TA flash

TAF16/1013
10/10/2016

Software

Objet : TA TITAN : une appliance GED & Backup haute sécurité

Modèles compatibles : MFP TA Triumph-Adler

Présentation / positionnement

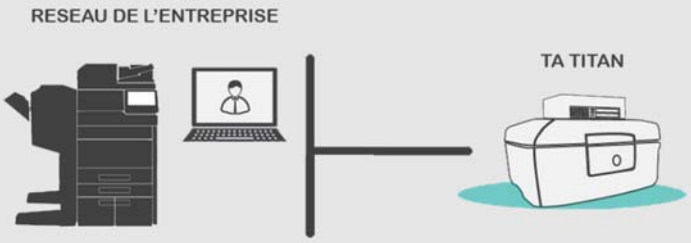
TA TITAN PERMET DE LUTTER CONTRE LES HACKERS !

La menace est grandissante, les attaques se multiplient : les rançongiciels* sont désormais un fléau… et TA TITAN FAIT FACE A CES VIRUS !

**ransonware ou cryptolocker*

Comment ?

Vos données stockées dans TA TITAN® via votre MFP TA Triumph-Adler ou vos ordinateurs peuvent-elles être attaquées par un rançongiciel ?



QU'EST-CE QU'UN RANÇONGICIEL (= RANSONWARE OU CRYPTOLOCKER)

C'est un micro-logiciel en .exe , caché sous un document au format PDF par exemple, bien souvent envoyé par e-mail : « Bonjour, vous trouverez ci joint notre facture n°12345 etc… ». La personne, intriguée par une facture, ouvre le fichier… Et là, c'est la catastrophe : l'exécutable caché sous une apparence pdf se lance, et crypte tous les fichiers de l'ordinateur… Pour les décrypter, le hacker demande une rançon… de 100 à 500 $ en fonction de ses envies du moment… et s'il le décide la somme demandées peut augmenter.

Tous les types de fichiers sont concernés, et principalement les plus courants dont doc, docm, docx, eps, indd, jpg, odt, pdf, ppt, pptm, pptx, psd, xls, xlsb, xlsm, xlsx…

QUE FAIT TA TITAN® FACE AU CRYPTOLOCKER ?

Que faire si le logiciel e-kup sauvegarde dans TA TITAN® le .pdf derrière lequel se cache le .exe de locking ?

Aucune inquiétude à avoir.
TA TITAN® ne lance pas d'exécutables (.exe) [sauf ceux installés par nos soins].

En clair : TA TITAN® l'enregistre… et puis c'est tout. Il n'attaquera en aucun cas les données sauvegardées dans TA e-kup ou TA-GEIDE… Enfin, TA TITAN® ne reçoit pas de mails, donc il ne peut pas recevoir directement le .exe sur les disques.

Et si un super-hacker arrive à pénétrer sur le réseau sécurisé de l'entreprise, qu'il pirate TA TITAN®, et qu'il arrive à lancer un .exe sur les disques du TITAN® ?

Il ne peut pas écrire sur les disques du TA TITAN®, bloqués par et pour e-kup… Seul TA e-kup peut les utiliser et agir dessus.

Oui, mais partons dans l'idée que le super-hacker arrive à faire quelque chose d'infaisable et arrive à lancer son ransonware.exe sur un disque dur du TA TITAN® ?

TA TITAN Backup® enregistre les fichiers dans deux formats qui n'intéressent pas les cryptolockers, pour la simple et bonne raison que ces deux extensions utilisées pour compacter et crypter les packs sont UNIQUEMENT utilisées par et pour la solution TA e-kup…

Toujours dans cette optique de gain de temps dans le cryptage des données, les crytpolockers ne s'attaquent pas à des fichiers exotiques alors qu'ils font face à des millions d'utilisateurs avec des fichiers .doc, mp3 et autres photos… Ce n'est pas une opération rentable pour eux. Ainsi, nous vous confirmons qu'il ne peut rien arriver aux données…

Au secours ! J'ai ouvert facture.pdf qui était en fait facture.exe… Tout est crypté, que faire?

Pas de soucis !
Même si la dernière sauvegarde a enregistré la version cryptées de vos fichiers, les 30 dernières versions sont encore disponibles… On peut donc récupérer l'avant-dernière sauvegarde : celle d'hier, où vous n'aviez pas encore ouvert le fichier-rançon ! Et vous ne perdrez rien.

Oui ! Mais je l'ai aussi enregistrée dans TA-Geide, cette fameuse facture !

Pas de soucis ! TA-Geide ne permet pas d'ouvrir de .exe… Supprimez-le fichier, tout simplement.

Avantages

LA PÉRENNITÉ :
Protection de votre patrimoine documentaire : TA TITAN® est un réel outil de protection de votre patrimoine documentaire. Notre procédé logiciel rend indélébile et inaltérable l'ensemble des documents sauvegardés

Principaux bénéfices

Optimisation de la sécurité de l'information et des documents

Retrouvez l'ensemble des « TA Flash » sur notre site internet Pro (connexion avec login et mot de passe) www.triumph-adler.fr, Rubrique TA Flash.

Pour plus d'informations, merci de contacter le Service Marketing TA Triumph-Adler : marketing@triumph-adler.fr