Les produits Apple peuvent-ils être infectés par des rançongiciels

Apple est excellent pour fournir une protection contre la plupart des logiciels malveillants, mais qu'en est-il des ransomwares? De tels logiciels malveillants peuvent-ils cibler votre Mac ou votre iPhone ?

NDLR: l'expression "jailbreak" dans le texte signifie:
Le jailbreak consiste à exploiter les failles d'un appareil électronique bridé pour installer un logiciel autre que celui fourni par le fabricant de l'appareil.
Le jailbreak permet au propriétaire de l'appareil d'avoir un accès total à la racine (« root ») du système d'exploitation et aux fonctionnalités.
« Jailbreak » signifie littéralement « libérer » l'appareil de la « prison » formée par les limites imposées sur l'appareil.
Le jailbreak est souvent utilisé pour l'iPhone : c'est le cellulaire considéré comme le plus « bridé » du marché.
Les premières versions de l'iPhone n'avaient pas d'App Store et l'interface iOS était considérée comme plus limitée qu'aujourd'hui pour les utilisateurs.
Aux États-Unis, le premier modèle de l'iPhone fonctionnait seulement sur le réseau d'AT&T et les utilisateurs qui voulaient utiliser d'autres fournisseurs étaient bien ennuyés, à moins d'avoir jailbreaké leur iPhone.

Katie Rees :

Les produits Apple ne sont pas entièrement imperméables aux logiciels malveillants, mais c'est beaucoup plus rare; les iPhones jailbreakés, par exemple, sont beaucoup plus susceptibles d'être affectés par des logiciels malveillants que ceux qui utilisent encore l'environnement sécurisé d'Apple, qui protège principalement contre les logiciels malveillants.

Mais les ransomwares constituent-ils une menace pour ces appareils ?
Un produit Apple peut-il être infecté par un rançongiciel.
Et est-ce très courant?

Votre appareil Apple peut-il héberger un ransomware?

Le ransomware est un type de malware très dangereux qui crypte les fichiers d'une victime, les rendant inaccessibles.
Pour retrouver l'accès à ses fichiers, la victime doit souvent payer le montant de la rançon exigée par l'attaquant.
Cela pourrait aller de quelques centaines à quelques millions de dollars.

Historiquement, les produits Apple n'ont pas été une cible de choix pour les attaquants. Les systèmes Windows et Linux sont généralement ce que les opérateurs de ransomware visent, mais il s'agit d'une tendance, pas d'une règle.

Les iPhones, iPads, Mac et MacBooks peuvent tous être infectés par des ransomwares, mais ce n'est pas parce que ces appareils ont une mauvaise protection de sécurité.

Apple est connu pour sa protection antivirus de haut niveau sur ses appareils.
Sur macOS et iOS, vous trouverez d'excellentes fonctionnalités de sécurité, telles que le chiffrement FileVault 2, la vérification de sécurité, Face ID et le mode de verrouillage.
Mais malgré ces attributs utiles, les ransomwares peuvent toujours présenter un risque pour vos produits Apple dans de rares cas.

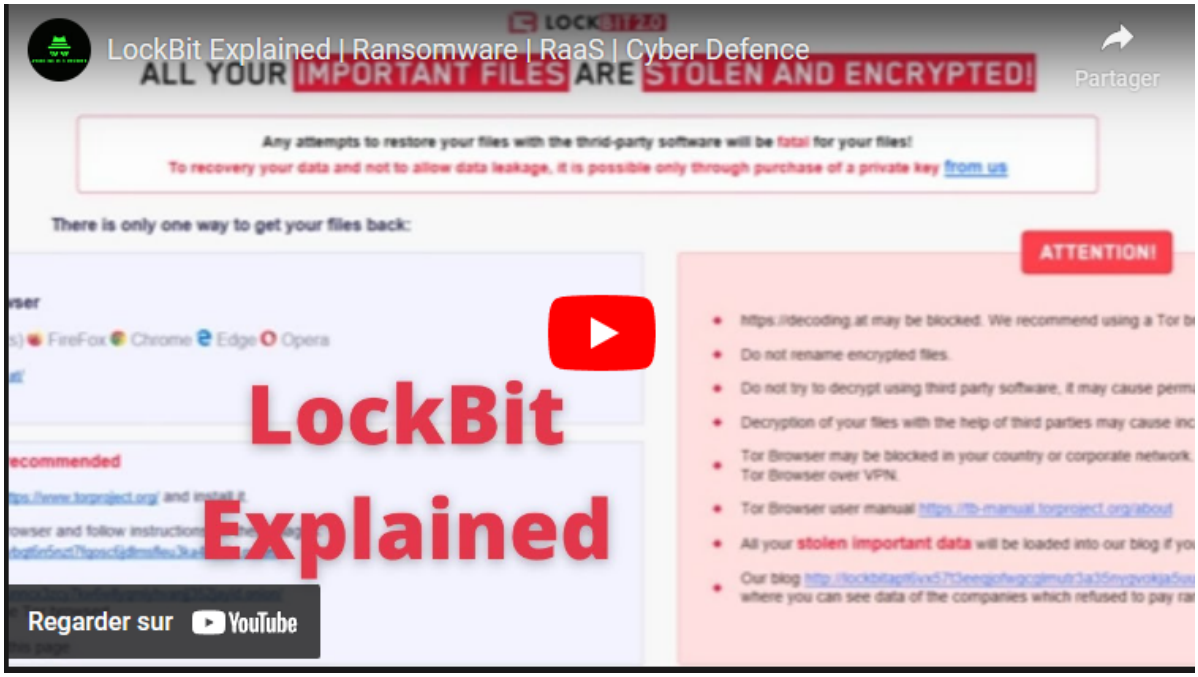
Aucun appareil ne peut être appelé complètement sécurisé.
Même avec les progrès technologiques réalisés au cours des dernières décennies, tous les appareils courent toujours le risque d'être infectés par un code malveillant.
Garantir une protection totale contre les virus et les logiciels malveillants est plus ou moins impossible, même les meilleurs programmes antivirus n'atteignant pas la barre des 100%.

Pour cette raison, la mince chance que votre appareil Apple rencontre un ransomware reste.

Quels types de rançongiciels ciblent les appareils Apple ?

Il existe de nombreux types de ransomware aujourd'hui, mais quels types sont connus pour cibler les produits Apple?

1. LockBit



Capture d'écran, pour visionner la vidéo, cliquer le lien YouTube suivant:

LockBit Explained | Ransomware | RaaS | Cyber Defence - YouTube

En ce qui concerne les ransomwares, LockBit est l'un des exemples les plus connus.
En fait, Malwarebytes a signalé que LockBit était le deuxième programme de ransomware le plus utilisé en mars 2023, juste derrière le ransomware CLOP.

LockBit est en fait une famille de ransomware, composée de trois variantes de ransomware distinctes.
Au moment d'écrire ces lignes, LockBit 3.0 est la variante la plus récente au sein de cette famille.

Il est devenu évident au début de 2023 que les MacBooks ne sont plus à l'abri du ransomware LockBit, bien que macOS ait réussi à échapper à cette menace pendant un certain temps.
En avril 2023, Bleeping Computer a déclaré que les opérateurs LockBit avaient créé des crypteurs pour cibler les appareils Mac pour la première fois.
On pense que cela a marqué la toute première campagne de ransomware axée sur macOS en particulier.

MalwareHunterTeam l'a annoncé après avoir découvert une archive ZIP sur VirusTotal. L'archive semblait contenir la plupart des crypteurs macOS LockBit disponibles à l'époque.
Les Mac fonctionnant sur la puce Apple Silicon étaient ciblés dans l'entreprise malveillante, bien qu'il semble que les crypteurs aient été conçus à l'origine pour attaquer les systèmes Windows.

Aucun cas d'attaques de ransomware macOS n'a été signalé en conséquence, mais cela ne veut pas dire que nous ne verrons pas les opérateurs LockBit cibler les appareils macOS dans un proche avenir.

2. ThiefQuest/EvilQuest

ThiefQuest (également connu sous le nom d'EvilQuest) est devenu une menace en juin 2020, après avoir été découvert par le chercheur Dinesh Devadoss.
Le programme a été trouvé caché dans des versions piratées de l'application Little Snitch, qui pouvait être trouvée sur une plate-forme torrent russe.

Cependant, il n'a pas fallu longtemps pour que ce programme ransomware soulève quelques sourcils.
ThiefQuest ne semblait pas agir comme un ransomware, car il contenait à la fois une porte dérobée et un code d'enregistrement de frappe.
Ce n'est pas du tout standard pour les ransomwares et a remis en question le malware de ThiefQuest et, avec un montant de rançon très faible, ThiefQuest lui-même.

Il s'est avéré que l'objectif de ThiefQuest n'était pas de crypter les données et de recevoir une rançon, ce qui est typique des ransomwares.
Il s'agissait plutôt d'un programme malveillant cherchant à voler des données précieuses.

Ce programme a réussi à infecter les appareils macOS, bien qu'il ne soit pas le premier programme de ransomware officiel à cibler macOS.
Comme indiqué précédemment, LockBit détient ce titre.

Comment éviter les ransomwares

Crédit d'image: Mike MacKenzie / Flickr

Il n'y a pas de solution unique pour éviter les ransomwares, mais il y a quelques choses que vous pouvez faire pour réduire le risque d'être victime de ce programme malveillant.

Tout d'abord, avoir un programme antivirus réputé installé est une nécessité.
L'antivirus est souvent la première ligne de défense contre les virus et les logiciels malveillants, et peut faire la différence entre conjurer et accueillir un programme malveillant.

Certains des meilleurs programmes antivirus disponibles aujourd'hui incluent:

- Mcafee.
- Norton.
- Kaspersky.
- **Bitdefender.**
- Malwarebytes.

Mais l'antivirus ne suffit pas toujours à échapper aux ransomwares, surtout si vous avez affaire à un programme sophistiqué.
Il existe d'autres avenues que vous devriez envisager de poursuivre, telles que l'utilisation de programmes anti-programme malveillant.
Les programmes antimalware ne sont pas un remplacement antivirus, mais les deux peuvent bien fonctionner en tandem.
Étant donné que les logiciels anti-programme malveillant peuvent détecter davantage de types de logiciels malveillants haut de gamme, vous pouvez rester à l'abri des programmes malveillants de base et complexes en les utilisant avec un programme antivirus de confiance.

Vous devez également vous assurer que tous les logiciels de votre appareil Apple sont tenus à jour, qu'il s'agisse de vos applications ou de votre système d'exploitation.
Les vulnérabilités logicielles sont couramment exploitées par les cybercriminels pour l'infection par des logiciels malveillants, car elles fournissent une porte ouverte dont les développeurs de logiciels peuvent ne pas être conscients.

Apple n'est pas étranger aux failles de sécurité, certaines ayant été exploitées dans le passé pour attaquer des victimes.
Grâce aux mises à jour, les failles et les vulnérabilités logicielles peuvent être corrigées, ce qui rend vos applications et votre système

d’exploitation plus sécurisés dans l’ensemble.

Il est également préférable de s’en tenir à des plates-formes réputées lors de l’installation d’applications.
Dans le cas des appareils Apple, utilisez l’App Store officiel d’Apple, car cette plate-forme vise à éliminer les applications malveillantes susceptibles d’héberger des ransomwares. Ne jailbreakez pas votre téléphone pour pouvoir télécharger du contenu à partir d’autres magasins d’applications, car ceux-ci pourraient ne pas être vérifiés.
Il est toujours préférable de rester dans le « jardin clos » d’Apple.

Prévention de la gravité des ransomwares

Il est utile de prendre certaines mesures pour réduire la gravité d’une attaque de ransomware si vous êtes ciblé.
Créer des sauvegardes de vos données (et les garder séparées de votre système) vous permet d’accéder à tous les fichiers cryptés en cas d’attaque de ransomware, ce qui signifie que vous n’êtes pas obligé de payer une rançon pour récupérer vos données.

Vous pouvez également envisager d’utiliser une plate-forme de stockage en nuage pour héberger vos fichiers, car il sera probablement plus facile d’accéder à nouveau à vos données lors d’une attaque de ransomware qu’à l’aide d’un disque dur.

Apple Ransomware n’est pas un mythe

Bien qu’Apple offre une protection de haute qualité à ses utilisateurs, les programmes de ransomware conçus pour exploiter les appareils iOS et macOS existent certainement. Prendre certaines précautions et faire attention à ce que vous faites en ligne peut vous aider à éviter ce type de programme néfaste, bien qu’il n’y ait aucun moyen de les couper complètement.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230806
"C'est ensemble qu'on avance"