Prenez garde à ce virus sur ordinateur Mac qui vise vos données personnelles

François Charron :

Capture d'écran, pour visionner la vidéo, cliquer le lien suivant de François Charron:

Prenez garde à ce virus sur ordinateur Mac qui vise vos données personnelles (francoischarron.com)

Les chercheurs en sécurité informatique de la firme Guardz alertent les utilisateurs d'ordinateurs Mac face à un dangereux virus.
Nommé ShadowVault, ce logiciel malveillant cible spécifique les ordinateurs et systèmes macOS d'Apple dans le but d'extirper les données personnelles des utilisateurs, les mots de passe, cartes de crédit, les témoins (cookies) de navigation et clés de portefeuilles de cryptomonnaies.

C'est un mythe qui doit constamment être déboulonné; les ordinateurs Mac d'Apple ne sont pas à l'abri des virus et logiciels malveillants!

En effet, on retrouve de nombreuses menaces dans l'écosystème de la pomme.

La différence avec les PC et les appareils Android, c'est qu'il y en a moins sur Mac.
Ceci s'explique par le fait qu'il y a largement plus d'utilisateurs de PC et d'appareils Android dans le monde.
Il y a donc plus de proies potentielles.

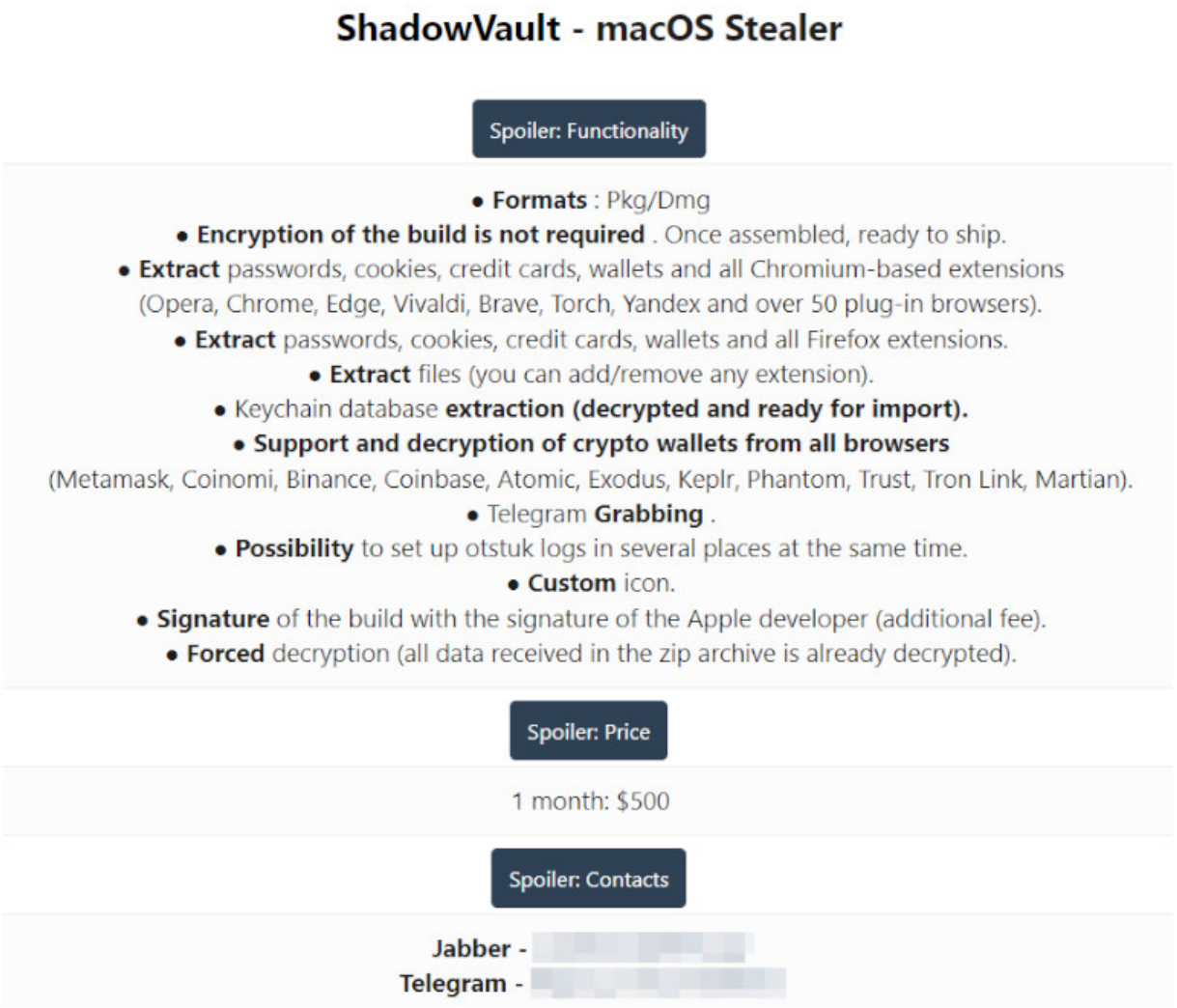
Ceci ne veut pas pour autant dire que les détenteurs de Mac ne sont pas des proies potentielles eux aussi.
En fait, ça en fait des proies de choix, puisque les utilisateurs de produits Apple sont généralement plus fortunés.

C'est cet élément qui semble justement intéresser les pirates informatiques utilisant le logiciel malveillant ShadowVault.

Qu'est-ce que le logiciel malveillant ShadowVault?

Ce sont des chercheurs en sécurité informatique de la firme israélienne Guardz qui ont publié un rapport sur le virus ShadowVault.

Ces derniers ont notamment aperçu des annonces pour ce logiciel malveillant sur le dark web.



Un exemple d'annoncer pour le logiciel malveillant ShadowVault. Crédit image: Guardz.

Son but est de voler les données personnelles des utilisateurs de Mac, les mots de passe, carte de crédit et témoins (cookies) de navigations.

À ce sujet, le virus en question viserait particulièrement les extensions des navigateurs web:

- Chrome
- Firefox
- Edge
- Brave
- Vivaldi
- Opera

Enfin, ShadowVault viserait aussi les portefeuilles de cryptomonnaies:

- Metamask
- Coinomi
- Binance
- Coinbase
- Atomix
- Exodus
- Keplr
- Phantum
- Trust

- Tron Link et
- Martian

Comment se propage le virus ShadowVault?

Le virus pour Mac ShadowVault est vendu sur le dark web pour 500$ par mois.
C'est donc dire que n'importe quel apprenti pirate qui le désire peut se le procurer.

Il est donc libre à ceux-ci de trouver le moyen de le propager et infecter les Mac.

De facto, il faut s'attendre à ce qu'il se propage via des courriels d'hameçonnage ainsi que des sites frauduleux.

Mais là où c'est particulièrement inquiétant, c'est qu'on remarque dans l'offre publicitaire que les concepteurs de ShadowVault vendent aussi une signature logicielle de développeurs d'Apple.

Cette licence est essentielle pour pouvoir publier une application sur l'App Store.
C'est d'ailleurs un des mécanismes de défense d'Apple pour éviter que des logiciels malveillants ne s'y infiltrent.
Ces derniers attribuent des licences à des développeurs certifiés.

Est-ce que les pirates mentent dans leur annonce?
Ce n'est pas impossible.
Mais il ne faut pas non plus écarter la possibilité que le virus s'infiltre dans des applications disponibles sur l'App Store.

Comment savoir si l'on a le virus ShadowVault sur Mac?

Comme bien d'autre virus, le logiciel malveillant ShadowVault est configuré pour être discret et agir en arrière-plan.

Ceci fait en sorte qu'il peut être difficile de remarquer une activité suspecte sur notre ordinateur.

Comment éviter et enlever un virus sur un ordinateur Apple?

La vigilance est toujours de mise afin d'éviter d'installer un virus comme ShadowVault sur notre ordinateur Mac.

Il est important de savoir comment reconnaître les courriels d'hameçonnage, détecter les sites frauduleux et reconnaître les liens suspicieux.

Mais l'ultime défense demeure de se procurer une des meilleures solutions de protection pour Mac.

La prestigieuse organisation indépendante AV-Compratives a d'ailleurs publié son rapport des meilleurs antivirus pour Mac.

Avec une solution de protection, non seulement on est averti lorsqu'on ouvre un courriel, un site ou un lien dangereux, mais il va également aider à bloquer l'installation de virus et logiciel malveillant.

Ça peut également nous aider à retirer une menace si on l'installe après coup.

Évidemment, le but est de se protéger avant!

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230715
"C'est ensemble qu'on avance"