jamf

Security 360 :

Rapport annuel sur les tendances de sécurité

Mac

Sommaire

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 s'intéresse principalement au paysage des menaces ciblant le Mac afin de mettre en lumière les risques auxquels les organisations sont confrontées dans ce domaine.

Nous examinons la diversité des vecteurs d'attaque mobilisés par les attaquants pour causer des dommages. La popularité croissante du Mac en fait une cible de choix pour les pirates informatiques, qui élaborent sans cesse de nouvelles tactiques pour infiltrer les appareils et voler des données.

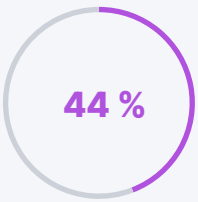
En complément de cette analyse des innovations dans le monde des menaces Mac, le rapport partage les perspectives et les éclairages du RSSI de Jamf à l'intention des responsables de la sécurité et des professionnels de l'informatique chargés de protéger les parcs mobiles.

Méthodologie de recherche

Pour comprendre et quantifier l'impact réel des tendances de sécurité identifiées dans ce rapport, nous avons examiné un groupe échantillon anonyme de plus de 150 000 Mac. Nous avons mené notre analyse à la fin de l'année 2025 en revisitant la période des 12 mois précédents. Les données incluses dans notre enquête sur les logiciels malveillants concernaient uniquement des appareils basés aux États-Unis, tandis que notre étude des vulnérabilités a pris en compte des données mondiales.

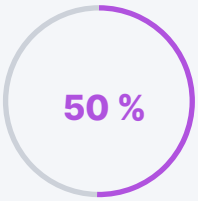
Dans le souci de respecter la vie privée des utilisateurs et les normes de sécurité les plus strictes concernant la collecte et le traitement des données, les métadonnées analysées dans cette recherche proviennent de journaux agrégés dépourvus d'informations permettant d'identifier des personnes ou des organisations.

Principales conclusions



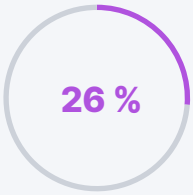
des **appareils** sont touchés par du **trafic réseau malveillant**

Les pirates cherchent par tous les moyens à compromettre vos appareils. Pour détecter et contenir le trafic malveillant, il faut une vigilance constante et les outils adéquats.



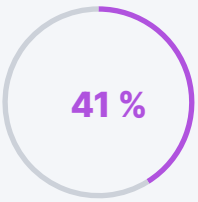
des **logiciels malveillants** affectant les Mac étaient des **chevaux de Troie**

Les chevaux de Troie arrivent en tête de classement cette année, avec plus de 33 points d'augmentation par rapport à 2024. Les chevaux de Troie sont des portes dérobées qui permettent de s'introduire dans vos systèmes pour y mener des attaques potentiellement dévastatrices.



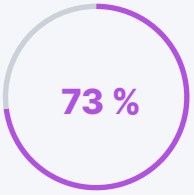
des **organisations** ont au moins **un appareil touché par un logiciel de cryptominage pirate**

Les attaques de cryptominage pirate utilisent la puissance de calcul de votre appareil pour miner de la cryptomonnaie. Les pirates s'enrichissent aux dépens de votre ordinateur qui perd en performance et en efficacité.



des **appareils** ont un système d'exploitation **gravement obsolète**

Lorsque vous imposez des versions minimales, vos appareils disposent toujours des derniers correctifs de sécurité, ce qui réduit le nombre de vulnérabilités connues exploitables.



des **appareils** ont des **applications vulnérables**

Votre système d'exploitation n'est pas le seul logiciel à présenter des risques. Les applications peuvent incorporer des bibliothèques vulnérables ou avoir été la cible d'attaques de la chaîne d'approvisionnement. La façon dont elles traitent vos données peut aussi être problématique. Pour gérer les risques, vous devez savoir ce qui est installé dans votre organisation.

Tendances clés du Mac en entreprise

1. Le Mac n'est plus une cible de niche.

Dans tous les secteurs d'activité, des entreprises de toutes tailles utilisent le Mac. Entre 2024 et 2025, la part de marché des Mac a augmenté de 16,4 % pour atteindre près de 10 %, un taux de croissance qui place le constructeur devant tous ses concurrents.

Avec plus de 2,7 millions de livraisons en 2025, le Mac est vraiment partout. Cette tendance n'a pas échappé aux pirates, et le Mac est devenu une cible privilégiée pour les exploitations. Malgré des caractéristiques de sécurité robustes, l'époque où « Mac ne pouvait pas être infecté par des virus » est révolue.

Avec la présence croissante du Mac en entreprise, les pirates font évoluer leurs tactiques et élaborent des menaces spécifiques pour voler vos données des Mac.

2. Les infostealers évoluent et n'ont jamais été aussi efficaces.

Les infostealers sont parmi les logiciels malveillants les plus répandus. Les pirates informatiques cherchent sans cesse des moyens efficaces de collecter vos données à grande échelle. La plupart du temps, ils agissent rapidement : ils collectent les identifiants, les jetons de session et les fichiers qui leur tombent sous la main avant que l'utilisateur ne s'aperçoive de quoi que ce soit.

Les infostealers sont souvent utilisés comme première étape dans des campagnes de plus grande envergure. Les données acquises peuvent être échangées contre une rançon ou servir à infiltrer d'autres comptes et systèmes. Cela explique la grande popularité des infostealers, que beaucoup de développeurs peu scrupuleux proposent sur le modèle « en tant que service ». Les infostealers modernes sont capables de créer une porte dérobée et d'assurer une persistance malgré les redémarrages et les déconnexions. Ils permettent même aux attaquants d'envoyer des commandes depuis un serveur C2.

3. Les groupes APT s'intéressent toujours à macOS.

Si vous parcourez le paysage des menaces qui pèsent sur le Mac, vous reconnaîtrez sans doute des visages familiers. Des menaces avancées, semblables à celles des groupes nord-coréens, continuent de cibler macOS ; citons notamment Contagious Interview, FlexibleFerret et les variantes de l'infostealer Odyssey.

Les portes dérobées et les mécanismes de persistance sont toujours autant utilisés. Jamf Threat Labs a observé ce phénomène dans le logiciel malveillant ChillyHell.

Pour en savoir plus sur les recherches de Jamf Threat Labs, reportez-vous à la fin de ce rapport.

Logiciels malveillants et menaces sur Mac

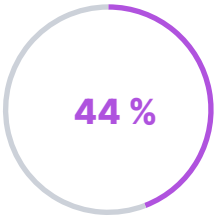
Les ordinateurs Mac et Windows sont différents, leurs logiciels malveillants aussi. Les pirates qui développent des logiciels malveillants pour Mac doivent connaître ses spécificités pour cibler l'exploitation. Première chose, ils sont obligés de contourner les dispositifs de sécurité :

1. **Gatekeeper**, qui vérifie que les applications sont légitimes et sûres en examinant leur **notarisation et la signature du développeur.**

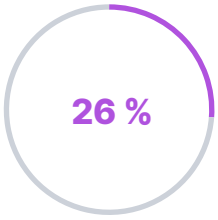
2. **La protection de l'intégrité du système (SIP),** qui restreint l'écriture dans les fichiers système critiques

3. **Le protocole Transparence, consentement et contrôle (TCC),** qui exige une autorisation explicite de l'utilisateur pour accéder à la caméra, au micro, aux fichiers et à d'autres contenus.

Malgré ces difficultés, **les acteurs malveillants parviennent à leurs fins.**



des **appareils** ont été touchés par du **trafic réseau malveillant**



des **organisations** ont été touchées par des **attaques de cryptominage pirate**

C'est pourquoi il est essentiel **de comprendre et de découvrir les dernières menaces.**
Et la situation évolue rapidement.

Plus de 26 000

C'est le nombre d'**échantillons de logiciels malveillants** que **Jamf Threat Labs** a ajouté à sa base de données en 2025.

Plus de 230

C'est le nombre de **règles YARA** ajoutées par **Jamf Threat Labs en 2025**

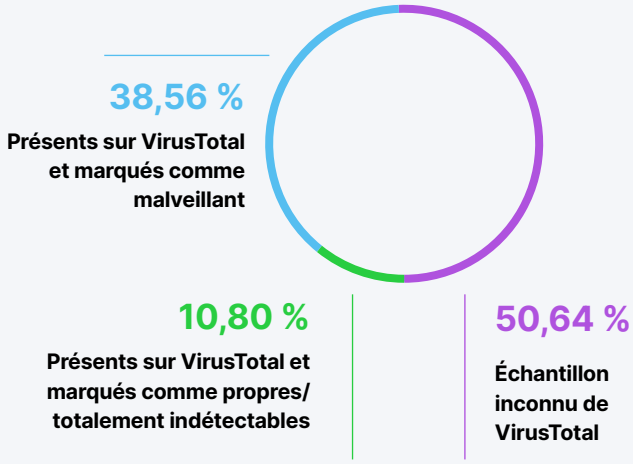
Une fois l'adversaire identifié, il faut apprendre à le détecter. Les **règles YARA** sont d'une grande utilité : les chercheurs les utilisent pour identifier et classer les échantillons de logiciels malveillants.

Mais que faire face aux menaces que nous ne connaissons pas ? Les pirates produisent régulièrement de nouvelles techniques qui ne sont pas immédiatement découvertes par la communauté de la cybersécurité.

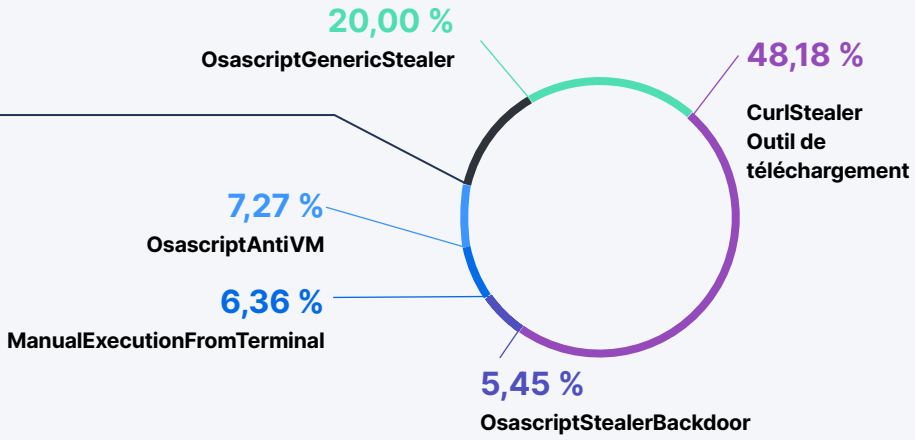
Jamf Threat Labs les traque en analysant des échantillons prélevés en environnement réel grâce à des règles statiques et basées sur le comportement. Une inspection avec VirusTotal révèle qu'environ **50 %** d'entre eux n'ont pas encore été déclarés par d'autres chercheurs.

Malheureusement, lorsque les logiciels malveillants deviennent trop faciles à identifier, les auteurs les modifient pour qu'ils échappent aux détections. Les chercheurs doivent donc s'appuyer sur des techniques avancées reposant davantage sur le *comportement* que les caractéristiques statiques des fichiers. Les alertes comportementales de haute gravité attirent l'attention des contrôles de sécurité avancés de Jamf et entraînent un blocage immédiat. Voici les plus courants en 2025 :

ÉCHANTILLONS TROUVÉS PAR JAMF THREAT LABS



DÉTECTIONS COMPORTEMENTALES AVANCÉES



Autres	**12,74 %**
StealerDataExfiltration	**3,64 %**
XcodeExecutesCurl	**2,73 %**
KnownMaliciousCurlCommand	**2,73 %**
MaliciousCurlUserAgent	**1,82 %**
InsecureCurlFromScriptEditor	**0,91 %**
NpmMaliciousPackage	**0,91 %**

Voici un aperçu du comportement de ces détections :

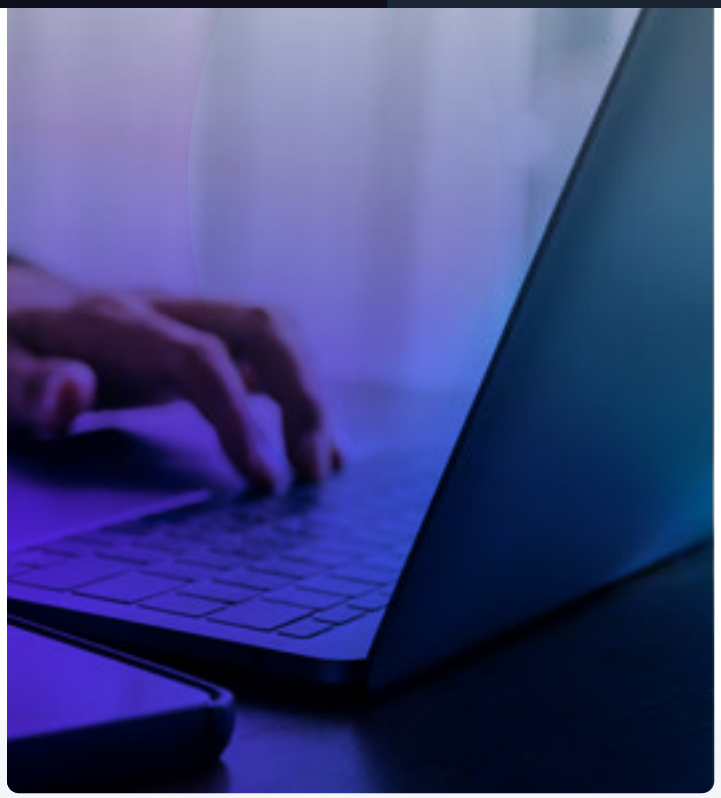
CurlStealerDownloader
utilisation suspecte de curl visant à télécharger et exécuter des charges utiles de type infostealer

OsascriptGenericStealer
activité d'infostealer macOS détectée via l'exécution d'AppleScript

XcodeExecutesCurls
commande curl malveillante exécutée pendant le processus de compilation Xcode

NpmMaliciousPackage
exécution d'un paquet NPM potentiellement malveillant, signalant une activité de script suspecte pendant l'installation ou l'exécution.

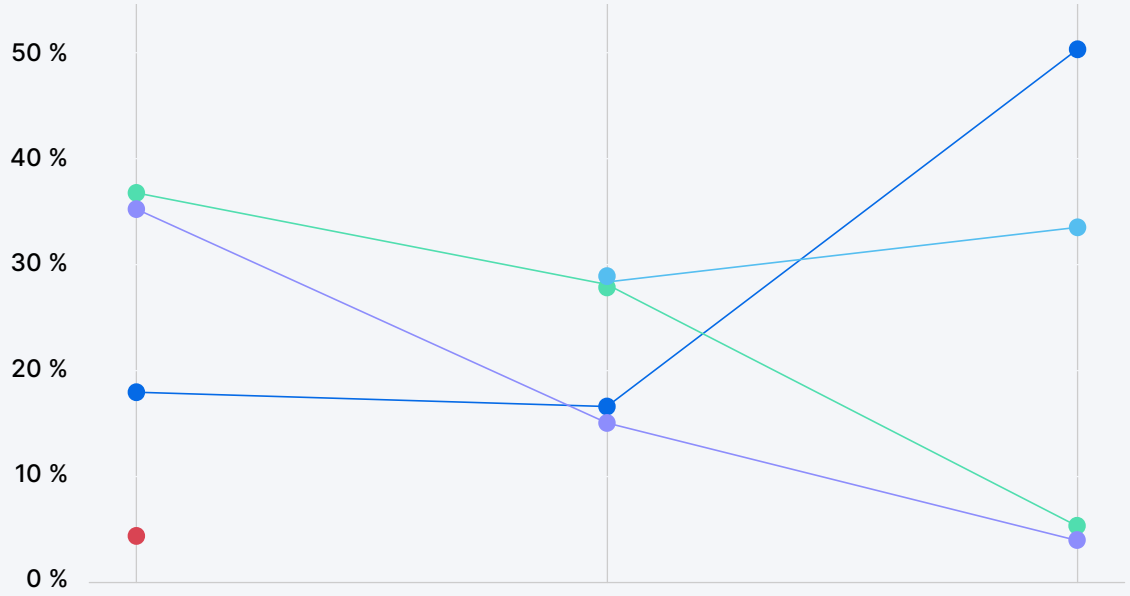
Le fait est que les menaces qui ciblent le Mac sont aussi courantes que variées. Les pirates ne créent pas seulement des logiciels malveillants pour leur propre compte ; certains les vendent au plus offrant, et la demande est plus forte que jamais. Pour s'en protéger, il faut d'abord connaître l'adversaire.



Les logiciels malveillants les plus courants sur Mac

Les stratégies d'attaque ont évolué en 2025. En 2024, les infostealers et les logiciels publicitaires dominaient le terrain : chacune de ces catégories représentait environ **28 %** des attaques. En 2025, les chevaux de Troie sont en tête du classement, avec près de la moitié des attaques, devant les infostealers qui sont encore responsables d'un tiers des malveillances. Pour comprendre ce phénomène, il faut savoir que certains infostealers ont évolué pour intégrer des portes dérobées. Si l'on compare les données de cette année aux études des années précédentes, on observe que la popularité des différentes catégories de menaces évolue :

LOGICIELS MALVEILLANTS : LES GRANDES TENDANCES



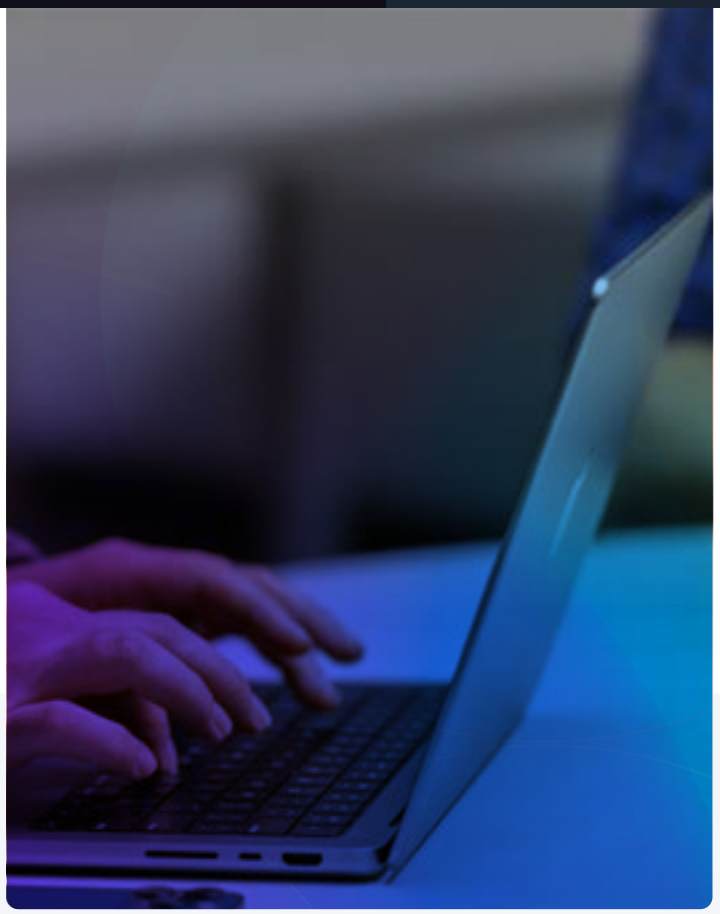
Malware Type	2023	2024	2025
Chevaux de Troie	17,96 %	16,61 %	50,32 %
Infostealers	-	28,36 %	33,52 %
Logiciels publicitaires	36,77 %	28,13 %	5,06 %
PUA	35,24 %	15,06 %	4,84 %
Exploit	4,40 %	-	-

Les quatre premiers types de logiciels malveillants représentent **plus de 90 % des attaques.** Voici le classement :

	Caractéristiques :	Intention :	Distribution :
Chevaux de Troie 50,40 %	Prennent l'apparence d'une application légitime	Grande diversité, généralement utilisés comme porte dérobée pour mener d'autres attaques	Ingénierie sociale, dépôts de fichiers, etc.
Infostealers 33,52 %	Volent les données du système immédiatement après l'infection	Récoltent des données sensibles (identifiants de connexion, informations personnelles identifiables, etc.).	Parfois proposés en tant que service et distribués par le biais de l'ingénierie sociale, de sites web malveillants et de téléchargements de logiciels.
Logiciels publicitaires 5,06 %	Affichent des publicités, peuvent suivre le comportement de l'utilisateur à des fins de publicité ciblée ou d'espionnage.	Génèrent des revenus publicitaires ou collectent des informations	Intégrés à d'autres logiciels, à des sites web ou à des pièces jointes malveillantes
Applications potentiellement indésirables (PUA) 4,84 %	Prennent de nombreuses formes ; peuvent collecter des données, ralentir les appareils ou perturber leur fonctionnement.	Ne sont pas toujours explicitement malveillants, mais peuvent monétiser les données des utilisateurs ou générer des revenus par d'autres moyens.	Intégrés à d'autres logiciels ou téléchargés via des tactiques de trompeuses

Autres 6,26 %

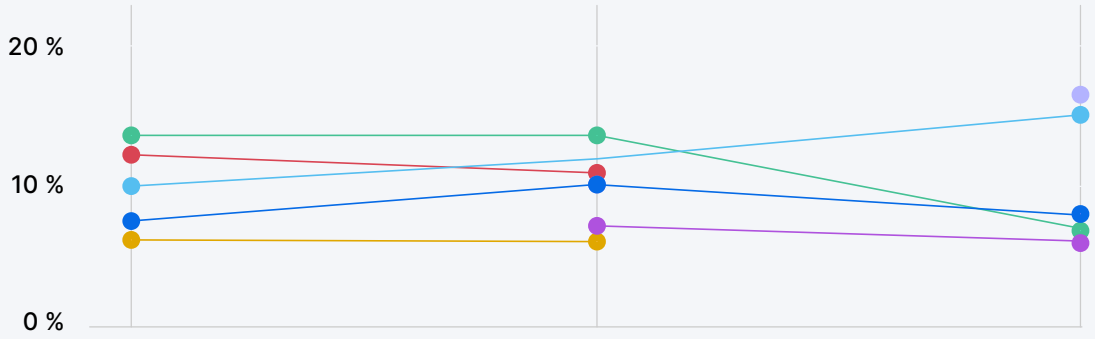
2,0 % Exploitation, **1,4 %** Outil de piratage, **0,9 %** Minage, **0,4 %** Outil de téléchargement, **0,4 %** Enregistreur de frappe, **0,3 %** Ransomware, **0,2 %** Outil de dépôt



Les logiciels malveillants les plus courants sur Mac

De nombreuses familles de logiciels malveillants affectent le Mac, sans qu'aucune ne se démarque clairement. En 2025, PuAgent était le plus répandu avec **16,41 %**. En 2023 et 2024, le logiciel publicitaire Genio était en tête (**13,63 %**), avant de reculer à la quatrième place du classement (**7,19 %**) en 2025.

LOGICIELS MALVEILLANTS : LES GRANDES TENDANCES



Malware Type	2023	2024	2025
PuAgent	-	-	16,41 %
Générique	10,02 %	-	15,09 %
Genio	13,63 %	13,63 %	7,19 %
Multiverze	6,84 %	9,44 %	7,47 %
Mackeeper	-	7,19 %	7,13 %
Imobie	12,25 %	10,96 %	-
TNT	6,19 %	6,07 %	-

	Caractéristiques :	Distribution :
PuAgent Logiciel publicitaire **16,4 %**	Modifie de nombreux réglages du navigateur : moteurs de recherche, page d'accueil, paramètres, extensions, etc. Déploie des fenêtres publicitaires et suit le comportement des utilisateurs.	Pièces jointes, téléchargements/liens malveillants, logiciels gratuits
Générique Divers **15,1 %**	Les fichiers présentent un comportement suspect indiquant la présence de logiciels malveillants, mais ils n'ont pas de signature propre à une famille connue.	Divers
Multiverze Cheval de Troie **7,5 %**	Collecte les données des utilisateurs : mots de passe, numéros de carte de crédit, portefeuilles de cryptomonnaie et autres informations privées. Peut enregistrer tout ce que vous tapez et voyez sur votre écran. Peut agir à l'insu de l'utilisateur.	E-mails d'hameçonnage, sites web malveillants, publicité malveillante, logiciels gratuits, réseaux sociaux
Genio Logiciel publicitaire **7,2 %**	Détourne le navigateur web pour collecter des informations sur les utilisateurs ; prend l'apparence d'un moteur de recherche pour afficher des résultats sponsorisés ; difficile à désinstaller.	Groupement avec des logiciels légitimes, téléchargements malveillants
Mackeeper PUA **7,1 %**	Prend l'apparence d'une application légitime, mais ne tient pas forcément ses promesses de performance. Ouvre des fenêtres publicitaires ; peut émettre de fausses affirmations sur la santé de l'appareil et dégrader ses performances.	Publicités malveillantes, téléchargements malveillants

Imobie 6,3 %

Revproxy 4,7 %

atomic_stealer 4,1 %

Ccleanmac 3,4 %

Macinformer 3,1 %

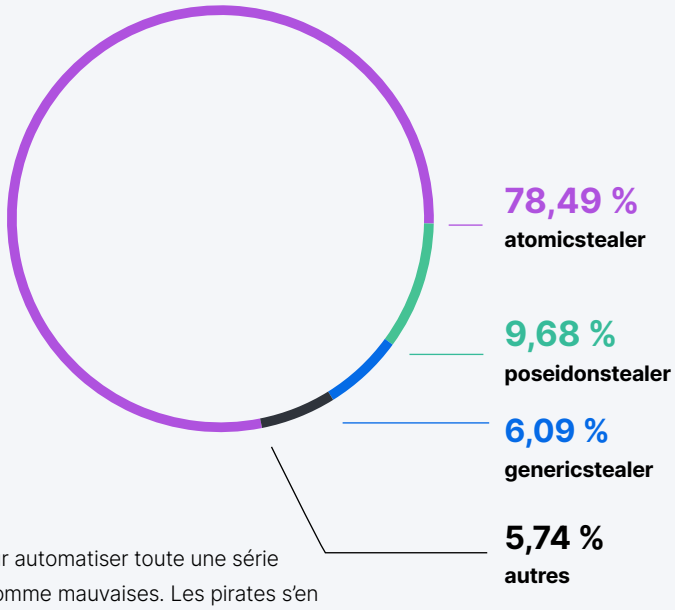
Others 25,1 %

Infostealers

Lorsqu'on veut quelque chose (ne faites pas ça chez vous), la rapidité d'action est le meilleur moyen de ne pas se faire prendre. Les infostealers s'efforcent généralement d'agir rapidement pour voler vos données juste après avoir infecté votre appareil. Certains s'effacent d'eux-mêmes une fois leur méfait accompli, mais des versions modernes s'implantent plus durablement.

> *Les infostealers jouent pour beaucoup dans la multiplication des logiciels malveillants au sein de l'écosystème macOS. AppleScript, malgré son utilité reconnue pour les utilisateurs chevronnés, a également fait l'objet d'abus via des logiciels malveillants.*
>
> Jaron Bradley, Jamf

LES INFOSTEALERS LES PLUS COURANTS



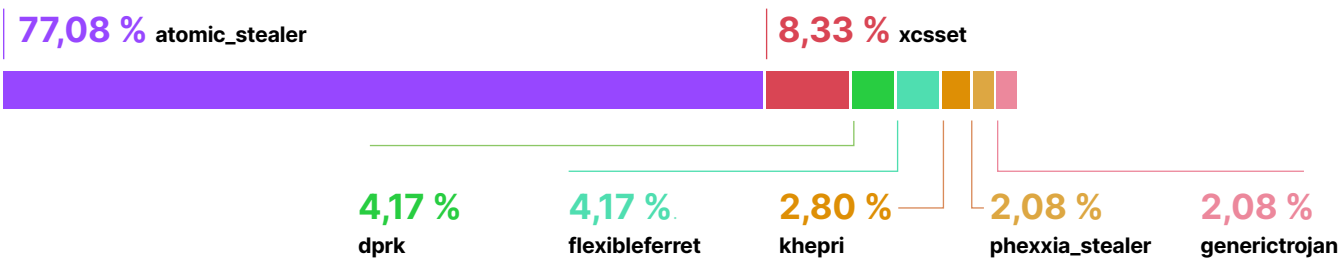
Les développeurs et les utilisateurs chevronnés utilisent AppleScript pour automatiser toute une série d'événements. C'est un outil puissant aux possibilités infinités, bonnes comme mauvaises. Les pirates s'en servent pour tromper les utilisateurs et leur dérober des informations.

Les infostealers sont devenus beaucoup plus fréquents après 2023 ; à l'époque, ils ne représentaient qu'à peine **0,25 %** des attaques. En 2024, ce pourcentage a considérablement augmenté, passant à **28,36 %**, pour finalement atteindre **33,52 % en 2025**. Malgré cette popularité, la plupart des attaques sont menées avec d'autres types de logiciels malveillants, comme les chevaux de Troie. D'ailleurs, à ce sujet...

Chevaux de Troie

Les chevaux de Troie ont gagné en popularité en 2025 : représentés dans **50,3 % des attaques**, ils sont même en tête du classement des logiciels malveillants. Le cheval de Troie le plus courant, **atomic_stealer**, était impliqué dans **77,08 % des attaques.** Vous avez sans doute remarqué un air de famille avec l'infostealer qui a dominé 2025. En effet, ce n'est pas une coïncidence. De nombreux infostealers utilisent des chevaux de Troie pour implanter une porte dérobée afin de se réintroduire dans le système.

CHEVAUX DE TROIE ACTIFS



Pour vaincre son adversaire, il faut d'abord le connaître.

La plupart des logiciels malveillants dont nous avons parlé sont bien connus. Votre logiciel de détection des menaces n'aura sans doute aucun mal à les identifier. Mais comme nous l'avons déjà mentionné, tous les logiciels malveillants ne sont pas identifiables par leur code. Il faut des détections avancées, capables de reconnaître les comportements suspects, pour trouver les menaces qui n'ont pas encore été analysées par la communauté de la cybersécurité. En adoptant des outils sophistiqués, vous contribuerez grandement à protéger votre organisation contre les attaques de type « zero-day ».

Les configurations ont aussi un rôle important à jouer. Les logiciels malveillants misent souvent sur le comportement de l'utilisateur, en proposant des téléchargements risqués ou en utilisant l'ingénierie sociale. Les règles de sécurité et la formation des utilisateurs sont très utiles pour atténuer ce risque.

La détection est cruciale, mais la prévention commence par le logiciel lui-même. Les cyberattaques s'appuient sur des vulnérabilités logicielles, des failles dans la conception des applications et des systèmes d'exploitation qui ouvrent une porte aux acteurs malveillants. Votre meilleure chance de combler ces vulnérabilités et d'empêcher les attaquants d'entrer consiste à appliquer les mises à jour de vos appareils et de vos applications. Nous y reviendrons dans la section suivante.

Le point de vue de notre RSSI

Avec la multiplication des appareils Apple dans les entreprises, il faut des solutions de sécurité conçues spécifiquement pour l'écosystème Apple, plutôt que des outils polyvalents d'abord pensés pour Windows. Les organisations ont tout intérêt à privilégier des produits de sécurité développés dès le départ pour macOS. De cette façon, les fonctions de détection des menaces, de mise en conformité et de réponse seront parfaitement alignées sur le mode de fonctionnement des plateformes Apple.

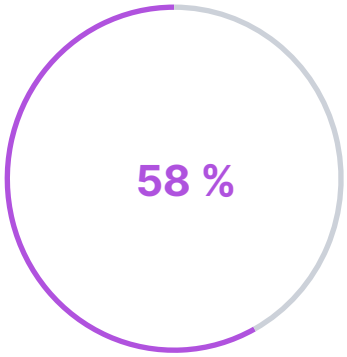
Vulnérabilités des applications et du système d'exploitation

Le système d'exploitation est la base d'un appareil. Il alimente les outils, les services, les applications et la sécurité de votre appareil. Les attaquants sont constamment à la recherche de failles dans ses défenses.

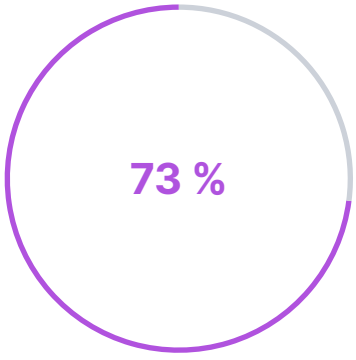
Les vulnérabilités ont des effets cumulatifs. Une faille mineure peut devenir une étape cruciale dans une attaque, et l'on sait que l'application des correctifs n'est pas toujours une priorité.

Puisqu'on en parle, les correctifs sont un enjeu majeur. En effet, même les systèmes d'exploitation les plus sûrs ont des points faibles. C'est inévitable, mais ce n'est pas incurable. Apple publie constamment des mises à jour logicielles pour corriger les vulnérabilités. Pour rester protégée, votre organisation doit appliquer ces mises à jour. Mais elle ne le fait pas toujours.

Les applications ne sont pas non plus à négliger. Elles ont, elles aussi, des vulnérabilités propres : elles appliquent des règles spécifiques de traitement des données et incluent des bibliothèques tierces, entre autres.



des **entreprises** possèdent au moins **un appareil** dont le **système d'exploitation est gravement obsolète**



des **appareils** *contiennent* au moins une **application vulnérable**

Qu'est-ce qu'une CVE ?

Le programme CVE (vulnérabilités et expositions communes) entretient une base de données des vulnérabilités découvertes par la communauté de la cybersécurité. Chaque CVE identifie le logiciel ou la bibliothèque concernés, précise le degré de gravité et propose des méthodes d'exploitation possibles.

Les logiciels obsolètes sont extrêmement fréquents. Les utilisateurs ne sont pas toujours enthousiastes à l'idée d'installer des mises à jour, surtout s'ils ont l'impression que cela va les interrompre dans leur travail. Pourtant, en imposant des délais de mise à jour et des versions minimales du système d'exploitation, vous contribuerez à protéger votre parc d'appareils et vos données contre l'exploitation de ces failles.

Vulnérabilités notables ciblant macOS, 2025

CVE-2025-46287 | Gravité : 9.8 (critique)	CVE-2025-43539 | Gravité : 8.8 (élevée)	CVE-2025-46285 | Gravité : 7.8 (élevée)
DESCRIPTION :		
Un pirate pourrait usurper une identité d'appelant FaceTime.	Le traitement d'un fichier peut entraîner une corruption de la mémoire.	Une application peut parvenir à obtenir des privilèges root.
COMPOSANT CONCERNÉ		
Framework d'appel	AppleJPEG	Noyau
IMPACT :		
En affichant des informations trompeuses, l'attaquant peut inciter l'utilisateur à prendre une mauvaise décision.	Un attaquant peut modifier des données pour exécuter un code non autorisé.	Un adversaire peut exécuter du code arbitraire.
SYSTÈME D'EXPLOITATION CORRIGÉ :		
macOS Tahoe 26.2, Sequoia 15.73 et Sonoma 14.8.3	macOS Tahoe 26.2, Sequoia 15.73 et Sonoma 14.8.3	macOS Tahoe 26.2, Sequoia 15.73 et Sonoma 14.8.3

Vulnérabilités découvertes par Jamf

CVE-2025-43296 | Oct 2025
Contournement de Gatekeeperdans les Réglages système, corrigé dans macOS Tahoe 26 .

CVE-2025-43348 | Nov 2025
Contournement de Gatekeeper dans Finder, corrigé dans macOS Tahoe 26.1.

Le tableau suivant présente d'autres vulnérabilités pour lesquelles nous avons des preuves d'exploitation en 2025.

ID CVE	COMPOSANT	IMPACT
CVE-2025-24113 Score CVSS : 4.3 | Gravité : **moyenne**	Safari	Visiter un site web malveillant peut conduire à une usurpation d'interface utilisateur.
CVE-2025-46289 Score CVSS : 5.5 | Gravité : **moyenne**	AppSandbox	Une application peut parvenir à accéder aux données protégées de l'utilisateur.
CVE-2025-43482 Score CVSS : 5.5 | Gravité : **moyenne**	Audio	Une application peut parvenir à provoquer un déni de service.
CVE-2025-43517 Score CVSS : 3.3 | Gravité : **faible**	Historique des appels	Une appli peut parvenir à accéder à des données utilisateur protégées en raison d'un problème de journalisation.
CVE-2025-43542 Score CVSS : 7.5 | Gravité : **élevée**	FaceTime	Des champs de mot de passe peuvent être révélés involontairement lors du contrôle d'un appareil à distance via FaceTime.
CVE-2025-43532 Score CVSS : 2.8 | Gravité : **faible**	Foundation	Le traitement de données malveillantes peut entraîner l'arrêt inattendu de l'application en raison d'une corruption de la mémoire.
CVE-2025-43512 Score CVSS : 7.8 | Gravité : **élevée**	Noyau	Une application peut parvenir à élever ses privilèges.

La gestion des vulnérabilités est un combat permanent, mais la victoire est possible.

Pour garder une longueur d'avance sur les vulnérabilités des logiciels, il faut une bonne stratégie. Pour simplifier, vous devez en permanence surveiller, identifier et atténuer les vulnérabilités qui affectent vos systèmes et vos appareils.

Les équipes informatiques et de sécurité n'ont pas toutes les effectifs et les compétences nécessaires aux activités de recherche des menaces. Heureusement, la communauté de la cybersécurité est à vos côtés. Les spécialistes de la recherche de menaces et les éditeurs de logiciels sont constamment à l'affût des dernières exploitations. Ils alimentent les bases de données de vulnérabilités pour aider les organisations à localiser leurs points faibles. Vos équipes peuvent s'y référer pour évaluer votre posture de sécurité actuelle et réagir en conséquence. Des outils de sécurité sont disponibles pour faciliter ce processus.

Les outils dont votre organisation a besoin varient en fonction de sa taille, de ses capacités, de son secteur d'activité et d'autres critères. Mais de façon générale, il lui faut une solution permettant de :

- **Configurer les appareils et appliquer des règles**
- **Gérer les comptes d'utilisateurs et les identités**
- **Maintenir les appareils et les logiciels à jour**
- **Contrôler la santé des appareils**
- **Appliquer des règles d'accès**

Les outils de gestion des appareils mobiles, de protection des points de terminaison, de gestion des identités et de télémétrie sont autant d'alliés qui vous aident à faire face aux menaces dès qu'elles se présentent.

Le point de vue de notre RSSI

Une stratégie de sécurité solide repose sur trois principes fondamentaux : visibilité, télémétrie et automatisation. Et la gestion des vulnérabilités est sans doute le domaine où ils jouent le plus grand rôle. Les **équipes de sécurité** doivent :

Comprendre les vulnérabilités

La première étape, cruciale, consiste à acquérir une visibilité sur les vulnérabilités dans l'ensemble de l'organisation. Avec une image complète des failles présentes sur les appareils des utilisateurs finaux et l'infrastructure, vous jetez les bases d'une posture de sécurité fondée sur les données. Les équipes peuvent alors analyser l'environnement applicatif, évaluer les risques et déterminer le rayon d'impact, afin de hiérarchiser les vulnérabilités en s'appuyant sur des données plutôt que sur des suppositions.

Mettre en œuvre une approche basée sur les risques pour évaluer l'accès des appareils

Lorsque des appareils non conformes tentent d'accéder aux ressources de l'entreprise, leur accès doit être bloqué jusqu'à ce que le problème soit corrigé ; les processus de remédiation doivent être aussi fluides et peu contraignants que possible pour l'utilisateur final.

Mettre en place un solide programme de gestion des correctifs

Pour revenir à la gestion des appareils mobiles, il est essentiel de disposer d'un outil capable d'appliquer les versions les plus récentes ou prises en charge d'un logiciel ou d'un système d'exploitation, afin de maintenir un environnement sain et sûr. Et s'il le fait sans aucun impact ou presque sur les utilisateurs finaux, l'adoption n'en sera que plus facile.

Lisez les dernières recherches de Jamf Threat Labs sur les menaces macOS

OpenClaw : le discret assistant IA qui pourrait devenir votre plus grande menace interne

FÉVRIER 2026

OpenClaw est un cadre open source pour la création d'agents d'IA autonomes capables d'exécuter des commandes shell, d'accéder à des fichiers et d'interagir avec des applications. Comme il n'intègre pas de limites de sécurité, il introduit des risques importants pour la sécurité de l'entreprise. Le danger de ce cadre vient de son accès illimité au système, du potentiel d'exfiltration des données et de la vulnérabilité aux attaques indirectes par injection de prompt, consistant à intégrer des instructions malveillantes à du contenu commercial légitime. Des avis de sécurité récents ont démontré que des pirates pouvaient exploiter différentes failles pour obtenir un accès persistant. Les déploiements d'OpenClaw peuvent donc être considérés comme une menace interne à haut risque nécessitant des stratégies complètes de détection, de prévention et de gouvernance dans les environnements d'entreprise.

Les acteurs malveillants intensifient leur exploitation de Microsoft Visual Studio Code

JANVIER 2026

Des acteurs malveillants associés à la Corée du Nord ont fait évoluer la campagne Contagious Interview pour manipuler les fichiers de configuration de tâches de Visual Studio Code. Cette tactique crée une porte dérobée JavaScript lorsque les victimes ouvrent des dépôts Git malveillants. Les pirates établissent ainsi une communication persistante de commande et de contrôle qui permet de recueillir des informations sur le système et d'exécuter du code à distance. Cette technique exploite les workflows de confiance des développeurs : lorsque les utilisateurs signalent un dépôt comme fiable, les fichiers de configuration malveillants exécutent automatiquement des commandes cachées. Cette méthode illustre l'inventivité des pirates lorsqu'il s'agit d'infiltrer les outils de développement légitimes.

De ClickFix à la signature de code : l'évolution discrète du logiciel malveillant MacSync Stealer

DÉCEMBRE 2025

MacSync Stealer a dépassé le stade du glisser-déposer dans le terminal. Le logiciel malveillant se déploie désormais par le biais d'une application Swift signée et notariée qui récupère et exécute silencieusement les charges utiles sans aucune interaction avec le terminal. Distribuée via de faux programmes d'installation, cette variante utilise un dropper sophistiqué qui effectue des contrôles de connexion, applique une limitation du débit, valide les charges utiles et supprime les attributs de quarantaine avant l'exécution. Cette évolution vers une livraison signée et notariée s'inscrit dans une tendance plus large consistant à déguiser du code malveillant en applications légitimes pour échapper à la détection et contourner les contrôles de sécurité de macOS.

Le logiciel malveillant FlexibleFerret continue de sévir

NOVEMBRE 2025

FlexibleFerret, une famille de logiciels malveillants rattachée à la Corée du Nord, cible les utilisateurs de macOS par le biais de fausses campagnes de recrutement sophistiquées. Les victimes sont incitées à exécuter des commandes malveillantes dans le terminal sous couvert de procéder à des évaluations. Cette attaque se déroule en plusieurs étapes. Elle utilise du JavaScript sur de faux sites d'offres d'emploi pour déployer une porte dérobée aux nombreuses capacités (exfiltration de fichiers, exécution de commandes), tout en récoltant des identifiants par le biais de fausses invites Chrome. Les données sont envoyées à des comptes Dropbox contrôlés par l'attaquant. Cette menace innovante contourne Gatekeeper en convainquant l'utilisateur d'exécuter manuellement des commandes. Il est donc crucial de sensibiliser le public au risque posé par les fausses évaluations de recrutement et la saisie d'instructions dans le terminal.

DigitStealer : un infostealer basé sur JXA qui laisse peu de traces

NOVEMBRE 2025

DigitStealer est un infostealer sophistiqué pour macOS qui est resté sous le radar de VirusTotal alors qu'il utilise des techniques anti-analyse avancées, comme la détection des caractéristiques matérielles qui limite son exécution aux puces M2 et plus récentes d'Apple. Le logiciel malveillant déploie quatre charges utiles en mémoire qui volent les données du navigateur, les portefeuilles de cryptomonnaies et les identifiants. Il transforme Ledger Live en cheval de Troie en fusionnant trois composants distincts pour échapper à la détection et s'implante au moyen d'une porte dérobée dynamique. L'attaque utilise des services Cloudflare légitimes pour héberger les charges utiles ainsi que des techniques de dissimulation en plusieurs étapes. Cette approche, qui démontre une connaissance approfondie des rouages de macOS, rend la détection comportementale absolument cruciale puisque la plupart des exécutions se déroulent entièrement en mémoire.

ChillyHell : exploration d'une porte dérobée modulaire pour macOS

Septembre 2025

Apparue en 2021, ChillyHell est une porte dérobée macOS sophistiquée longtemps restée notariée et non détectée. Elle était liée à l'origine à des attaques ciblant des fonctionnaires du gouvernement ukrainien. Ce logiciel malveillant modulaire en C++ établit de multiples mécanismes de persistance et communique via DNS et HTTP. Il déploie des capacités telles que le reverse-shell, la mise à jour automatique, la livraison de charges utiles et le piratage de mot de passe par force brute. Ses techniques d'évasion avancées prouvent que, même signée et notariée, une application n'est pas toujours sûre.

Vol avec signature : de nouvelles informations sur l'infostealer Odyssey

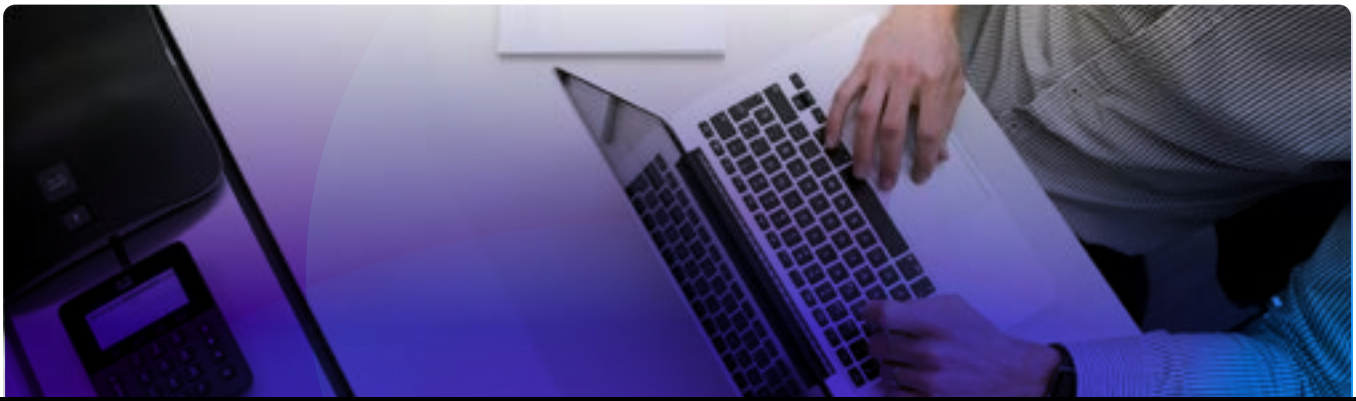
Juillet 2025

Un infostealer macOS sophistiqué a réussi à obtenir la signature de code et la notarisation d'Apple. Il a ainsi pu contourner les contrôles de sécurité intégrés pour déployer une porte dérobée persistante, dans le but de remplacer des applications de cryptomonnaie légitimes par des chevaux de Troie. Le logiciel malveillant utilise une interface SwiftUI trompeuse pour récolter des mots de passe ; il télécharge dynamiquement des charges utiles dissimulées et établit une communication C2 pour exécuter du code à distance. Le plus inquiétant est qu'il analyse soigneusement l'environnement de sécurité et inscrit les systèmes de détection sur une liste noire pour leur échapper. Ce degré de sophistication ne peut être que le travail d'un groupe au service d'un État-voyou.

Un python déguisé : dissection du logiciel malveillant PyInstaller sur macOS

Mai 2025

Des pirates utilisent PyInstaller pour déguiser du code Python malveillant en exécutable macOS natif ; c'est la première fois que cette technique est observée dans des infostealers ciblant macOS. Le logiciel malveillant s'exécute sans nécessiter l'installation de Python, dérobe des identifiants à l'aide de fausses invites, et récolte les données du Keychain et les portefeuilles de cryptomonnaies en multipliant les couches de dissimulation pour échapper à toute détection. Cette technique représente une évolution significative dans la distribution des logiciels malveillants macOS : elle facilite le déploiement d'infostealers sophistiqués tout en contournant les mécanismes de sécurité traditionnels.



jamf

Contactez-nous pour en savoir plus sur le paysage des menaces Mac.