Ransomwares : des clés pas toujours si privées

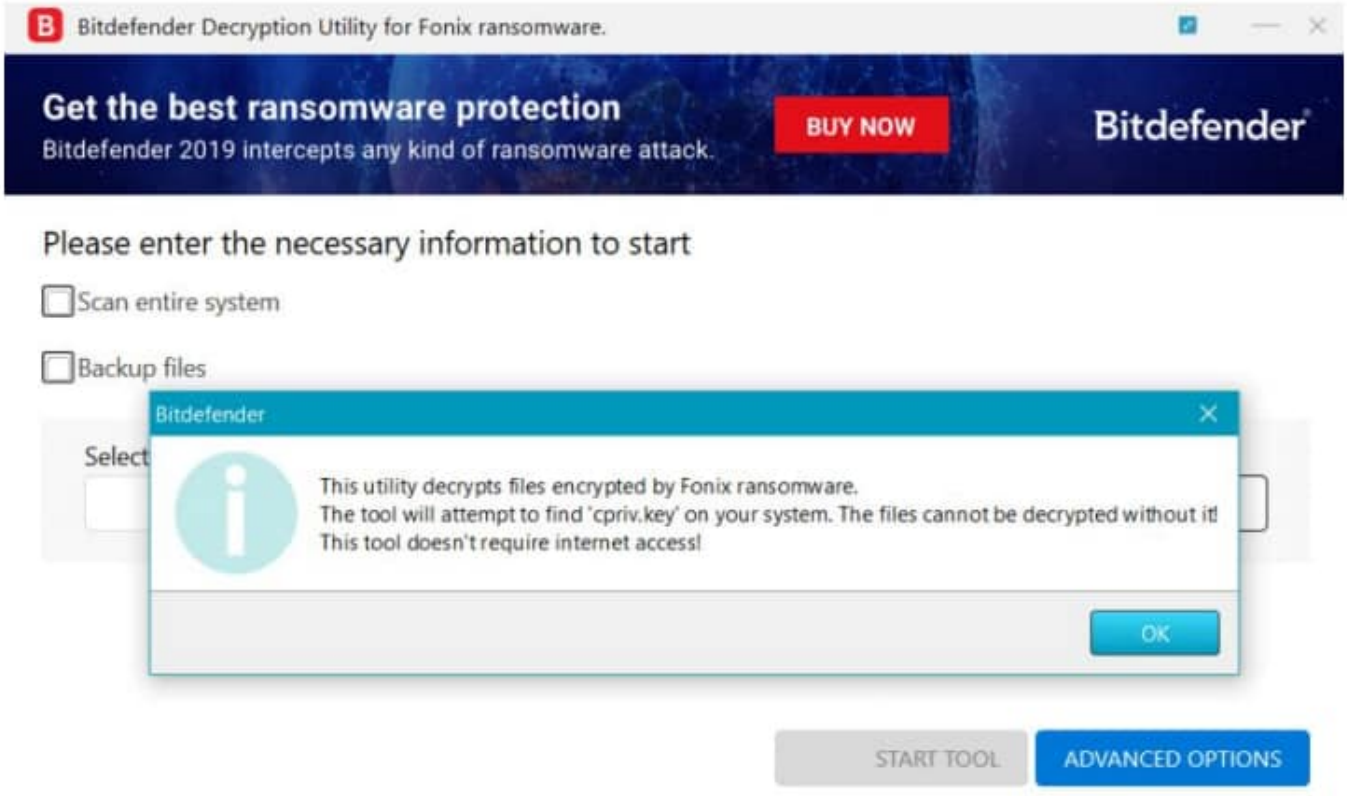
Victimes de *ransomwares*, conservez vos fichiers chiffrés même si vous n'avez pas l'intention de payer : un jour peut-être, la clé sortira. Kaspersky l'avait rappelé il y a quelques semaines, à l'heure où Fonix arrivait en fin de parcours.

> *End of FonixCrypter Project :#Fonix #ransomware #XINOF #FonixCrypter #close_project #hack #Malware #raas #ransomware_as_a_service pic.twitter.com/wQdmp61juX*
>
> *— fnx (@fnx67482837) January 29, 2021*

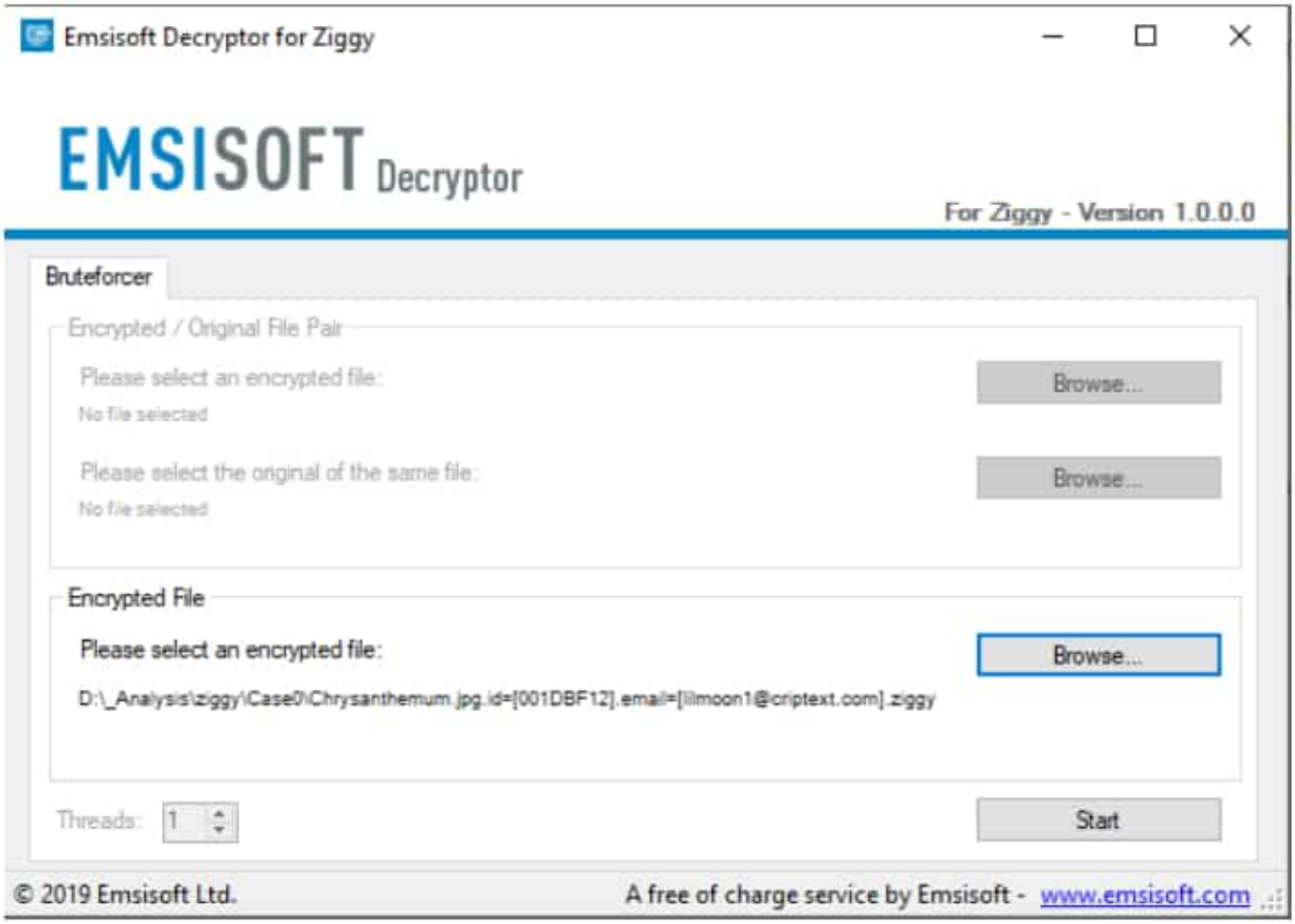
Parallèlement à la fermeture du projet, la clé de chiffrement maîtresse avait été publiée.

> *Fonix Ransomware Master RSA Key (Spub.key & Spriv.key) and Sample Decryptor : #Fonix #ransomware #XINOF #FonixCrypter #close_project #hack #Malware #raas #ransomware_as_a_servicehttps://t.co/JcijzvOKvf*
>
> *— fnx (@fnx67482837) January 29, 2021*

La publication de cette clé a permis le développement d'outils de déchiffrement. On en retrouve, en particulier, un sur le site de No More Ransom.



Un autre *ransomware* a suivi la même voie : Ziggy. Début février, ses créateurs ont signé son arrêt de mort. Ils ont publié, à cette occasion, un fichier contenant près d'un millier de clés pour autant de victimes. Et y ont adjoint un outil de déchiffrement prêt à l'emploi. Ainsi que le code source d'un deuxième outil, repris là aussi sur No More Ransom.



Quand les clés privées deviennent publiques

Récemment, les exploitants de Ziggy s'étaient engagés à rembourser les victimes. Ils viennent de se dire officiellement prêts, invitant les intéressés à leur envoyer un mail avec la preuve de paiement et un identifiant de machine infectée. La somme – réglée en bitcoins – serait restituée sous deux semaines…

En toile de fond, des opérations internationales de police survenues ces derniers temps contre plusieurs ransomwares. Parmi eux, le « poids lourd » Egregor.

> *To all #Ziggy ransomware victims who paid money:*
> *Contact ziggyransomware@secmail.pro for giving your money back.@BleepinComputer @malwrhunterteam @demonslay335 https://t.co/tP0ngMXNyi pic.twitter.com/GNf7icMQiQ*
>
> *— M. Shahpasandi (@M_Shahpasandi) March 28, 2021*

Pas de clés ni de remboursement pour Mamba (HDDCryptor), mais une faiblesse qui pourrait donner de l'espoir aux victimes. Ce *ransomware*, actif depuis des années, s'appuie sur le logiciel *open source* DiskCryptor.
Il se trouve que la clé de chiffrement est stockée dans le fichier de configuration de ce logiciel… et que le fichier est accessible en clair. En tout cas pendant le processus de chiffrement, qui dure environ deux heures. Une fois la machine relancée et la note de rançon affichée, il est trop tard.

Illustration principale © lolloj – Shutterstock