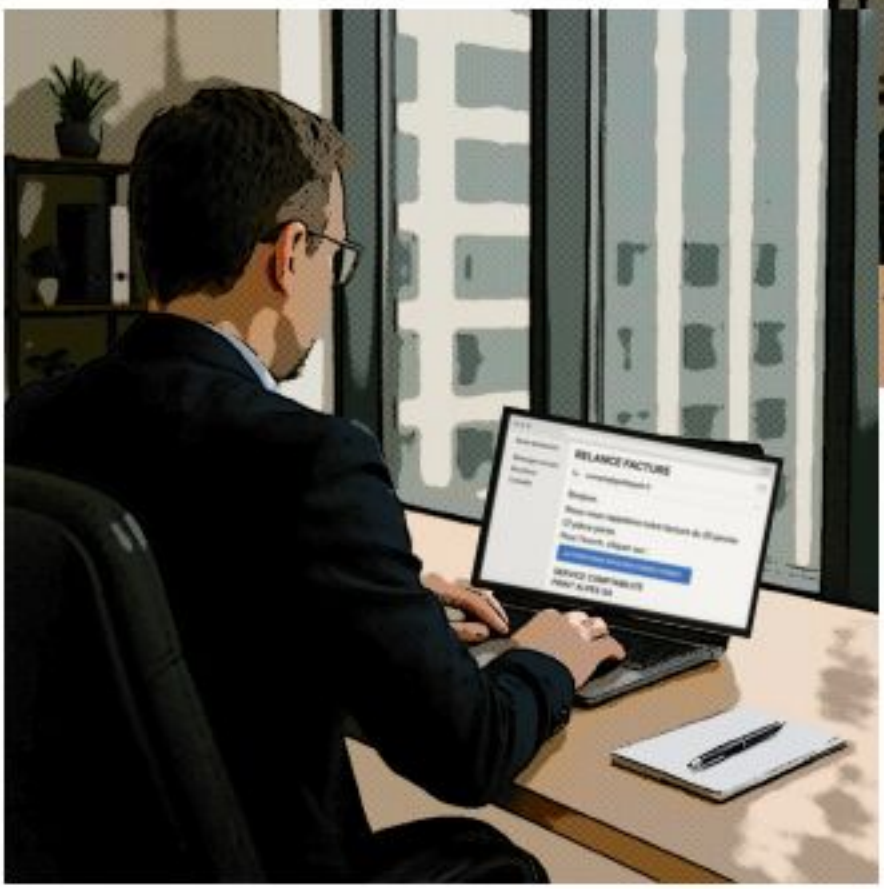
MAURICE, RACONTE-NOUS LA CYBER ATTAQUE DU 02 AVRIL 2025 !

ET BIEN VOICI LA CYBER ATTAQUE DU 02 AVRIL, TELLE QUE JE L'AI VÉCUE.

MARDI 2 AVRIL CHEZ S.A. GOLD APPLE, EQUIPEMENTIER AUTOMOBILE DE 75 EMPLOYÉS - C.A. 9M€ - TOUT VA BIEN ...

... MARDI 2 AVRIL 9H03 TOUT VA BIEN ÉGALEMENT POUR JEAN-LOUIS, DIRECTEUR FINANCIER, QUI OUVRE SON PORTABLE...

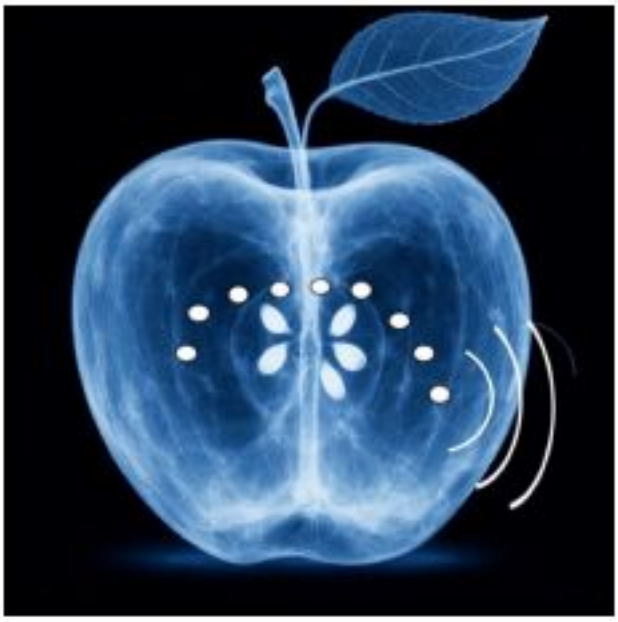


PUIS IL OUVRE SON PREMIER MAIL. OBJET : RELANCE FACTURE, AVEC UNE PIÈCE JOINTE : LA COPIE DE LA FACTURE.

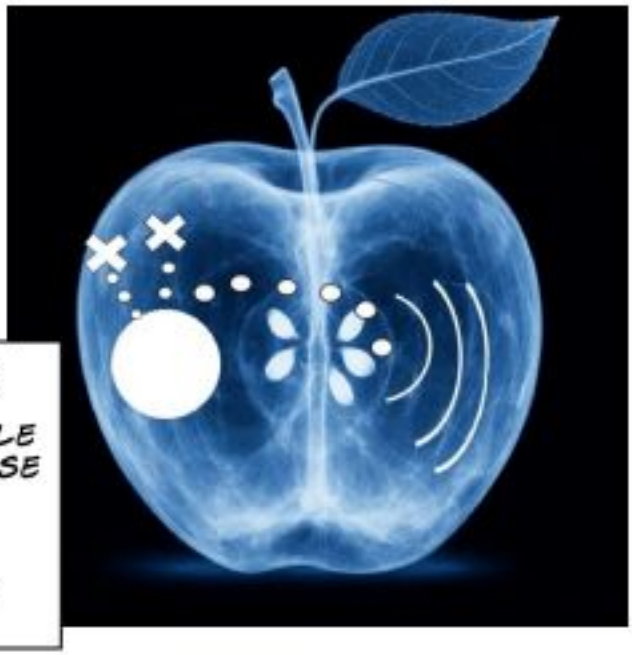
UNE FACTURE IMPAYÉE ?, SE DIT-IL, CE N'EST PAS LE STYLE DE LA MAISON !

MAIS LA PIÈCE JOINTE S'OUVRE SUR :

TOUT VA ENCORE BIEN POUR LA "SA GOLD APPLE", MAIS JEAN-LOUIS NE LE SAIT PAS ENCORE, UNE CONNEXION ANORMALE S'EST CRÉÉE DE SON POSTE VERS UN SERVEUR AUX USA



JEAN-LOUIS NE LE VOIT PAS, MAIS UN OUTIL SE CHARGE EN MÉMOIRE, RÉCUPÈRE LES IDENTIFIANTS DE SESSION ET REBONDIT VERS UN SERVEUR DE FICHIERS.



JEAN-LOUIS NE LE SAIT PAS ENCORE, MAIS L'ATTAQUANT DÉSACTIVE LES SAUVEGARDES CONNECTÉES, REPÈRE LE CONTRÔLEUR DE DOMAINE ET IL POUSSE UN EXÉCUTABLE SUR UNE DIZAINE DE MACHINES EN S'APPUYANT SUR LES DROITS D'UN ANCIEN COMPTE D'ADMINISTRATEUR RESTÉ ACTIF POUR L'INFOGÉRANCE.

– A 11H03, LES FICHIERS SONT COPIÉS ET CHIFFRÉS : TOUT EST CADENASSÉ ...
BACKUP
ON
S.A.GOLD APPLE
02 AVRIL, 11H04, L'ATTAQUANT SORT DE L'OMBRE ET APPARAIT SUR TOUS LES ÉCRANS.
VOS DONNÉES SONT CHIFFRÉES ET COPIÉES.
PAYEZ 10 BTC SOUS 72H
AH ZUT !

MARDI 2 AVRIL 11H20 – GESCO EST CONVOQUÉ À LA RÉUNION DE CRISE CHEZ SA GOLD APPLE.

MERCREDI 3 AVRIL – PREMIÈRES INTERVENTIONS DES URGENTISTES DATTAK

JEUDI 4 AVRIL - 16H35
RÉUNION DE CRISE DE LA 72ÈME HEURE

ET C'EST ENFIN L'HEURE DU BILAN...

CÔTÉ COMMUNICATION, LES SPÉCIALISTES "GESTION DE CRISE" DE DATTAK AIDENT À CADRER LES MESSAGES.
TROIS CLIENTS CRITIQUES SONT APPELÉS DANS L'APRÈS-MIDI.
AUCUNE ACTION NE LEUR EST DEMANDÉE.
LE DPD* PRÉPARE UN SIGNALEMENT À L'AUTORITÉ DE PROTECTION DES DONNÉES.
PLAN DE COMMUNICATION PRÊT, PAS DE PANIQUE.

* DÉLÉGUÉ À LA PROTECTION DES DONNÉES

... DÉSORMAIS, CHAQUE FOIS QU'UN SALARIÉ SE VERSE UN CAFÉ, UNE AFFICHE LUI RAPPELLE LA RÈGLE ÉLÉMENTAIRE DE SÉCURITÉ INTERNET :

ET AUJOURD'HUI, 29JANVIER 2026, 16H, M. DAMIEN DAMMANE, VOULEZ-VOUS PRENDRE LA PAROLE ...

... EN TANT QUE PDG DE DATTAK ?

MERCI DE ME DONNER LA PAROLE DANS DANS VOTRE 32ÈME VISIO-CONFÉRENCE ...

... PERMETTEZ-MOI DE PROFITER DE CETTE OCCASION POUR VOUS DONNER LES RÈGLES D'OR DE LA SÉCURITÉ INFORMATIQUE :

- DÉSACTIVER PAR DÉFAUT LES MACROS,
- MAINTENIR SÉPARÉS LES COMPTES ADMINS,
- DEMANDER SYSTÉMATIQUEMENT LA MFA,
- TESTER MENSUELLEMENT LES SAUVEGARDES 3-2-1,
- FORMALISER LES EXERCICES DE SÉCURITÉ ...

... SANS OUBLIER L'AFFICHETTE AU-DESSUS DE LA MACHINE À CAFÉ !

ET SOUHAITANT VOUS RENCONTRER PROCHAINEMENT? PAR EXEMPLE POUR UN AUDIT SÉCURITÉ DE VOTRE SYSTÈME D'INFORMATION.

UN DE VOS INTERVENANTS M'A CONFIÉ QUE POUR LUI, IL Y AURAIT UN "AVANT" ET UN "APRÈS" LE 02 AVRIL 2025

ET POUR UNE GARANTIE FINANCIERE CONTRE LES CONSEQUENCES D'UNE ATTAQUE CYBER :

GESCO
tel : 01 48 37 68 68
e-MAIL : info@assurances-gesco.com