Alerte : 2 applications infectées sous Android et macOS

Alerte : 2 applications infectées sous Android et macOS

Les chercheurs ESET® ont découvert 2 menaces, l'une agissant sous macOS® et l'autre sous Android™. Le malware sous macOS a fait 1 000 victimes. Quant à la menace sous Android, plus de 5 500 téléchargements ont été effectués.

OSX/Proton, ou le voleur de données

Les chercheurs ESET sont entrés en contact avec l'éditeur Eltima®, à la suite de la découverte d'une version de leurs applications compromises. Environ 1 000 utilisateurs auraient été infectés par le kit OSX/Proton, disponible sur les marchés underground.

Les applications Elmedia Player® (lecteur multimédia) et Folx® (gestionnaire de téléchargement) sont concernées. OSX/Proton est une backdoor qui possède de nombreuses fonctionnalités et permet de récupérer :

• les détails de l'OS : numéro de série de l'appareil, nom complet de l'utilisateur actuel…
• les informations provenant des navigateurs : historique, cookies, marque-pages, données de connexion…
• les portefeuilles de cryptomonnaie : Electrum / Bitcoin Core / Armory
• les données contenues dans ./ssh
• le trousseau macOS grâce à une version modifiée de chainbreaker
• la configuration du VPN Tunnelblick®
• les données GnuPG
• les données de 1password
• la liste de toutes les applications installées

ESET fournit la liste des indicateurs de compromission ainsi que la méthode de nettoyage en cas d'infection sur le lien suivant : https://www.welivesecurity.com/2017/10/20/osx-proton-supply-chain-attack-elmedia/

Cryptomonnaie : une version compromise de Poloniex® sur Google™ Play

Avec plus de 100 cryptomonnaies au compteur, Poloniex est l'un des principaux sites d'échange de cryptomonnaie au monde. Les cyberpirates ont profité du fait qu'il n'y ait pas d'application officielle de Poloniex pour développer 2 versions malicieuses.

En plus de récolter les identifiants de connexion à Poloniex, les cybercriminels incitent les victimes à leur accorder l'accès à leur compte Gmail™. Les pirates peuvent ensuite effectuer des transactions depuis le compte de l'utilisateur et effacer toutes les notifications de connexions et de transactions non autorisées depuis la boîte de réception.

La première des applications malveillantes se nomme « POLONIEX » et a été installée 5 000 fois, malgré les avis négatifs. La deuxième application, « POLONIEX EXCHANGE », a été téléchargée 500 fois avant d'être retirée du Google store, suite à la notification d'ESET.

Vous trouverez les mécanismes utilisés par les pirates et les moyens de se prémunir contre ce malware en cliquant sur le lien suivant :
https://www.welivesecurity.com/2017/10/23/fake-cryptocurrency-apps-google-harvesting-credentials/

LE NET EXPERT

:

• **SENSIBILISATION / FORMATIONS** :
- **CYBERCRIMINALITÉ**
- **PROTECTION DES DONNÉES PERSONNELLES**
- AU **RGPD**
- À LA **FONCTION DE DPO**
• **MISE EN CONFORMITÉ RGPD / CNIL**
- **ÉTAT DES LIEUX RGPD** de vos traitements)
- **MISE EN CONFORMITÉ RGPD** de vos traitements
- **SUIVI** de l'évolution de vos traitements
• **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
- ORDINATEURS (**Photos / E-mails / Fichiers**)
- TÉLÉPHONES (récupération de **Photos / SMS**)
- SYSTÈMES NUMÉRIQUES
• **EXPERTISES** & **AUDITS** (certifié ISO 27005)
- TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES
- **SÉCURITÉ** INFORMATIQUE
- SYSTÈMES DE **VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité**, **Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).

Réagissez à cet article

Source : *Boîte de réception (715) – denis.jacopini@gmail.com – Gmail*