Apple a posé le verrou final

La sécurité est pour Apple un argument marketing de poids, comme on le voit sur une page qui vante les mérites de la dernière version Big Sur de macOS :

> *Sécurité. Directement intégrée. Nous avons intégré dans le matériel et les logiciels du Mac des technologies avancées qui travaillent ensemble pour exécuter les apps de façon plus sécurisée, protéger vos données et garantir votre sécurité sur le Web.*

(source)

On sait que le prix des appareils Apple les met hors de portée de beaucoup d'internautes, mais c'est un autre prix que les inconditionnels d'Apple vont devoir accepter de payer, celui de la liberté de faire « tourner » des applications. Comme l'explique ci-dessous un responsable de la sécurité chez Librem (*la traduction Framalang conserve au dernier paragraphe quelques lignes qui font la promotion de Purism/Librem), la dernière version de macOS donne l'illusion du contrôle mais verrouille l'utilisateur, tant au niveau logiciel que matériel désormais.

Traduction Framalang : goofy, Julien / Sphinx, framasky, Steampark, mo

Apple a pris le contrôle sur ses utilisateurs

par Kyle Rankin

Kyle est *Chief Security Officer* chez Librem (Mastodon)

On entend souvent dire des pirates informatiques qu'ils ont « pris le contrôle » (en anglais *owned* ou *pwned*) d'un ordinateur. Cela ne veut pas dire qu'ils ont pris possession physiquement de l'ordinateur, mais qu'ils ont *compromis* l'ordinateur et qu'ils ont un contrôle à distance si étendu qu'ils peuvent en faire ce qu'ils veulent. Lorsque les pirates informatiques contrôlent un ordinateur, ils peuvent empêcher l'exécution de logiciels, installer les logiciels de leur choix et contrôler le matériel à distance, même contre la volonté du propriétaire et généralement à son insu.

Les pirates informatiques comprennent intuitivement une chose que beaucoup d'utilisateurs d'ordinateurs ne comprennent pas : la propriété n'est pas une question de *possession*, mais de *contrôle*. Si votre entreprise vous donne un ordinateur, ou même si vous apportez le vôtre, mais qu'elle contrôle à distance la façon dont vous l'utilisez et peut passer outre à vos souhaits, c'est l'ordinateur de l'entreprise, pas le vôtre. Selon cette définition, la plupart des téléphones, aujourd'hui, sont la propriété du vendeur, et non de l'utilisateur, et comme je l'ai exposé dans The General Purpose Computer in Your Pocket [1] :

> *L'un des plus beaux tours que Big Tech ait jamais joué a été de convaincre les gens que les téléphones ne sont pas des ordinateurs à usage général et qu'ils devraient suivre des règles différentes de celles des ordinateurs portables ou de bureau. Ces règles donnent commodément au vendeur un plus grand contrôle, de sorte que vous ne possédez pas un smartphone mais que vous le louez.*

> *Maintenant que le public a accepté ces nouvelles règles pour les téléphones, les vendeurs commencent à appliquer les mêmes règles aux ordinateurs portables et aux ordinateurs de bureau*

L'illusion du contrôle

L'illusion selon laquelle les utilisateurs d'Apple ont le contrôle de leurs ordinateurs a été rapidement mise à mal cette semaine quand Apple a distribué dans le monde entier sa nouvelle version de macOS « Big Sur ». Des utilisateurs ont commencé à remarquer dès la diffusion de la mise à jour qu'ils avaient des problèmes pour exécuter des applications locales : ces applications bégayaient et macOS lui-même ne répondait plus par moments, même si l'utilisateur n'avait pas encore mis à jour son OS vers Big Sur. Drôle de coïncidence que la sortie d'un nouvel OS puisse bloquer des applications locales et même des applications ne venant pas d'Apple.

Comme cet article d'Ars Technica l'explique, des utilisateurs ont été capables de déboguer ce problème assez rapidement :

> *Il n'a pas fallu longtemps à certains utilisateurs de Mac pour se rendre compte que `trustd`, le processus de macOS chargé de vérifier avec les serveurs d'Apple si une application est authentifiée, tentait de se connecter au domaine ocsp.apple.com mais échouait de manière répétée.*

… ce qui a provoqué des ralentissements sur tout le système, entre autres quand les applications essayaient de se lancer. Pour résumer le problème, à chaque fois que vous lancez une application signée sur macOS, un service d'enregistrement « notarial » envoie des informations sur l'application aux serveurs d'Apple pour vérifier que les signatures concordent. Si c'est le cas, votre système d'exploitation autorise l'application à démarrer. Quand l'ordinateur est hors connexion, la vérification échoue mais l'application est encore autorisée à fonctionner. Mais quand l'ordinateur est connecté, la signature est appliquée et comme le service était actif mais lent, les applications se sont arrêtées pendant que le système d'exploitation attendait une réponse.

La prise de contrôle à distance grâce à la signature du code.

Les applications utilisent souvent la signature du code comme moyen pour l'utilisateur de détecter les altérations. Le développeur signe le logiciel avec sa clé privée et l'utilisateur peut vérifier cette signature avec une clé publique. Seul le logiciel qui n'a pas été modifié correspondra à la signature. Dans le monde du logiciel libre, les distributions comme PureOS comprennent des clés publiques installées sur l'ordinateur local, et les mises à jour de logiciels vérifient automatiquement que les signatures correspondent avant d'appliquer la mise à jour elle-même. Quand on utilise ainsi les signatures, on peut tester une application avant son installation pour savoir si elle a été modifiée, c'est ainsi que l'utilisateur bénéficie d'un contrôle total sur le processus.

Apple a fait franchir à la signature de code un pas supplémentaire en incluant ce service « notarial ». Toutes les applications signées, qu'elles viennent ou non d'Apple, doivent demander l'autorisation de démarrer au service notarial distant. Ce qui signifie que l'entreprise Apple non seulement connaît toutes les applications que vous avez installées, mais elle est informée aussi **à chaque fois que vous les exécutez**. Ce qui n'était autrefois qu'un service facultatif est devenu aujourd'hui obligatoire. À partir de Big Sur, vous ne pourrez plus utiliser un outil comme Little Snitch pour bloquer ce service, ni le faire passer par Tor pour gagner en confidentialité. Apple et tous ceux qui ont accès à la communication en texte brut peuvent savoir quand vous avez lancé le navigateur Tor ou d'autres outils nécessaires à la protection de la vie privée, ou encore à quelle fréquence vous utilisez des applications de la concurrence.

***[Mise à jour** : il semble que les services notariaux d'Apple n'envoient pas d'informations sur l'application, mais envoient plutôt des informations **sur le certificat de développeur** utilisé pour les signer (ce qui est plus logique étant donné la façon dont l'OSCP fonctionne). Cela signifie qu'Apple peut savoir, par exemple, que vous avez lancé une application de Mozilla, mais ne peut pas nécessairement dire si vous avez lancé Firefox ou Thunderbird. Si un développeur ne signe qu'une seule application, bien sûr, on peut établir une corrélation entre le certificat et l'application. Le service semble également mettre en cache une approbation pendant un certain temps, de sorte que le fait qu'il envoie des informations à Apple chaque fois que vous exécutez une application dépend de la*

fréquence à laquelle vous la lancez].

J'imagine que beaucoup de personnes ont été surprises de découvrir cette fonctionnalité, mais je soupçonne également que beaucoup l'accepteront au nom de la sécurité. Pourtant, comme c'est le cas pour de nombreuses fonctionnalités d'Apple, la sécurité est un terme de marketing alors que la véritable motivation c'est le contrôle. Alors que la signature de code permettait déjà à Apple de contrôler si vous pouviez installer ou mettre à jour un logiciel, cette fonctionnalité lui permet de **contrôler si vous pouvez exécuter des applications**. Apple a déjà utilisé la signature de code sur iOS pour retirer les applications de ses concurrents de l'App Store et aussi pour désactiver à distance des applications au prétexte de la sécurité ou de la confidentialité. Il n'y a aucune raison de croire qu'ils n'utiliseront pas le même pouvoir sur macOS maintenant qu'il ne peut plus être contourné. Le but ultime d'Apple avec la signature de code, son coprocesseur Secure Enclave et sa puce Silicon propriétaires, c'est de s'assurer le contrôle et la propriété totales du matériel que vend l'entreprise.

Reprenez le contrôle

Vous devriez demeurer en pleine possession des ordinateurs que vous achetez. Ni les pirates informatiques ni les vendeurs ne devraient avoir le droit de vous contrôler à distance.
Nous construisons des ordinateurs portables, des ordinateurs de bureau, des serveurs et des téléphones sûrs, respectueux de la vie privée et de la liberté, qui vous redonnent le contrôle et vous garantissent que lorsque vous achetez un ordinateur Purism, c'est vous qui en êtes vraiment propriétaire.

Voir aussi :

- Un autre article de Jeffrey Paul sur la question
- Tristan Nitot réagit vivement

« Secure. » par Wysz, licence CC BY-NC 2.0