MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

ALERTECYBERGEND 80
Groupement de gendarmerie départementale de la Somme

ATTAQUE PAR RANÇONGICIEL

⚡ *DOUBLE EXTORSION & PARALYSIE TOTALE* ⚡

*Une société basée dans le **département de la Somme** a subi une cyberattaque majeure par **rançongiciel** avec **double extorsion.***

🔍 DÉCRYPTAGE DU MODE OPÉRATOIRE

- **INFILTRATION :** Les attaquants s'introduisent dans le **réseau** (hameçonnage, failles non corrigées ou identifiants compromis).
- **PROGRESSION :** Ils se déplacent latéralement pour prendre le **contrôle** des serveurs clés.
- **NEUTRALISATION :** Ils ciblent et corrompent spécifiquement les **sauvegardes** pour empêcher toute restauration autonome.
- **BLOCAGE DU SYSTÈME (1ÈRE EXTORSION) :** Ils paralysent les **serveurs** et chiffrent les **données**, provoquant un **arrêt total** de l'activité.
- **VOL & CHANTAGE (2NDE EXTORSION) :** Ayant exfiltré les **données sensibles** au préalable, ils envoient un e-mail de **rançon** avec des preuves du vol pour forcer le paiement sous menace de **divulgation** publique.

🛡️ MESURES PRÉVENTIVES POUR PRÉMUNIR VOTRE ORGANISATION

- **SAUVEGARDES (RÈGLE DU 3-2-1) :** 3️⃣ **copies** sur 2️⃣ **supports** différents, dont 1️⃣ **hors ligne** (déconnectée du réseau).
- **CLOISONNEMENT RÉSEAU :** Segmentez vos **infrastructures** pour bloquer l'attaquant et isolez drastiquement les **accès aux sauvegardes**.
- **AUTHENTIFICATION FORTE (MFA) :** Activez la **double authentification** sur tous les accès distants (VPN, e-mails, cloud) et comptes administrateurs.
- **MISES À JOUR RIGOUREUSES :** Appliquez sans délai les **correctifs de sécurité** sur vos serveurs et logiciels.
- **SENSIBILISATION :** Formez en continu les **collaborateurs** à détecter le phishing.

⚠️ EN CAS D'ATTAQUE

🌐❌ **Isolez les machines** (débranchez les câbles réseau, ne les éteignez pas) et contactez cybermalveillance.gouv.fr.

🚫✉️ **Ne répondez jamais** à l'e-mail des pirates sans l'aide d'un expert en crise cyber. Toute interaction confirme que vous êtes actif et sous pression, ce qui augmente l'agressivité de leur chantage.

❌💰 **Ne payez jamais la rançon**.

Groupement de Gendarmerie
Départementale de la Somme

#ALERTE CYBERGEND 80 – 18 juin 2026

Retrouvez notre guide d'hygiène informatique
« LES 7 PILIERS DE VOTRE CYBERSÉCURITÉ »
en scannant le QR code ci-contre :

Suivez-nous sur les réseaux sociaux de la Gendarmerie de la Somme :

ou sur www.gendarmerie.interieur.gouv.fr