



CYBERSÉCURITÉ NEWS

DARK NET / DARK WEB NEWS

AI NEWS

OSINT NEWS

PROTOCOLE D'ALERTE ZATAZ

ZATAZ COMMUNITY

17CYBER

BREAKING NEWS

aine du 29 mars 2025

► Quand les voleurs traquent en silence

► Cybermenace sur l'Europe : les nouvelles ar

PARTENAIRES ☐

[Ma page de dépôt sécurisée](#)



## Fuite chez EDF ? Entre bluff et baroud d'honneur des derniers membres de Kernel ?

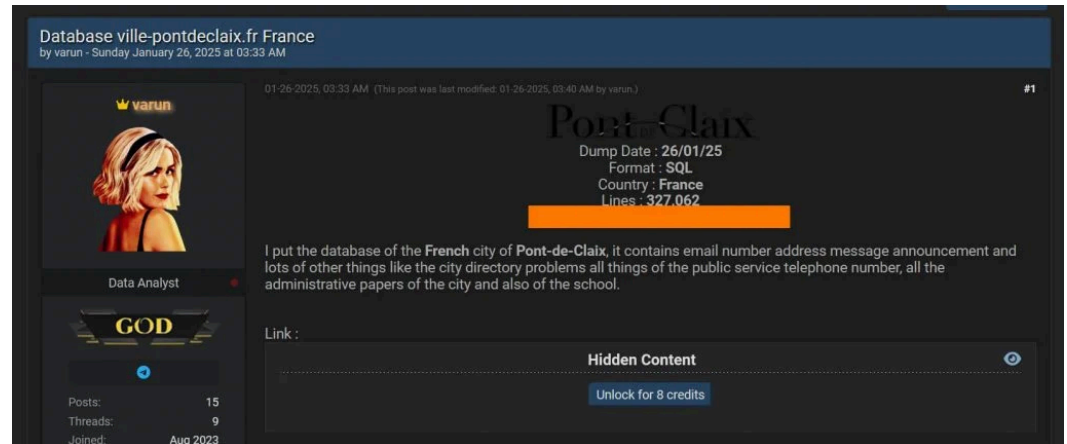
Posted On 04 Fév 2025 By : Damien Bancal Comment: Off Tag: Chatnoir, Epsilon Group, Lapsus\$, varun



## Depuis quelques jours, le forum pirate Breached affiche des petites annonces proposant la commercialisation de données d'EDF, de Leclerc, de Conforama. Du bluff d'un membre de la bande à Kernel ?

Un utilisateur, sous le pseudonyme de **Varun**, a posté sur Breached, un espace dédié au commerce de données piratées. Il affirme vendre des bases de données issues des systèmes numériques d'EDF, de Leclerc Énergie, de Conforama et même de la mairie de Pont-de-Claix. Comme à son habitude, il publie quelques exemples censés prouver l'authenticité de ces fuites. Une fois encore, il aura suffi de quelques posts sur les réseaux sociaux pour que des médias en parle, sans vérifier. **Sauf que...**

### PUBLICITÉ ☐

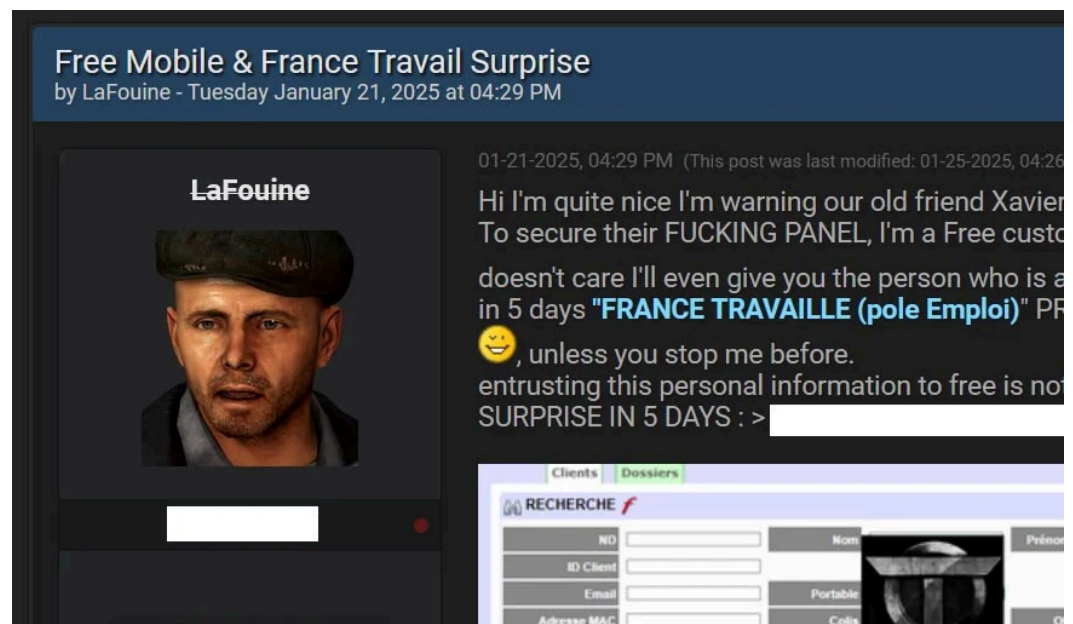


Les exemples fournis par ce Varun datent, pour les plus récents, de 2023. Par exemple, des données avaient déjà été mises en vente l'année dernière par d'autres pirates, une bande bien connue dont les fuites ont déjà impacté LDLC, Boulanger, et bien d'autres. Certains de leurs membres étaient proches de **ChatNoir**, un pirate récemment arrêté.

### DATA SECURITY ☐

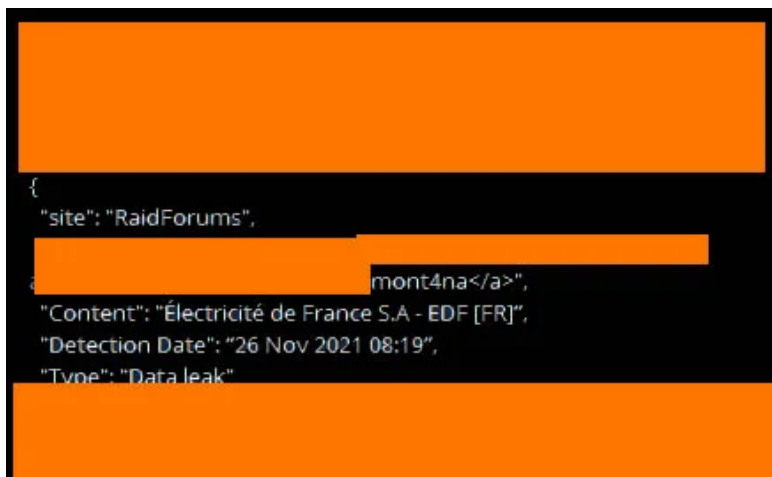
- Root écope de 900 000 € d'amende pour avoir exposé les données de 45 000 clients 27/03/2025
- Violation massive de données à la Pennsylvania State Education Association : plus de 500 000 personnes affectées 27/03/2025
- Cyberattaque sur le bureau du procureur général de Virginie : le groupe Cloak revendique la responsabilité 27/03/2025
- Rakuten face à une vague d'escroqueries par hameçonnage : les clients

Autre incohérence : parmi les échantillons diffusés, plusieurs ne correspondent pas à une fuite d'EDF, mais plutôt à d'anciennes compromissions, comme celle de LDLC, dont un espace professionnel avait été piraté par ... **la bande de Kernel**.



- appelés à renforcer leur sécurité 27/03/2025
- Chrome sous attaque : une faille critique exploitée dans une campagne de cyber espionnage 27/03/2025
- Prison ferme requise contre une vendeuse de téléphones Encrochat 25/03/2025
- La Chine dévoile un puissant coupe-câble sous-marin : un bouleversement potentiel de l'ordre mondial 25/03/2025
- Le Trésor américain lève les sanctions contre Tornado Cash 25/03/2025
- DollyWay : la menace invisible qui frappe WordPress depuis 2016 25/03/2025
- La justice annule la condamnation de Paige Thompson pour le piratage de Capital One 20/03/2025
- Immersive World : la création de malwares voleurs de mots de passe via l'IA 20/03/2025
- Microsoft coupe les ponts : Huawei bascule sur HarmonyOS et Linux 20/03/2025
- Créer un inventaire des actifs d'IA : une nécessité stratégique pour la sécurité et la conformité 17/03/2025
- Un outil gratuit pour vaincre le ransomware Akira sur Linux 17/03/2025
- Mora\_001 : un nouveau ransomware exploite des failles Fortinet 17/03/2025
- La cybercriminalité en France en 2024 : analyse des 348 000 infractions enregistrées 17/03/2025

Dans les cercles cybercriminels, Kernel et son groupe sont connus sous le nom d'**Epsilon Group**. **ZATAZ** a déjà évoqué ces individus, notamment à travers l'histoire de jeunes **internauts ayant mal tourné après s'être rencontrés sur Discord**. Bref, Varun pourrait être un ancien membre de Shiny Hunter dont le pseudo n'est pas inconnu (Il débute par un S).



Quant aux données attribuées à EDF, elles couvrent la période **2020-2023** et ressemblent fortement à celles divulguées par le groupe **Lapsus\$** lors de leur pseudo retraite en juin 2024, ou encore à des fichiers diffusés en 2021 par le pirate **Montana** sur Raid Forum. Bref, pour des données soit disant volées en 2025, il y a un problème dans les dates !

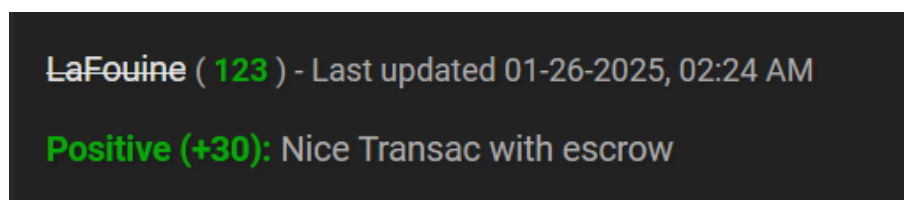
Concernant la mairie de **Pont-de-Claix**, des fuites avaient déjà été révélées par trois pirates différents, quelques jours avant la mise en vente annoncée par Varun.



Trois pirates (peut-être le même) ont diffusé la BDD de Pont-de-Claix avant qu'elle ne soit « vendue » par Varun.

Vous l'aurez compris : **Varun joue la carte du « pro »**, se nourrissant de posts sur les réseaux sociaux qui le présentent comme un expert reconnu, un pirate « **reconnu par ses pairs** ». Pourtant, il n'est qu'un simple **copycat**, possédant plusieurs comptes sur Breached pour gonfler artificiellement sa crédibilité, ses points de réputation. Ca n'a intrigué personne que le « gars » se retrouve avec 300 crédits de réputations en 3 semaines alors que son compte est ouvert depuis le 15 août 2023 !

D'ailleurs, lui et ses amis ont déjà signé sous les pseudos **LaFouine** (fausse vente Free), **Souwu**, **Sanortep**, **Essaye** (comptes fantômes) et **Willfox** (**fausse vente Free**). Ils recyclent tout et n'importe quoi, espérant un coup de bluff réussi. Un bluff qui ira gonfler les posts sur les réseaux sociaux.



➤ DeepSeek : 12 000 Clés API  
Exposées — L'IA, nouvelle  
faille de sécurité ?  
10/03/2025

|               | Positives | Neutrals | Negatives |
|---------------|-----------|----------|-----------|
| Last week     | 6         | 0        | 1         |
| Last month    | 12        | 0        | 1         |
| Last 6 months | 12        | 0        | 1         |
| All Time      | 12        | 0        | 1         |

Alors, derrière ce pseudonyme, se cache-t-il **Kernel** lui-même ? La rumeur évoque son arrestation dans le Sud de la France (Marseille ? Nîmes ?). Mais les rumeurs... vous savez ce qu'on en pense, surtout dans le monde du « *clicks and hack* ». Nous serons malheureusement vite fixé. Les membres de Shiny Hunter / Epsilon ont toujours aimé faire des coups

d'éclat, et diffuser l'intégralité (ou une grosse partie) des informations en leur possession.

Pour rester informé sur les enjeux de cybersécurité, inscrivez-vous à [la newsletter de ZATAZ](#). Rejoignez également [notre groupe WhatsApp](#) et [nos réseaux sociaux](#) pour accéder à des informations exclusives, des alertes en temps réel et des conseils pratiques pour protéger vos données.



### Au sujet de l'auteur

Damien Bancal (damienbancal.fr) est un expert internationalement reconnu en cybersécurité. Il a fondé le projet Zataz en 1989. ZATAZ.com est devenu une référence incontournable en matière d'information sur la sécurité informatique et les cybermenaces pour le grand public. Avec plus de 30 ans d'expérience, Damien Bancal s'est imposé comme une figure majeure dans ce domaine, contribuant à la sensibilisation et à la protection des internautes contre les cyberattaques. Sa carrière est marquée par une forte implication dans l'éducation à la cybersécurité, notamment à travers des conférences et des publications spécialisées. Il est l'auteur de plusieurs ouvrages (17) et articles (plusieurs centaines : 01net, Le Monde, France Info, Etc.) qui explorent les divers aspects du piratage informatique et de la protection des données. Il a remporté le prix spécial du livre du FIC/InCyber 2022. Finaliste 2023 du 1er CTF Social Engineering Nord Américain. Vainqueur du CTF Social Engineering 2024 du HackFest 2024 (Canada). Damien Bancal a également été largement reconnu par la presse internationale dont le New York Times, qui souligne non seulement son expertise mais aussi son parcours inspirant. Par exemple, un portrait de La Voix du Nord le décrit comme "Monsieur Cybersécurité", soulignant son influence et son rôle essentiel dans ce domaine. Enfin, il figure parmi les personnalités les plus influentes dans la cybersécurité, comme le souligne Le Big Data, et a été classé parmi les 500 personnalités tech les plus influentes en 2023 selon Tyto PR. Chroniqueur TV et Radio (France Info, M6, RTL, Medi1, Etc.) Volontaires de la réserve citoyenne - Gendarmerie Nationale et de l'Éducation Nationale. Médaillé de la DefNat (Marine Nationale) et de la MSV (Gendarmerie Nationale). Entrepreneur, il a lancé en 2022 la société veillezataz.com.





☐ *Previous Story*  
**CLIPPER CHIP is back ? Vers la fin  
du chiffrement et un risque majeur  
pour la cybersécurité**

*Next Story* ☐  
**Le protocole d'alerte ZATAZ :  
version 2025**

## Articles connexes



**Un adolescent au cœur de multiples  
cyberattaques : entre piratage et  
justice**



**Adolescents hackers : jeunes,  
inconsciens et redoutables ?**



**Les pirates du groupe LAPSUS\$  
prennent leur retraite**



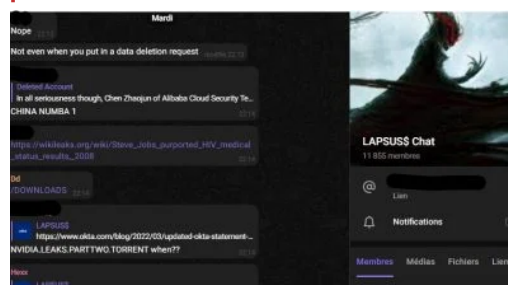
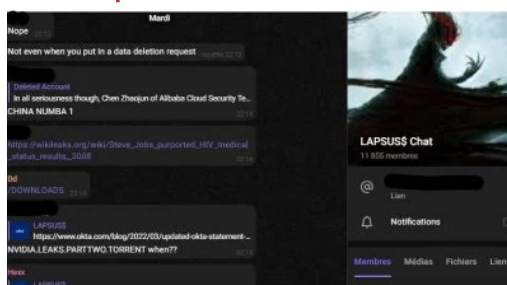
**Piratage d'Activision : le frag grenade  
qui fait mal**



**Lapsus\$ is back ? Nouvelles fuites de  
données pour Uber**



**Les pirates du groupe YanLuoWang  
piratés**



Op Dark Cloud : un nouveau membre  
du groupe Lapsus\$ arrêté

Des données d'employés de la société  
LG diffusées par un pirate

## PARTENAIRES DE ZATAZ ☐





ZATAZ

Réseaux Sociaux

YOUTUBE

TWITTER

INSTAGRAM

TIKTOK

TWITCH

FACEBOOK

```

,r.resetText|n.data("resetText",n[i]()),n[i](r[ie])|th
attr(t,t):n.removeClass(t).removeAttr(t)),0)),t.protot
radio"']');e=e.find("active").removeClass("active"),t
on(n){return e.hasClass("active"),i-r.da
n="toggle"i.r.toggle().set(n).e.fn.button
n.noConflict().fn.button(n,this),eid
(t){var n=e(t).arg().hasClass(n).closest(
=function(t){return e(t).indicators=th
hover"&&thxy(this).pa
on(t){return e(t).use().clear
interval:1000).next().this.optio
nt.find(".item.active"),this.$items=this.$active.paren
this.getActiveIndex(),r=this;if(t>this.$items.length-1
r.to(t)):n
this.$element
this.$element
cle(0)),clearInterval(intervalenu
),prev:function(){if(this.sliding)return this.s
ve"),i-n|r
is=i.length/3
this.$indicators.length>this.$indicators.find("activ
indicators.children()[a.getActiveIndex()];t&&t.addClass
e.$element.t
e.support.t
e.$element.t
veClass([t,
)),a.sliding=1,setTimeout(function(){a.$element.tri
turn;r.removeClass("active").addClass("active"),this
ar n=e.fn.ca
carousel.def
typeof n="
to(n).o?i[o]().s.interval&&i.pause
n()}{return
], [data-sli
s),r,i.e(n.
e.extend({,data:{,n.data(),,carousel(s),o:n.a
Default()}})(window.jQuery),ifunction(e){"use strict";
se.defaults,
tor:t,dimens
ent.hasClas
his.transitioning||this.$element.hasClass("in"))return
is.$parent.find("> .accordion-group > .in");if(r&&r.le
("hide"),i||r.data("collapse",null))this.$element[t](0
his.$element[t](this.$element[0][n]),hide:function(){
mension(),this.reset(this.$element[t]()),this.transiti
on(e){var t=this.dimension();return this.$element.rem
all?"addClass":"removeClass"}("collapse"),this,transi
sitioning=0,i.$element.trigger(r));this.$element.trig

```

PUBLICITÉS ☐

RECHERCHER UNE INFO ☐

OPTIMISÉ PAR Google

Rechercher

| mars 2025 |    |    |    |    |    |    |
|-----------|----|----|----|----|----|----|
| L         | M  | M  | J  | V  | S  | D  |
|           |    |    |    |    | 1  | 2  |
| 3         | 4  | 5  | 6  | 7  | 8  | 9  |
| 10        | 11 | 12 | 13 | 14 | 15 | 16 |
| 17        | 18 | 19 | 20 | 21 | 22 | 23 |
| 24        | 25 | 26 | 27 | 28 | 29 | 30 |
| 31        |    |    |    |    |    |    |
| « F  v    |    |    |    |    |    |    |

- 

**Retour du chantage par mail : je vous vois    poil !**

210 Comments
- 

**Escroquerie : chantage par mail    l'encontre de milliers de Fran  ais**

206 Comments
- 

**Chantage par mail : NON vous n'avez pas   t   pirat  **

150 Comments



## SUR LE OUEB

Revue de presse : ZATAZ

Revue de presse

Réseaux sociaux :

TW/FB/BSK/TK/Masto/LK

**DSB** : Data Security Breach

Page officielle Damien Bancal

## DIVERS

**Remonter un problème.**

Mentions légales.

Certaines images viennent de

Freepik.

Typo titre : adrien-coquet.com

Service Client

## PROTOCOLE D'ALERTE ZATAZ

**Protocole** ZATAZ (2023) : **80 876**

**Taux de correction** (100 derniers cas) : **97 %**

**Alerter** anonymement.

**Page sécurisée Bluefiles**

pour transmettre à ZATAZ un fichier.

## SERVICE VEILLE ZATAZ

Espaces pirates **sous**

**surveillance**: +50 000 **Alertes envoyées** au 01/12/2025 :

+190 000 **Fuites constatées**

en 2024 : +20 milliards Service

veille ZATAZ : **Service Veille**

ZATAZ