantités limitées ou affectées par des pénuries internationales. On note également de nombreuses escroqueries d'assistance technique. Comme si ça n'était pas assez, la collecte d'informations intéresse de plus en plus les pirates.

Vol de données en ligne

Les logiciels publicitaires, les logiciels espions, et les plus récents logiciels de traque sont tous des logiciels malveillants utilisés 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.



Le relais de coordonnées GPS, la journalisation de messages déchiffrés et la surveillance/ l'enregistrement d'appels téléphoniques sont quelques exemples des nombreuses infractions en matière de confidentialité, d'après un rapport de Kaspersky Labs.

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 permettra, en fin de compte, d'incorporer des logiciels malveillants plus profondément dans les systèmes concernés.

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

Situation des antivirus pour Mac

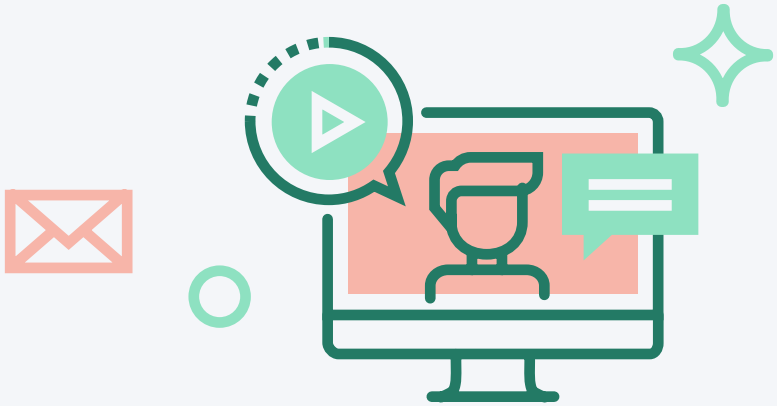
La bonne nouvelle pour les utilisateurs de Mac, c'est que le nombre de détections globales de logiciels malveillants sur des appareils Mac a chuté de plus 38 % en 2020, selon un rapport de Malwarebytes Labs sur l'état des logiciels malveillants publié en 2021.

La mauvaise, c'est que le secteur de l'éducation est souvent considéré comme l'un des moins sûrs. Les universités n'ont donc pas le choix : elles doivent constamment s'efforcer de faire évoluer leur stratégie et leur posture de sécurité, sous peine de succomber à des menaces au visage changeant.

Plusieurs facteurs influencent cette évolution, dont voici les trois principaux :

- La croissance continue du marché d'Apple et des Mac dans l'enseignement supérieur
- Les utilisateurs qui optent pour des appareils Apple lorsque les programmes destinés aux étudiants ou aux enseignants leur laisse le choix, ou que leur laboratoire propose des MacBooks
- La tendance mondiale à l'adoption de programmes d'apprentissage à distance, qui a brouillé la ligne de démarcation qui séparait autrefois le campus et la maison.

Ne vous réjouissez pas trop vite



Si les particuliers peuvent se réjouir de cette baisse, 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 utilisateurs personnels de produits Mac, les programmes potentiellement indésirables et les logiciels publicitaires tentent d'accéder à des informations d'identification personnelle. Et la distribution de publicités malveillantes, le traçage des données privées et les application douteuse prétendant nettoyer votre Mac peuvent avoir des conséquences dramatiques.

Panachés de logiciels malveillants

On constate de nouvelles formes de rançongiciels dans les attaques – et ce n'est sûrement que la partie visible de l'iceberg. 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 tels que celui-ci peuvent évoluer au fil du temps, tout comme les logiciels normaux : ils acquièrent des fonctionnalités supplémentaires qui causent plus de dommages, et deviennent 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 dubliquer 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 atteindre des niveaux critiques de destruction. 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. La formation des utilisateurs est également nécessaire pour qu'ils puissent identifier les types de menaces les plus courants, tels que les tentatives de phishing, ou éviter d'installer des logiciels inconnus.

Le service informatique doit être vigilant pour renforcer et préserver la position en matière 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 au service informatique 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 à des menaces détectées, car il est essentiel de résoudre les problèmes trouvés. 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. Apple s'efforce de faciliter l'expérience utilisateur et de la rendre extraordinaire. 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 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. Enfin, l'association de Jamf Pro et Jamf Protect avec Jamf Connect forme un trio gagnant hautement sécurisé. Il permet une gestion des identités en liant votre Mac aux ressources de l'établissement à l'aide de services d'identité dans le cloud pour l'accès aux appareils et aux ressources. Les données des utilisateurs sont ainsi sécurisées puisque leurs appareils sont protégés de bout en bout.

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 l'Apple Enterprise Management, propose les produits et les solutions qui vous aideront à mettre en œuvre la stratégie de sécurité la plus adaptée à votre institution et à vos utilisateurs.

Faites-vous votre propre avis.

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

Pour protéger votre parc de Mac contre les menaces de sécurité grandissantes et les logiciels malveillants connus, mais aussi pour remédier aux comportements dangereux, demandez un essai gratuit ou contactez votre revendeur Apple habituel.

jamf

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

Demander une version d'essai

Ou contactez votre revendeur habituel de matériel Apple.