Veille technologique

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

BF

Cyberattques visant les institutions françaises :
Décembre 2025 – janvier 2026

Briard Arthur

Sommaire

Réunion d'urgence pour les services IT

Réunion non prévue où sont conviés tout les services IT du ministère de l'intérieur.

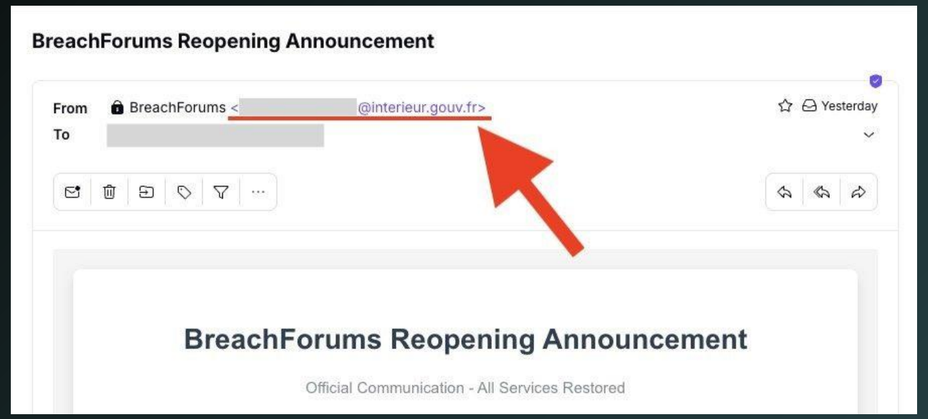
Comme premières informations :

- Attaque du ministère de l'intérieur
- Changement des mots de passe de messagerie
- Vérifications des messageries
- MAJ urgentes à faire sur tous les postes sans exception

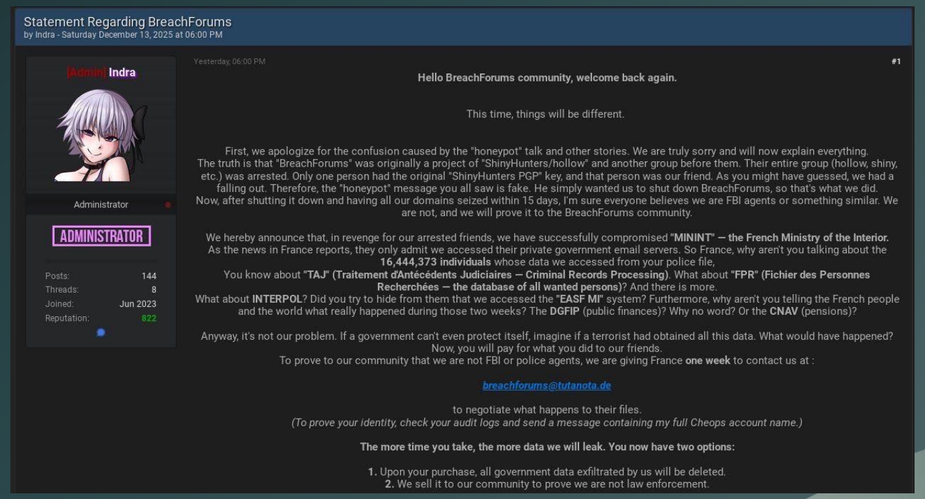
Premières grosses informations

Cibles	Description
Serveurs du ministère de l’intérieur	Accès au TAJ (fichier des antécédents judiciaires). Accès au fichier FPR (Personnes recherchées). Accès à des fichiers “sensibles” liés à la police.
Accès aux messageries professionnels	Récupération de code d’accès via des mails envoyés entre utilisateurs.
Accès aux infrastructures internes	- Réseau interne (LAN / WAN ministériel). - Serveurs métiers (Police, justice, agriculture). - Applications internes (CHEOPS, interface qui permet de consulter les permis de conduire, les signalements de drones, mais surtout les bases de données judiciaires.).

Déclaration des attaquants

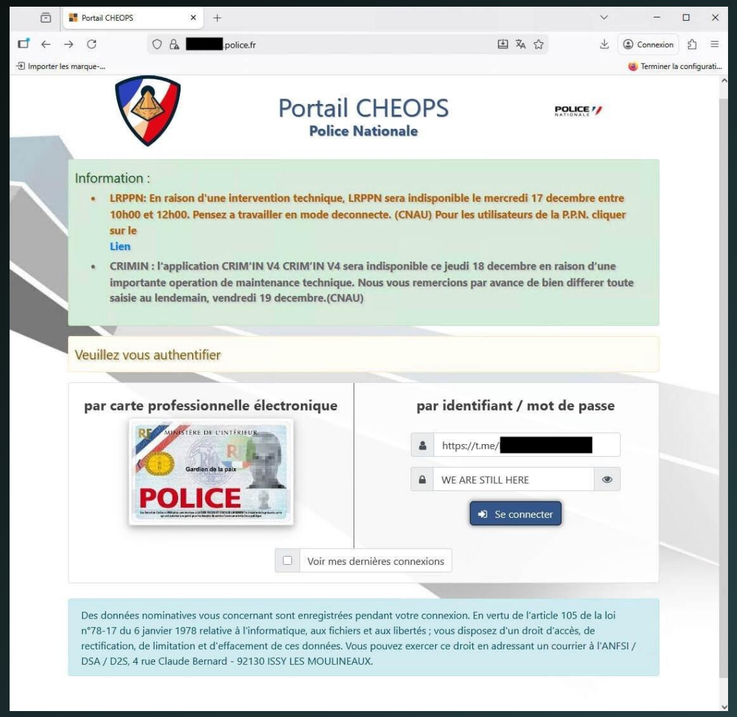


Premier message des attaquants concernant la réouverture du célèbre site « BreachForums » en utilisant un mail en @interieur.gouv.fr

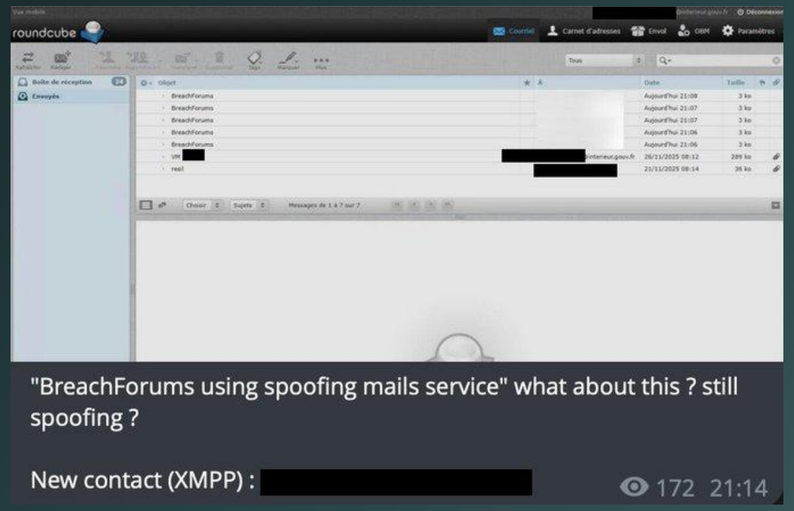


Déclaration des attaquants proclamant avoir accès à plus de 16 millions données. Ce qui implique qu'ils ne les ont pas forcément exfiltrées des serveurs du ministères.

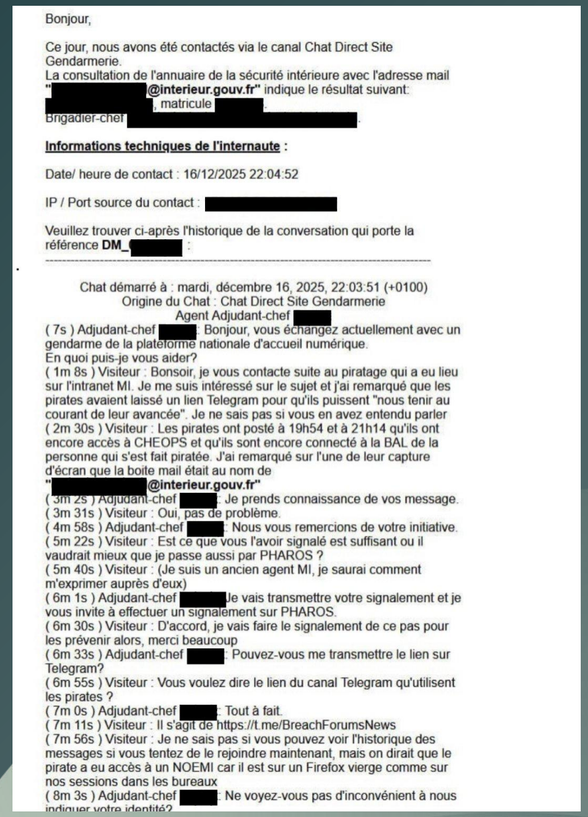
Déclaration des attaquants



Message des attaquants « prouvant » leur accès à CHEOPS, logiciel utilisé seulement en local donc prise de contrôle d'un poste MI. Mais aucune preuve qu'il peut se connecter.



Après plusieurs accusations de spoofing de la part d'internautes les hackers ont voulu prouver l'accès aux mails du MI.



Bonjour,

Ce jour, nous avons été contactés via le canal Chat Direct Site Gendarmerie.
La consultation de l'annuaire de la sécurité intérieure avec l'adresse mail "[redacted]@interieur.gouv.fr" indique le résultat suivant:
[redacted], matricule [redacted]
Brigadier-chef [redacted].

Informations techniques de l'internaute :

Date/ heure de contact : 16/12/2025 22:04:52

IP / Port source du contact : [redacted]

Veuillez trouver ci-après l'historique de la conversation qui porte la référence **DM_[redacted]** :

Chat démarré à : mardi, décembre 16, 2025, 22:03:51 (+0100)
Origine du Chat : Chat Direct Site Gendarmerie
Agent Adjudant-chef [redacted]
(7s) Adjudant-chef [redacted]: Bonjour, vous échangez actuellement avec un gendarme de la plateforme nationale d'accueil numérique.
En quoi puis-je vous aider?
(1m 8s) Visiteur : Bonsoir, je vous contacte suite au piratage qui a eu lieu sur l'intranet MI. Je me suis intéressé sur le sujet et j'ai remarqué que les pirates avaient laissé un lien Telegram pour qu'ils puissent "nous tenir au courant de leur avancée". Je ne sais pas si vous en avez entendu parler
(2m 30s) Visiteur : Les pirates ont posté à 19h54 et à 21h14 qu'ils ont encore accès à CHEOPS et qu'ils sont encore connecté à la BAL de la personne qui s'est fait piratée. J'ai remarqué sur l'une de leur capture d'écran que la boite mail était au nom de "[redacted]@interieur.gouv.fr"
(3m 2s) Adjudant-chef [redacted]: Je prends connaissance de vos message.
(3m 31s) Visiteur : Oui, pas de problème.
(4m 58s) Adjudant-chef [redacted]: Nous vous remercions de votre initiative.
(5m 22s) Visiteur : Est ce que vous l'avoir signalé est suffisant ou il vaudrait mieux que je passe aussi par PHAROS ?
(5m 40s) Visiteur : (Je suis un ancien agent MI, je saurai comment m'exprimer auprès d'eux)
(6m 1s) Adjudant-chef [redacted]: Je vais transmettre votre signalement et je vous invite à effectuer un signalement sur PHAROS.
(6m 30s) Visiteur : D'accord, je vais faire le signalement de ce pas pour les prévenir alors, merci beaucoup
(6m 33s) Adjudant-chef [redacted]: Pouvez-vous me transmettre le lien sur Telegram?
(6m 55s) Visiteur : Vous voulez dire le lien du canal Telegram qu'utilisent les pirates ?
(7m 0s) Adjudant-chef [redacted]: Tout à fait.
(7m 11s) Visiteur : Il s'agit de https://t.me/BreachForumsNews
(7m 56s) Visiteur : Je ne sais pas si vous pouvez voir l'historique des messages si vous tentez de le rejoindre maintenant, mais on dirait que le pirate a eu accès à un NOEMI car il est sur un Firefox vierge comme sur nos sessions dans les bureaux
(8m 3s) Adjudant-chef [redacted]: Ne voyez-vous pas d'inconvénient à nous indiquer votre identité?

Fichier judiciaire balancé par les attaquants recueillant le témoignage d'une personne ayant alerté sur l'intrusion.

Prise de parole du minister de l'intérieur

- “C’est très grave”
- Il y a eu consultation de quelques dizaines de fiches
- Il n’y a pas eu d’export de millions de données
- Le ou les hackers sont restés plusieurs jours, et non plusieurs semaines
- Ils ont compromis une boîte mail et ont pivoté en utilisant des mots de passe contenus en clair dans des e-mails

BreachForums

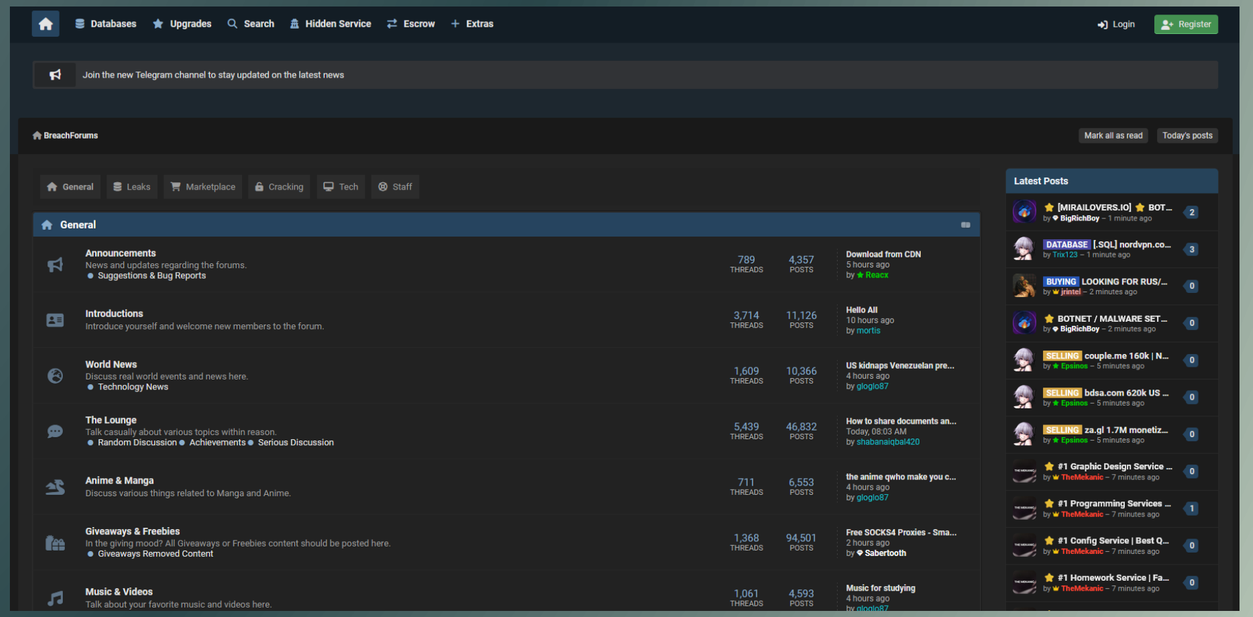
Qu’est ce que **BreachForums** et quel est son rôle dans tout ça ?

Forum cybercriminel anglophone dédié au hacking, au commerce de données volées et à l’échange d’outils ou d’accès illégaux.

- Marketplace de données piratées : diffusion, achat/vente de bases de données issues de fuites massives contenant des informations personnelles, identifiants, e-mails, etc.
- Espace d’échange pour les cybercriminels : discussions sur techniques de piratage, outils (malware, scripts d’exploitation, etc.) et opportunités d’accès illégaux.

HISTORIQUE :

- Créé le 4 mars 2022 par Conor Brian Fitzpatrick c’est le successeur direct de RaidForums.
- Le 15 mars 2023 Conor Fitzpatrick a été arrêté par le FBI
- Un autre administrateur connu sous le nom “Baphomet” a fermé temporairement le forum le 21 mars 2023, invoquant des préoccupations concernant des investigations des forces de l’ordre.
- Arrestations en France d’opérateurs liés au forum.



MAJ

Durcissement des règles

A2F / Revoir les accès aux applications et messageries

Analyse des systèmes

Analyse renforcée des serveurs et des comptes de messagerie pro

Sensibilisation interne

Rappels des bonnes pratiques de sécurité

Coordination avec l’ANSSI

L’ANSSI à coopéré avec le ministère

Les attaques récentes :

La poste :

Attaque DDOS avec une puissance inédite, des milliards de connexion par seconde.

Michelin :

300Go

- Documents internes et opérationnels
- Données techniques et fichiers projets
- Exports de bases de données fragmentées
- Informations pouvant concerner employés et partenaires
- Archives exploitables à des fins malveillantes
- Données structurées facilitant indexation et revente

- Documents internes confidentiels (Airbus Defence & Space, Thales Alenia Space)
- Répertoires de code source et pipelines CI/CD
- Fichiers de configuration (Terraform, SQL, scripts)
- Interfaces internes (Jira, Bitbucket, plateformes de déploiement)
- Informations techniques sensibles liées à des programmes spatiaux

Au service de notre protection sociale

SERVICE PAJEMPLOI

URSAFF

- Noms & prénoms
- Dates et lieux de naissance
- Adresses postales complètes
- NIR (numéro de sécurité sociale)
- Statuts d'activité (ASSMAT, GED, etc.)
- IBAN : début + fin visibles
- BIC en clair
- Identité du titulaire du compte
- Historique administratif (accords, renouvellements, cessations)

BUSINESS LAB FOR SOCIETY

GEA :

- Identités complètes • Emails et numéros de téléphone
- Adresses postales
- Parcours académiques
- Informations professionnelles
- Centres d'intérêt (formations, webinaires, événements)
- Segmentation interne, opt-in / opt-out, adresses IP

OFII

OFFICE FRANÇAIS DE L'IMMIGRATION ET DE L'INTÉGRATION

OFFI :

2,3 millions de personnes concernées

- Identités complètes : noms, prénoms, civilité
- Dates et lieux de naissance
- Nationalité, pays d'origine, langues parlées
- Numéros de téléphone (fixe et portable)
- Adresses postales complètes (commune, département)
- Numéros de dossiers administratifs
- Informations liées au séjour en France
- Motifs et nature des demandes
- Décisions préfectorales et statuts administratifs.

Sources et historique :

- Sources personnelles
- CYBERNEWS
- Sud Radio
- BreachForums

2001