La Cyber-Lettre
de la
GENDARMERIE
RÉGION GRAND EST

Année 2026 – Janvier 2026

Le partage d'écran, de bureau ...

L'ingénieux vol de données des cybermalfaiteurs

DIFFUSION LIBRE

🎭 Les cybermalfaiteurs ont trouvé dans les logiciels de partage de bureau à distance, tel que AnyDesk, un outil simple, rapide et discret parfaitement adapté à leurs exactions.

Tout commence par la réception d'un mail 📧 (*phishing*) ou un appel 📱 (v*ishing*) d'un escroc se faisant passer pour un technicien, un conseiller bancaire ou un service officiel tel que les finances publiques.

Il sème alors le trouble dans l'esprit de son interlocuteur en générant une situation d'urgence : ''une fraude en cours sur son compte bancaire", "une demande de vérification urgente de conformité bancaire", "un important remboursement du en attente", etc.

Sous pression et ne sachant pas toujours comment réagir, la victime navigue (sur les conseils du cybermalfaiteur) vers un site de partage d'écran ou de bureau à distance. L'escroc communique ensuite un code de session qui lui permet de prendre la main sur la machine de la victime.

À partir de cet instant, le cybermalfaiteur 🦹 peut voir tout ce qui se passe à l'écran (y compris les frappes claviers réalisées par son interlocuteur). Grâce à l'autorisation de prise de contrôle ⌨️, il peut ouvrir le navigateur, consulter les mots de passe enregistrés, accéder aux fichiers ou même réaliser des opérations bancaires en direct (parfois en masquant l'écran avec une fenêtre blanche afin que la victime ne voit rien).

L'attaque 👩‍💻 est d'autant plus sournoise qu'elle s'appuie sur la collaboration involontaire de la victime. Résultat : en quelques minutes, des informations sensibles sont exfiltrées, des comptes sont compromis et des virements frauduleux peuvent être réalisés.

💡 Bon à savoir :

Les administrations et les organismes d'État ne vous demanderont **jamais** de vous connecter sur des sites ou des applications de prise de main à distance.

Rappelez-vous que ce type de comportement est risqué car l'interlocuteur autorisé peut accéder à tout le contenu de l'ordinateur y compris vos documents, logins et mots de passe.

Vous devez absolument être certain de l'identité de la personne distante que vous autorisez à prendre possession de votre environement numérique.

Vous ne laisseriez pas les clés de votre domicile à n'importe qui !

🛡️ Comment se protéger ?

✅Ne jamais autoriser la prise de contrôle sans certitude absolue de l'identité de l'interlocuteur.

✅Utiliser uniquement un dépanneur identifié, connu et légitime.

✅S'assurer de quitter une application de prise de main à distance après utilisation et désactiver l'autotisation d'accès permanent.

✅Au moindre doute, stopper immédiatement l'échange et appeler l'organisme officiel.

Vous êtes victime ?

Appelez immédiatement le 📞**17** ou 💻 contacter :

LE 17 CYBER

Une cyberattaque, échangez avec un cybergendarme - 24h/24 7j/7
https://17cyber.gouv.fr/

GRAND EST CYBERSECURITE

Assistance cyberattaque gratuite
Tel : 0 970 512 525
www.cybersecurite.grandest.fr

+ D' INFO

LA CNIL

Prévenir en cas de fuite de données personnelles, réelle ou supposée.

CYBERMALVEILLANCE

Pour vous faire assister, vous informer ou vous former
www.cybermalveillance.gouv.fr

LA BRIGADE NUMÉRIQUE

Échangez avec un gendarme 24h/24 7j/7

L'ANSSI

Assiste les entités essentielles et les entités importantes, fournit des guides
https://cyber.gouv.fr

THÉSÉE

Déposer plainte en ligne pour les victimes d'e-escroqueries

APPLICATION MA SÉCURITÉ

Trouver des informations de prévention et les démarches en ligne.

Vous souhaitez joindre un Référent Cyber de la Région de Gendarmerie du Grand-Est ou vous abonner à la Cyber-lettre
prevention-ggdXX@gendarmerie.interieur.gouv.fr
(Remplacez les XX par votre département)

01010010 01001001 01010011 01000011 01001000