SODICOM ORGANISATION

WOOXO
IT security for business continuity

Bulletin de prévention
Novembre 2016

BETABOT - CERBER, L'ASSOCIATION D'UN VOLEUR ET D'UN BRAQUEUR... ATTENTION, TANDEM EXPLOSIF !

► Betabot - Ceber : qu'est-ce que c'est ?

Le cheval de Troie BETABOT, comme le rançongiciel CERBER sont deux acteurs bien connus du paysage cybercriminel. Le premier s'emploie à dérober les mots de passe stockés sur les équipements infiltrés, le second les infecte et crypte les données qui y sont stockées afin de rançonner les victimes.

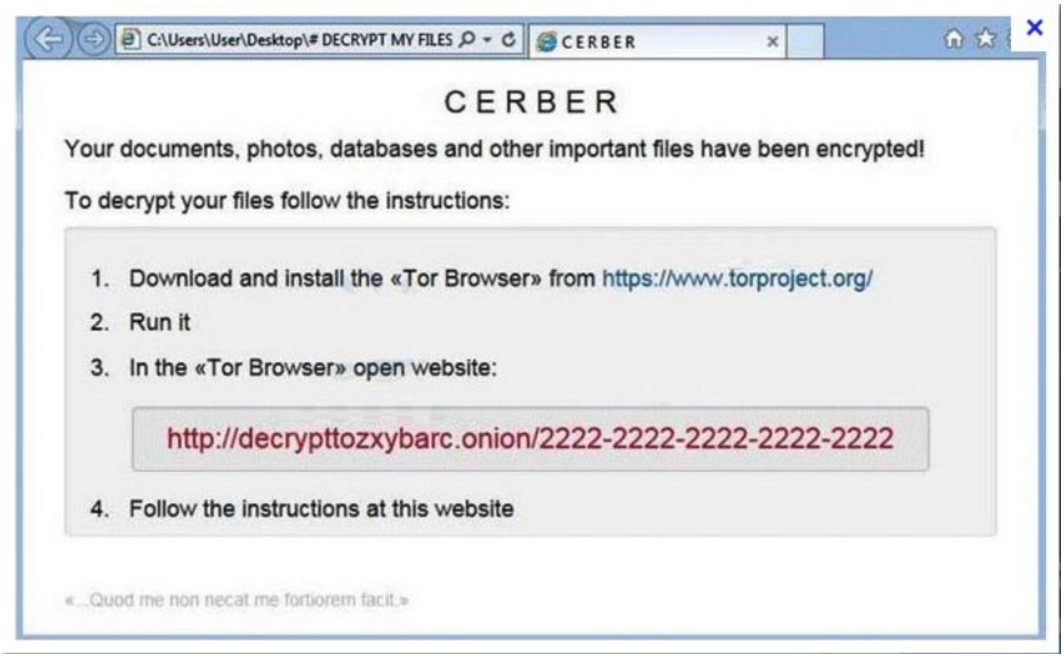
Ce qui est **nouveau**, c'est leur **association diabolique** afin d'accroître la rentabilité des campagnes malveillantes menées par des cybercriminels.

Au produit de la vente des mots de passe dérobés sur le dark net (en moyenne 170€), s'ajoute le fruit de la rançon : 1 bitcoin (646€), payée dans plus d'un tiers des cas en milieu professionnel.

► Comment se déroule la contamination ?

De nombreuses campagnes de **spams** déferlent dans les boites aux lettres des messageries professionnelles depuis le mois de juillet. Les messages contiennent en pièce jointe **un document Word modifié pour contenir des scripts macro de Betabot** : CVs, factures, bons de livraison ... Le cheval de troie est protéiforme afin d'optimiser le taux d'ouverture des pièces jointes et activer les scripts afin de lancer le téléchargement et l'installation de Betabot.

Une fois que les **mots de passe** ont été **volés**, **le Betabot télécharge et exécute le ransomware Cerber.** Ce dernier va généralement s'activer au redémarrage du poste et chiffrer l'ensemble des fichiers trouvés. Les victimes sont alors invitées, au travers d'une boîte de dialogue, à payer un bitcoin pour obtenir la clé de déchiffrement supposée leur permettre de récupérer leurs fichiers.



Boîte de dialogue du Ransomware Betabot - Cerber

► Que faire pour se prémunir ?

Ne pas ouvrir les documents en pièces jointes d'un message électronique non sollicité.

Désactiver l'exécution automatique des macros dans les suites bureautiques
[Rappel pour la désactivation dans Microsoft Office :
Fichier / Options / Centre de gestion de la confidentialité / Paramètre du Centre de gestion de la confidentialité / Paramètres des macros / Cochez Désactiver toutes les macros avec notifications]

Maintenir à jour le système d'exploitation et l'antivirus de vos postes de travail

Effectuer des sauvegardes saines et fréquentes des systèmes et des données (postes de travail, serveurs mais aussi ordinateurs portables itinérants) et conserver un minimum de 3 versions pour chaque document sauvegardé. Pour rappel les disques durs externes ne sont pas des dispositifs de sauvegarde fiables, ils peuvent être cryptés par les Rançongiciels. **Optez pour une appliance de sauvegarde professionnelle.**

► Que faire en cas de survenance d'une telle attaque ?

Si vous avez malencontreusement cliqué sur le lien et téléchargé Betabot, il est trop tard pour éviter le vol de vos mots de passe, nous vous recommandons **d'éteindre immédiatement le poste infecté et de le déconnecter du réseau.**

L'objectif est de bloquer le travail du parasite et si possible sa diffusion sur le réseau.

Recherchez et supprimez tous les messages similaires dans les messageries des utilisateurs connectés à votre réseau.

Procédez enfin à une **réinstallation complète** du poste infecté et à la **restauration des fichiers à partir d'une sauvegarde réputée saine**.

Pensez aussi à modifier tous vos mots de passe pour éviter leur utilisation malveillante par les acheteurs potentiels mal intentionnés.

Si vous disposez d'un Plan de reprise d'activité, vous pourrez récupérer toutes vos données après un reformatage complet de votre disque dur et une restauration complète de vos sauvegardes.