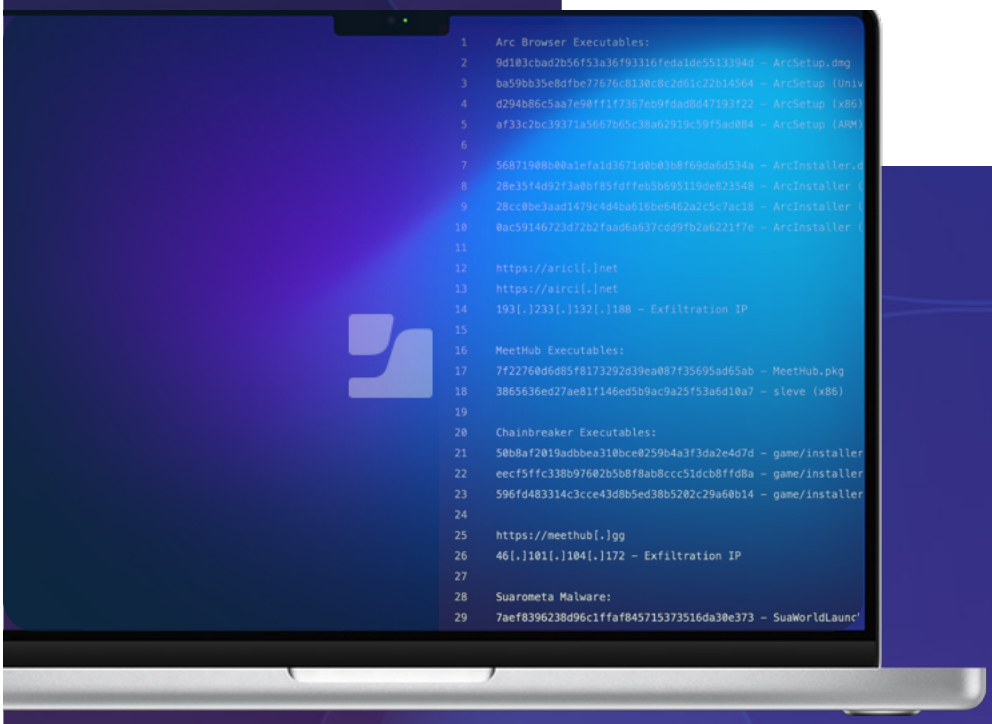
jamf

Security 360 :
Rapport annuel sur les tendances de sécurité

Mac



Avant-propos

Chez Jamf, nous adorons le Mac. C'est la première machine pour laquelle nous avons développé des logiciels, et nous sommes toujours nombreux à avoir une passion pour elle. (Nous sommes **contributeur officiel au Projet de conformité sécurité macOS**). Tout au long de notre histoire, nous avons vu Mac prendre une place **de plus en plus importante dans l'environnement de travail.** Ce qui était au départ une machine destinée aux créatifs et aux cadres trouve aujourd'hui sa place dans les opérations quotidiennes des ingénieurs et de bien d'autres rôles. Mais son intégration croissante au milieu du travail en fait une cible de choix pour les acteurs malveillants.

Le paysage des menaces Mac est plus diversifié que jamais, et les pirates font preuve d'une grande créativité pour compromettre ces machines. Notre mission est d'« aider les organisations à réussir avec Apple ». C'est pourquoi nous nous intéressons au paysage des menaces qui pèsent sur les Mac, pour mieux servir nos clients et la communauté Apple dans son ensemble.

– **Jaron Bradley,**
directeur, Jamf Threat Labs

Introduction

Le rapport « Security 360 » de Jamf est le fruit de l'analyse d'incidents réels vécus par nos clients, de recherches sur les menaces et de l'étude d'événements survenus au cours de l'année écoulée. Ce rapport explore principalement le paysage Mac afin de mettre en lumière les risques auxquels les organisations sont confrontées.

Nous proposons une évaluation des différents vecteurs d'attaque (logiciels malveillants, vulnérabilités et ingénierie sociale) qui sont activement utilisés pour tromper les utilisateurs, compromettre les appareils et infiltrer les organisations. L'analyse porte en particulier sur les vulnérabilités des appareils, les menaces réseau et les nouveaux malwares.

Outre l'analyse des tendances dans le domaine des menaces, le rapport apporte le point de vue du CISO de Jamf, qui nous éclaire sur les priorités des responsables de la sécurité chargés de protéger les Mac, leurs utilisateurs, les applications et le réseau.

Méthodologie de recherche

Pour comprendre et quantifier l'impact réel des tendances de sécurité identifiées dans ce rapport, nous avons étudié un groupe d'échantillons composé de 1,4 million d'appareils protégés par Jamf. Nous avons mené notre analyse au cours du premier trimestre 2025, en revisitant les 12 mois précédents et en couvrant 90 pays.

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.

Objectif de la recherche

Dans cette analyse, notre intention est de permettre aux organisations et aux utilisateurs de comprendre l'évolution des tendances actuelles de la cybersécurité, mais également de mettre en avant les mesures que peuvent prendre les organisations et les utilisateurs pour atténuer les risques. Le rapport présente également un aperçu des recherches les plus importantes menées par Jamf Threat Labs, et notamment des découvertes de logiciels malveillants et de vulnérabilités.

Tout le monde peut agir à différents niveaux pour améliorer la sécurité de son Mac. Par exemple, en ne téléchargeant des logiciels qu'à partir de sources fiables. Mais les organisations peuvent également mettre en œuvre bien d'autres bonnes pratiques :

- Mises à jour continues et rapides des systèmes d'exploitation
- Éducation et formation des utilisateurs
- Vérification des applications
- Authentification multifacteur
- Cadres de sécurité Zero Trust
- Règles d'utilisation acceptable pour les données de l'entreprise
- Mise en œuvre des workflows optimisés Apple dans tous les cas d'utilisation

Si certaines de ces pratiques sont incontournables dans toutes les organisations, d'autres exigences de sécurité des appareils sont spécifiques à chaque cas. Par exemple, les organisations d'un secteur réglementé devront peut-être respecter des critères ou des cadres industriels, comme les critères du CIS ou la loi HIPAA.

Cette année, nous articulons notre analyse selon trois catégories de risques qui, selon nous, sont prioritaires pour les organisations du monde entier :

I. Risque lié aux applications et logiciels malveillants

II. Gestion des vulnérabilités

III. Ingénierie sociale

Nous avons également rédigé un rapport Security 360 axé sur les **appareils mobiles**, que vous pouvez consulter **ici**.

Une grande partie des analyses contenues dans ce rapport s'appuie sur les renseignements sur les menaces de Jamf. Cette vaste collection d'informations provient de recherches originales sur les menaces, de mesures d'utilisation réelles, d'analyses des actualités et de flux de données. Les renseignements sur les menaces de Jamf proviennent des recherches menées par les membres des équipes du Jamf Threat Labs et de Data Science, qui surveillent les appareils, les applications et le trafic réseau pour détecter les risques, les menaces et les vulnérabilités zero-day.

Principales tendances pour le Mac en entreprise

Les logiciels malveillants introduisent des risques, même sur les plateformes sécurisées

Apple élabore ses **plateformes en faisant de la sécurité une priorité**. Cette philosophie se retrouve non seulement dans les plateformes elles-mêmes, mais aussi dans la manière dont Apple communique la sécurité à ses utilisateurs. En témoigne le **site Sécurité de la plateforme Apple**, dont une page informe les utilisateurs Apple sur la protection contre les logiciels malveillants ciblant macOS. Les différentes technologies d'Apple (App Store, XProtect et Gatekeeper, notamment) assurent une protection contre les malveillances à différents stades du cycle de vie des applications.

Pour les Mac en entreprise, la sécurité est un véritable exercice d'équilibriste : il faut fournir aux utilisateurs les applications dont ils ont besoin pour travailler, tout en empêchant l'accès à celles qui peuvent introduire des risques. Les applications Mac prennent de nombreuses formes : applications Mac natives, applications web et applications hybrides, toutes créées et conçues par des développeurs pour servir une variété de cas d'usage. Mais aujourd'hui, **une grande part des applications professionnelles courantes pour Mac** ne provient pas du Mac App Store : elles sont directement conditionnées par le développeur. Dernier point, les utilisateurs peuvent télécharger des applications à partir de n'importe quel site.

Il suffit d'une vulnérabilité pour que des pirates obtiennent un accès à l'ensemble du système

C'est une réalité : des vulnérabilités apparaissent dans les logiciels (OS et applications) que nous utilisons quotidiennement.

L'Institut national des standards et de la technologie (NIST) est très clair : « Dans un logiciel typique, les erreurs et les vulnérabilités sont présentes à une fréquence estimée à 25 erreurs environ pour 1000 lignes de code. » Les vulnérabilités et expositions communes (CVE), publiées dans la base de données nationale sur les vulnérabilités (NVD), communiquent au public :

- Des explications sur les CVE
- Le produit ou le fournisseur touché
- Une description des menaces

Les dommages peuvent survenir entre le moment où une vulnérabilité est découverte et celui où elle est corrigée. Lorsqu'un correctif est publié, il faut encore qu'il soit installé sur les appareils concernés. Munies d'outils de sécurité qui signalent les vulnérabilités présentes et quelles sont les plus critiques, les équipes informatiques et de sécurité sont en mesure de hiérarchiser l'application des correctifs et d'améliorer leurs processus.

L'ingénierie sociale, une menace toujours concrète pour les utilisateurs

L'ingénierie sociale, phishing en tête, reste l'une des techniques d'attaque les plus répandues des pirates, et elle exerce toujours une forte influence sur le paysage des menaces. En septembre 2024, **Apple a publié un article de blog** pour donner des conseils aux utilisateurs et les aider à « éviter les escroqueries et savoir réagir face à des e-mails, des appels téléphoniques ou d'autres messages suspects ». Les pirates redoublent de créativité dans leurs techniques et se font passer pour des recruteurs, des membres de la famille, des marques de confiance, etc. Quel que soit le niveau sécurité d'une plateforme ou d'un système d'exploitation, les techniques d'ingénierie sociale sont conçues pour accéder aux données de l'entreprise en passant par l'élément le moins sécurisé d'un appareil : son utilisateur.

1re partie : Les logiciels malveillants ciblant Mac

Dans ce rapport, nous faisons le point sur les logiciels malveillants qui visent les Mac, les types de malware que nous avons observés, l'impact qu'ils exercent sur les organisations et la fréquence de leur apparition. La présence croissante du Mac sur le lieu de travail, utilisé pour accéder à des applications stratégiques, explique que les utilisateurs de toute l'organisation puissent être ciblés.

La défense d'Apple contre les logiciels malveillants est structurée en trois étapes :

1. **Empêcher le lancement ou de l'exécution des logiciels malveillants**
2. **Bloquer l'exécution des logiciels malveillants sur les systèmes des clients**
3. **Remédier aux logiciels malveillants qui se sont exécutés**

Les technologies d'Apple – App Store, GateKeeper, XProtect et Notarization – offrent aux utilisateurs des moyens natifs d'atténuer les menaces. XProtect, par exemple, est un antivirus intégré. En cas de découverte d'un logiciel malveillant, Apple peut réagir de plusieurs façons, notamment en révoquant l'ID d'un développeur.

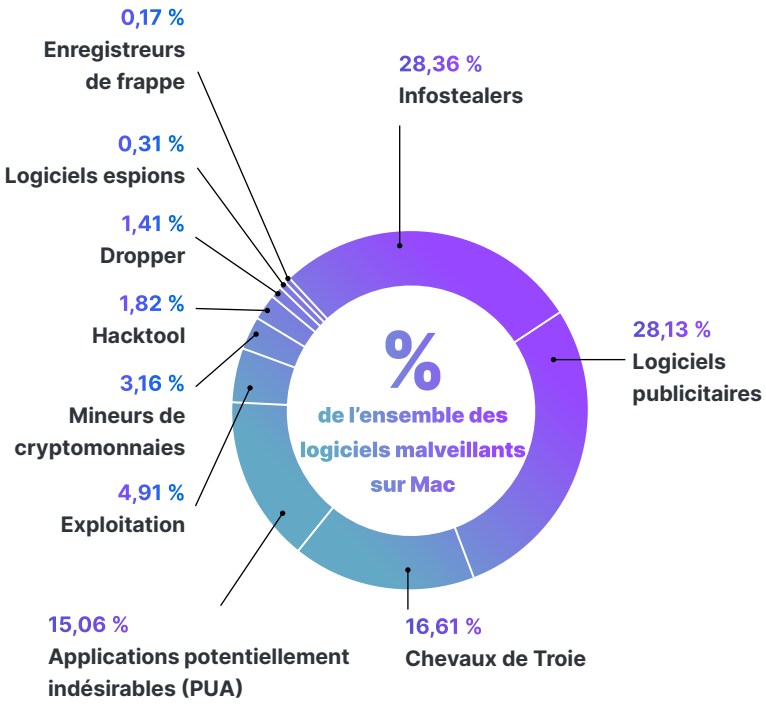
Malgré ses solides mécanismes de sécurité intégrés, macOS n'est pas à l'abri des logiciels malveillants. **En mars de cette année**, les équipes Jamf Threat Labs et Data Science ont collaboré à un article pour discuter du mythe de l'absence de logiciels malveillants sur Mac. Elles y comparent les nouveaux logiciels malveillants aux malwares connus pour mieux les comprendre et mettent en évidence les vecteurs des logiciels malveillants sur macOS avec Titan, un outil de visualisation 3D développé par Jamf Threat Labs. Titan apporte du contexte et identifie les échantillons de logiciels malveillants connexes. Les familles de logiciels malveillants découvertes illustrent « le nombre toujours plus grand de nouveaux malwares sur mesure » pour macOS. Qu'est-ce que cela signifie ? Les logiciels malveillants Mac existent, on peut les classer en plusieurs familles et ils sont de plus en plus utilisés par les pirates informatiques.

Cette année, Jamf Threat Labs a découvert un logiciel malveillant possiblement lié à la République populaire démocratique de Corée (RPDC) **et intégré dans une application basée sur Flutter**. Flutter est couramment employé pour la prise en charge multiplateforme, mais cette attaque est remarquable pour une raison bien particulière : c'est la première fois que l'équipe Jamf Threat Labs voit ce cadre utilisé pour cibler des appareils macOS. L'équipe dissèque le logiciel malveillant ainsi que ses variantes en Python et Golang. Selon elle, « ce logiciel malveillant est probablement un test en vue d'attaques plus poussées ». Il faut également souligner que Flutter obscurcit par inadvertance le code écrit par les utilisateurs du cadre.

Familles de logiciels malveillants Mac

Voici l'inventaire complet des nouvelles instances de logiciels malveillants Mac étudiées en 2024, sur la base de nos observations :

Que nous apprennent ces données ? Si on les compare avec le rapport de l'année dernière, on peut dégager certaines constantes : les logiciels publicitaires, les chevaux de Troie, les PUA (applications potentiellement indésirables) et les exploitations (applications connues pour profiter d'un exploit) restent en tête du classement des logiciels malveillants. L'année dernière, les chevaux de Troie représentaient le plus grand nombre de familles (17 %). Ils sont en léger recul cette année (16,6 %), et la première place revient aux infostealers Ceux-ci ont en effet connu une augmentation globale de 28,08 % de leur part.



La présence des infostealers est conforme aux recherches menées par Jamf Threat Labs au cours de l'année écoulée : les environnements macOS sont constamment attaqués par ce type de logiciel malveillant. Soulignons un point intéressant dans ces tactiques : les pirates n'utilisent pas seulement des infostealers pour accéder aux données qu'ils veulent, ils y ajoutent également une autre stratégie déjà mentionnée dans ce rapport, l'ingénierie sociale. Ils cherchent donc à combiner différents principes pour tromper leurs victimes. Pour les employés et les organisations des secteurs particulièrement visés, comme celui des cryptomonnaies, il est indispensable de faire preuve de vigilance en misant à la fois sur la formation et les outils de sécurité. Les attaques ne sont pas seulement le fruit du hasard, elles sont le produit d'un plan élaboré.

Enquête sur l'utilisation de PyInstallers pour le déploiement d'infostealers sur macOS

En avril 2025, Jamf Threat Labs a découvert de nouveaux échantillons d'infostealer macOS jusque-là non détectés, qui encapsulent du code Python dans des exécutables Mach-O à l'aide de PyInstaller. (Jamf Threat Labs a découvert trois stealers non détectés sur VirusTotal).

PyInstaller est un outil légitime et open source qui permet aux développeurs d'empaqueter des scripts Python dans des binaires autonomes. Les pirates emploient aujourd'hui cette même technique pour distribuer des charges utiles malveillantes qui s'exécutent sans problème sur macOS. L'équipe a examiné plusieurs fonctions clés pour révéler la véritable nature du logiciel malveillant : un infostealer. Voici les fonctions en question :

- Tente de collecter des identifiants utilisateur par le biais de boîtes de dialogue trompeuses,
- Exécute des charges utiles applescript arbitraires à partir d'un serveur d'attaque,
- Extrait les identifiants sauvegardés et les informations sensibles directement du trousseau de clés de macOS,
- Scanne le système de fichiers à la recherche de portefeuilles de cryptomonnaies connus pour exfiltrer les clés privées et voler des cryptoactifs.

Les infostealers sont de plus en plus fréquents dans le paysage des menaces macOS, et les pirates cherchent inlassablement de nouveaux moyens de les distribuer. Fort heureusement, les organisations peuvent prendre des mesures concrètes pour se protéger contre ce type de malware. Par exemple :

- Limiter l'exécution des logiciels aux seules applications signées par Apple et par des développeurs identifiés,
- Apposer une marque sur les invites osascript utilisées pour les processus informatiques légitimes et former le personnel à vérifier la marque avant de saisir des identifiants.

Les logiciels malveillants à surveiller

Poolrat

Tristement célèbre pour son implication dans la compromission de la chaîne d'approvisionnement 3CX, la porte dérobée macOS Poolrat autorise les pirates à collecter des données système cruciales et à exécuter des commandes et des opérations sur les fichiers simultanément. Une version allégée de Poolrat, baptisée Pondrat, a récemment été découverte.

Pondrat

Pondrat, une porte dérobée qui présente des similitudes avec AppleJeus et Poolrat, a été distribuée par l'intermédiaire de paquets PyPi malveillants. Dès son installation, Pondrat établit des connexions avec des serveurs de commande et de contrôle (C2) pour télécharger des fichiers, interrompre les opérations pendant une durée prédéterminée et exécuter des commandes arbitraires.

NotLockBit

Ce ransomware basé sur Golang prend l'apparence d'une variante du tristement célèbre ransomware LockBit. Depuis son échantillon initial, le ransomware utilise une clé publique intégrée pour énumérer et chiffrer une liste d'extensions codées en dur. Les variantes les plus récentes de NotLockBit exfiltrent des données vers un bucket S3 contrôlé par les pirates et utilisent osascript pour modifier le fond d'écran du bureau (LockBit 2.0). NotLockBit ferait l'objet d'un développement actif.

ThiefBucket

Thiefbucket, une famille de logiciels malveillants liée au Lazarus Group de Corée du Nord, cible ses victimes par le biais de campagnes d'ingénierie sociale sophistiquées. Il prend la forme d'une charge utile de deuxième stade, délivrée sous l'apparence d'un défi de code. La porte dérobée présente plusieurs capacités, et en particulier une fonctionnalité d'infostealer automatisé. Mais elle en possède encore bien d'autres : mécanismes de persistance, interruption de processus, suppression de fichiers, téléchargement/chargement de fichiers, auto-effacement, exécution de commandes shell, recherche rapide de fichiers via Spotlight, communication avec des serveurs de commande et de contrôle.

HZ Rat

HZ Rat, une porte dérobée pour macOS, ciblait initialement les utilisateurs de Windows. Depuis, elle a évolué pour cibler les utilisateurs de macOS en prenant l'apparence d'installeurs de logiciels légitimes. Une fois installée, HZ Rat établit des connexions avec des serveurs de commande et de contrôle (C2) qui permettent aux pirates d'exécuter des commandes, de voler des fichiers et d'extraire des informations sensibles – noms d'utilisateur, e-mails, numéros de téléphone et autres données personnelles provenant de WeChat et DingTalk.

BansheeStealer

BansheeStealer, 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. Comme bien d'autres infostealers, Banshee 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. Banshee utilise diverses techniques d'évasion, notamment des mesures anti-VM et anti-débogage pour échapper à l'analyse, et détecte les systèmes en langue russe.

InvisibleFerret

InvisibleFerret est un cheval de Troie basé sur Python qui a été utilisé par des logiciels malveillants intégrés à contrefaçons d'applications. D'après nos observations, il a notamment été distribué par BeaverTail InfoStealer (attribué par certains à la Corée du Nord) comme implant de stade 2. Le script Python malveillant est multiplateforme. Il permet à un pirate d'effectuer un large éventail d'opérations : reconnaissance, exfiltration de données, extraction du presse-papier et exécution de commandes à distance. Il est également capable d'installer le logiciel AnyDesk pour mettre en place une commande à distance.

BeaverTail

BeaverTail est un infostealer déguisé en application légitime et distribué aux victimes via des campagnes d'ingénierie sociale. À l'instar d'autres infostealers, il extrait de précieuses informations du trousseau de la victime, des cookies du navigateur, des portefeuilles de cryptomonnaies, etc. et les transfère sur un serveur contrôlé par le pirate. Il peut encore exécuter des charges utiles à distance sur le système de la victime, comme la porte dérobée InvisibleFerret. Certains analystes le relient à la Corée du Nord.

PoseidonStealer

Poseidon, un concurrent d'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. Comme Atomic, Poseidon 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, ce logiciel malveillant a également été promu par le biais de Google Ads.

Kuiper

Kuiper est un ransomware-as-a-Service (RaaS) développé en Go, promu sur des forums clandestins par un utilisateur nommé Robinhood. Il combine RSA, ChaCha20 (pour les fichiers de moins de 600 Mo) et AES (pour les fichiers de plus de 600 Mo) pour chiffrer les fichiers. Si la plupart des fonctionnalités de ce malware sont axées sur Windows, la variante macOS génère une clé aléatoire et un vecteur d'initialisation aléatoire (IV) en utilisant « /dev/urandom », décode une note de rançon, chiffre la cible de manière récursive (en ajoutant l'extension « .kuiper »), efface la clé et l'IV de la mémoire, et redémarre le système.

Logiciels malveillants observés sur Mac

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

Nom de famille	Catégorie	Pourcentage
Genieo	Logiciels publicitaires	**13,63**
Imobie	PUA	**10.96**
Multiverze	Logiciels publicitaires	**9.44**
Mackeeper	PUA	**7.19**
Tnt	PUA	**6.07**
jailbreak	PUA	**5.74**
Ccleanmac	Logiciels publicitaires	**4.33**
Puagent	Troyens	**3.07**
Macinformer	PUA	**2.33**
Pirrit	Logiciels publicitaires	**2.33**

Ces chiffres sont clairs : si de nombreux types de logiciels malveillants, infostealers en tête, se multiplient à grande vitesse, les logiciels publicitaires et les applications potentiellement indésirables (PUA) restent les logiciels les plus fréquemment téléchargés et installés par les utilisateurs. Cette tendance s'observe d'ailleurs sur toutes les plateformes d'OS, ce qui s'explique par la portée considérable des logiciels publicitaires, contrairement aux infostealers, bien plus ciblés.

Jamf Threat Labs a publié un article de blog sur les **infostealers ciblant les acteurs du secteur des cryptoactifs**. L'objectif des pirates ? Récolter les identifiants et les données de portefeuilles de cryptomonnaies. L'équipe a repéré deux attaques visant à introduire des infostealers dans le système des victimes :

1. Par le biais d'annonces Google sponsorisées : une annonce Google était présentée aux utilisateurs recherchant « Arc Browser », et cette annonce les redirigeait vers un site malveillant.
2. Via des réunions virtuelles : les pirates prétendent vouloir discuter d'une opportunité ou d'une offre d'emploi, et suggèrent pour cela d'utiliser Meethub.

Dans deux cas, les utilisateurs étaient invités à télécharger l'application en contournant Gatekeeper et à saisir leur mot de passe de connexion à macOS.

Les familles de logiciels malveillants que nous avons étudiées et les exemples que nous présentent soulignent à quel point il est crucial de respecter un certain nombre de principes de sécurité fondamentaux :

- Acquérir les applications auprès de sources légitimes
- Appliquer un processus de vérification (en faisant appel à un tiers de confiance comme le Mac App Store ou à un fournisseur de gestion des appareils)
- Utiliser des logiciels de sécurité à jour

Le point de vue du RSSI

- **Mettez en place une solution EDR spécialement conçue pour le Mac :** Bien souvent, les logiciels sont d'abord pensés pour Windows et traitent les appareils Apple comme une plateforme secondaire dans l'entreprise. Cette époque est révolue depuis longtemps, surtout en ce qui concerne la sécurité. Il faut rechercher des produits de sécurité qui sont développés dès le départ pour les produits Apple pour s'adapter à l'évolution du paysage des menaces.
- **Mettez en œuvre une solution MDM robuste :** La gestion des appareils est indispensable pour les sécuriser. Compte tenu de la liberté dont jouissent les utilisateurs et des accès qu'ils peuvent avoir, il est primordial de disposer d'un cadre robuste pour gérer les appareils et les utilisateurs. C'est comme cela que vous pourrez arrêter dans l'œuf les épidémies de logiciels malveillants potentielles.
- **Établissez des stratégies de communication solides :** Pensez aussi bien à la collaboration entre les équipes de sécurité et d'informatique qu'à la réputation de la marque en matière de sécurité, aux programmes de formation, à la sensibilisation des utilisateurs finaux et aux notes de la direction. En communiquant efficacement sur votre programme de sécurité, les outils que vous utilisez et vos stratégies actuelles, vous aiderez tous les acteurs à s'aligner et à se concentrer sur un objectif commun.

Gestion des vulnérabilités

Les vulnérabilités se suivent, mais ne se ressemblent pas. Leur degré de gravité varie et c'est pourquoi on attribue un score à la plupart d'entre elles. **Apple** fournit une liste des failles de sécurité corrigées qui affectent macOS, ainsi que la version du système d'exploitation qui corrige chaque vulnérabilité. En 2024, par exemple, Apple a publié macOS 15.1.1 en réponse aux **CVE-2024-44308** et **CVE-2024-44309**, qui pouvaient permettre à un contenu web malveillant de quitter la sandbox de contenu web. Cette CVE affichait un score de gravité élevé. Mais Apple publie également des mises à jour de sécurité pour les CVE dont le score est faible. Qu'est-ce que cela signifie ? Il est essentiel d'établir des priorités. Lorsque les équipes informatiques et de sécurité ont une vue d'ensemble des vulnérabilités présentes sur leurs appareils, leurs systèmes et leurs applications, elles peuvent s'attaquer aux problèmes les plus urgents.

Apple a mis en place un système spécial de mises à jour de sécurité. Appelées Rapid Security Responses, ces mises à jour apportent d'**importantes améliorations de sécurité** entre les changements de version. Quel est l'intérêt de ces correctifs ? Ce sont des mises à jour légères, qui peuvent être automatiquement appliquées sans interrompre les systèmes internes. Par exemple, entre juin 2024 et avril 2025, Apple a documenté **20 mises à jour de sécurité** corrigeant des CVE associées à des versions majeures et mineures de macOS.

Exploration d'une vulnérabilité en environnement réel Contournement du cadre Transparence, consentement et contrôle (TCC)

Dans les systèmes d'exploitation Apple, le cadre Transparence, consentement et contrôle (TCC) invite les utilisateurs à accepter ou refuser les demandes d'accès à des données sensibles – microphone, webcam, intégralité du disque – émanant des applications. Une vulnérabilité de contournement du TCC permet de désactiver ce contrôle et d'autoriser une application à accéder à des informations privées à l'insu de l'utilisateur. Autrement dit, des pirates peuvent obtenir un accès non autorisé aux fichiers et dossiers de l'utilisateur, à ses données médicales, à son micro ou à sa caméra, entre autres, sans qu'il en soit averti.

Jamf Threat Labs a découvert la **CVE-2024-44131, une vulnérabilité de contournement du TCC** affectant le fournisseur de fichiers sur les appareils Mac. Apple a rapidement réagi à cette découverte en proposant un correctif pour macOS 15. Les CVE telles que CVE-2024-4413 soulignent à quel point il est nécessaire de s'armer d'outils capables de détecter et de bloquer les comportements inattendus. En prenant des mesures proactives pour superviser le comportement des applications et prévenir les accès non autorisés aux données, les organisations auront une longueur d'avance et resteront protégées en attendant la publication d'un correctif.

Intéressons-nous à quelques vulnérabilités notables traitées dans des mises à jour récentes d'Apple (ce rapport a été rédigé en avril 2025) :

Correction de la CVE par Apple	Date	Score de la vulnérabilité	Impact
macOS Sequoia 15.4.1	Avril 2025	CVE-2025-31200 Score CVSS : 7,5 | Gravité : élevée	CoreAudio
macOS Sequoia 15.4	Mars 2025	CVE-2025-24234 Score CVSS : 7.8 | Gravité : élevée	AccountPolicy
macOS Sequoia 15.4	Mars 2025	CVE-2025-24180 Score CVSS : 8.1 | Gravité : élevée	Services d'authentification
macOS Sequoia 15.3	Janvier 2025	CVE-2025-24085 Score CVSS : 7.8 | Gravité : élevée	CoreMedia

Comme nous l'avons dit plus haut, les vulnérabilités sont inévitables dans le développement logiciel (on compte environ 25 erreurs pour 1 000 lignes de code). Pour les professionnels de la sécurité, l'essentiel est de pouvoir visualiser ces vulnérabilités pour y remédier et préserver la sécurité des données. Il n'est pas toujours possible de tenir les systèmes d'exploitation à jour (parce qu'il faut tester des applications ou des agents, par exemple), mais les organisations doivent rester informées et protégées.

Les vulnérabilités ne se limitent pas au système d'exploitation. Fin novembre 2024, l'Agence de cybersécurité a publié **un rapport sur les vulnérabilités les plus couramment exploitées en 2023** (il s'agit de l'édition la plus récente). Le rapport étudie en détail les 15 CVE les plus préoccupantes, en précisant les possibilités qu'elles offrent aux acteurs malveillants. Les vulnérabilités sont présentes dans tous les systèmes d'exploitation, mais aussi dans les applications utilisées au quotidien par les travailleurs et les étudiants. Comme le mentionne le rapport, « les pirates ont exploité davantage de vulnérabilités zero-day pour compromettre les réseaux d'entreprise en 2023 qu'en 2022, ce qui leur a permis de mener des opérations contre des cibles hautement prioritaires. » L'agence de cybersécurité précise ensuite ce que les développeurs et les organisations utilisatrices peuvent faire pour atténuer ces vulnérabilités. Pour les organisations, le rapport recommande de :

- Mettre à jour les logiciels, OS, applications et micrologiciels dans les meilleurs délais
- Procéder régulièrement à la découverte automatisée des actifs
- Mettre en place un processus robuste de gestion des correctifs
- Documenter des configurations de référence sécurisées
- Effectuer régulièrement des sauvegardes sécurisées des systèmes
- Tenir à jour le plan de réponse aux incidents de cybersécurité

Comme nous l'avons dit, Apple met régulièrement à jour les OS qui présentent des vulnérabilités connues. Nous ne cessons de le répéter, mais il est absolument crucial de mettre à jour les logiciels. En entreprise, l'approche la plus courante pour tenir à jour les OS (et les applications professionnelles de leurs employés) consiste à utiliser une solution de gestion des appareils mobiles. Mais elles ont aussi à leur disposition d'autres couches de cyberdéfense. Les plans de réponse aux incidents, la collecte et l'analyse de données télémétriques et les processus internes de gestion des correctifs sont, eux aussi, d'excellents moyens de garder une longueur d'avance sur les cybercriminels. La mise en œuvre de ces mesures active également d'autres couches de cyberdéfense, comme l'identification des niveaux de vulnérabilité des logiciels ou les workflows de recherche des menaces, qui permettent de découvrir les risques dormants dans les terminaux. Tous ces éléments se conjuguent pour aider les organisations à atténuer les risques.

Jamf Threat Labs a découvert une vulnérabilité Gatekeeper dans macOS, répertoriée sous le numéro CVE-2023-41067. Cette vulnérabilité affecte les services de lancement et peut permettre l'exécution d'une application non signée et non notariée sans que les invites de sécurité appropriées ne soient présentées à l'utilisateur. Gatekeeper est la première ligne de défense pour bloquer les applications téléchargées sur Internet qui n'ont pas été signées avec un ID de développeur valide. Cette CVE ait été rapidement corrigée par Apple, mais elle est la preuve que des vulnérabilités peuvent apparaître dans n'importe quel système. Des contrôles spécifiques et un programme de formation adapté permettent encore d'atténuer les risques causés par des vulnérabilités telles que celle que l'équipe Jamf Threat Labs a découverte dans Gatekeeper.

Au cours des douze derniers mois, nous avons constaté que

32 %

des organisations utilisent au moins un appareil présentant des vulnérabilités critiques (et qu'il est possible de corriger).

Le point de vue du RSSI

- **Assurez la visibilité des vulnérabilités au sein de votre organisation :**
  Avant toute chose, efforcez-vous d'obtenir autant d'informations que possible sur les vulnérabilités présentes sur les appareils des utilisateurs et dans l'infrastructure. Ces données vous permettront ensuite d'analyser l'empreinte des applications, les risques, le rayon d'impact, etc. C'est un excellent moyen de commencer à hiérarchiser vos vulnérabilités.
- **Mettez en place un solide programme de gestion des correctifs :**
  Pour revenir à la MDM, vous devez vous munir d'un outil qui vous puisse vous dire quelles sont les versions prises en charge et les versions les plus récentes des OS et des logiciels de votre environnement. Et s'il le fait en n'exerçait aucun impact ou presque sur les utilisateurs finaux, l'adoption n'en sera que plus facile.
- **Mettez en œuvre une approche d'accès basée sur le risque :**
  Si un appareil non conforme tente d'accéder aux ressources de l'entreprise, bloquez l'accès jusqu'à ce que l'utilisateur final puisse corriger la situation et remettre l'appareil en conformité, si possible de la façon la plus simple possible.

3e partie : L'ingénierie sociale

L'ingénierie sociale est une approche qui vise à manipuler des individus pour les amener à fournir des données sensibles ou des identifiants. Selon le rapport **Perspectives de cybersécurité mondiales 2025** du Forum économique mondial, « 42 % des organisations ont subi une attaque d'ingénierie sociale réussie au cours de l'année écoulée. »

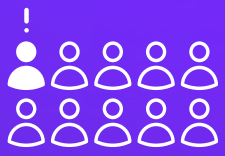
Le phishing, qui est une catégorie spécifique d'ingénierie sociale, est l'une des menaces les plus courantes et les plus préjudiciables qui pèsent sur les organisations d'aujourd'hui. S'il est plus répandu sur les appareils mobiles (en raison de leur petit écran, de leur portabilité et de leur utilisation hors des murs de l'entreprise), il vise également les Mac (et tous les ordinateurs de bureau ou PC), qui constituent une cible attrayante pour les pirates. N'oublions pas que les Mac sont toujours utilisés par le maillon le plus vulnérable de la chaîne de cybersécurité : l'utilisateur.

Les pirates font preuve d'une grande créativité et leurs imitations sont de plus en plus réalistes, si bien que nos données personnelles et professionnelles sont constamment en danger. Les appareils Mac étant de plus en plus répandus au travail, ils forment une surface d'attaque croissante. Les pirates emploient des tactiques toujours plus sophistiquées et créent des interfaces et des expériences réalistes en adoptant des styles de communication authentique pour attirer les victimes dans leur piège. Fort heureusement, les organisations peuvent mettre en place certaines mesures de protection (formation continue des employés, outils de prévention des menaces) pour protéger leurs utilisateurs et leurs données.

Au cours des douze derniers mois, nous avons découvert que :

25 %

des organisations avaient été touchées par une attaque d'ingénierie sociale



1 utilisateur sur **10**

a déjà cliqué sur un lien de phishing malveillant.

Jamf Threat Labs a publié un article sur **une enquête menée par le FBI**, selon laquelle la Corée du Nord utiliserait des moyens illicites pour en tirer des gains financiers, en particulier dans le domaine des cryptomonnaies. L'équipe évoque une attaque spécifique « au cours de laquelle un utilisateur a été contacté sur LinkedIn par un individu qui prétendait être un recruteur dans l'équipe RH d'une entreprise technologique. » Les pirates envoient à l'utilisateur un dossier zip contenant un exercice de code pour évaluer ses compétences (une étape courante dans le recrutement d'un développeur de nos jours). Lorsque l'utilisateur clique sur ce zip, le logiciel malveillant se lance ; dans ce cas, il s'agissait d'un infostealer. On comprend donc qu'il est indispensable de former les employés pour les inciter à la prudence sur les réseaux sociaux et lors du téléchargement de logiciels.

Les 20 marques les plus utilisées dans des campagnes de phising

Au cours de nos recherches, nous avons observé que certaines marques à forte notoriété sont fréquemment exploitées dans le cadre d'attaques de phishing, sans doute à cause de la confiance qu'inspire leur nom. Nous avons réparti ces marques en quatre catégories :

1. Divertissement	2. Opérations	3. Utilitaires	4 Personnel
Netflix	Outlook	United States Postal Service	Amazon.com Inc
Bet365	Office365	Gazprom	Telegram
Steam	Allegro	AT&T Inc	Facebook Inc
	InterActive Corp	Orange S.A.	Chase
	Tencent	DHL	WhatsApp
		BT Group	Yahoo, Inc.

Qu'il s'agisse de postuler à un emploi, de télécharger une application ou de travailler dans un secteur spécifique comme la cryptographie, le Mac a d'innombrables usages que les acteurs n'hésitent pas à exploiter pour accéder aux données. Dans le tableau ci-dessus, nous présentons les vingt sites les plus utilisés dans les attaques de phishing, répartis en quatre catégories.

Ces marques, en raison de leur popularité, de leur prestige et de leur omniprésence pour les entreprises et les particuliers, sont exploitées par les cybercriminels qui ciblent leurs victimes en utilisant l'ingénierie sociale. Elles sont un rouage involontaire dans un jeu de plus en plus sophistiqué. Soulignons également que cette liste n'est pas exhaustive et ne contient pas toutes les marques dont l'identité est usurpée par des acteurs malveillants. Ce sont les 20 marques les plus couramment observées l'année passée. Cette liste peut évoluer au fil des semaines, mais elle nous éclaire sur le mode de pensée des pirates. Ils misent sur la confiance que les marques ont cultivée auprès de leur clientèle pendant des années. Avec le développement du télétravail et des pratiques hybrides, les pirates imaginent de nouvelles façons d'inciter les utilisateurs à cliquer sur un lien malveillant.

Dans le monde moderne, nos informations personnelles sont constamment en danger. Les Mac étant de plus en plus répandus au travail, ils forment une surface d'attaque croissante. Les pirates emploient des tactiques toujours plus sophistiquées et créent des interfaces et des expériences réalistes en adoptant des styles de communication authentique pour attirer les victimes dans leur piège. Fort heureusement, les organisations peuvent mettre en place certaines mesures de protection (formation continue des employés, outils de prévention des menaces) pour protéger leurs utilisateurs et leurs données.

Sur les 12 mois de la période de l'étude, Jamf a recensé environ **10 millions d'attaques de phishing** menées contre notre échantillon de **1,4 million d'appareils**. En outre, nous avons constaté que **1,5 à 2 %** de ces attaques étaient classées comme « zero-day » ; autrement dit, les pirates créent de nouveaux domaines pour héberger des attaques de phishing, et ces sites ne sont pas encore recensés dans les bases de données communes de malveillances. En identifiant et en inspectant les attaques de phishing de type zero-day, les organisations peuvent protéger les utilisateurs contre les nouveaux sites d'hameçonnage.

Le point de vue du RSSI

- **Mettre en place un programme de formation complet :** Cette initiative joue un rôle central dans notre réussite. Nous menons des campagnes de phishing sophistiquées, nous organisations des formations ludiques et proposons aux utilisateurs qui le souhaitent des formations ponctuelles. Les utilisateurs ont la possibilité de signaler les e-mails de phishing et reçoivent du feedback sur leurs signalements tout au long de l'année. Notre approche ne s'arrête pas à une simple formation annuelle.
- **Tenez-vous au courant des nouvelles tendances et tactiques :** Cela peut sembler évident, mais les pirates exploitent toutes les pistes possibles, y compris les nouvelles qui bouleversent l'actualité. Vous devez adapter votre formation et vos tactiques de blocage pour faire face à ces situations. Cela peut susciter un certain malaise chez les utilisateurs, mais la transparence est essentielle. Cette formation doit les préparer à réagir face à un pirate potentiel qui n'aura pas de compassion pour eux et cherchera souvent à susciter une réaction émotionnelle pour les faire céder.
- **Adoptez une approche à plusieurs niveaux :** Il n'existe pas de solution ou d'outil uniques pour se protéger d'une campagne de phishing ciblée. Il faut donc couvrir tous les angles. Bloquez les domaines malveillants. Mettez en place l'AMF. Adoptez une approche « Zero Trust ». Activez des règles d'ubiquité impossible, etc. Une ou deux de ces mesures ne suffiront sans doute pas. La meilleure approche consiste à les multiplier pour éviter d'être à votre tour victime d'une attaque de phishing.

Principaux points à retenir

Les logiciels malveillants ciblant Mac sont de plus en plus nombreux. Heureusement, les organisations peuvent agir pour atténuer les risques liés aux logiciels malveillants sur macOS. Par exemple, la collecte et l'analyse de données télémétriques permettent d'identifier les logiciels malveillants et de signaler leur présence. Les acteurs malveillants cherchent sans cesse de nouveaux moyens de compromettre les utilisateurs et les systèmes. Mais en mettant les bons outils en place, les organisations peuvent réduire l'impact des logiciels malveillants.

Une bonne hygiène de sécurité permet d'atténuer les risques. C'est en mettant régulièrement à jour les systèmes d'exploitation et en désactivant les fonctionnalités inutiles (à commencer par les boutiques d'applications tierces) que les organisations peuvent assurer leur conformité aux profils de référence internes comme aux cadres externes. Une boutique d'applications d'entreprise, regroupant des logiciels validés en continu (en particulier dans le cas des applications privées et personnalisées), permet de superviser plus étroitement les applications vulnérables pour appliquer rapidement les correctifs.

L'ingénierie sociale est l'un des moyens les plus couramment employés par les pirates pour accéder à des informations sensibles. Plus de 90 % des cyberattaques ont le phishing comme point de départ. Le phishing prend de nombreuses formes, et l'e-mail n'est pas le seul vecteur. Il faut donc protéger l'ensemble de l'appareil (navigateurs et applications) pour mettre les utilisateurs et les organisations à l'abri.

jamf

Contactez-nous pour en savoir plus sur les menaces qui pèsent sur le Mac. Ou contactez votre revendeur habituel.

© 2025 Jamf, LLC. Tous droits réservés.