macOS ET CYBERSÉCURITÉ

FAUSSES IDÉES ET CROYANCES COURANTES

Data Security Guide

ESET

EST-CE QUE LES APPAREILS APPLE ONT BESOIN D'UN LOGICIEL DE SÉCURITÉ ?

macOS est considéré par beaucoup comme un modèle à suivre pour la cybersécurité. Certains fans pourraient même considérer que leur ordinateur portant la marque à la pomme est immunisé contre les attaques des cybercriminels. Apple estime même que les mesures de sécurité intégrées à macOS sont suffisantes pour les menaces qui visent ses appareils. Il existe cependant des menaces pour la cybersécurité et la confidentialité spécifiques à macOS. Ainsi, même si vous pensez que les appareils macOS ne sont pas ouvertement menacés par des malwares, un logiciel de sécurité pour endpoints peut certainement apporter une valeur ajoutée, en particulier pour les appareils connectés à un réseau d'entreprise. Les chercheurs d'ESET examinent de plus près les cinq croyances courantes associées à la cybersécurité sur macOS.

L'attaque contre la chaîne d'approvisionnement de SolarWinds, les vulnérabilités de Microsoft Exchange et les innombrables ransomwares ne sont que quelques-unes des cyberattaques les plus marquantes qui ont fait la une des actualités au début de l'année 2021. Et de nouvelles menaces apparaissent presque quotidiennement. Elles ont tous une chose en commun : les problèmes de sécurité concernent généralement les systèmes Microsoft. En comparaison, le système macOS d'Apple n'apparaît que dans une poignée de cas chaque année.

Cela peut s'expliquer par le fait que Windows reste le système d'exploitation le plus utilisé sur les endpoints et les serveurs des entreprises. Néanmoins, Apple a augmenté lentement mais sûrement sa part de marché, et à mesure que le nombre d'appareils utilisant les systèmes d'exploitation d'Apple augmente, l'intérêt des cybercriminels monte en flèche également.

Dans les environnements professionnels, les Macs sont plébiscités parmi les métiers autour de la créativité tels que les graphistes et les réalisateurs de vidéos, ainsi que pour la publication assistée par ordinateur. Dans le cadre d'un usage personnel, les MacBooks et les iMacs offrent une interface intuitive et conviviale pour le système d'exploitation et les applications, et une conception haut de gamme.

Mais quel est le niveau de sécurité de macOS, et les croyances populaires concernant ses défenses sont-elles fondées ? Examinons certaines d'entre elles.

Croyance n° 1 :
« Il n'existe pas de malwares pour macOS »

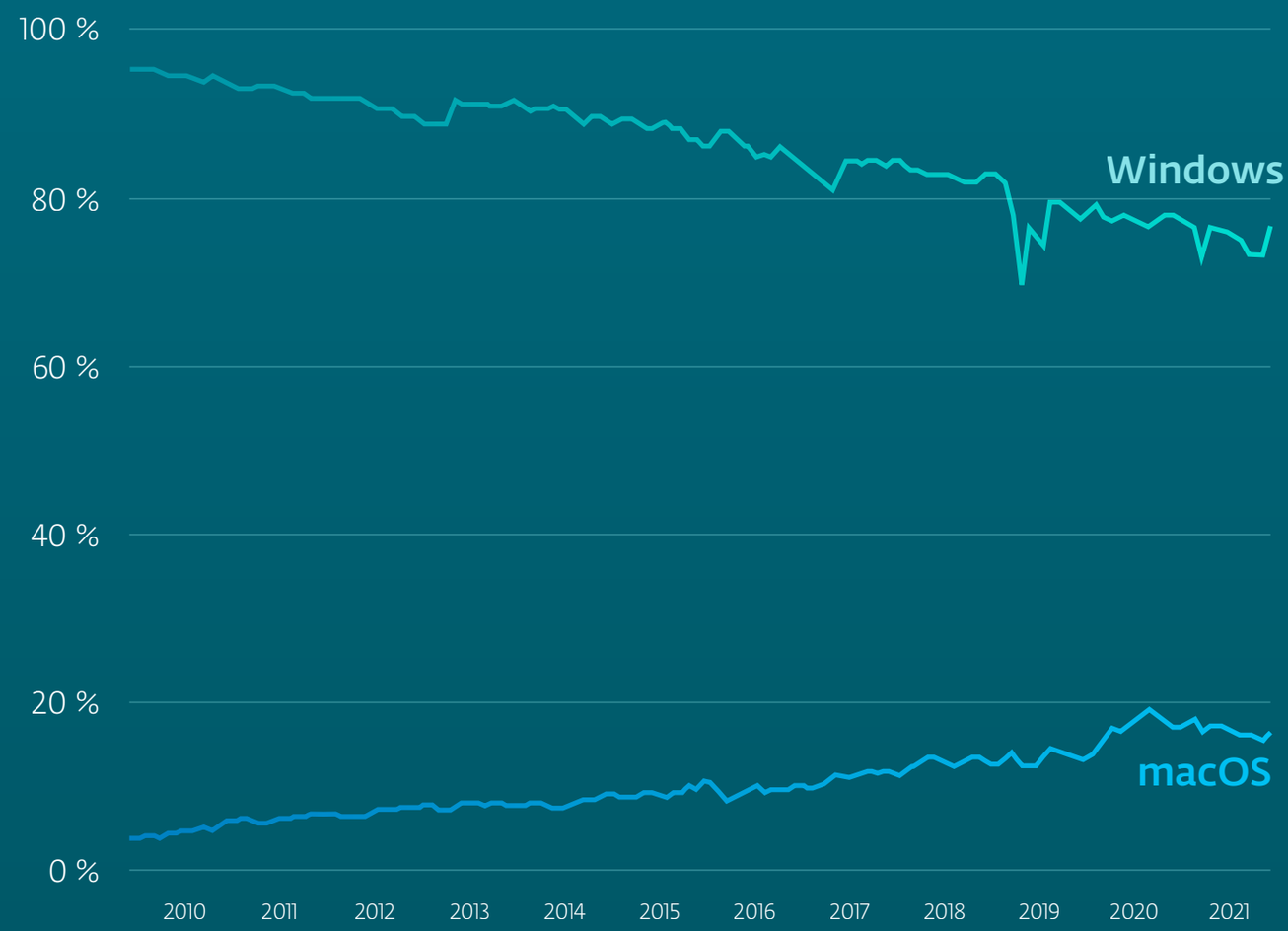
Croyance n° 2 :
« macOS est sécurisé dès la conception »

Croyance n° 3 :
« Ces quelques vulnérabilités ne veulent rien dire »

Croyance n° 4 :
« Les pirates ne s'intéressent pas à Apple »

Croyance n° 5 :
« Les Macs n'ont pas besoin d'une solution de sécurité »

Part de marché mondiale des systèmes d'exploitation pour ordinateurs de bureau



Source : StatCounter

Croyance n° 1 :

« Il n'existe pas de malwares pour macOS »

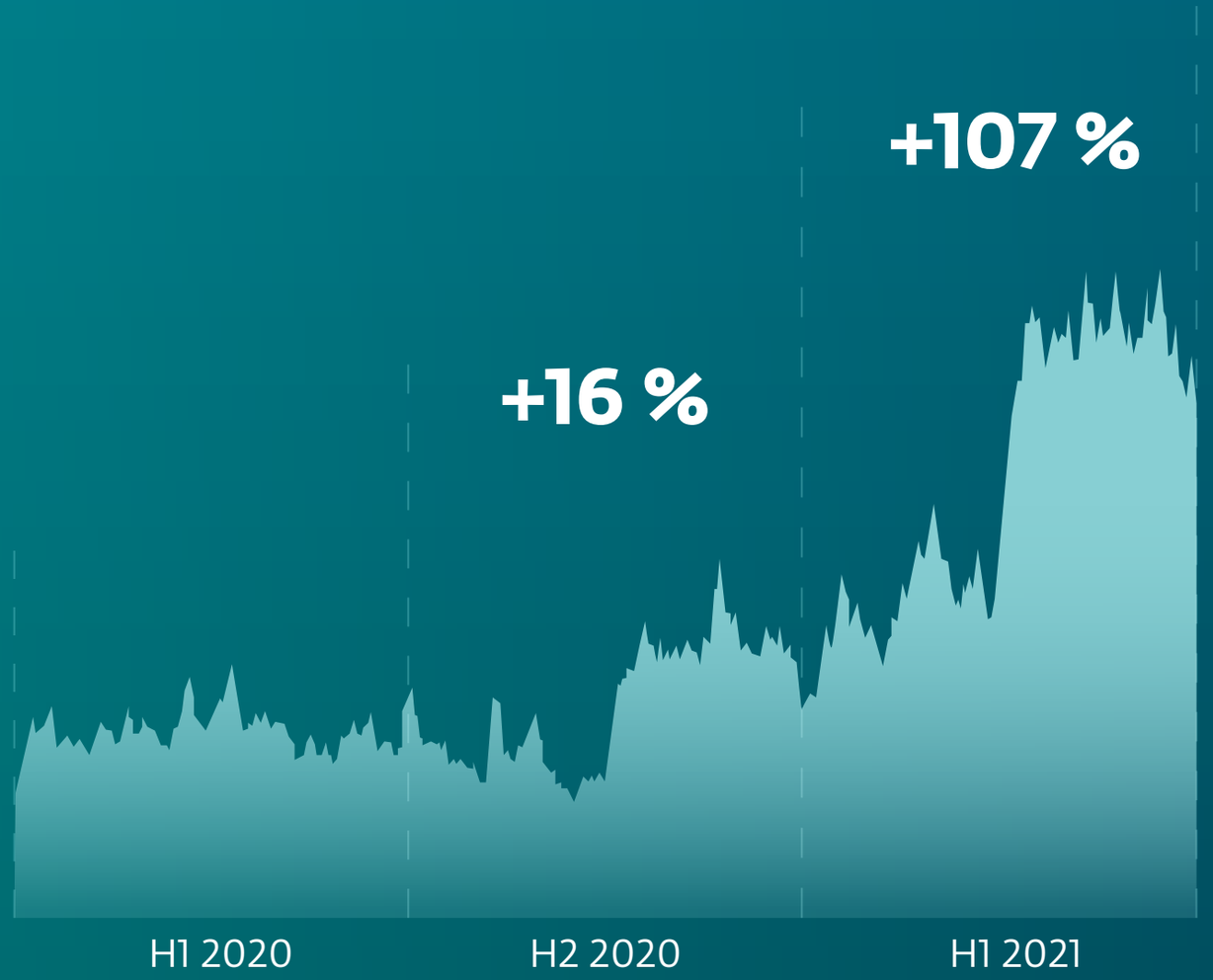
FAUX : Il existe des milliers de familles de malwares ciblant macOS. La télémétrie d'ESET montre des dizaines de milliers d'événements de détection de chevaux de Troie à l'échelle mondiale tout au long de l'année 2020, avec une augmentation significative de leur activité depuis le dernier trimestre de 2020.

En novembre 2020, l'entreprise de la Silicon Valley a présenté de nouveaux Mac équipés de puces Apple Silicon M1. Cette nouvelle semble avoir attiré l'attention des cybercriminels, qui ont diffusé de nouveaux malwares quelques semaines seulement après le lancement des puces. L'application GoSearch22 est une variante de la famille de logiciels publicitaires Pirrit, une menace courante pour les utilisateurs de Mac. Elle affiche généralement de faux coupons, des bandeaux et des pop-ups,

et fait la promotion de sites web douteux. Dans certains cas, elle collecte également des données de navigation et d'autres informations sensibles. La version ciblant les puces M1 s'installe sous forme d'extension Safari et un agent de lancement assure sa persistance.

La popularité croissante des cryptomonnaies s'est également reflétée dans la variété de menaces sur Mac. ESET a détecté une famille de malwares qui se fait passer pour un logiciel d'échange de cryptomonnaie pour macOS, mais qui vole les cookies du navigateur et les identifiants des portefeuilles de cryptomonnaie, et fait des captures de l'écran de la victime. Pour atteindre leur objectif, les acteurs malveillants associent une application de trading légitime à leur malware, rebaptisent les « nouvelles versions » en utilisant des noms tels que Cointrazer, Cupatrade, Licatrade et Trezarus, puis les diffusent via un faux site web imitant le site légitime.

Détection de chevaux de Troie sur macOS



Source : Télémétrie ESET

Croyance n° 2 :

« macOS est sécurisé dès la conception »

EN GRANDE PARTIE VRAI : Apple a fait beaucoup pour protéger macOS contre les cybermenaces actuelles en employant plusieurs couches de protection, notamment une protection de base s'appuyant sur des signatures contre les malwares, un pare-feu, le chiffrement intégré et une solution de sauvegarde. Pour améliorer encore la sécurité de certains de ses modèles les plus récents, Apple a même ajouté un scanner d'empreintes digitales (« Touch ID ») comme moyen d'authentification multifacteur.

macOS utilise également App Sandbox pour limiter les dommages potentiels causés par des logiciels compromis. Cette technologie limite l'accès des applications aux ressources sensibles et aux données de l'utilisateur au strict minimum nécessaire à l'accomplissement de sa tâche. Toutes les applications diffusées par l'App Store d'Apple sont soumises à un processus d'authentification qui permet de détecter toute activité malveillante. Avant qu'une application approuvée puisse être lancée, une autre technologie intégrée appelée Gatekeeper vérifie sa signature et s'assure qu'elle n'a pas été modifiée depuis sa signature par Apple ou par un « développeur identifié ».

eset

Malgré ces mécanismes de protection, il arrive de temps à autre qu'un malware passe entre les mailles du filet. Et même Apple fait parfois des erreurs en termes de sécurité :

#IAmRoot

Pour exploiter la vulnérabilité dite #IAmRoot, il suffisait à toute personne ayant un accès physique à un appareil d'utiliser « root » comme nom d'utilisateur, de laisser le champ du mot de passe vide dans tout processus d'autorisation et d'appuyer plusieurs fois sur la touche retour. Seule la première tentative était rejetée, mais en raison d'un bug, n'importe laquelle des tentatives suivantes accordait des droits élevés.

Spectre et Meltdown

Ces failles, qui touchent les processeurs Intel, AMD et ARM, permettent à un processus malveillant de lire toute la mémoire virtuelle sans requérir d'autorisation. L'espace mémoire protégé peut souvent stocker des informations sensibles, notamment des pilotes, des mots de passe et des clés cryptographiques. Des attaquants pourraient exploiter cette vulnérabilité pour contourner d'importantes mesures de sécurité telles que l'App Sandbox, et importer du code malveillant dans le système ciblé.

Problèmes initiaux de Big Sur

La transition vers macOS Big Sur n'a pas été aussi transparente que les fans d'Apple auraient pu l'espérer : de longs temps de téléchargement et des plantages causés par le serveur de signatures d'Apple qui est conçu pour détecter et bloquer les malwares. Ces ratés initiaux ont également entraîné des problèmes de confidentialité, car les appareils Apple envoyaient des données non chiffrées sur les logiciels ouverts, à quel moment et via quelle adresse IP, de sorte que toute personne ayant accès au réseau était en mesure de les récupérer. Apple affirme avoir résolu les problèmes signalés via des mises à jour.

Croyance n° 3 :

« Ces quelques vulnérabilités ne veulent rien dire »

FAUX : En décembre 2020, Apple a publié d'importants correctifs de sécurité pour macOS Mojave et Catalina. Ces mises à jour corrigent plus de 50 vulnérabilités, dont plusieurs sont classées comme critiques dans les CVE qui leur sont associées. Parmi les domaines concernés : des pilotes graphiques pour AMD et Intel, App Store, Audio, Bluetooth, CoreAudio, CoreText, FontParser, HomeKit, ImageIO, Kernel, Paramètres système et WLAN. Certaines de ces failles permettent à des attaquants d'exécuter un malware avec des droits élevés, ce qui rend ces vulnérabilités exceptionnellement dangereuses.

S'il s'agissait d'un incident isolé, cette croyance serait probablement fondée, mais les statistiques de la base de données des vulnérabilités maintenue par la communauté, VulDB.com, montrent que ce n'est pas le cas. Les dernières données suggèrent même que le nombre de vulnérabilités signalées pour les logiciels Apple dépasse celui des autres éditeurs populaires, notamment Oracle, Microsoft et Google.

Nombre de vulnérabilités signalées

Source : VulDB.com, 25 juin 2021

Croyance n° 4 :

« Les pirates ne s'intéressent pas à Apple »

PARTIELLEMENT VRAI : Pendant longtemps, macOS ne semblait pas être très lucratif pour les cybercriminels. Un nombre relativement faible d'utilisateurs et un système d'exploitation relativement sûr signifiaient beaucoup de travail pour un gain financier minimal. Néanmoins, avec la popularité croissante des appareils Apple, les préférences des pirates pourraient également commencer à changer.

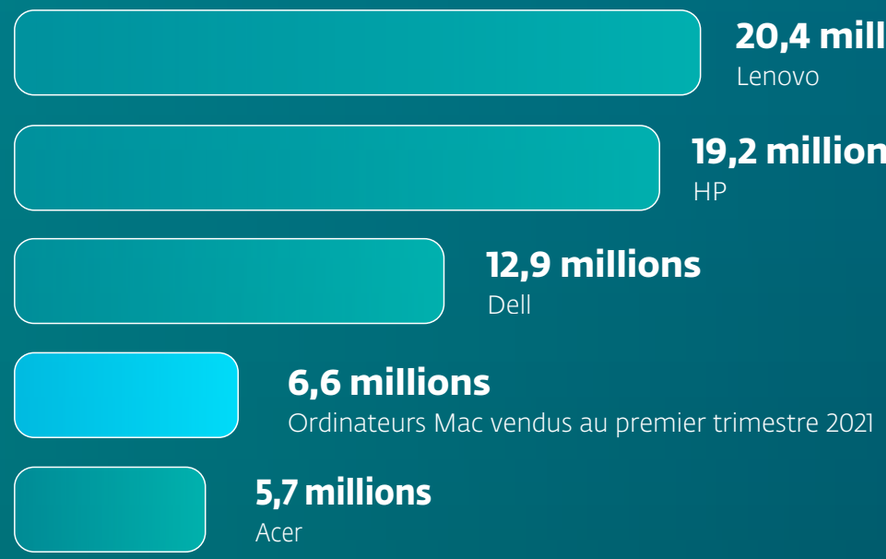
Une fois que vous avez acheté un iPhone ou un iPad et que vous en êtes tombé amoureux, il est également plus probable que vous vous tourniez vers des ordinateurs Mac plutôt que vers des PC Windows. C'est ce que semblent confirmer les chiffres de vente actuels publiés par Canalys, une société spécialisée dans l'analyse des marchés. Apple a vendu environ 6,6 millions d'appareils Mac au cours du premier trimestre de 2021. Par rapport au même trimestre de l'année précédente, cela représente

une croissance de 105 %, soit une performance nettement supérieure à la moyenne du marché (55 %). La part de marché mondiale d'Apple a également augmenté, passant de 6 à 8 % d'une année à l'autre au premier trimestre 2021.

Pourtant, ce n'est pas seulement le nombre croissant d'adeptes du Mac qui rend ce système d'exploitation attrayant pour les cybercriminels. Selon une enquête américaine réalisée par RJI Online, les possesseurs d'appareils Apple semblent gagner plus d'argent que les utilisateurs d'Android. Pour les acteurs malveillants, cela signifie une cible plus juteuse et financièrement beaucoup plus attrayante.

Il n'est donc pas étonnant qu'il y ait un nombre croissant de failles de sécurité Apple qui soient activement recherchées, exploitées et rendues publiques seulement plus tard. Grâce à ces vulnérabilités, les cybercriminels n'ont pas à attendre que les utilisateurs commettent une erreur qui les laisserait entrer, et peuvent trouver d'autres moyens d'accéder aux précieuses données des victimes ou de déployer des ransomwares.

Ventes d'Apple par rapport aux autres marques de PC



105 %

Croissance annuelle, par rapport à la moyenne du marché de 55 %

6 → 8 %

Augmentation de la part de marché du 1er trimestre 2020 au 1er trimestre 2021

Source : Analyse PC de Canalys, avril 2021

Croyance n° 5 :

« Les Macs n'ont pas besoin d'une solution de sécurité »

PARTIELLEMENT VRAI : De nombreux utilisateurs de Mac ne savent pas que leur ordinateur est déjà doté d'une solution de sécurité intégrée, appelée XProtect, qui est constamment à l'affût des malwares. Contrairement à de nombreuses solutions tierces, cette technologie utilise uniquement la détection par signature. Pour identifier les malwares, le système utilise des signatures YARA régulièrement mises à jour qui reposent sur la surveillance du paysage des menaces par Apple. Pour veiller à ce que les utilisateurs de Mac soient protégés contre les toutes dernières menaces dès que possible, XProtect met à jour ces signatures indépendamment des autres mises à jour du système.

Malgré toutes les mesures de protection, des malwares peuvent toujours se frayer un chemin sur les Mac. Pour ces cas, Apple propose un autre outil intégré appelé Malware Removal Tool (MRT). Ce moteur est conçu à des fins de remédiation et supprime les malwares dès qu'il reçoit les dernières mises à jour. Il continue également de rechercher des infections après le redémarrage et la connexion.

En général, XProtect et MRT protègent efficacement les utilisateurs de Mac. Cependant, si l'appareil est connecté à un réseau d'entreprise ou personnel avec des PC Windows, il peut servir de tremplin pour infecter le réseau. Si les Macs ne sont pas protégés en conséquence, un malware peut les utiliser pour contourner le pare-feu réseau ou la sandbox, et s'introduire clandestinement dans un environnement autrement sûr.

Pour éviter ce scénario dans les environnements mixtes, une solution antimalwares multicouche qui protège à la fois les ordinateurs Mac et Windows contre les dernières cybermenaces est nécessaire. Pour les entreprises qui suivent le modèle de sécurité Zero Trust, elle est même indispensable.

CONCLUSION

Le système macOS fait actuellement partie des systèmes d'exploitation les plus sûrs du marché. Indépendamment de ses lacunes de sécurité décrites ici, Apple propose une très bonne architecture de sécurité qui est constamment développée et actualisée. Les problèmes causés par Spectre et Meltdown devraient être résolus par l'emploi des nouveaux processeurs « Apple Silicon », qui devraient également permettre à Apple de contrôler beaucoup mieux ses produits. Les prochains systèmes d'exploitation devraient être adaptés de manière optimale aux puces d'Apple, ce qui pourra contribuer à la sécurité des appareils. Cela étant dit, même macOS peut devenir une cible pour les cybercriminels, et certains pourraient même essayer de l'utiliser comme une porte d'entrée dans des environnements autrement sûrs.

Par conséquent, une solution de sécurité multicouche fiable, capable de protéger les Mac ainsi que les autres systèmes d'exploitation, est nécessaire pour que les utilisateurs et leurs appareils restent à l'abri des menaces.

Pour commencer à protéger vos appareils macOS dès maintenant, et discuter de la façon dont les solutions ESET peuvent vous être utiles, veuillez nous contacter sur clientsfinaux@eset-nod32.fr.

Data Security Guide

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique pour protéger le patrimoine numérique des entreprises, les infrastructures critiques et les consommateurs du monde entier contre des cybermenaces. Nous protégeons les terminaux fixes et mobiles, les outils collaboratifs, et assurons la détection et le traitement des incidents. Établis dans le monde entier, nos centres de R&D récoltent et analysent les cybermenaces pour protéger nos clients et notre monde numérique.