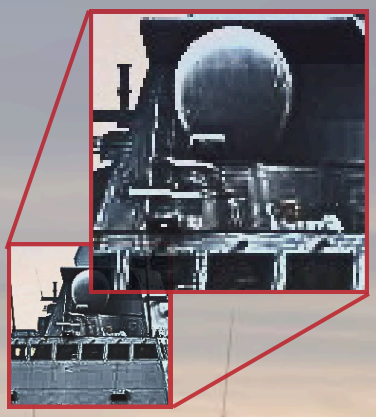
CYBERATTAQUE, OU OPÉRATION RÉPUTATIONNELLE ?

#OSINT
#INFLUENCE

NAVAL GROUP
EN EAUX TROUBLES



RAPPORT D'INVESTIGATION

TIMOUR.

David SALGADO co-fondateur
Mathis B. co-fondateur

Publication : 08 / 2025

P04 - P07

PRÉFACE ET INTRODUCTION

P08 - P24

FORENSIC OSINT

- Chronologie des faits — P09 - P12
- Autopsie des publications — P13 - P18
- Publications non attribuables — P19 - P20
- Analyser les extraits — P21 - P22
- Qui est Neferpitou ? — P23 - P24

P25 - P29

HYPOTHÈSES

P30 - P42

PISTES D'ÉLUCIDATION

- Vecteur de diffusion — P31 - P33
- Incohérences — P34 - P34
- Typologie des données — P35 - P35

PISTES D'ÉLUCIDATION (suite)

Concurence dangeureuse — P36 - P38

Cours de Thales — P39 - P40

Leak des sous-marins russes — P41 - P42

RETEX DE L'ATTAQUE

P43 - P55

Leaks et attaque réputationnelle — P44 - P48

Fake News — P49 - P49

Erreurs de l'attaquant — P50 - P52

Presse internationnale — P53 - P54

Gestion de crise de Naval Group — P55 - P55

CONCLUSIONS

P56 - P60

BIBLIOGRAPHIE

P61 - P67

PRÉFACE ET INTRODUCTION

Dans le cadre de ses activités de recherche en Intelligence Économique, Timour publie des travaux théoriques et opérationnels ; d'analyse et d'investigation en libre accès. Ces travaux peuvent être complétés sur commande.

Ces recherches ont pour but de promouvoir la connaissance de l'Intelligence Économique, de sensibiliser les acteurs du tissu économique aux pratiques de Guerre Économique, de Guerre Informationnelle, aux enjeux d'Influence et de propagande par de l'information de qualité.

Timour enquête sur des sujets nouveaux, sur des tendances qui émergent, souvent dans l'angle mort des analystes. Notre démarche rigoureuse apporte toujours de l'information sourcée, qualifiée, analysée et contextualisée.

Avec Timour, dissipez le brouillard.

TIMOUR

Cabinet de recherche.
Renseignement d'affaires, Défense Réputationnelle, Influence

Timour aussi appelé **Tamerlan** fut le fondateur de l'un des empires les plus étendus d'Asie au XIVe siècle. Maître de la **stratégie** et de **l'anticipation,** il a réussi à manœuvrer dans des environnements fragmentés. C'est aussi notre approche : comprendre les **rapports de force, cartographier les ambitions, et agir au bon moment avec l'information juste.**

Timour est un cabinet de recherche spécialisé dans la collecte, l'analyse et la mise en action de l'information stratégique.
Notre mission : accompagner les **décideurs, entreprises, personnalités publiques** pour tirer profit de leur **environnement informationnel, sécuriser leurs activités et se développer.**

EXPERTISE

L'expertise de Timour repose sur trois piliers lui permettant d'agir sur l'ensemble du cycle de l'information :

La gestion de crise avec un prisme sur les manœuvres de déstabilisation réputationnelle.

La recherche en source ouverte appliquée à l'analyse d'entreprises, de personnes clés ou d'opérations.

L'influence stratégique avec une lecture des écosystèmes (acteurs, échiquiers, narratifs, réseaux, agendas).

PRESTATIONS

Timour protège votre entreprise et sa réputation, vous apporte de l'information à haute valeur ajoutée et vous accompagne dans votre développement.

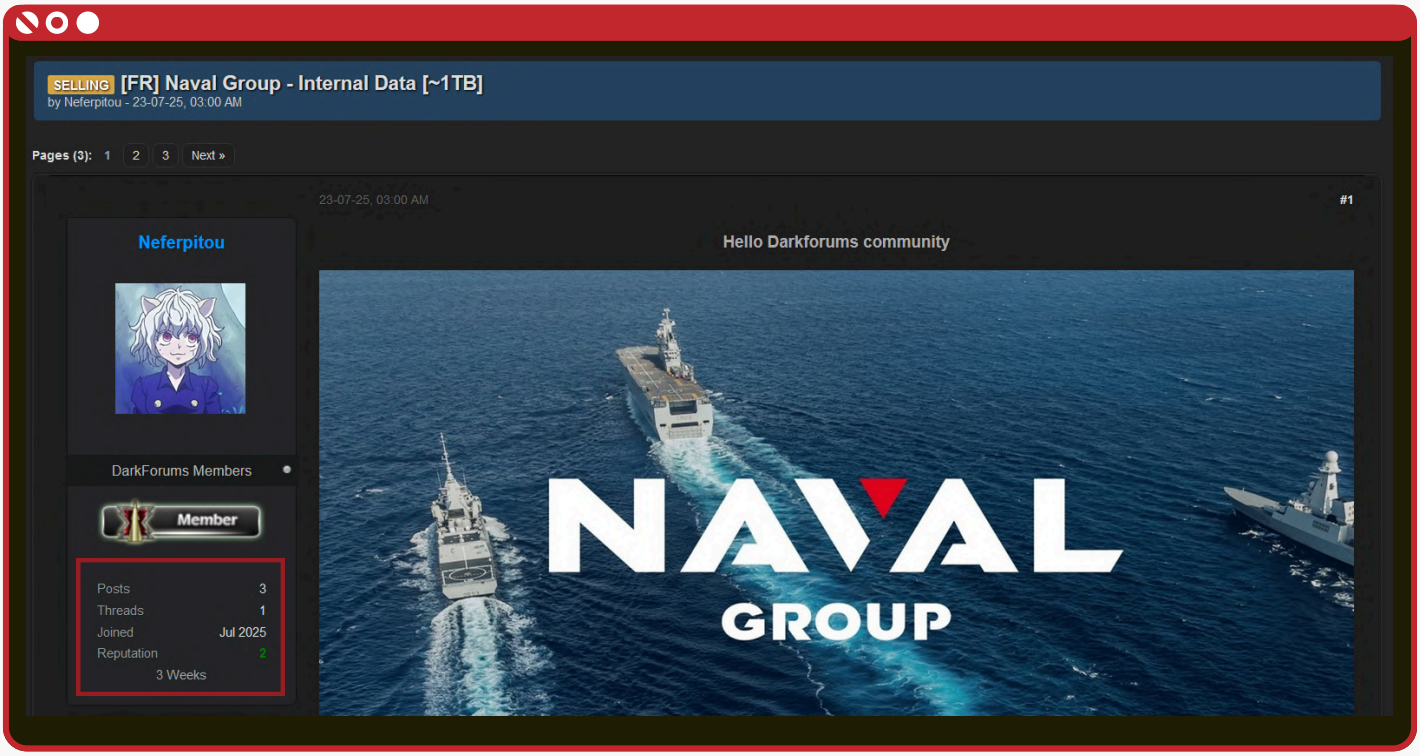
ENQUÊTES **RÉPUTATION** **CROISSANCE**

Nous opérons avec une forte valeur ajoutée en France et sur les marchés complexes, hautement concurrentiels ou opaques :

- **Europe de l'Est et Asie centrale ;**
- **Monde hispanophone ;**
- Marchés émergents.

Pour en savoir plus, rendez-vous sur timour.org

INTRODUCTION



Le 23 juillet 2025 à 5 heures du matin, un utilisateur nommé Neferpitou publie un message dans la section vente du marketplace du forum Darkforums :

[FR] Naval Group – Internal Data [~1TB].

Il affirme détenir environ 1 téraoctet de données sensibles appartenant à Naval Group, et propose même un échantillon de 13 Go. Il exige que l'entreprise le contacte sous 72 heures, faute de quoi il menace de publier l'intégralité des données en ligne.

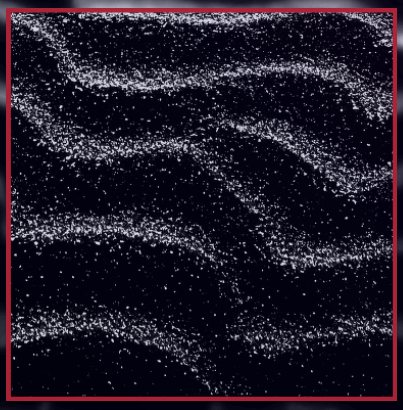
Son auteur demeure mystérieux, aucune publication à son actif, le compte semble avoir été créé pour l'occasion, et son pseudonyme est inconnu dans la communauté du site ou du hacking.

Pourtant, il aurait réussi une opération extrêmement ambitieuse, à la fois pointue d'un point de vue technique, pour avoir pu accéder à des données parmi les plus protégées du pays, et à la fois humiliante pour *Naval Group*. Un hacker aurait accédé au plus profond des secrets du chantier naval.

Selon la description du leak, le contenu serait hautement stratégique, notamment en lien avec des programmes sensibles comme la dissuasion nucléaire, dans le cadre des SNLE (sous-marins nucléaires lanceurs d'engins). Si cela est avéré, il pourrait s'agir du piratage le plus grave ayant jamais touché l'industrie de défense française.

L'entreprise affirme n'avoir détecté « aucune intrusion », mais a déclenché un audit avec l'*ANSSI* et le *parquet de Paris*.

FORENSIC OSINT



CHRONOLOGIE DES FAITS

Avant d'aborder l'analyse de l'attaque, il convient de s'intéresser à la chronologie de l'affaire qui commence en fait bien avant le 23 juillet. Au début du mois de juillet, un collectif de hackers russes avait déjà annoncé détenir des données confidentielles de *Naval Group*, sans donner plus de détails, et sans que ça ne fasse plus de bruit.

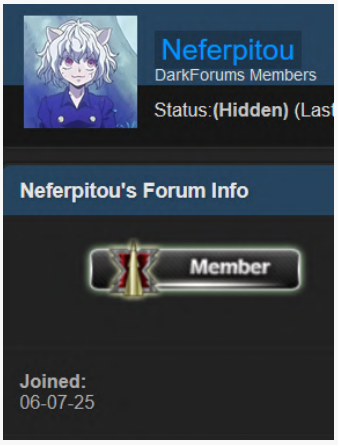
7 juillet 2025

Le groupe de hackers russes *NoName057(16)* déclare obtenir des informations sensibles provenant de *Naval Group*, sans préciser lesquelles, l'histoire ne fait pas beaucoup de bruit.

L'absence d'engouement est due à plusieurs facteurs. Le premier étant le fait qu'ils ne donnent aucune information sur les données volées, ce qui donne assez peu de substance aux médias pour relayer. Le deuxième tient au fait que *NoName057(16)* est plus considéré comme un groupe d'activistes cherchant à attirer l'attention des Occidentaux que comme un groupe de hackers. En effet, ils sont surtout responsables d'attaques par déni-de-service (DDoS). Qui est en soi un type d'attaque gênant mais pas du niveau d'un vol de données d'une entreprise stratégique.

6 juillet 2025

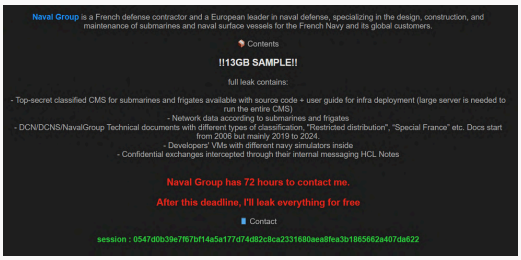
Le compte de *Neferpitou* est créé sur le forum « Darkforums ».



23 juillet 2025, 5 heures du matin

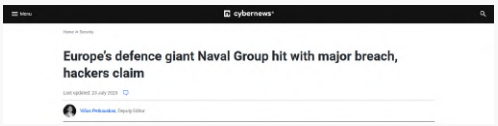
(heure française, puisque le forum est en UTC/GMT+0, soit deux heures en retard sur la France à cette période de l'année)

Neferpitou publie son premier post, il y décrit le contenu général du leak comme analysé dans la partie précédente.



23 juillet 2025, 9h33 du matin

Cybernews publie le premier article parlant de l'affaire.

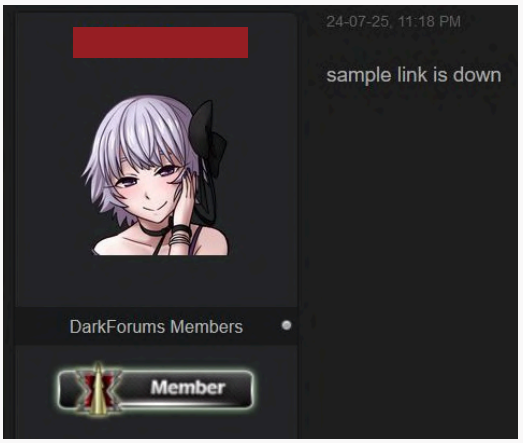


C'est un site d'actualité sur la cybersécurité, dont la majorité des journalistes sont lituaniens, particulièrement actif dans la révélation de l'existence de leaks pour le grand public.

L'article note que les documents ont l'air légitimes et poste même une capture d'écran, mais l'auteur s'étonne de l'absence de motivation apparente de l'attaquant. Selon eux, le premier échantillon contiendrait : « divers contrats, des informations supposées provenir du CMS lui-même, et des éléments multimédias comprenant des vidéos provenant de ce qui semble être un système de surveillance des sous-marins ». L'auteur mentionne également que le document le plus vieux date de 2003.

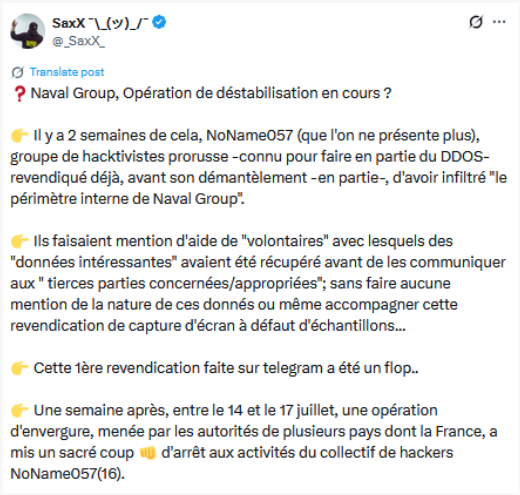
24 juillet 2025, 13h18

Première confirmation que le lien donnant accès au premier échantillon est mort.



24 juillet 2025, 10h32 du matin

La nouvelle atteint les sphères d'information francophones pour la première fois, à la suite d'un tweet de @_SaxX_. Celui-ci reste très prudent et ne tire pas de conclusions hâtives.


SaxX ¯_(ツ)_/¯
@_SaxX_

Translate post

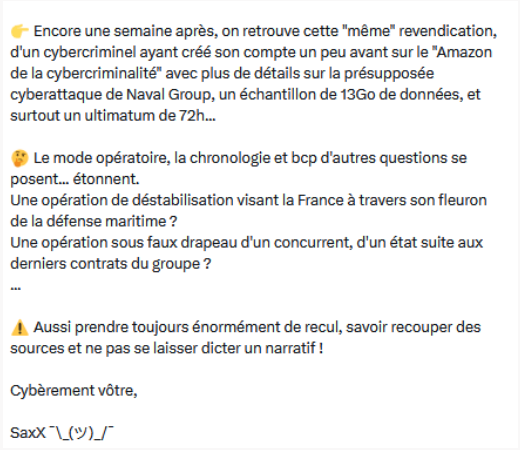
❓ Naval Group, Opération de déstabilisation en cours ?

👉 Il y a 2 semaines de cela, NoName057 (que l'on ne présente plus), groupe de hacktivistes prorusse -connu pour faire en partie du DDOS- revendiqué déjà, avant son démantèlement -en partie-, d'avoir infiltré "le périmètre interne de Naval Group".

👉 Ils faisaient mention d'aide de "volontaires" avec lesquels des "données intéressantes" avaient été récupéré avant de les communiquer aux " tierces parties concernées/appropriées"; sans faire aucune mention de la nature de ces donnés ou même accompagner cette revendication de capture d'écran à défaut d'échantillons...

👉 Cette 1ère revendication faite sur telegram a été un flop..

👉 Une semaine après, entre le 14 et le 17 juillet, une opération d'envergure, menée par les autorités de plusieurs pays dont la France, a mis un sacré coup 👊 d'arrêt aux activités du collectif de hackers NoName057(16).


👉 Encore une semaine après, on retrouve cette "même" revendication, d'un cybercriminel ayant créé son compte un peu avant sur le "Amazon de la cybercriminalité" avec plus de détails sur la présupposée cyberattaque de Naval Group, un échantillon de 13Go de données, et surtout un ultimatum de 72h...

🤔 Le mode opératoire, la chronologie et bcp d'autres questions se posent... étonnent.
Une opération de déstabilisation visant la France à travers son fleuron de la défense maritime ?
Une opération sous faux drapeau d'un concurrent, d'un état suite aux derniers contrats du groupe ?
...

⚠️ Aussi prendre toujours énormément de recul, savoir recouper des sources et ne pas se laisser dicter un narratif !

Cybèrement vôtre,

SaxX ¯_(ツ)_/¯

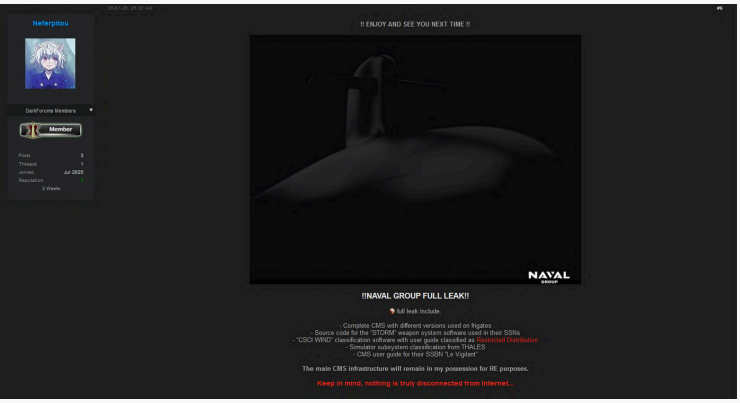
25 juillet 2025, 7h30 du matin

Neferpitou publie un deuxième post dans lequel il dévoile un nouvel échantillon. Il annonce qu'il ne reste que 24 heures au groupe pour le contacter. Celui-ci contiendrait :

- La première partie du CMS utilisé sur ces frégates (binaire, bibliothèques, exercice d'entraînement au CMS, documentation associée) ;
- Des images détaillées du CMS avec plus d'une centaine de captures d'écran ;
- Des données réseau incluant les tests de performance et le fonctionnement du CMS (journal du CMS, arrêt, redémarrage, etc.) ;
- Un document classé "Distribution restreinte" concernant l'utilisation du CMS sur les FREMM.

26 juillet 2025, 7h30 du matin

Alors que les 72 heures sont dépassées, *Neferpitou* publie son dernier post pour annoncer qu'il garde la majorité des données pour lui, dans un but de recherche et développement. Probablement dans un but de rétroingénierie, ou dans un but purement intellectuel.

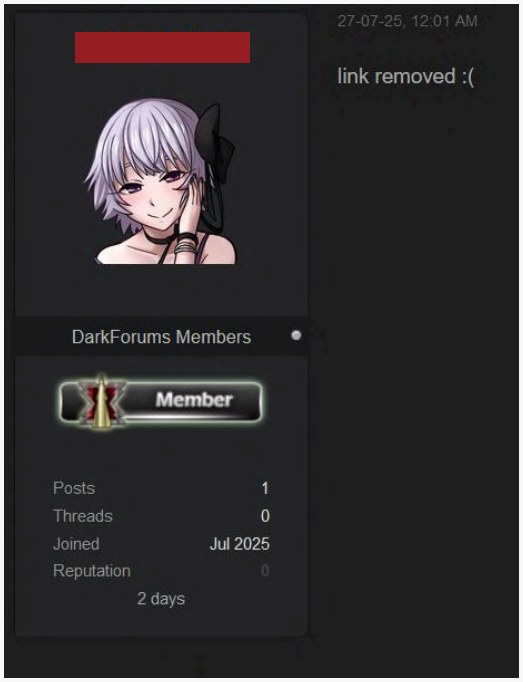


Celui-ci donne un dernier échantillon censé contenir cette fois :

- Le CMS complet avec différentes versions utilisées sur les frégates ;
- Le code source du logiciel du système d'armement « STORM » utilisé dans les SSN ;
- Le logiciel de classification « CSCI WIND » avec guide de l'utilisateur classé en distribution restreinte ;
- La classification du sous-système de simulation de *Thales* ;
- Le guide d'utilisation du CMS pour le SNLE « Le Vigilant ».

27 juillet 2025, 14h01

Tous les liens menant aux leaks sont officiellement morts (dans le sens où la communauté du site le déclare). En réalité, il est probable que ce moment ait eu lieu avant, mais c'est la seule confirmation disponible jusqu'ici.



26 juillet 2025, 18h48

Naval Group publie un communiqué pour annoncer qu'aucune intrusion n'a été détectée, et qu'ils continuent à travailler sur le sujet. L'entreprise considère également qu'il s'agit d'une attaque réputationnelle et pas seulement d'une attaque cyber.


NAVAL GROUP

POSITION DE NAVAL GROUP

Paris, le 26 juillet 2025

Dans un contexte international, commercial et informationnel sous tension, générant une intensification des tentatives de déstabilisation, Naval Group constate être la cible d'une attaque réputationnelle, caractérisée par la revendication d'un acte de cyber malveillance.

Au regard des faits constatés, des enjeux de souveraineté de Naval Group et de la nécessité de protéger les données de nos clients, une plainte a été déposée pour faire la lumière sur ces actes de malveillance.

Conformément à nos procédures de cybersécurité, nous avons immédiatement déclenché des investigations techniques, en s'appuyant sur une équipe d'experts en cybersécurité et sur le CERT Naval Group, en collaboration étroite avec les services de l'Etat.

Toutes nos équipes et tous les moyens sont actuellement mobilisés pour analyser et vérifier dans les plus brefs délais l'authenticité la provenance et l'appartenance des données concernées.

À ce stade, aucune intrusion dans nos environnements informatiques n'a été détectée et aucun impact sur nos activités n'est à signaler.

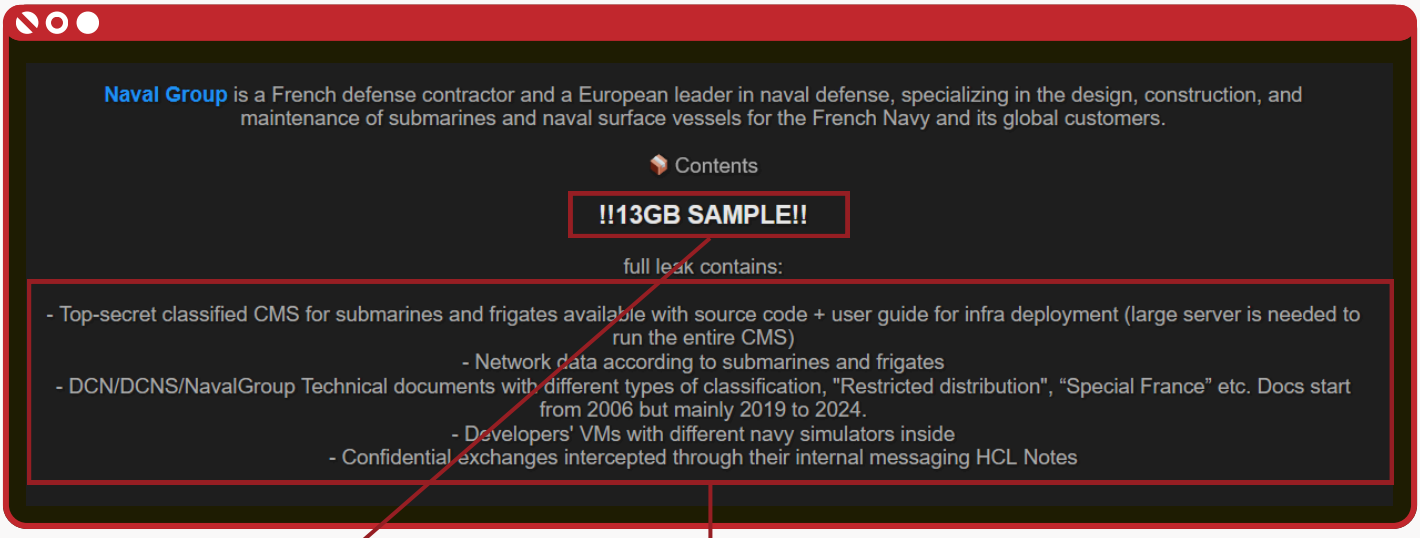
Cette chronologie permet de faire quelques premières remarques.

Celle-ci s'arrête le 27 juillet car depuis, il n'y a pas eu d'évolutions (le 31 juillet à l'heure où nous écrivons ces lignes). Le sujet est resté actif sur le forum, mais les liens sont restés muets et il semblerait que personne n'ait eu de nouveau accès aux données. Même s'il semblerait que l'auteur soit revenu sous un autre pseudo (créé le 31 juillet), rien ne permet de prouver qu'il s'agit bien de lui, et les liens qu'il a donnés étaient dès le départ inopérants.

Un autre point notable concerne la rapidité avec laquelle les médias se sont saisis de l'affaire. L'article de *Cybernews*, par exemple, a été publié seulement 4 heures et demie après la fuite. Cela implique un travail rapide de détection, d'analyse et de rédaction, d'autant plus que le leak a eu lieu tôt le matin, aux alentours de 6 heures, heure locale en Lituanie où sont basés de nombreux rédacteurs du site. Bien que les entreprises spécialisées en cybersécurité disposent de dispositifs de veille et d'astreinte pour ce type de situations, la réactivité observée ici reste remarquable. Cet aspect sera exploré plus en détail ultérieurement.

AUTOPSIE DES PUBLICATIONS

1ÈRE PUBLICATION



La première publication inclut un extrait du leak de 13 Go, ces extraits sont typiques dans les fuites de données et permettent de crédibiliser l’authenticité du reste du leak.

Dans son message initial, *Neferpitou* énumère les catégories de fichiers contenus dans son leak :

- **CMS classifiés "Top Secret" pour sous-marins et frégates, avec code source et documentation.**

Les CMS (Combat Management Systems) sont des systèmes informatiques embarqués chargés de gérer les capteurs, les armes et les communications d’un navire de guerre. Ils centralisent et traitent les données tactiques (radar, sonar, guerre électronique, etc.) pour aider à la prise de décision en temps réel : désignation de cible, riposte, coordination, etc.

Dans ce contexte, la fuite inclurait le code source, c’est-à-dire les fichiers définissant le comportement interne du CMS, ainsi que des guides d’utilisation.

La classification "top secret" n’a ici pas de sens puisque celle-ci n’existe pas dans les classifications françaises.

- **Données réseau relatives aux sous-marins et aux frégates**

La description est ici trop vague pour en évaluer précisément la sensibilité. Il pourrait s’agir de topologies réseau embarquées, d’adresses IP internes, de plages de communication, ou encore de protocoles utilisés à bord. L’ambiguïté rend difficile l’évaluation du niveau de risque, mais le potentiel de compromission reste élevé selon le contenu exact.

- **Documents techniques *DCN / DCNS / Naval Group* avec classifications variées ("Diffusion restreinte", "Spécial France", etc.)**

Les acronymes *DCN* (Direction des Constructions Navales) et *DCNS* désignent les anciens noms de *Naval Group* avant 2017.

Les documents mentionnés seraient classés selon des niveaux de confidentialité :

"Diffusion restreinte" : classification interne, destinée à un cercle restreint de personnels autorisés. Elle ne relève pas du secret-défense, mais protège des données sensibles (procédures, interfaces logicielles, etc.).

“Spécial France" : mention complémentaire visant à restreindre la divulgation d’une information ou d’un support aux seuls ressortissants français.

Là encore, l’absence de détails concrets empêche d’évaluer avec certitude la gravité, bien que l’auteur précise que ces documents couvriraient la période 2019–2024.

- **Machines virtuelles de développement avec simulateurs navals intégrés**

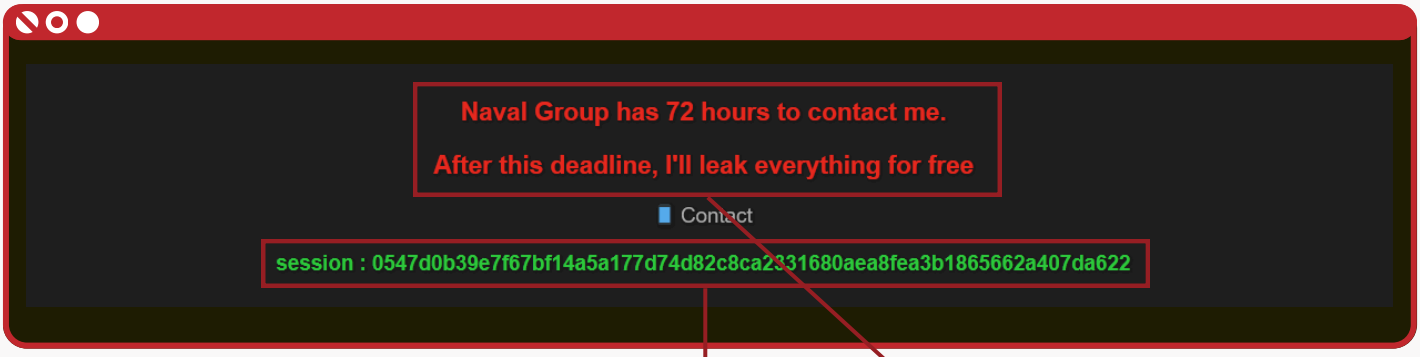
Les machines virtuelles (VM) sont des environnements logiciels qui simulent des ordinateurs complets, permettant aux développeurs de tester des logiciels embarqués sans accéder directement aux systèmes réels. Dans ce cas, les VM contiendraient des simulateurs reproduisant les systèmes embarqués sur sous-marins ou frégates (sonars, capteurs, systèmes de combat), du code source, des outils de test, ainsi que des configurations réseau internes. Une telle fuite représenterait une menace majeure si elle permettait à un acteur hostile de comprendre ou d’exploiter les logiciels militaires français.

- **Échanges confidentiels interceptés via la messagerie interne HCL Notes**

HCL Notes est une messagerie d’entreprise utilisée pour les courriels, documents, calendriers et workflows, avec un haut niveau de sécurité.

Là encore, le terme employé est trop vague. Il est difficile de savoir s’il s’agit d’échanges hautement confidentiels ou de simples messages internes. Par ailleurs, toutes les communications via HCL Notes sont en principe confidentielles par nature, ce qui rend la formulation floue.

La mention session ainsi que la suite de nombres hexadécimaux font référence à une messagerie pour que *Naval Group* le contacte. *Session* est similaire à *Signal* dans son fonctionnement pour l’utilisateur, elle est aussi également cryptée, mais se vend comme plus sure pour les données utilisateurs.



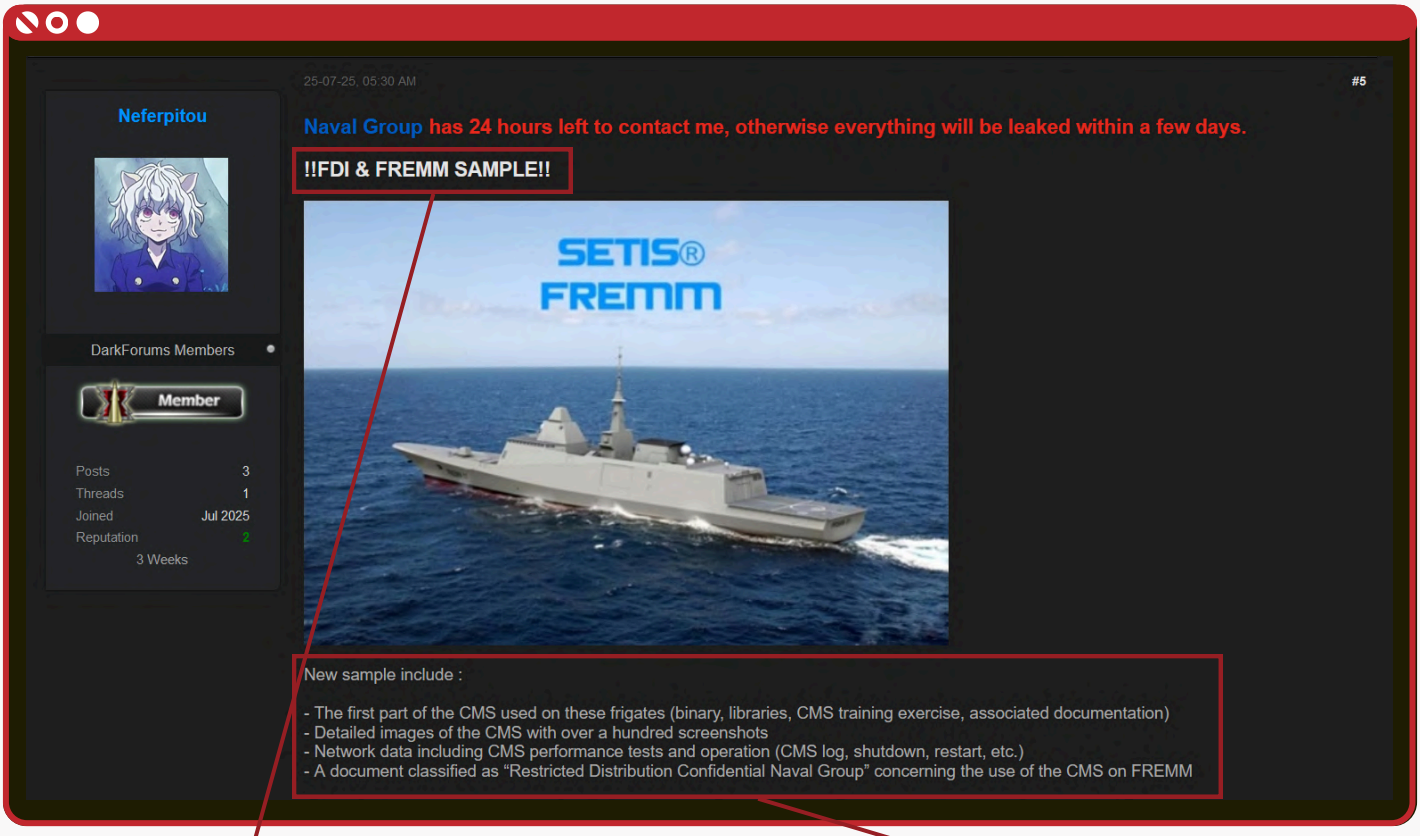
L'annonce de *Neferpitou* mélange des éléments très généraux et d'autres étonnamment précis, rendant difficile l'évaluation de la véritable portée du leak. Certains éléments relèvent clairement de la sécurité nationale, tandis que d'autres sont trop peu détaillés pour en tirer des conclusions solides.

Son premier message se termine sur une date limite, *Naval Group* a 72 heures pour lui envoyer un message. Passé ce délai, *Neferpitou* publiera en accès libre l'ensemble des données.

Une adresse de contact est donnée, celle-ci renvoie vers la messagerie cryptée *session*.

À l'issue du délai de 72 heures, la majorité des données promises n'ont été publiées que partiellement, et retirées rapidement. Plusieurs médias ont alors émis l'hypothèse qu'il s'agirait davantage d'une opération à visée réputationnelle que d'une fuite massive de type cyberespionnage.

2ÈME PUBLICATION



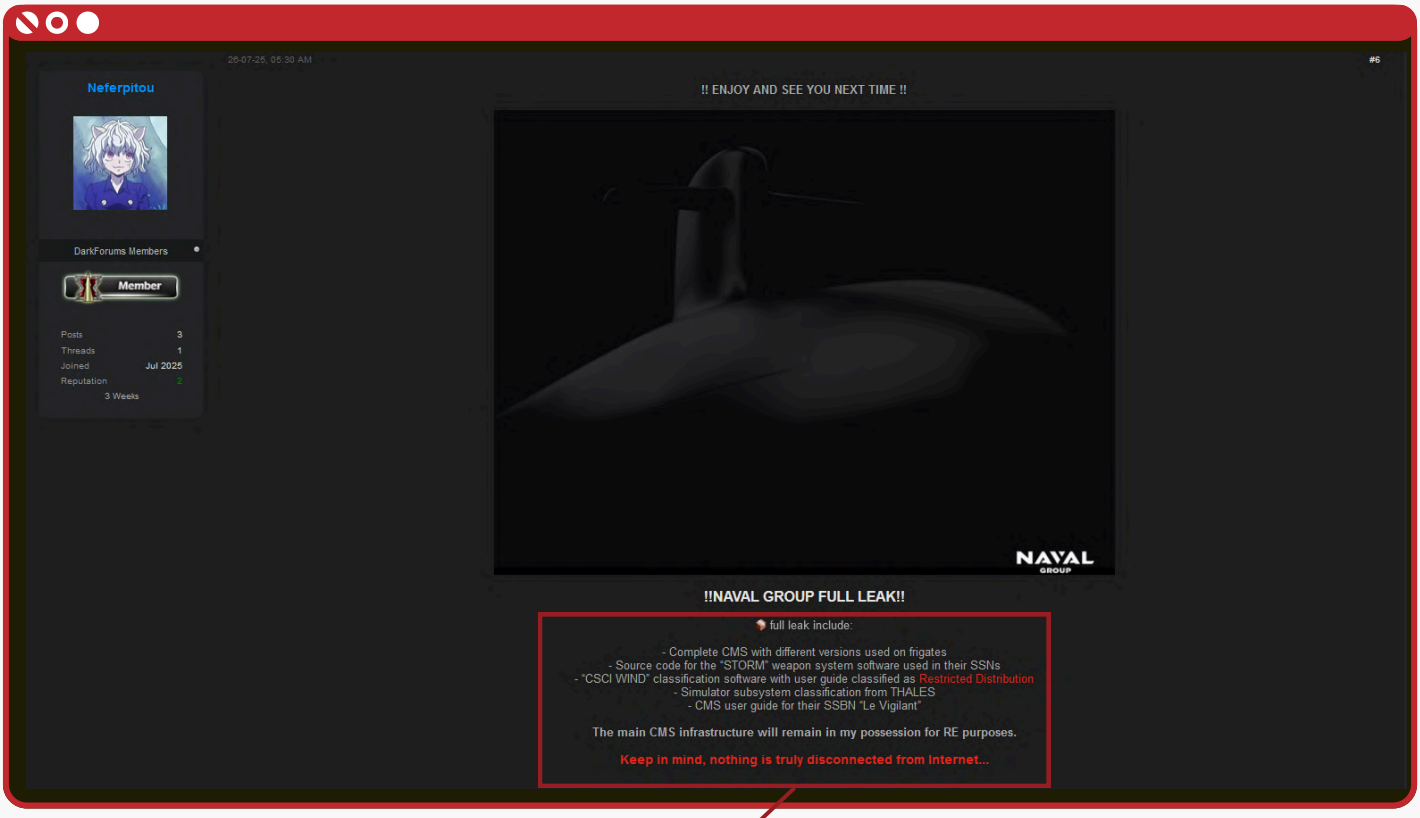
Mention de 2 types de frégates fabriquées par Naval Group :

- FDI : frégate de défense et d'intervention.
- FREMM : frégate multimission.

Contenu annoncé de l’échantillon :

- La première partie du CMS utilisé sur ces frégates (binaire, bibliothèques, exercice de formation CMS, documentation associée) ;
- Les images détaillées du CMS avec plus d'une centaine de captures d'écran ;
- Des données réseau, y compris les tests de performance et le fonctionnement du CMS (journal CMS, arrêt, redémarrage, etc.) ;
- Un document classé « Distribution restreinte confidentielle *Naval Group* » concernant l'utilisation du CMS sur FREMM.

3ÈME PUBLICATION



Contenu annoncé de l'échantillon :

- **Le CMS complet avec différentes versions utilisées sur les frégates ;**
- **Le code source du logiciel du système d'armes « STORM » utilisé dans leurs SSN ;**

STORM ou STORM3 dans les dossiers du leak fait très probablement référence à un logiciel interne de Naval Group (probablement non confidentiel, mais difficilement accessible).

SSN fait probablement référence à "Ship Submersible Nuclear" dans la classification *OTAN*.

- **Le logiciel de classification « CSCI WIND » avec guide d'utilisation classé « Distribution restreinte » ;**

Nous n'avons pas réussi à déterminer avec certitude ce qu'était le logiciel de classification « CSCI WIND ». Il fait visiblement référence au programme Barracuda (bien qu'il soit appelé projet dans les captures d'écran du leak) de *Naval Group*, qui est un programme de construction de 3 types de sous-marins.

- **La classification du sous-système de simulation de *THALES* ;**

Ici aussi la formulation est encore très vague, on ne sait ni quels sont les critères de classification ni de quels systèmes de simulation il s'agit.

- **Le guide d'utilisation du CMS du SSBN « Le Vigilant ».**

SSBN est l'acronyme anglais qui se réfère aux sous-marins nucléaires lanceurs d'engins, et Le Vigilant est un sous-marin français de ce type.

L'auteur précise qu'il détient encore une grande partie de l'infrastructure CMS, notamment à des fins de recherche et développement, par exemple pour effectuer de la rétroingénierie.

Concernant l'analyse des extraits publiés, plusieurs points méritent d'être soulignés :

La fuite ne semble pas concerner uniquement *Naval Group*. Bien qu'il soit possible que certains documents proviennent d'autres entreprises de la défense, il n'est pas exclu que *Naval Group* en ait eu possession dans un cadre professionnel.

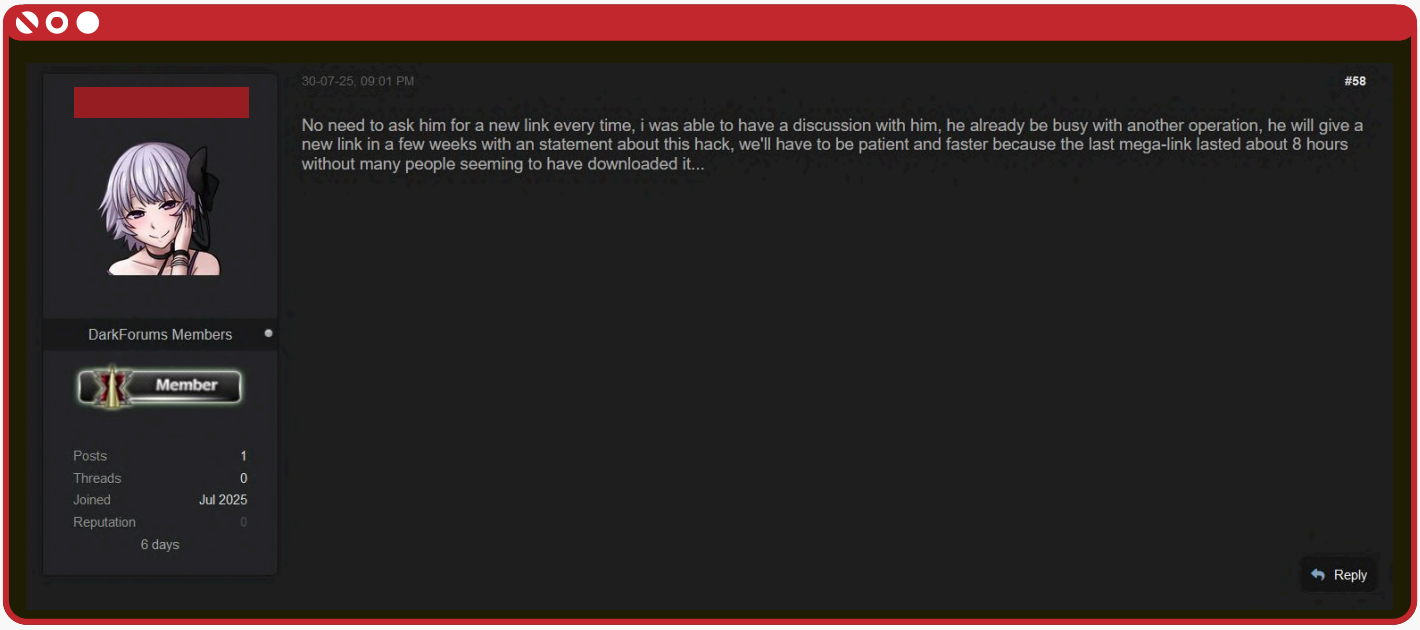
Certains extraits sont décrits de manière très vague, ce qui rend difficile leur interprétation ou l'identification précise de leur contenu.

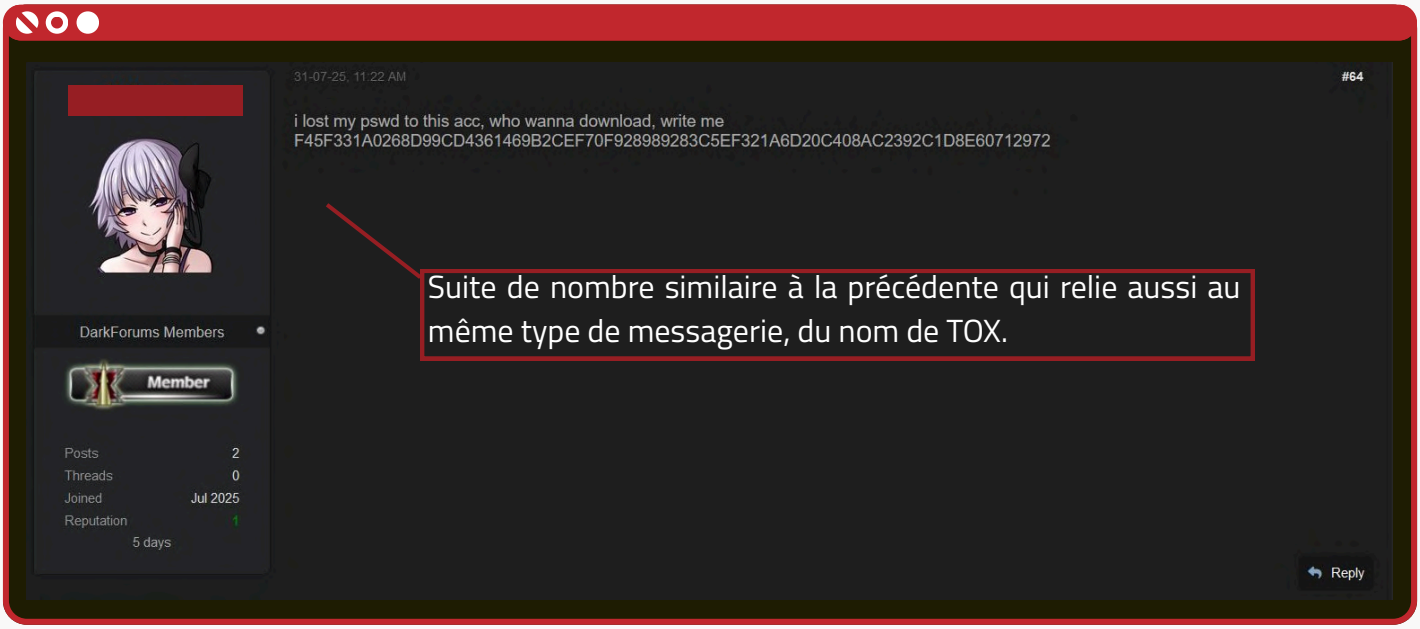
D'autres documents, en revanche, semblent contenir des références internes spécifiques à *Naval Group*. Ces éléments ne relèvent probablement pas du secret-défense mais ils ne sont pas facilement accessibles publiquement pour autant.

L'ensemble de la fuite semble assez hétérogène : certains fichiers sont très détaillés, tandis que d'autres sont à peine exploitables. Cela peut s'expliquer par la faiblesse intrinsèque de certains éléments ou par un accès partiel à l'information lors de la constitution du dossier.

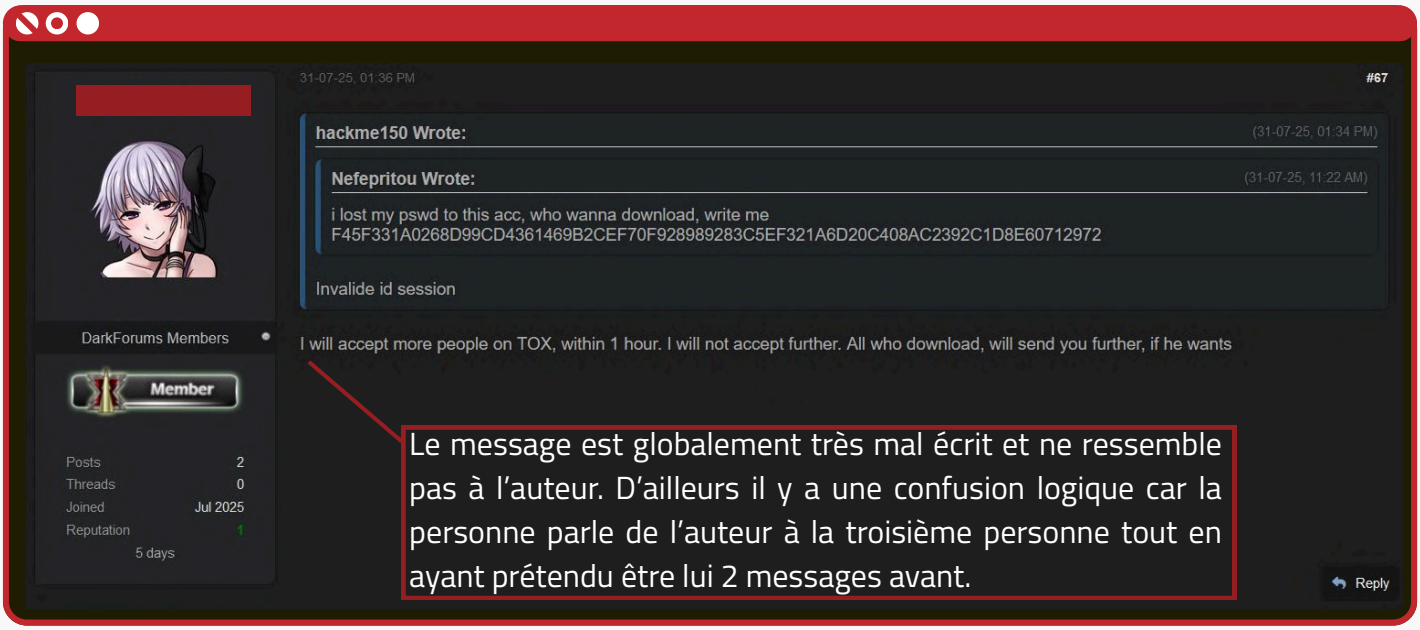
PUBLICATIONS NON ATTRIBUABLES

Depuis la publication de son dernier message, l'auteur semble s'être officiellement retiré. Toutefois, sur le fil de discussion, plusieurs personnes affirment soit être l'auteur, soit avoir été en contact avec lui. Il est actuellement impossible de vérifier l'authenticité de ces déclarations, mais il est globalement peu probable qu'il s'agisse réellement de l'auteur. Ces interventions visent principalement soit à proposer de nouveaux moyens d'accéder aux données divulguées, soit à annoncer une éventuelle future prise de parole de l'auteur.





Suite de nombre similaire à la précédente qui relie aussi au même type de messagerie, du nom de TOX.



Le message est globalement très mal écrit et ne ressemble pas à l'auteur. D'ailleurs il y a une confusion logique car la personne parle de l'auteur à la troisième personne tout en ayant prétendu être lui 2 messages avant.

Site de ecommerce en vietnamien (créé le 7 juillet 2025), dont un des produits est le leak, avec un formulaire de contact.

Sur le forum, personne ne semble avoir réussi à accéder aux données, malgré les différentes méthodes proposées. Le seul moyen qui paraît potentiellement légitime est le site web, dont la création coïncide approximativement avec celle du compte de l'auteur. Cela pourrait indiquer qu'il s'agissait d'une option envisagée dès le départ pour diffuser la fuite.

Même en supposant qu'il s'agisse bien de l'auteur à chaque prise de parole, les différentes stratégies mises en avant apparaissent comme incohérentes d'un point de vue opérationnel. Elles donnent l'impression que l'auteur cherche à éviter d'utiliser la solution la plus simple et efficace pour assurer la pérennité du leak : l'hébergement sur un serveur personnel, une option pourtant suggérée par certains membres du forum.

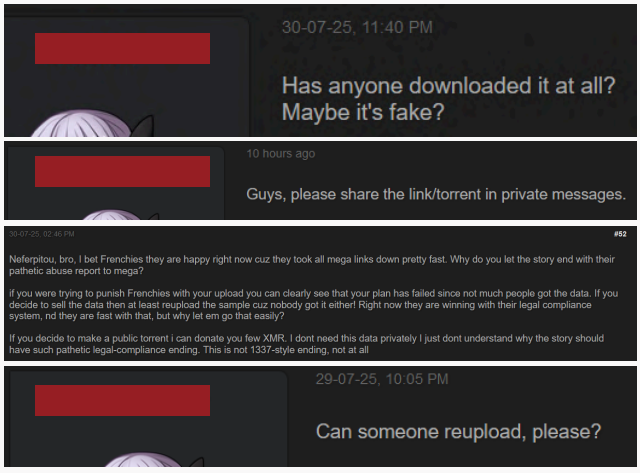
ANALYSER LES EXTRAITS

Les données mises en ligne semblaient légitimes dès le début, ce qui a été confirmé par *Naval Group* auprès de plusieurs médias. Cependant, de nombreuses personnes ont douté de leur caractère sensible, une position partagée par l'entreprise, qui affirme qu'aucune des informations divulguées n'est classifiée "secret défense", ni ne met en péril la sécurité ou les activités du groupe.

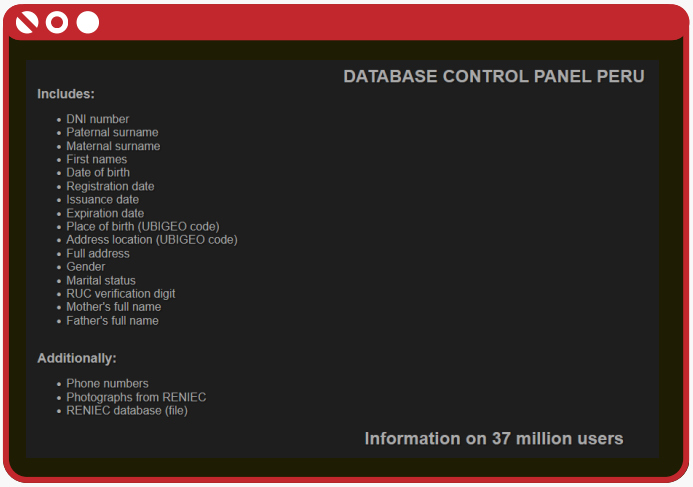
De plus, ces données ont été peu consultées, pour deux raisons principales.

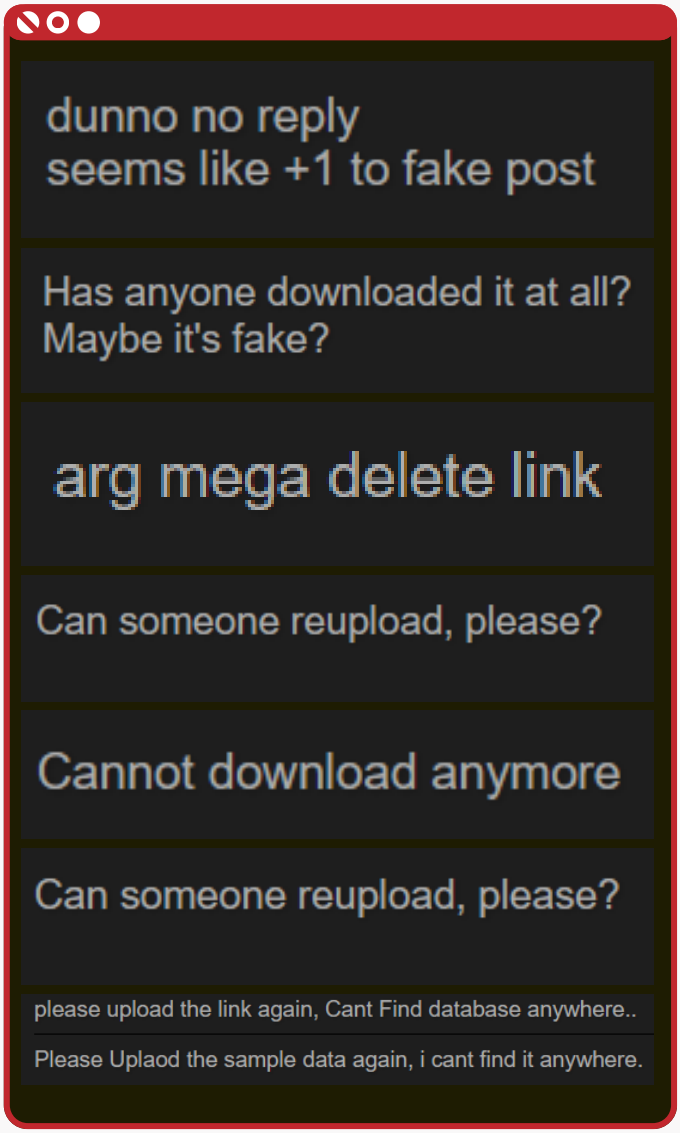
Premièrement, les fichiers étaient hébergés sur *Megaupload*, un choix discutable pour ce type de contenu. La plateforme est connue pour sa tolérance envers les téléchargements illégaux de films et de séries, et occasionnellement pour l'hébergement de fuites mineures. Mais dans le cas de données confidentielles provenant d'une entreprise de défense, il était prévisible que *Megaupload* désactive rapidement les liens à la moindre demande officielle de *Naval Group*.

Deuxièmement, et ce point est moins souvent abordé dans les médias, la fuite a eu peu d'écho initial sur le forum où elle a été publiée. Le sujet n'a réellement suscité de l'intérêt qu'à partir du moment où plusieurs médias ont relayé l'affaire, c'est-à-dire à un moment où les liens étaient déjà inactifs. Cela se reflète clairement dans le fil de discussion : l'engouement initial était faible. Après la publication du premier échantillon, seules trois personnes ont commenté, dont une pour signaler que le lien ne fonctionnait plus. Entre le deuxième et le troisième échantillon, aucun message n'a été posté. Ce n'est qu'après la médiatisation de l'affaire que le sujet est devenu actif, principalement avec des messages demandant un nouvel accès aux fichiers.



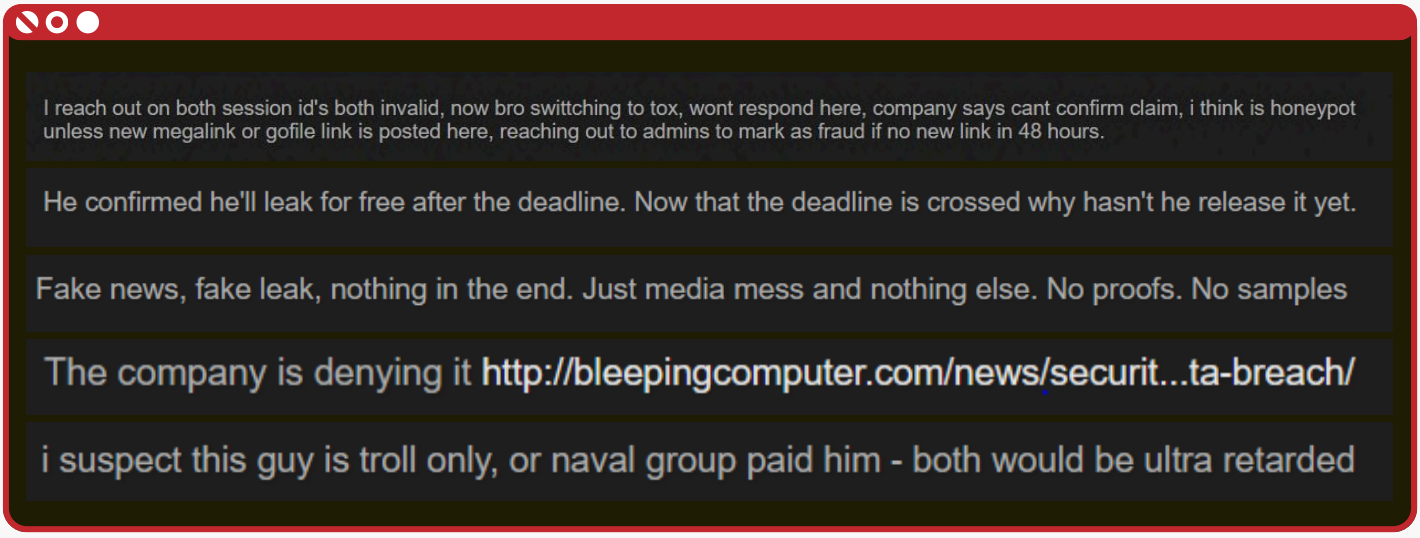
A titre d'exemple, ce leak d'une moins grande importance stratégique sur une base de données d'état civil péruvienne a généré beaucoup plus d'engagement. Cinq personnes se sont montrées intéressées dans les 3 heures suivant l'ouverture du sujet.





Malgré tout, certaines images restent accessibles (pas sur le forum, mais sur les réseaux sociaux). On trouve par exemple une capture d'écran d'une vidéo attribuée à un système de surveillance de sous-marins (premier échantillon), des captures du répertoire contenant les noms de fichiers du troisième échantillon, ainsi qu'une photo de la page de couverture d'un dossier lié au deuxième échantillon.

Les données ayant été disponibles pendant un laps de temps extrêmement court, cela est devenu le principal sujet de discussion parmi les personnes intéressées par la fuite. Cette brièveté d'accès a même suscité des doutes sur l'existence réelle des fichiers et sur la crédibilité de l'auteur.



QUI EST NEFERPITOU ?

Neferpitou a créé son compte sur le forum le 6 juillet 2025, et il semble être complètement inconnu du monde du hacking. Son pseudo fait référence à un personnage du manga Hunter X Hunter. Mais en dehors de ces éléments, il est difficile d'en savoir plus.

https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fnormandie.ccibusiness.fr%2Fsites%2Fdefault%2Ffiles%2F2023-01%2FNGp.jpg&f=1&nofb=1&ipt=3394bef3f395fcc78ed8f1137c94d1b2b443369b646d9a3e4d3e04fe091c9247

Il y a tout de même un détail à considérer qui pourrait ouvrir des pistes pour l'identifier, même si une partie de la réflexion se base sur des hypothèses.

Des trois images qui servent à illustrer les posts de *Neferpitou*, deux sont hébergées sur des sites spécialement dédiés (imgur et ibb), mais une ne l'est pas. Elle trouve son origine dans un article de la *CCI Normandie* de 2023, pour lequel l'attaquant a repris le lien de l'image pour le copier-coller dans son post. Sur ce forum, pour illustrer les posts avec des images, le lien de l'image suffit.

L'image en elle-même est assez commune puisque beaucoup de sites l'ont reprise, mais la présence de cette image avec ce lien précisément pose des questions. L'URL indique que la recherche a été faite avec le moteur de recherche pour images de DuckDuckGo. DuckDuckGo est un moteur de recherche qui met en avant la protection de la vie privée.

Lors de la consultation de l'image, l'URL ne renvoie ainsi pas directement au site de la CCI Normandie d'où l'image est issue mais est hébergée par DuckDuckGo. Dans le cas contraire, il aurait été possible que sa connexion sur le site de la CCI y ait été enregistrée.

Cependant, deux points importants sont à considérer :

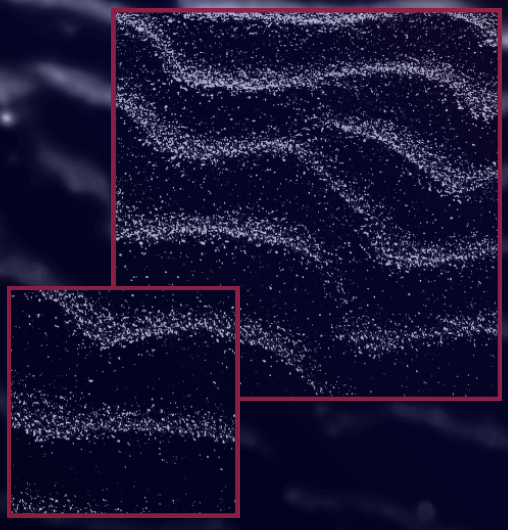
- L'article en lui-même fait référence à une réorganisation interne de Naval Group, ce qui aurait pu être une information utile pour l'attaquant. Il est donc possible qu'il se soit connecté au site de la CCI dans le cadre de sa préparation de l'attaque.
- Pour faire apparaitre ce résultat, il faut inscrire une requête spécifique dans le moteur de recherche, mentionnant la "naval group" et "normandie" ou "organisation". Ces termes peuvent être écrits indistinctement dans d'autres langues et amener au même résultat. Il s'agit de termes peu communs pour obtenir une image d'illustration du groupe.

Nous formulons donc 2 hypothèses sur ce sujet :

- L'attaquant a téléchargé l'image en cherchant à illustrer son post. Neferpitou chercherait probablement une image d'illustration en lien avec la Normandie, on peut s'interroger sur ce choix de requête pour illustrer une fuite d'information stratégique. En cherchant des logos ou des photos de frégates de Naval Group, l'image apparait aussi mais non avec le même lien.
- L'attaquant a fait une cartographie et un screening complet et très approfondis du groupe, soit pour préparer son attaque cyber, soit pour sourcer des informations par un biais différent du hacking, comme en exploitant des données en source ouverte, et a enregistré des liens d'illustration trouvés à cette occasion.

Il peut avoir découvert cette image de deux manières différentes, soit en cherchant des images figuratives sur la Normandie, soit en cherchant des informations sur l'organisation du groupe. Dans cette dernière hypothèse, il est possible que celui-ci se soit bien connecté au site, pour chercher un organigramme par exemple. Le sujet de la réorganisation ayant été peu abordé dans les médias, il est également possible qu'il ait essayé de lire l'article, et donc éventuellement laissé des traces. Pour se protéger il aurait ensuite utilisé le lien de l'explorateur d'images de DuckDuckGo et pas de l'image en elle-même.

HYPOTHÈSES



FAITS :

Publication sur un forum de hacking annonçant détenir 1To d'informations sensibles sur *Naval Group*. La publication inclut des extraits et demande à *Naval Group* de contacter le publicateur.

TYPE D'ATTAQUE :

Attaque pour rétribution.
Une telle attaque viserait à obtenir une rétribution en échange des données. Cette dernière peut être demandée/obtenue de *Naval Group* (ce qui semble être l'exigence de l'attaquant), de l'État français ou d'un éventuel acheteur tiers.

Attaque réputationnelle.
Une telle attaque viserait à nuire à la réputation de *Naval Group* ou, par proxy, d'un tiers. La qualité de l'information n'est pas un élément déterminant de l'attaque, aussi, les informations prétendument incluses dans le leak peuvent être fausses, partielles, exagérées ou réelles et importantes.

AUTEUR :

Un attaquant isolé.

Il aurait eu accès à des informations à faible, moyenne ou haute valeur ajoutée via une attaque cyber sur *Naval Group* ou ses sous-traitants, un accès privilégié aux données (employé, vol de matériel,...), ou un contact. Il est aussi possible qu'il n'ait eu accès à aucune donnée et qu'il mentionne des informations semi-sensibles mais peu connues.

Un groupe d'attaquants.

Utilisant les mêmes méthodes, ils auraient monté une opération plus complexe et de plus grande envergure permettant l'accès à des données proportionnellement plus sensibles.

Attaque d'origine étatique.

Un État hostile aux intérêts français ou à ceux de *Naval Group* a engagé une opération visant à nuire réputationnellement à l'une de ces parties ou à détourner l'attention d'un autre sujet.

Attaque d'origine privée.

Une entreprise privée concurrente de *Naval Group* ou de l'un de ses fournisseurs a entrepris une opération pour la discréditer en vue d'obtenir un avantage compétitif. Il est aussi possible qu'il s'agisse d'une entreprise de spéculation visant à déstabiliser le cours de *Naval Group* en vue de réaliser un profit financier.

HYPOTHÈSES PROBABLES PAR ORDRE D'INTÉRÊT :

Attaque réputationnelle d'un concurrent.

Dans un contexte économique tendu, il est de plus en plus courant que les concurrents recourent à des moyens d'actions multidimensionnels afin d'obtenir une position plus favorable ou de nuire à leurs concurrents. Dans ce cadre, les attaques réputationnelles font partie du panel d'actions offensives des entreprises. Dans un secteur ultraconcurrentiel comme la BITD, où les contrats sont aussi profitables que rares, ce type d'action est particulièrement répandu. L'auteur de l'attaque peut viser *Naval Group* par exemple dans le cadre d'un appel d'offres international. Mais il est aussi possible que cette attaque vise l'un des fournisseurs de l'entreprise en étant orchestrée par l'un de ses concurrents. Dans ce cas, le contenu des leaks se révélera incriminant pour le fournisseur auprès de *Naval Group* et nuira à la confiance, voire entrainera des pénalités et une exclusion du panel fournisseur.

Attaque réputationnelle sur le cours de Thales.

L'actionnariat de *Naval Group* est divisé entre l'État (62,5%) et *Thales* (35%). Les deux entreprises sont donc liées par un lien capitalistique mais aussi réputationnel. Attenter à l'image de *Naval Group* aura alors pour impact mécanique la chute du cours en bourse de *Thales*. Ce type d'attaque est exploitable par les fonds spéculatifs de type hedge funds ou spécialisés en short selling mais aussi par des acheteurs agressifs souhaitant optimiser le prix d'entrée.

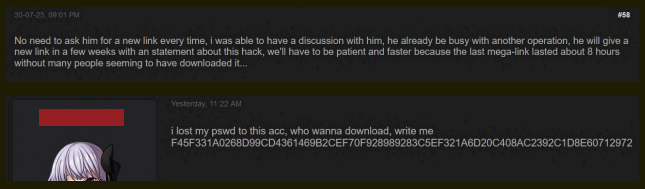
Attaque réputationnelle d'un État hostile ou opportuniste.

Un État ayant réussi à obtenir les informations annoncées contenues dans le leak n'aurait pas annoncé les détenir sur un forum. Les posséder apporte déjà un avantage stratégique dans son exploitation et annoncer posséder celles mentionnées mènerait au contraire à une perte de valeur de ces données. L'attaqué s'empressant d'entreprendre des correctifs pour neutraliser l'exploitation. De même, et comme cela a été le cas, l'attaqué entreprend des démarches afin d'identifier la source de la fuite de données, ce qui limite les potentielles attaques futures en corrigeant les fuites. Dans ce cas les informations mentionnées dans le leak ne sont certainement pas pertinentes. Il est cependant probable qu'un tel État ait été à l'initiative d'une opération réputationnelle sans détenir les informations annoncées afin de discréditer l'entreprise visée ou de nuire au prestige de la France dans le domaine militaire. Il est aussi possible que cette opération permette de distraire l'attention et entraine un gaspillage de ressources des analystes, des services de l'État, de l'entreprise ou de la société civile vis-à-vis d'une information plus importante. Cela peut être d'une autre attaque cyber, d'une fuite similaire le concernant, ou d'un autre événement.

HYPOTHÈSES PROBABLES PAR ORDRE D'INTÉRÊT :

Attaque d'un individu isolé pour rétribution réputationnelle.

La stratégie adoptée pourrait correspondre à un hacker solitaire en quête de reconnaissance. Il se pourrait qu'il ait été dépassé par les événements, ce qui expliquerait pourquoi il n'a pas mis à jour les liens morts menant aux documents divulgués. Il est également possible qu'il ait exagéré l'importance des informations qu'il possédait, dont la majorité proviendrait en réalité d'une bonne connaissance des nomenclatures utilisées par *Naval Group*, de ses programmes combinés à des données à faible valeur plus facilement accessibles, via par exemple des prestataires ou des clients (comme dans le cas du leak de 2016). Certaines personnes sur le forum affirment avoir échangé avec lui et rapportent qu'il aurait promis de revenir prochainement. pour faire des annonces, mais il est impossible de vérifier s'il s'agissait réellement de lui. D'autres utilisateurs prétendent être lui, sous un autre pseudonyme, mais là encore, rien ne permet de le confirmer. Il est d'ailleurs probable que ces affirmations soient fausses dans les deux cas. S'il était en effet en quête de reconnaissance, l'effet inverse semble même se produire. Étant donné que peu de personnes ont pu accéder au leak, et qu'un nombre croissant d'utilisateurs estiment qu'il n'est pas aussi impressionnant qu'annoncé, la crédibilité de *Neferpitou* commence à être remise en question. Ce scepticisme est renforcé par certaines incohérences dans ses messages et par un amateurisme apparent.



Attaque d'un individu pour rétribution financière.

La présence d'un lien de contact destiné à *Naval Group* sur le premier leak doublée d'une ligne conductrice demandant à l'entreprise de le contacter semble montrer que l'auteur de l'attaque souhaite obtenir quelque chose de *Naval Group*. Cette demande demeure floue, elle pourrait être financière ou d'un autre ordre. Le manque de clarté ne contribue pas à renforcer cette hypothèse.

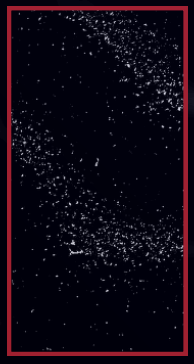
Attaque d'un groupe pour rétribution.

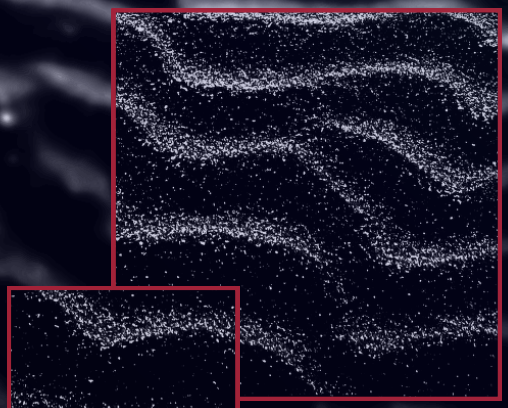
La stratégie de diffusion utilisée permettrait aux attaquants de ne pas revendiquer l'attaque pour augmenter le niveau d'opacité et de protection. Il s'agit de l'hypothèse la moins probable en raison des pratiques communes du milieu du hacking de revendication des actions afin d'apporter prestige et reconnaissance au groupe impliqué.

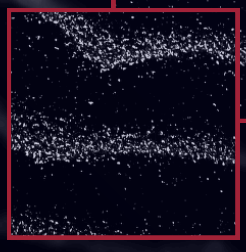
On remarque que les hypothèses les plus probables ont toutes un volet réputationnel, elles ont soit pour objectif d'augmenter le prestige de l'attaquant ou de le protéger, soit de nuire à celui de l'attaqué. Nous mettrons en lumière dans la suite de ce rapport les éléments étayant ou discréditant ces hypothèses.

Nous remarquons aussi que Naval Group n'est pas forcément la cible finale de l'attaque. Attaquer une telle entreprise peut être utile afin d'attaquer les parties prenantes comme l'actionnariat, l'État ou même un fournisseur.

PISTES D'ÉLUCIDATION







VECTEUR DE DIFFUSION

La stratégie de diffusion semble s'inscrire dans une logique où la génération de viralité est l'un des objectifs principaux. Cette stratégie est cohérente aussi bien dans l'hypothèse d'un attaquant agissant seul que dans celle d'une opération de déstabilisation à visée réputationnelle. Dans le premier cas, cela lui permet de gagner en visibilité et en notoriété ; dans le second, cela renforce l'impact de l'opération.

L'objectif de recherche de viralité se retrouve autant dans le vecteur utilisé (le choix de l'environnement) pour faire passer le message que dans sa charge utile (le leak en lui-même).

Concernant la stratégie de choix du vecteur de diffusion, plusieurs observations peuvent être faites :

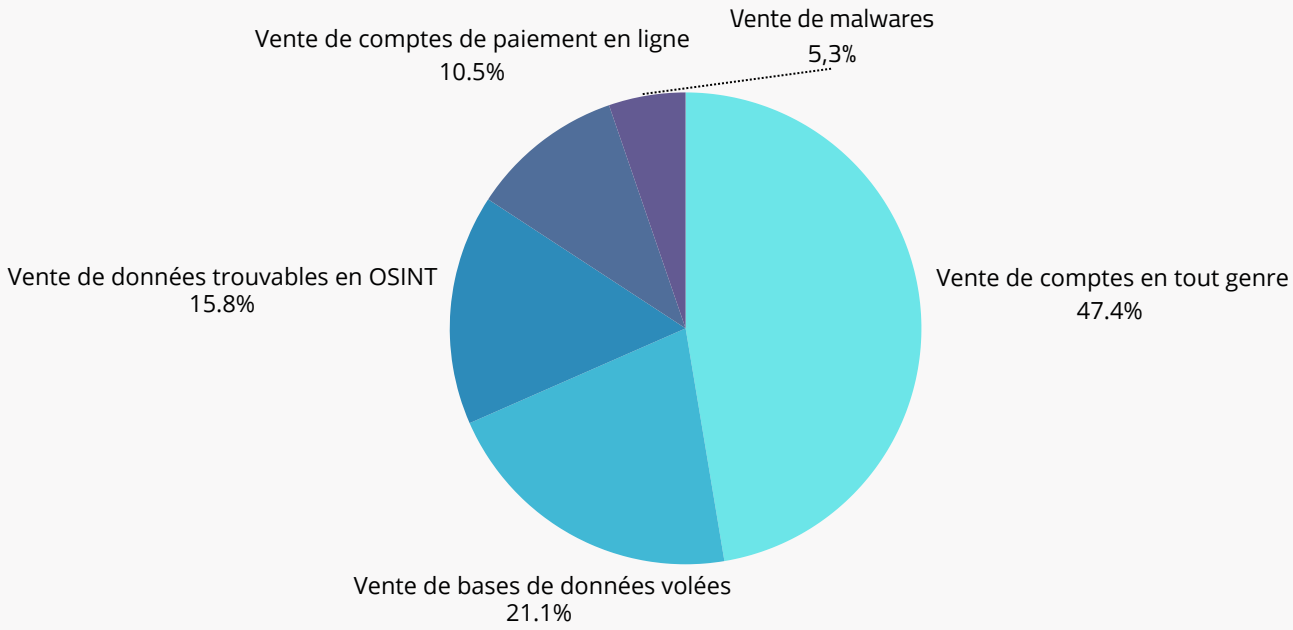
L'action a été menée sur un forum bien connu dans le milieu des leaks, bien qu'il ne soit généralement pas associé à des fuites d'une telle ampleur.

Nous avons réalisé un graphique représentant ce qui se vend à un instant T sur le forum, puis l'avons comparé à d'autres périodes. Il en ressort que les proportions évoluent peu dans le temps.

Environ deux tiers des offres concernent des comptes piratés (Facebook, Gmail, PayPal, sites d'e-commerce), ce qui est assez courant sur ce type de forum.

Une autre part est constituée de bases de données accessibles via l'OSINT, probablement collectées à l'aide d'outils de scrapping ou obtenues grâce à une bonne connaissance des

Produits ou services en vente sur Darkforums



sources disponibles en ligne (bases de CV, adresses e-mail, etc.).

Enfin, une minorité des publications concerne de véritables fuites de données. Cependant, leur ampleur reste généralement limitée (beaucoup d'informations d'état civil assez peu opérationnalisables, à part pour des commerciaux ou du phishing), à l'exception d'un cas notable contenant des numéros de sécurité sociale américains.

D'autant plus que la seule fuite de documents sensibles (comparable à ce qui a été annoncé pour *Naval Group*) concernant la défense où une grande entreprise que nous avons pu identifier a eu lieu en février 2025, où un utilisateur a posté une base de données de données volées à l'*OTAN* qui contiendrait plus de trois téraoctets de documents classifiés, de rapports techniques et d'informations sur les membres et les partenaires de l'*OTAN* et de diverses organisations gouvernementales. Les documents incriminés portent différents niveaux de classification de sécurité, notamment « restreint », « confidentiel » et « secret ». Mais le caractère sensible de ces documents n'a jamais pu être établi.

En dehors de celle-ci, le seul grand leak pour lequel le forum est connu est celui de ses propres utilisateurs. Puisqu'en juin 2023, un hacker a révélé qu'il possédait un grand nombre de données sur les utilisateurs du forum, notamment leurs adresses IP. Une fuite plus tard confirmée par les administrateurs de l'époque. C'est à cette époque que le forum va migrer sur TOR.

Darkforums présente donc beaucoup de caractéristiques d'un forum très classique dans le monde du hacking : facilité d'accessibilité, présence sur le clear web, contenu en vente relativement attendu pour un forum de hackers, etc.

De plus, les fuites revendiquées comme portant sur des données sensibles d'entreprises du secteur de la défense n'apparaissent généralement pas sur des forums aussi accessibles et, dans bien des cas, elles ne sont publiées sur aucun forum public. Quelques exceptions existent, comme en 2023, lorsque l'utilisateur *IntelBroker* a mis en vente sur *BreachForums* (le « jumeau » de *DarkForums*) des données présentées comme sensibles et appartenant à *General Electric*, incluant supposément des informations militaires.

Cela s'explique par le fait que, la plupart du temps, ce type de données fait l'objet de demandes de rançon directes entre les cybercriminels et l'entreprise ciblée. De nombreux cas illustrent cette stratégie, notamment les campagnes du groupe *LockBit*, qui a rançonné des entreprises comme *Boeing*. Dans ce genre de scénario, les attaquants utilisent leur propre site de fuite (leak site) pour accroître leur sécurité opérationnelle. Et s'ils publient des échantillons pour faire pression, ils le font directement sur leur site, sans passer par des forums publics.

La notoriété du forum implique également une forte visibilité de celui-ci : il est régulièrement consulté par des entreprises spécialisées en veille cybersécurité, des acteurs de secteurs sensibles, ainsi que par les autorités. D'ailleurs, le site *Cybernews* a publié un article sur le sujet seulement 4 heures et 30 minutes après la publication du leak.

Darkforums est parmi les forums de hackers les plus populaires du darkweb. Ces grands forums partagent plusieurs caractéristiques :

- Ils sont relativement peu fermés et ne sont pas réservés à un cercle d'initiés ;
- Ils ont généralement une adresse sur le clearweb ;
- Ils sont relativement vulnérables à la fermeture par les autorités, ainsi qu'aux fuites de données.

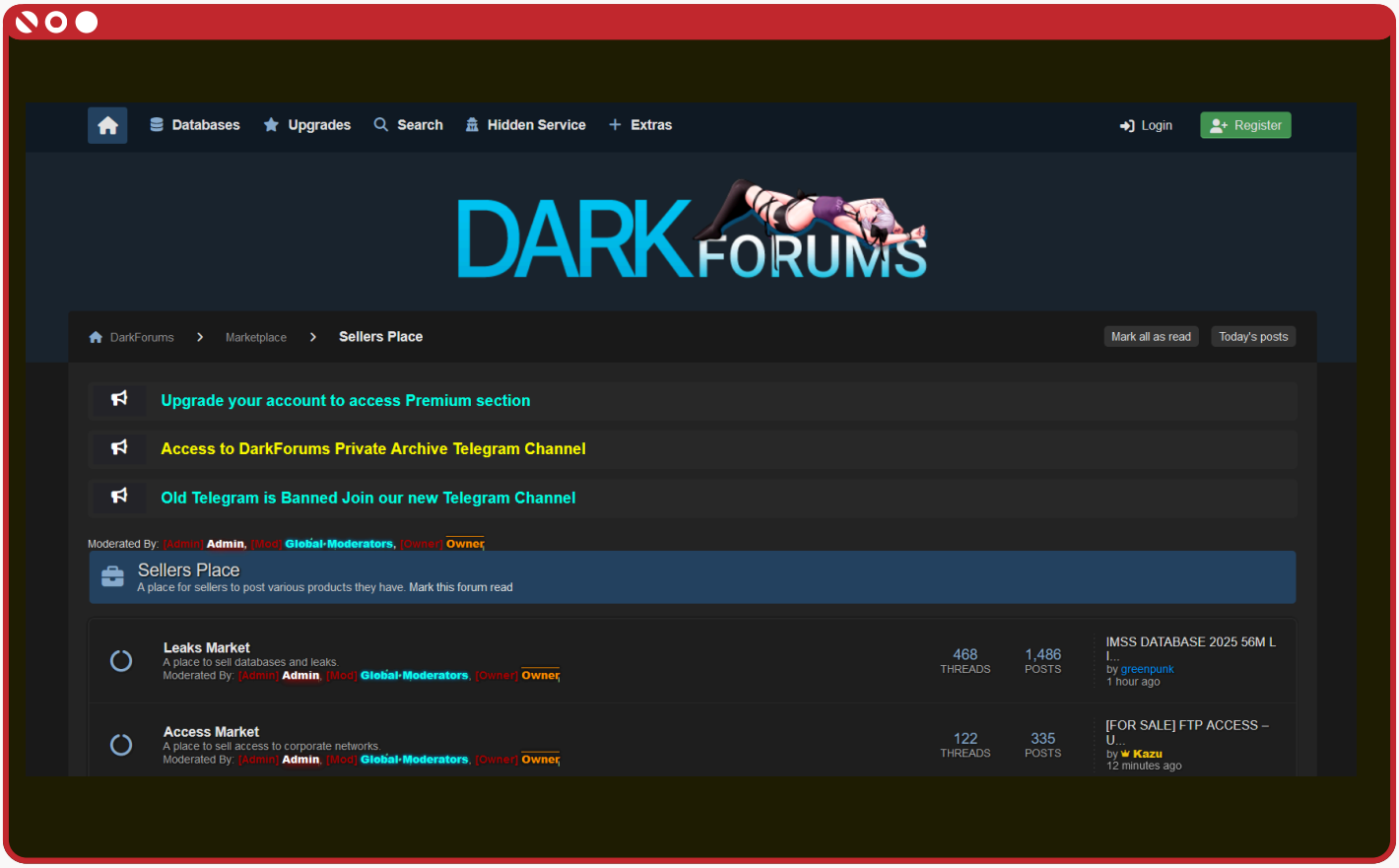
En moyenne, ces grands forums comptent un peu moins de 30 000 inscrits, sachant que *Darkforums* en compte 35 000.

A partir de ces différents constats (leak original et inattendu dans le milieu choisi, une première dans l'histoire du forum, un forum populaire et très accessible), on peut déduire que l'opération a été conçue avant tout pour être virale, et non pour rester confinée à un cercle restreint d'initiés.

Concernant les motivations de *Neferpitou*, plusieurs éléments méritent d'être relevés. Ses motivations restent floues.

Il ne formule aucune demande financière et se contente d'exprimer le souhait d'entrer en contact avec *Naval Group*, sans pour autant expliquer les raisons de cette démarche.

Ce qui tranche avec le fait que ce n'est pas une démarche très commune dans ce genre de fuites.



INCOHÉRENCES

Toute cette stratégie présente un certain nombre d'incohérences, tant par rapport à l'effet final recherché que vis-à-vis des pratiques habituellement observées dans le monde du hacking.

La première de ces incohérences concerne l'ampleur du leak. Si les informations publiées sont authentiques dans leur totalité, il serait surprenant qu'une seule personne soit à l'origine d'une opération d'une telle envergure. Des groupes organisés comme *LockBit*, connus pour des fuites similaires en volume et en sensibilité, mobilisent plusieurs individus. Récupérer des données auprès d'une entreprise aussi protégée que *Naval Group* représente un travail titanesque, difficilement réalisable en solitaire.

Par ailleurs, ces groupes exigent généralement des rançons, même lorsque leur objectif est principalement réputationnel plutôt que financier. Ce comportement s'explique facilement : détenir des données sensibles sur une entreprise offre une opportunité de pression, et donc de monétisation. Pourtant, *Neferpitou* ne fait à aucun moment mention d'une quelconque volonté de faire chanter l'entreprise ou d'en tirer un bénéfice financier. Un autre point surprenant concerne l'intention affichée de publier l'intégralité du leak. En exposant les vulnérabilités au grand public, l'intérêt stratégique de posséder ces données s'en trouve largement réduit. Certes, à court terme, cela représente une menace pour la sécurité de *Naval Group*, mais à moyen et long terme, cela annule toute exclusivité d'exploitation. Un acteur malveillant réellement intéressé par ces informations aurait plutôt intérêt à les garder confidentielles aussi longtemps que possible.

On observe également, dans la démarche de *Neferpitou*, des signes d'amateurisme, visibles à travers plusieurs détails :

- L'utilisation de *MegaUpload* pour héberger un leak présenté comme étant aussi sensible.
- Le décompte accompagnant la publication semble avoir été pensé pour commencer à 7h30 du matin (en se basant sur les deux derniers messages), mais le message initial est publié 2h30 plus tôt, sans explication.
- Enfin, son incapacité à héberger les données sur un serveur personnel, solution pourtant proposée gratuitement par certains membres du forum interroge, surtout dans une logique de pérennisation du leak.

Tous ces éléments contredisent, ou du moins nuancent fortement, l'image d'un attaquant solitaire compétent, capable de compromettre un acteur stratégique de l'industrie de la défense.

TYPOLOGIE DES DONNÉES

Comparativement à d'autres fuites de taille équivalente dans le secteur de la défense ou des technologies sensibles, ce type de contenu est à la fois classique et très ciblé. D'autres leaks de plusieurs centaines de Go à plusieurs To dans des grandes entreprises ou organismes sensibles peuvent contenir des types de données plus étendus allant, par exemple, de données financières, de ressources humaines, de plans commerciaux à des secrets industriels très variés. Ici, la diversité est plus technique et spécifique aux systèmes militaires navals.

Parmi les données annoncées dans les leaks ou dans les extraits, ne semblent avoir été confirmés que les éléments suivants :

- Documents internes classifiés (mais non « secret défense ») liés aux sous-marins et frégates ;
- Vidéos d'un ancien système de surveillance sous-marin datant de 2003 ;
- Plus d'une centaine de captures d'écran liées aux frégates de défense et d'intervention et aux frégates multimissions ;
- Une partie du code source du logiciel du système d'armes STORM utilisé dans les sous-marins nucléaires d'attaque ;
- Fichiers liés aux systèmes de gestion de combat (CMS) embarqués sur sous-marins et frégates ;
- Documents techniques couvrant la période 2019-2024.

Il est intéressant de constater que parmi l'entièreté des données annoncées, deux tropismes semblent présents :

- Un accent important sur les documents liés aux frégates, notamment des frégates de défense et d'intervention (FDI) et des frégates multimissions (FREMM). Ces documents comprennent des captures d'écran, des guides, et des données techniques spécifiques à ces bâtiments.

- Une focalisation marquée sur le CMS (système de gestion de combat) et des éléments logiciels associés. L'attaquant a notamment publié une partie du code source du logiciel du système d'armes STORM, utilisé dans les sous-marins nucléaires d'attaque, ainsi que des fichiers liés aux systèmes de gestion de combat embarqués à bord des sous-marins et frégates. *Naval Group* a confirmé que ces documents logiciels font partie des données volées et publiées.

Ces deux orientations constituent la majeure partie du contenu révélé, ce qui peut apporter des informations pertinentes sur les objectifs de l'attaque. S'il s'agit d'une attaque réputationnelle réalisée par un concurrent de *Naval Group* ou d'un concurrent de l'un de ses sous-traitants, elles pourraient éclairer le type de contrats ou le domaine de concurrence.

CONCURRENCE DANGEUREUSE

On peut s'interroger sur les véritables objectifs de cette opération, en partant du principe qu'il ne s'agit pas simplement d'une tentative de cyberattaque ayant en partie échoué, et surtout au regard du fait que son auteur ne semblait pas être motivé par l'argent. On peut émettre l'hypothèse qu'il s'agisse d'une opération qui vise surtout à s'en prendre à la réputation du groupe.

En réalité, ce n'est pas la première fois que *Naval Group* est la cible d'une fuite de données. En 2016, peu après avoir remporté l'appel d'offres pour la conception des sous-marins australiens, l'entreprise a été confrontée à une fuite massive de documents concernant les sous-marins Scorpène destinés à l'Inde.

Si les vecteurs et les contextes techniques diffèrent sensiblement de ceux d'aujourd'hui, les suites de cette enquête peuvent être utiles au regard du leak de 2025. En 2016, le journal *The Australian* a révélé la fuite de plus de 22 000 pages de documents sensibles portant sur les six sous-marins Scorpène construits par la France pour le compte de la marine indienne. Ces documents étaient supposés détailler, entre autres, les capacités de combat, les performances techniques, les fréquences utilisées pour la collecte de renseignements, les niveaux de bruit à différentes vitesses, ainsi que les profondeurs de plongée.


Scorpene submarine leak: Huge setback for India as 22,000 pages of secret data leaked

Scorpene Submarine data leak: If the secret data was indeed leaked from France, this is bound to strain India's defence relationship with France.

Cependant, l'enquête a révélé que les documents provenaient d'un ancien sous-traitant de *DCNS* (ancien nom de *Naval Group*), qu'ils étaient partiellement censurés, faiblement classifiés, et surtout très anciens. À la suite de cette évaluation, les autorités indiennes ont conclu qu'ils ne représentaient aucun risque significatif pour la sécurité nationale.

New Scorpene submarine details emerge, navy says leak not serious

L'affaire, qualifiée rétrospectivement de « pseudo-fuite » par certains médias, a été classée sans suite par l'Inde un an plus tard, faute de contenu réellement sensible dans les documents diffusés.

Au regard de ce passif, il est possible que cette attaque soit plus informationnelle que cyber. Le but étant d'attenter à la crédibilité du groupe plutôt que de vider son portefeuille. *Naval Group* est un élément essentiel de la dissuasion nucléaire française, mais c'est également une entreprise très performante à l'export. Une attaque de ce type viserait probablement plus la crédibilité de l'entreprise à l'export que sa capacité à gérer la dissuasion nucléaire française.

En effet, une telle attaque prendrait tout son sens, car *Naval Group* est actuellement impliqué dans plusieurs appels d'offres, comme par exemple :

- **L'appel d'offres pour 12 sous-marins au Canada.**

Naval Group a longtemps étudié la possibilité d'une candidature suite à des déconvenues dans le passé avec le pays. Le groupe a finalement officialisé sa candidature en février 2025. Il s'agirait d'un contrat à 40 millions d'euros pour 12 sous-marins à propulsion conventionnelle. *Naval Group* semble vouloir proposer une version à propulsion classique du SNA Barracuda.

> Le français Naval Group devrait finalement participer à l'appel d'offres des futurs sous-marins canadiens

Dans cet appel d'offres, l'entreprise est en concurrence avec : l'Allemagne et la Norvège (sous-marin U212CD) la Corée du Sud (sous-marins KSS-III Batch 2), la Suède et les Pays-Bas (C-71 Oceanic) et l'Espagne (S-80).

- **L'appel d'offres pour les nouvelles frégates de la Norvège.**

Le groupe espère vendre cinq à six frégates FDI à la marine norvégienne, et est en compétition avec les États-Unis (la Constellation), les Britanniques (la T26), et les Allemands (la Meko A-400).

En plus de commercial, cet appel d'offres a une dimension aussi stratégique puisque la France et la Norvège veulent approfondir leur relation en matière de défense. raison pour laquelle le président s'est déplacé en Norvège pour la première fois depuis 41 ans.

- **Le programme de Corvette européenne (PESCO EPC/MMPC).**

Naval Group est impliqué dans le programme de corvette européenne à travers le consortium Naviris (joint venture entre Naval Group et Fincantieri), qui a été choisi en 2023 par l'OCCAR (Organisation for Joint Armament Cooperation) pour coordonner le projet. Le projet total a une valeur totale de 87 millions d'euros.

La première phase pour laquelle le consortium a été choisi vise à concevoir un design pour la nouvelle génération de corvettes.

- **Le contrat de maintenance pour corvettes Gowind.**

Naval Group a construit les deux corvettes pour les Émirats arabes unis, livrées respectivement en 2022 et 2023, pour un contrat d'une valeur de 850 millions d'euros. Sachant que le contrat prévoit une clause qui n'a pas encore été exercée pour l'achat de deux corvettes supplémentaires. En 2025, le groupe a également signé un autre contrat avec le royaume pour la maintenance et la formation sur ces deux corvettes.

> **Naval Group signs a maintenance contract with the UAE for the Gowind corvettes**

Dans ce contexte, une attaque de ce type visant la réputation et la crédibilité du groupe à l'export pourrait venir d'un concurrent. Ce qui n'exclut pas les alliés de la France puisque les principaux concurrents de *Naval Group* à l'export sont des pays européens, ou plus largement des pays alliés. C'est d'ailleurs une hypothèse souvent avancée sur les réseaux sociaux. D'autant plus que l'attaque ne visait clairement pas à complètement détruire le groupe (sinon les leaks auraient été plus consistants) mais surtout à entacher sa réputation.

Les éléments mentionnés dans le leak sont nombreux, mais il semble se concentrer sur les frégates, en particulier la FDI et la FREMM, ainsi que sur les SSN. Dans ce contexte, plusieurs appels d'offres en cours, ou récemment attribués mais dont les livraisons n'ont pas encore été effectuées, méritent une attention particulière en tant que candidats potentiels aux motivations de l'attaque.

Le plus évident est le contrat signé avec l'Indonésie pour la livraison de deux sous-marins Scorpène. L'élément le plus convaincant en faveur de cette hypothèse est le timing : le contrat est officiellement entré en vigueur le 23 juillet, soit le jour même du début de l'attaque.

Cependant, une telle action s'apparenterait davantage à une tentative désespérée. L'Indonésie a déjà validé l'accord ; l'annuler lui coûterait cher en pénalités contractuelles. De plus, le pays bénéficie largement de ce partenariat : *Naval Group* prévoit un transfert de technologies, permettant à l'Indonésie de construire elle-même les sous-marins, avec à la clé des retombées positives pour l'économie locale et le développement de son industrie de défense.

Entrée en vigueur du contrat Scorpène® Evolved pour l'Indonésie

Le contrat pour la livraison de deux sous-marins Scorpène® Evolved, qui seront construits en Indonésie, par et pour l'Indonésie, au sein du chantier naval de PT PAL grâce à un transfert de technologie de Naval Group, est entré en vigueur le 23 juillet 2025.

Dans une moindre mesure, un deuxième candidat potentiel est le contrat passé avec la Grèce. Depuis 2020, *Naval Group* a régulièrement signé des accords avec le gouvernement grec pour la vente de frégates FDI. Plus récemment, en juin 2025, le ministre grec de la Défense a annoncé l'achat d'une nouvelle frégate, renforçant encore la coopération entre les deux pays.

Plusieurs éléments appuient cette hypothèse, notamment le timing, mais aussi le contenu du leak, qui accorde une place importante aux frégates FDI dans les différents échantillons publiés.

De plus, la réaction grecque à l'annonce de la fuite a été particulièrement marquée : la Grèce est le troisième pays, après la France, à avoir publié le plus d'articles sur le sujet entre le 23 juillet et le 2 août. Cela pourrait refléter une inquiétude spécifique de la part des autorités ou des médias grecs, en particulier au regard du fait qu'ils s'inquiètent que la Turquie ait accès à des informations sur leurs frégates.

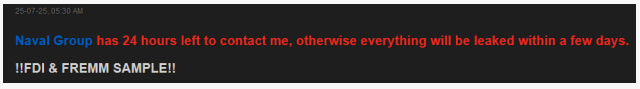
Grèce
Les groupes de défense grecs ferraillent pour s'arrimer à Naval Group

Enfin, il est également possible que l'attaque vise l'appel d'offres des frégates norvégiennes mentionnées plus haut. Dans ce cas précis, les contenus du leak et timing correspondent également.

Le vainqueur de cet appel d'offres pour lequel *Naval Group* est en shortlist devrait être connu pendant l'été selon les autorités norvégiennes. Donc ce type d'attaque interviendrait au bon moment, juste avant la décision finale pour départager les candidats.

Bien sûr, il y a le marché des frégates. Interrogé sur le sujet, Jonas Gahr Støre l'a rappelé : « nous voulons voir de plus en plus de frégates françaises devant nos côtes. Cette présence est très appréciée. Nos navires s'entraînent ensemble, c'est un signe de solidarité entre alliés et de professionnalisme ». Mais au sujet de l'appel d'offres pour 5+1 frégates, dont le lauréat devrait être connu durant l'été, il le répète : « la Norvège choisira le meilleur bateau au meilleur prix avec le meilleur partenaire. Nous le ferons de la manière la plus transparente et nous sommes toujours dans une période où nous considérons que nous avons quatre excellents candidats ».

Ensuite, comme mentionné plus haut, une partie assez significative du leak et des échantillons se concentre sur ces fameuses frégates. Au milieu de beaucoup d'éléments généraux annoncés et difficiles à qualifier, c'est un de ceux qui sont les plus précisés.



COURS DE THALES

Le 28 juillet, *Reuters* relaie le leak, l'agence note que *Thales* possède 35% des parts de *Naval Group*. La bourse s'agite, le volume échangé sur le titre monte de 75% et sur cette même journée *Thales* perd 3,4% de sa capitalisation boursière. Autre fait intéressant, *Thales* annonce ses résultats semestriels le même jour que la publication du premier post du leak.

Un cas similaire bien documenté concerne *Hindenburg Research* qui a exploité un lot de courriels et de factures extraits d'un fournisseur d'*Adani Group* pour appuyer son rapport ; la capitalisation du conglomérat a fondu de 150 Mds $ et la régulation indienne enquête encore sur cette opération.

Plusieurs cas ont lié des leaks (codes source, mails, données techniques) à une stratégie de vente à découvert (short selling). Ces stratégies visent à provoquer une déstabilisation du cours et éventuellement un effet de masse entrainant le cours d'un titre vers le bas.

Le ciblage d'une filiale non cotée comme *Naval Group* pour atteindre la maison mère cotée est aussi une stratégie déjà utilisée. Les incohérences relevées pourraient alors prendre sens dans une telle stratégie.

Bien qu'intéressante, cette théorie perd en substance en analysant le registre public des positions courtes de la *bourse de Paris*. Ce registre publie toutes les positions shorts sur cette place boursière supérieures à 0,5% de la valeur de l'entreprise. Nous pouvons ainsi y analyser qu'aucune position de la sorte et massive n'a été placée.

Pour ces raisons, l'attaque ne pouvait viser une baisse durable du cours de l'action de *Thales*. Il est tout de même possible qu'un plus petit acteur, moins organisé et avec moins de ressources, ait organisé ce type d'opération pour des gains rapides modestes. Mais ce type d'opération reste rare, surtout en France, et aucune preuve supplémentaire ne vient étayer l'hypothèse.

De même, aucun rapport de l'un des fonds d'investissement ayant recours à cette pratique n'a été révélé. L'attaque est peu crédibilisée, que ce soit par le nom/pseudonyme de l'auteur des publications, qui n'est pas rattaché à un organisme, et ses preuves ne légitiment pas son action.

Dernier élément qui affaiblit cette théorie, d'autres annonces ont été faites conjointement à celle du leak concernant l'impact des tarifs douaniers américains et leur impact sur la BITD. Il est plus probable que la réaction des marchés soit une conséquence naturelle et non instrumentalisée de la médiatisation du leak et de ces nouvelles.

LEAK DES SOUS-MARINS RUSSES

Le 3 août 2025, soit 10 jours après la publication de *Neferpitrou*, la *Direction principale du renseignement militaire ukrainien (HUR)* a publié sur son site et ses canaux *Telegram* un lot de documents présenté comme « l'ensemble du dossier technique interne » du K-555 Knyaz Pozharsky, sous-marin nucléaire lanceur d'engins russe de la classe Boreï-A officiellement admis au service le 24 juillet 2025.

En moins de deux semaines, deux fuites de données stratégiques concernant des sous-marins militaires ont eu lieu, un type de donnée extrêmement rare et difficile à obtenir. Qui plus est, de deux puissances rivales.

Les pièces diffusées (plans de coque, schémas de survivabilité, organigrammes d'équipage, extrait du carnet de service quotidien) indiqueraient les procédures de combat, les points de maintenance critiques et les limites de furtivité du bâtiment ; le *HUR* affirme que ces informations « révèlent des vulnérabilités applicables à toute la flotte Boreï ».

Ces publications constituent une source primaire ; elles n'ont toutefois pas été authentifiées par une expertise indépendante. Les médias ukrainiens (*Kyiv Independent, United24 Media*) et plusieurs titres internationaux (*The Times, Business Insider, Bitdefender HotForSecurity*) se sont appuyés sur ces fichiers ou sur la courte note explicative du *HUR* pour relayer l'affaire, sans accès aux systèmes russes ni corroboration technique externe.

Côté russe, le *ministère de la Défense* et le constructeur *Sevmash* n'ont fait aucune déclaration. L'absence de démenti brutal, fréquente dans la doctrine informationnelle de Moscou, ne vaut ni confirmation ni infirmation. Plusieurs analystes indépendants (*Moscow Digital Security Lab, CIT*) notent que la mise en ligne de schémas complets, si elle était falsifiée, exposerait rapidement *HUR* à un démenti vérifiable ; leur prudence indique que la fuite pourrait être partielle mais authentique. D'autres experts – notamment chez *Bitdefender* – rappellent qu'« aucune signature numérique ou empreinte d'intégrité n'accompagne les fichiers » et qu'il est donc impossible, pour l'instant, de valider l'intégralité du lot.

Si elle est confirmée, l'opération inflige un double dommage : elle offre à l'Ukraine (et potentiellement à ses alliés *OTAN*) une radiographie détaillée du dernier maillon de la triade nucléaire russe et expose la faillibilité des protocoles de protection russes. La fuite pourrait forcer Moscou à réviser tout ou partie des procédures de maintenance, au prix d'arrêts techniques longs et coûteux.

Si l'écho avec l'affaire française est plus que proéminent, plusieurs différences notables sont importantes à souligner et tendent à valider la supposition initiale qu'il n'y a pas eu de hacking de la part d'un État étranger sur *Naval Group*. D'abord les données partagées par le *HUR* l'ont été en son nom propre ce qui diverge grandement de l'acte non signé sur *Naval Group*. Ensuite l'intégralité des données .

a été partagé et non des échantillons douteux.

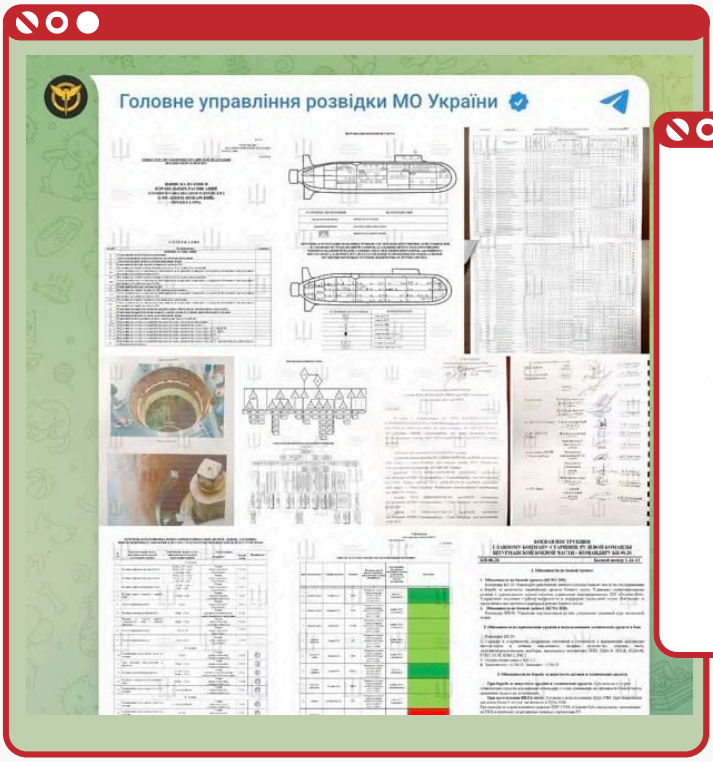
Les données partagées par Kiev ont aussi un intérêt stratégique à être partagées. Le pays n'a pas forcément les moyens d'exploiter pleinement le potentiel de ces ressources et pourra par la diffusion utiliser les autres rivaux de la Russie pour attenter à ses intérêts tout en économisant des moyens à Kiev.

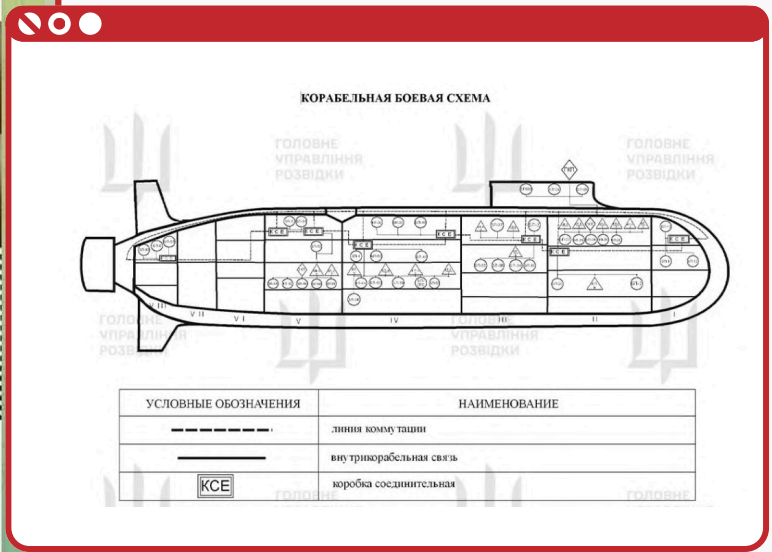
D'autre part la Russie a des moyens de réaction limités, les données fuitées concernent des éléments stratégiques très difficilement remplaçables, en particulier le personnel de bord qualifié, et le nouveau sous-marin en lui-même qui a pris plus de dix ans de développement. Enfin il est à souligner que l'Ukraine a un enjeu réputationnel immense à défendre dans le cadre de cette opération puisqu'elle contribue à légitimer ses services de renseignement et contribue à discréditer l'armée russe. Ces informations poussent à donner bien plus de crédit aux données fournies par le *HUR*.

Il reste que la temporalité est suspecte. Il est possible que les services russes aient détecté l'intrusion ukrainienne et aient engagé une attaque réputationnelle sur l'un de ses rivaux afin de diverger l'attention hors de cette humiliation. La Russie est habituée à de telles opérations de guerre informationnelle.

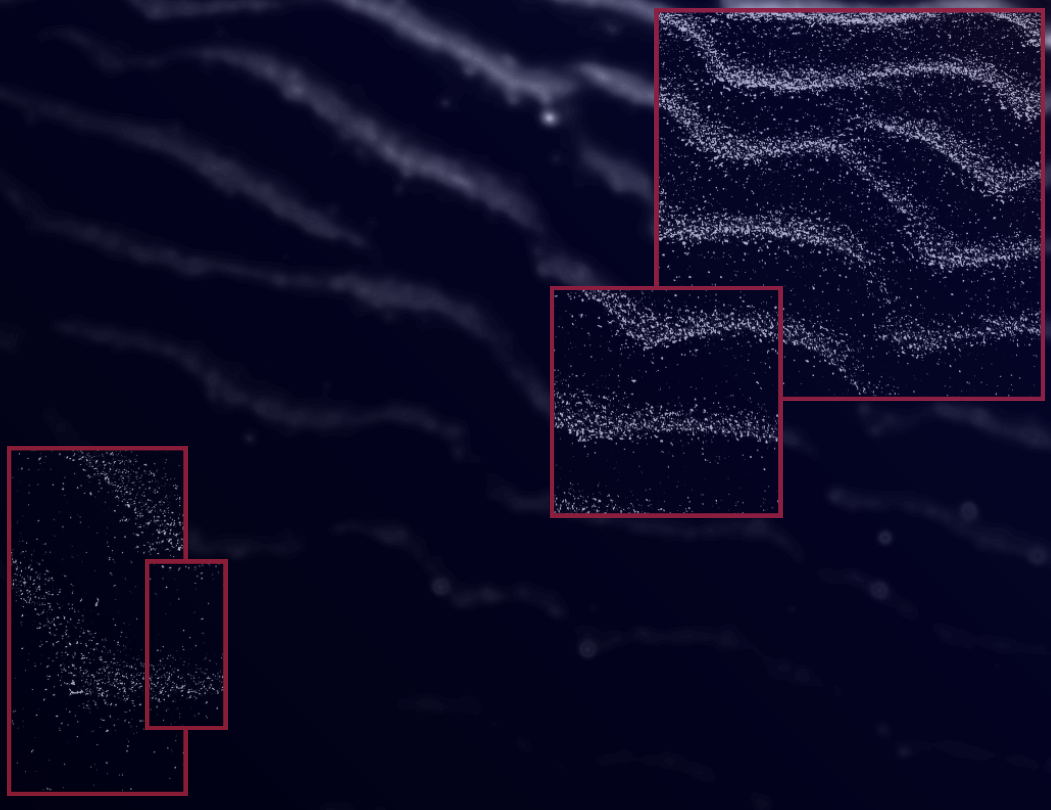
S'il pourrait alors paraitre aisé de conclure à l'implication de la Russie dans cette attaque sur *Naval Group*, plusieurs éléments sont dissonants avec cette hypothèse. Ils reposent principalement sur l'apparent amateurisme de l'opération en contraste avec l'expertise russe en la matière. De plus, l'affaire a eu un écho dans les médias russes mais extrêmement tardivement, au même rythme que le reste du monde.

Si l'opération visait spécifiquement l'occultation de l'information en France sur le hacking du *HUR*, on peut s'interroger sur l'intérêt d'une telle manœuvre. La manœuvre a trop rapidement été contrée par *Naval Group*, ce qui empêche un retentissement efficace en France comme dans d'autres pays.





RETEX DE L'ATTAQUE



LEAKS ET ATTAQUE RÉPUTATIONNELLE

De manière générale, et au regard de ce que l'on sait des fuites d'informations (leaks), il semble que la stratégie mise en œuvre repose sur l'exploitation de plusieurs biais cognitifs propres à l'audience ciblée.

La fascination pour le contenu caché et le culte du secret

Le simple fait de présenter une information comme « cachée » ou difficile d'accès ne signifie pas nécessairement qu'elle soit sensible ou réellement exploitable. Dans bien des cas, ces données sont déjà connues des acteurs véritablement intéressés ou sont de faible valeur opérationnelle.

Un exemple parlant est celui des fuites récurrentes sur les forums de *War Thunder*, où des manuels techniques de chars ou d'avions militaires sont régulièrement divulgués. Bien que ces documents puissent violer des clauses de confidentialité, les armées ou services de renseignement susceptibles d'en tirer parti disposent souvent déjà de ces informations par d'autres canaux. Pourtant, pour un public non initié, ces publications alimentent l'idée d'une révélation exceptionnelle ou dangereuse.

Ces leaks sont typiquement publiés sur *War Thunder* par des gens qui travaillent dans l'armée, dans le but de rendre le jeu plus fidèle à la réalité, ce qui fascine les gens extérieurs à cette communauté. Ce mécanisme récurrent pouvant des fois être utilisé pour des campagnes d'influence.

Ce biais est renforcé par une tendance fréquente à surprotéger des contenus qui, en réalité, n'ont qu'une faible valeur stratégique. Les restrictions de communication ou les niveaux de classification excessifs peuvent alors créer un effet paradoxal : plus un document est protégé, plus il attire l'attention, car il semble précieux. À l'inverse, un contenu peu protégé sera souvent ignoré, perçu comme sans valeur. L'idéal, dans une optique de sécurité discrète, serait de trouver un équilibre entre ces deux extrêmes.

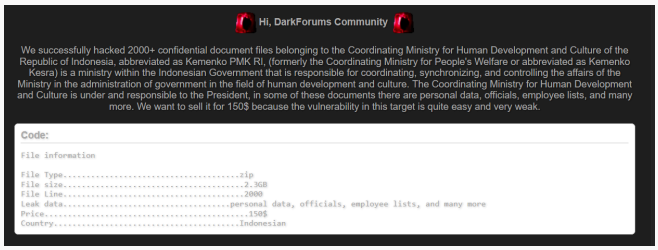
Ce biais psychologique est bien connu dans le monde des leaks, et il fonctionne presque systématiquement, car il n'existe pas de réponse simple. Si l'auteur d'une fuite construit un narratif cohérent autour d'un supposé contenu secret (en jouant sur le culte du secret ou de la dissimulation), l'effet sera efficace : la plupart des observateurs ne chercheront pas à vérifier la véracité de ces affirmations.

Dans le cas de l'affaire *Naval Group*, ce mécanisme a bien fonctionné dans un premier temps. L'attaque a été perçue pour beaucoup d'observateurs étrangers comme la démonstration d'une incapacité de l'entreprise à protéger des secrets industriels.

Mais à mesure que les données ont été examinées, des voix d'experts se sont élevées pour nuancer, voire contester, le caractère réellement sensible de ce qui avait été exposé.

Autrement dit : dans le cas d'un leak qui vise à attenter à la réputation d'une organisation, l'emballage du secret compte parfois plus que son contenu réel.

Cette stratégie est également fréquemment utilisée par les vendeurs de leaks, que leur objectif soit de nuire à une organisation ou simplement de susciter l'intérêt pour maximiser leur profit ou leur notoriété.



Par exemple, dans l'exemple suivant, le vendeur propose une base de données hackée appartenant au *Ministère du Bien-être social* indonésien, et contenant globalement des listes d'employés et quelques adresses de contact (vendues comme informations personnelles). Un effort a été fait pour donner un peu de consistance au leak en disant que le ministère répond directement du président pour l'effet dramatique. Mais en réalité, et surtout dans le cas d'un organisme public, cette liste peut être constituée facilement avec quelques outils et en source ouverte.

L'utilisation du jargon technique et l'effet de masse

Le recours à un langage très technique sert souvent à donner une apparence de légitimité à une fuite. Même lorsque ce jargon est peu pertinent, il suffit que la majorité des lecteurs ne le comprennent pas pour qu'ils associent automatiquement le contenu à des informations sensibles, voire classifiées.

Cet effet est particulièrement puissant et insidieux, car il peut persister longtemps. Lorsqu'une fuite contient plusieurs milliers de pages, les analyses expertes prennent du temps à émerger. Entre-temps, le public a tout le loisir d'extrapoler, spéculer, voire fantasmer sur la gravité des documents.

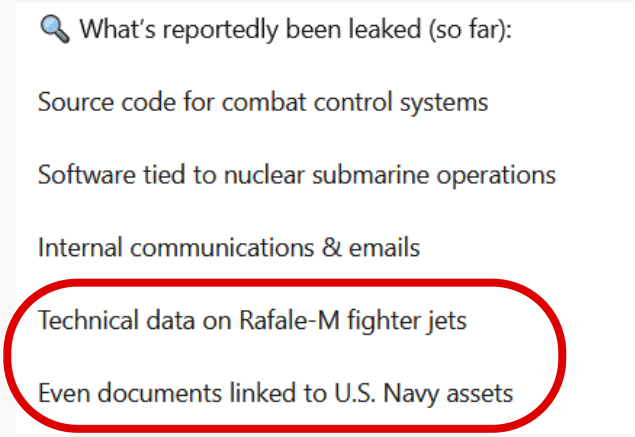
La méthode est d'autant plus efficace si le leaker maîtrise les termes spécifiques, acronymes, nomenclatures et autres éléments de langage propres à l'organisation ciblée.

Dans le cas de *Naval Group*, ce levier a clairement été utilisé pour donner de la consistance à l'ensemble. Comme évoqué dans le premier chapitre, le leackeur alterne entre :

- des éléments extrêmement précis (noms de programmes, CRM internes) ;
- et d'autres très vagues ou génériques (comme "communications") sans préciser leur nature ou leur contenu.

L'objectif est clair : exploiter ce biais cognitif pour produire un effet de masse. En mobilisant le jargon identifiable et crédible, on donne du poids à la partie la plus floue du leak, en l'occurrence les "communications", qui restent invérifiables et probablement exagérées, voire fictives.

Ces zones d'ombre nourrissent d'autant plus la spéculation : chaque lecteur peut y projeter ses propres inquiétudes ou interprétations. C'est ainsi que des affirmations ou des documents non mentionnés dans le leak initial ont commencé à circuler sur les réseaux sociaux, preuve que le storytelling a pris le dessus sur le contenu réel.



L'accès restreint aux liens de téléchargement

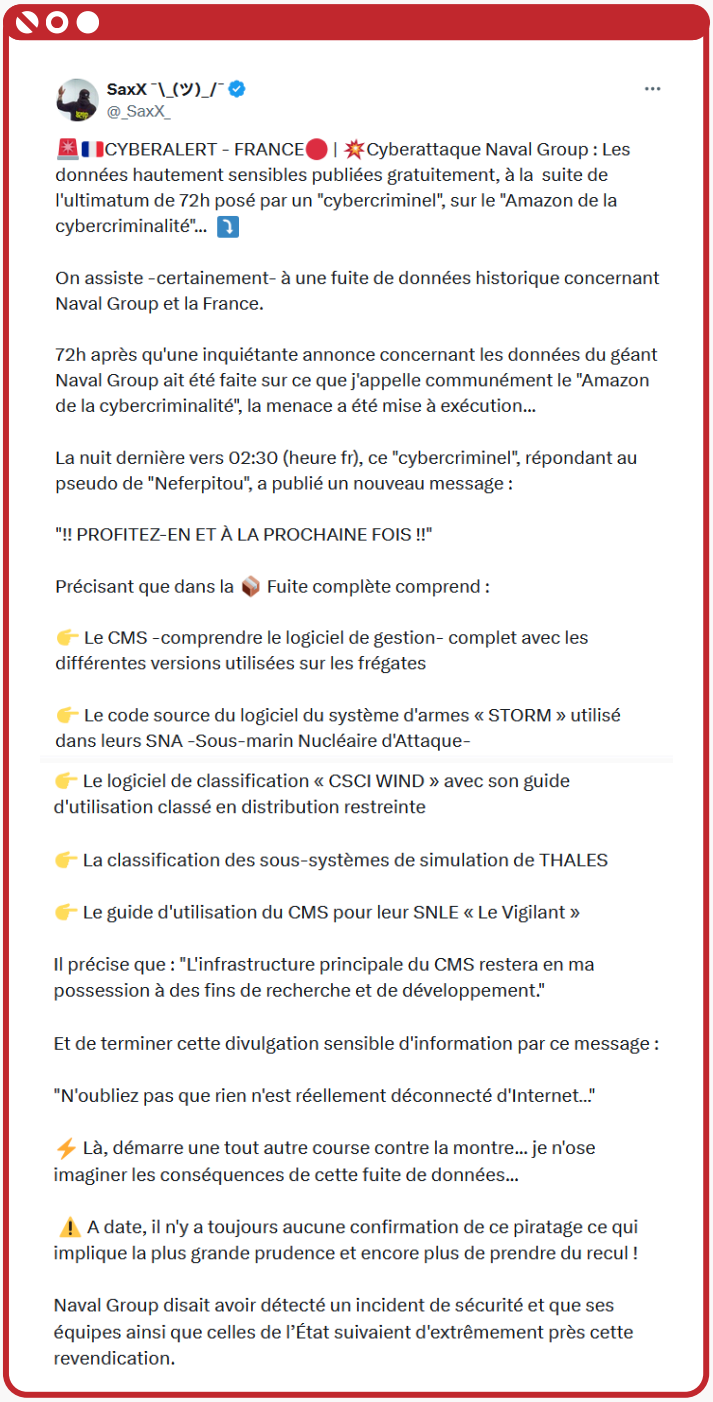
L'un des effets les plus durables de cette affaire pourrait être la perception amplifiée de la sensibilité des données, davantage que leur contenu réel. En l'absence de republication des fichiers fuités, une forme de rareté s'est construite autour du leak. Très peu de personnes y ont effectivement eu accès, ce qui renforce la tendance à en parler dans des termes impressionnants ou alarmants.

Ce phénomène crée un déséquilibre : le grand public, n'ayant pas vu les documents, est davantage enclin à croire qu'ils contiennent des informations hautement confidentielles, surtout si ceux qui y ont eu accès emploient un langage technique ou adoptent un ton grave.

Ce biais s'ancre d'autant plus facilement dans les environnements numériques où la mise en scène de l'expertise est valorisée.

C'est notamment le cas sur les réseaux sociaux professionnels comme *LinkedIn*, où certains utilisateurs partagent des extraits du leak (comme des captures des arborescences de dossiers, sans contenus spécifiques). Ce type de publication peut permettre de gagner en visibilité ou en légitimité dans des cercles où ce genre d'événement est perçu comme une opportunité d'analyse ou de prise de position.

Un exemple particulièrement révélateur est celui des captures publiées par @SaxX, qui semblent être les seules images disponibles montrant la structure des dossiers contenus dans le leak. Ces tweets ont été postés à peine une trentaine de minutes après la publication de l'échantillon. Il semble donc peu probable que leur auteur ait eu le temps d'analyser en profondeur les documents, d'autant plus qu'il s'agit de données techniques utilisant une nomenclature spécifique à *Naval Group*.



SaxX ¯_(ツ)_/¯
@_SaxX_

🚨🇫🇷CYBERALERT - FRANCE🔴 | 💥Cyberattaque Naval Group : Les données hautement sensibles publiées gratuitement, à la suite de l'ultimatum de 72h posé par un "cybercriminel", sur le "Amazon de la cybercriminalité"... ⤵️

On assiste -certainement- à une fuite de données historique concernant Naval Group et la France.

72h après qu'une inquiétante annonce concernant les données du géant Naval Group ait été faite sur ce que j'appelle communément le "Amazon de la cybercriminalité", la menace a été mise à exécution...

La nuit dernière vers 02:30 (heure fr), ce "cybercriminel", répondant au pseudo de "Neferpitou", a publié un nouveau message :

"!! PROFITEZ-EN ET À LA PROCHAINE FOIS !!"

Précisant que dans la 📦 Fuite complète comprend :

👉 Le CMS -comprendre le logiciel de gestion- complet avec les différentes versions utilisées sur les frégates

👉 Le code source du logiciel du système d'armes « STORM » utilisé dans leurs SNA -Sous-marin Nucléaire d'Attaque-

👉 Le logiciel de classification « CSCI WIND » avec son guide d'utilisation classé en distribution restreinte

👉 La classification des sous-systèmes de simulation de THALES

👉 Le guide d'utilisation du CMS pour leur SNLE « Le Vigilant »

Il précise que : "L'infrastructure principale du CMS restera en ma possession à des fins de recherche et de développement."

Et de terminer cette divulgation sensible d'information par ce message :

"N'oubliez pas que rien n'est réellement déconnecté d'Internet..."

⚡ Là, démarre une tout autre course contre la montre... je n'ose imaginer les conséquences de cette fuite de données...

⚠️ A date, il n'y a toujours aucune confirmation de ce piratage ce qui implique la plus grande prudence et encore plus de prendre du recul !

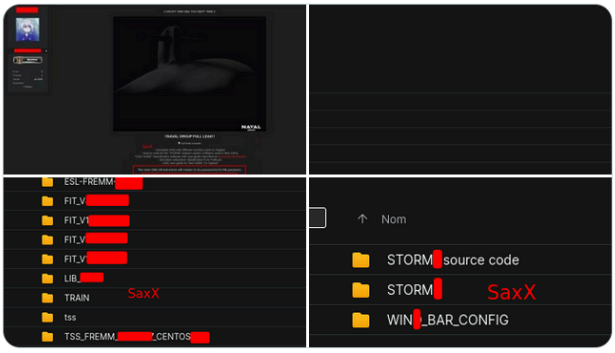
Naval Group disait avoir détecté un incident de sécurité et que ses équipes ainsi que celles de l'État suivaient d'extrêmement près cette revendication.

👀 Ce cybercriminel -que dis-je, NON ce n'est pas un cybercriminel mais PLUS UN ACTEUR MALVEILLANT ÉTATIQUE ou SEMI-ÉTATIQUE- semble avoir préparé depuis longtemps son coup au regard de l'actualité du Group, de celle de la France.

Diffuser gratuitement toutes ces informations sans monnayer une seule fois ces données hyper sensibles, il y a un agenda et des motivations qui restent à trouver...

Cybèrement vôtre,

SaxX ¯_(ツ)_/¯



8:06 AM · 26 juil. 2025 · **382,7 k** vues

Cependant, le ton alarmiste du message et la simple présence de captures d'écran crédibilisent la publication. Cela a largement contribué à façonner la perception dominante du leak, notamment sur *Twitter* et *LinkedIn*, où les mêmes éléments ont été repris à de nombreuses reprises, souvent dans des termes similaires.

French defence tech company Naval Group breached in a cyber attack.

The data leak, now up after a 72hr ultimatum, includes:

- the internal CMS
- weapon system software source code for a nuclear attack submarine
- classification software
- simulation subsystems

Makes you wonder:

How is the cyber security posture of all the defence tech startups coming up in India?

Afficher la traduction

Data breach targeting Naval Group, the French military-industrial giant specializing in submarines and advanced naval platforms. The leaked package, posted openly on a dark forum by a user named SaxX / Neferpitou, contains:

Full CMS (Combat Management System) source code for French FREMM frigates and SSBN submarines.

Simulator subsystems classified under THALES.

Weapon system software used on nuclear-powered submarines (SSBNs like Le Vigilant).

The complete STORM3 submarine CMS package, including source code, test benches, and network config folders.

Classified guides, internal documentation, and even CSCI WIND classification schemas.

The hacker claims the main CMS infrastructure remains in their possession for "RE purposes", likely reverse engineering or further leverage.

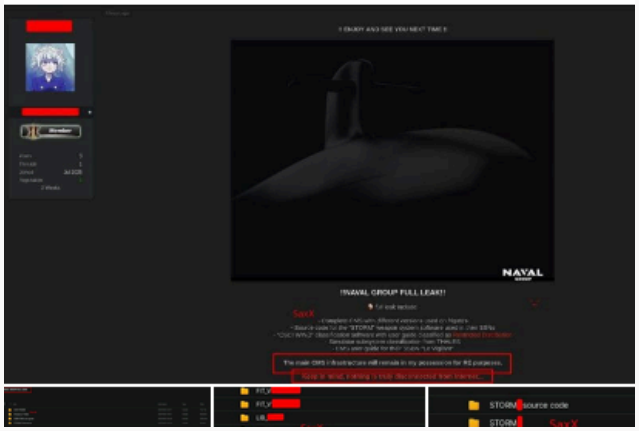
This is arguably the most devastating leak in French defense history. Naval Group, THALES, Dassault, and Safran are all implicated due to their collaborative integration layers. Internal documents suggest simulator environments were also compromised, raising the risk of replication or spoofing of French submarine behaviors.

No ransom. No conditions. Just a brutal, free release.

Quote from the leaker:

"Keep in mind, nothing is truly disconnected from Internet..."

Afficher la traduction



When France's nuclear submarine source code leaks, can we just file a GDPR 'right to be forgotten' request? ... plus

Afficher la traduction

Dans le but d'alimenter cet effet de rareté et de spéculation, il est également possible que le choix d'héberger les échantillons sur *Megaupload* ne soit pas anodin. Si l'attaque a été véritablement réfléchie, il est probable que l'auteur savait que les liens ne resteraient pas en ligne très longtemps, mais qu'ils suffiraient à permettre à quelques personnes de les télécharger, puis d'en parler. Cela aurait suffi à faire circuler l'idée d'un contenu sensible, sans que celui-ci soit largement accessible.

C'est une stratégie risquée, qui aurait aussi pu aboutir à ce que personne n'y accède, ce qui est d'ailleurs presque ce qui s'est produit.

Partant du principe qu'il s'agit d'une attaque à la réputation, le but de l'attaque était de s'en prendre à la crédibilité du groupe. Le leak était conçu pour être viral, d'où le choix judicieux du vecteur. Et le contenu était fait pour exploiter des biais classiques de l'audience, dans un but là aussi de viralité (l'accès restreint aux liens de téléchargement), mais aussi de légitimité du tout (jargon technique, effet de masse et fascination pour le contenu caché). Mais plusieurs éléments dans l'exécution ont limité l'impact de cette campagne et, dans ce contexte, ont offert à *Naval Group* des conditions relativement favorables pour gérer la situation sur le court terme.

🚨 Naval Group Cyberattack: A National Security Risk

France's leading naval defense contractor, #Naval_Group, has reportedly suffered a major cyberattack exposing 13GB of sensitive data, including:

1- Source code for Submarine Combat Management Systems
2- Classified technical documents
3- Internal network data & Developer Virtual Machines
4- Confidential communications

This breach isn't just operational; it's a direct threat to national security. Adversaries gaining access to this data could compromise France's naval capabilities.

The lesson:
Business Continuity & Disaster Recovery is critical. When systems and secrets are on the line, rapid response and recovery can make the difference between containment and catastrophe.

#CyberSecurity #CyberResilience #BCDR #DataBreach #NationalSecurity #Naval(

1 terabyte of sensitive data from NAVAL GROUP is now circulating on cybercrime forums 💥
This is not a simulation.

🇫🇷 France's leading naval defence contractor has allegedly been breached, with leaks reportedly including:
- Combat submarine system files,
- Technical schematics,
- Internal IT infrastructure documents.

A 13 GB "proof pack" was posted.
The rest, nearly 1 TB, is being leveraged in what appears to be a silent extortion campaign.

This is not just a breach.
It is a strategic exposure.

In 2025, nation-state-grade leaks no longer require sophisticated zero-days.
They only require one gap.
In a supply chain.
In a process.
In a decision not made.

For defence contractors and public entities:
- Cybersecurity is now a matter of sovereignty,
- Detection is not enough, containment must be immediate
- Technical silos must give way to national coordination

Cybernews 👉 https://lnkd.in/dMK-z2Ef

Illustration: Falconfeeds.io

—
First time here? I'm Romain Premaz, cybersecurity enthusiast.
Follow me for daily insights and cyber news. Let's connect!

France's Naval Group hit by major cyberattack, leaking 30GB of data, including nuclear sub weapon codes, Rafale-M docs, and US Navy combat systems.

Hacker Neferpitou's free dump after a 72hr ultimatum suggests ideological motives.

With France's $5.6B nuclear spending and 70% of EU critical infrastructure outdated, this exposes Western cyber vulnerabilities.

Risks of tech theft by China threaten NATO's naval edge amid Ukraine's $19B aid gap.

« Incredible that this isn't major news everywhere! Not seeing much of this story and not prominent. Not very difficult to imagine who is responsible. It's war. »
« France has suffered its biggest defense hack in history — codes for combat systems and software for nuclear weapons were stolen, the Financial Times reported.
The attack targeted the French defense company Naval Group, which produces submarines and warships. Hackers accessed classified data, including:

▪ Source code for combat systems
▪ Software for submarine nuclear weapons
▪ Documentation for Rafale-M fighter jets
▪ Internal management emails and network data
▪ Simulation systems

The hackers released 30 GB of information, which they claim also includes data on the combat control systems of US Navy submarines and frigates. US and French authorities have launched an investigation to verify the authenticity of the leaked data. »

FAKE NEWS

L'accès restreint aux liens de téléchargement et, plus généralement, au contenu du leak a également favorisé l'apparition de nombreuses informations erronées ou sujettes à caution. L'une des plus notables concerne une prétendue fuite de données sur le Rafale, largement relayée, notamment dans les médias russes, les 29 et 30 juillet.

Or, aucune partie du leak, ni aucune personne y ayant eu accès, n'a mentionné le Rafale. De plus, les articles évoquant cet avion illustrent souvent leur propos par une capture d'écran de l'annonce du leak… sur laquelle le Rafale n'apparaît pas.

D'où vient alors cette information ?

La trace la plus ancienne que nous ayons pu identifier remonte au 28 juillet, dans un article publié par un site kosovar nommé *Telegrafi*.


Local Telegraph · Latest Articles · telegrafi · Jobs · Real Estate · Deals

Home · NEWS · THE WORLD · Finance · Sports · Entertainment · Cult · Females · Styles · Health · kitchen · Cars · technology · Fun · Video

THE WORLD › From the World › Evropa ›

France faces largest cyberattack in history – secret defense data falls into the hands of hackers

The software that controls nuclear weapons deployed on French submarines;

Technical documentation for the Rafale-M fighter jets, used by the French air force and navy;

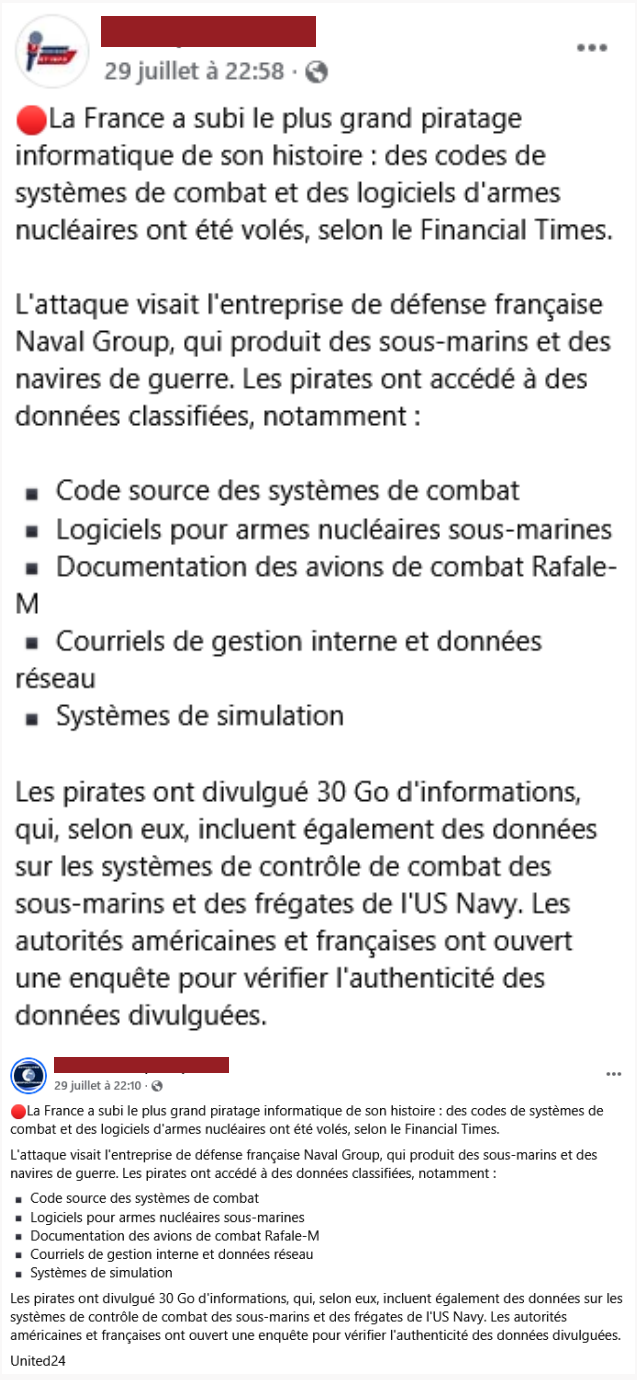
Internal emails of company executives, as well as internal communication network data.

`article_publication_date: "Mon, 28 Jul 2025 20:17:14 CEST"`

TELEGRAPH Ltd
St. Rexhep Mala, Aktash, No. 34, Pristina, Kosovo info@telegrafi.com 038 224 093 - +383 48 222 355

Cette information a ensuite été reprise à plusieurs endroits, le lendemain en fin de journée. Une chose en particulier interroge.

Certains articles ou posts mentionnent des sources qui n'ont visiblement jamais donné ces informations, comme le *Financial Times United24* ou *United24*, un média ukrainien, dans des messages copiés-collés à l'identique.


[redacted]
29 juillet à 22:58 ·

La France a subi le plus grand piratage informatique de son histoire : des codes de systèmes de combat et des logiciels d'armes nucléaires ont été volés, selon le Financial Times.

L'attaque visait l'entreprise de défense française Naval Group, qui produit des sous-marins et des navires de guerre. Les pirates ont accédé à des données classifiées, notamment :

- Code source des systèmes de combat
- Logiciels pour armes nucléaires sous-marines
- Documentation des avions de combat Rafale-M
- Courriels de gestion interne et données réseau
- Systèmes de simulation

Les pirates ont divulgué 30 Go d'informations, qui, selon eux, incluent également des données sur les systèmes de contrôle de combat des sous-marins et des frégates de l'US Navy. Les autorités américaines et françaises ont ouvert une enquête pour vérifier l'authenticité des données divulguées.

[redacted]
29 juillet à 22:10 ·

La France a subi le plus grand piratage informatique de son histoire : des codes de systèmes de combat et des logiciels d'armes nucléaires ont été volés, selon le Financial Times.

L'attaque visait l'entreprise de défense française Naval Group, qui produit des sous-marins et des navires de guerre. Les pirates ont accédé à des données classifiées, notamment :

- Code source des systèmes de combat
- Logiciels pour armes nucléaires sous-marines
- Documentation des avions de combat Rafale-M
- Courriels de gestion interne et données réseau
- Systèmes de simulation

Les pirates ont divulgué 30 Go d'informations, qui, selon eux, incluent également des données sur les systèmes de contrôle de combat des sous-marins et des frégates de l'US Navy. Les autorités américaines et françaises ont ouvert une enquête pour vérifier l'authenticité des données divulguées.

United24

ERREURS DE L'ATTAQUANT

Dès les premières heures, plusieurs failles majeures dans la stratégie de l'auteur ont pu être observées. Ces erreurs ont largement contribué à limiter la portée de l'opération.

Le timing

Le rythme très soutenu des publications n'a pas permis d'instaurer une pression progressive dans le temps. En diffusant rapidement l'ensemble des échantillons, l'auteur a lui-même levé l'incertitude qui aurait pu peser durablement sur l'entreprise. Cette précipitation a probablement facilité l'analyse interne du contenu publié, permettant à *Naval Group* d'évaluer rapidement la nature et la portée des fuites.

Par ailleurs, la présence d'un décompte associé aux publications a donné à la fuite une fin annoncée : il suffisait d'attendre. Comme *Naval Group* a conclu, dès le premier échantillon, que les données n'étaient pas sensibles, l'entreprise a choisi de laisser passer l'orage, tout en faisant supprimer les liens de téléchargement au fur et à mesure.

Les difficultés techniques

Si la faible disponibilité des fichiers a, comme expliqué précédemment, contribué à créer un effet de rareté à moyen terme, elle a surtout entravé la diffusion initiale du leak. Cela a eu un impact immédiat sur la captation de l'attention et a compromis la pérennité de l'opération. On peut même se demander si le leak n'aurait pas été quasiment ignoré, en l'absence de quelques captures d'écran, les seules preuves tangibles que certains contenus avaient bien été publiés.

La captation tardive de l'audience

Une large partie de la stratégie reposait sur l'effet viral, qui ne s'est toutefois pas déclenché immédiatement, ce qui a significativement réduit l'impact global de l'opération. Comme le montre le graphique de la page suivante, c'est le communiqué de *Naval Group* qui a, paradoxalement, contribué à rendre l'affaire visible, bien plus que la fuite en elle-même.

Cela s'explique en partie par la difficulté d'accès aux fichiers, mais pas uniquement. Au départ, les premiers relais de l'information appartenaient tous à la sphère cybersécurité (experts, journalistes spécialisés, comptes techniques sur les réseaux sociaux), ce qui était logique, étant donné que le leak avait été posté sur un forum public connu de cette communauté.

Mais l'information est restée enfermée dans ce cercle restreint, sans véritable diffusion au-delà. Le forum lui-même, pourtant lieu de publication du leak, a montré peu d'activité autour du sujet, ce qui s'explique à la fois par l'indisponibilité rapide des liens, et par la formulation du post initial.

Ce dernier a été publié vers 5h30 du matin, une heure creuse où peu d'utilisateurs sont actifs. Dès le début de la matinée (entre 8h et 10h), il a été rapidement noyé parmi les autres publications plus visibles. Il est aussi probable qu'une partie importante des utilisateurs du forum ne connaisse pas Naval Group, ce qui a pu conduire à percevoir ce leak comme une fuite banale d'une entreprise quelconque , phénomène fréquent sur ce type de forum. Le titre du post ne laissait en effet aucunement entendre qu'il s'agissait d'un acteur du secteur de la défense.

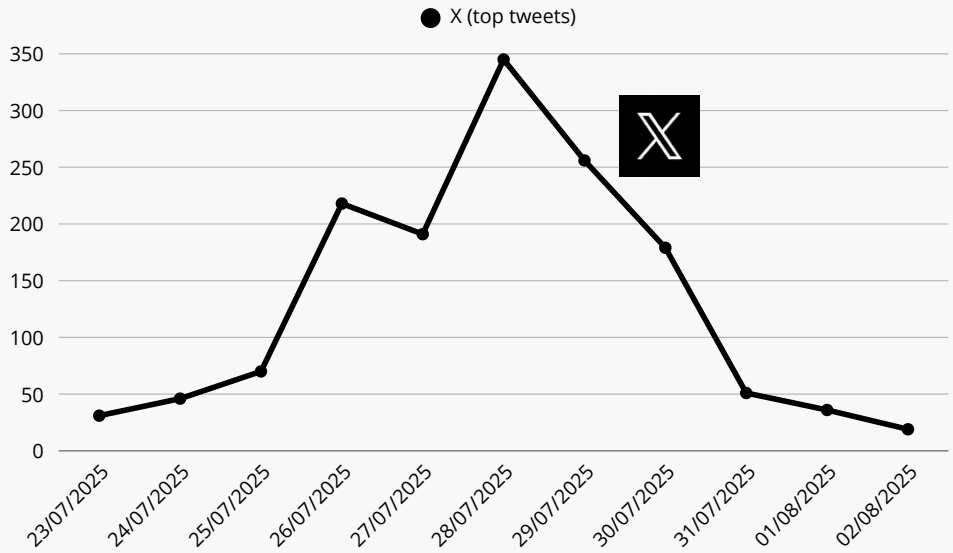
Les graphiques suivants montrent les mentions du leak sur différentes plateformes (toutes langues confondues). Comme on peut le voir, celui-ci ne commence à exister médiatiquement qu'à la fin du décompte, au moment où *Naval Group* fait son communiqué. Avant ça, celui-ci reste essentiellement dans un cercle restreint de gens du monde de la cybersécurité.

Ce constat se voit aussi dans le contenu des différents posts ou articles, car la majorité d'entre eux ne font que paraphraser des articles en français sortis précédemment, et reprendre le communiqué du groupe.

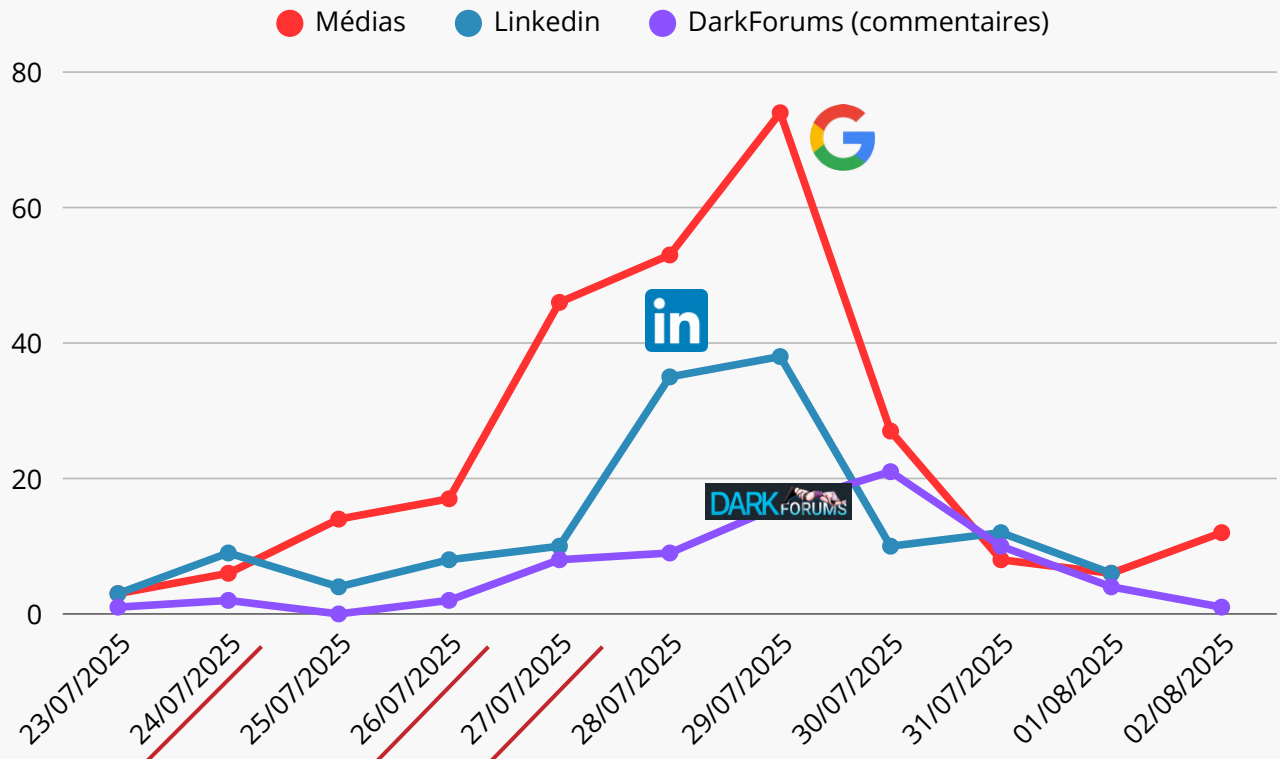
La stratégie globale

Comme analysé dans le chapitre précédent, la stratégie de l'attaquant semblait cohérente avec ses objectifs initiaux. Cependant, les trois éléments évoqués ci-dessus ont affaibli plusieurs leviers d'impact clés. Seul l'effet lié à la restriction d'accès aux fichiers semble avoir pleinement fonctionné, en créant un sentiment de mystère et de spéculation autour du contenu.

Mentions du leak sur X depuis le 23 juillet jusqu'au 2 aout 2025

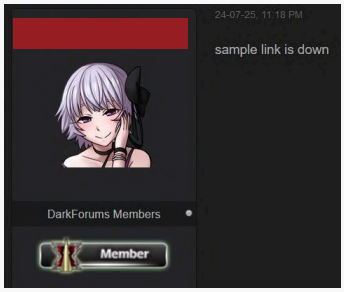


Mentions du leak sur différentes plateformes depuis son apparition le 23 juillet jusqu'au 2 aout 2025



24 juillet 2025, 13h18

Première confirmation que le lien donnant accès au premier échantillon ne fonctionne plus.



26 juillet 2025, 18h48

Naval Group publie un communiqué pour annoncer qu'aucune intrusion n'a été détectée, et qu'ils ont ouvert une enquête et que l'attaque serait réputationnelle.


NAVAL GROUP

POSITION DE NAVAL GROUP

Paris, le 26 juillet 2025

Dans un contexte international, commercial et informationnel sous tension, générant une intensification des tentatives de déstabilisation, Naval Group constate être la cible d'une attaque réputationnelle, caractérisée par la revendication d'un acte de cyber malveillance.

Au regard des faits constatés, des enjeux de souveraineté de Naval Group et de la nécessité de protéger les données de nos clients, une plainte a été déposée pour faire la lumière sur ces actes de malveillance.

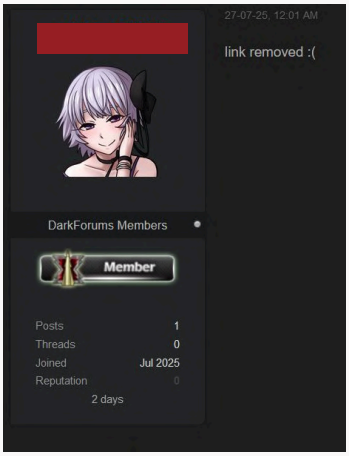
Conformément à nos procédures de cybersécurité, nous avons immédiatement déclenché des investigations techniques, en s'appuyant sur une équipe d'experts en cybersécurité et sur le CERT Naval Group, en collaboration étroite avec les services de l'Etat.

Toutes nos équipes et tous les moyens sont actuellement mobilisés pour analyser et vérifier dans les plus brefs délais l'authenticité la provenance et l'appartenance des données concernées.

À ce stade, aucune intrusion dans nos environnements informatiques n'a été détectée et aucun impact sur nos activités n'est à signaler.

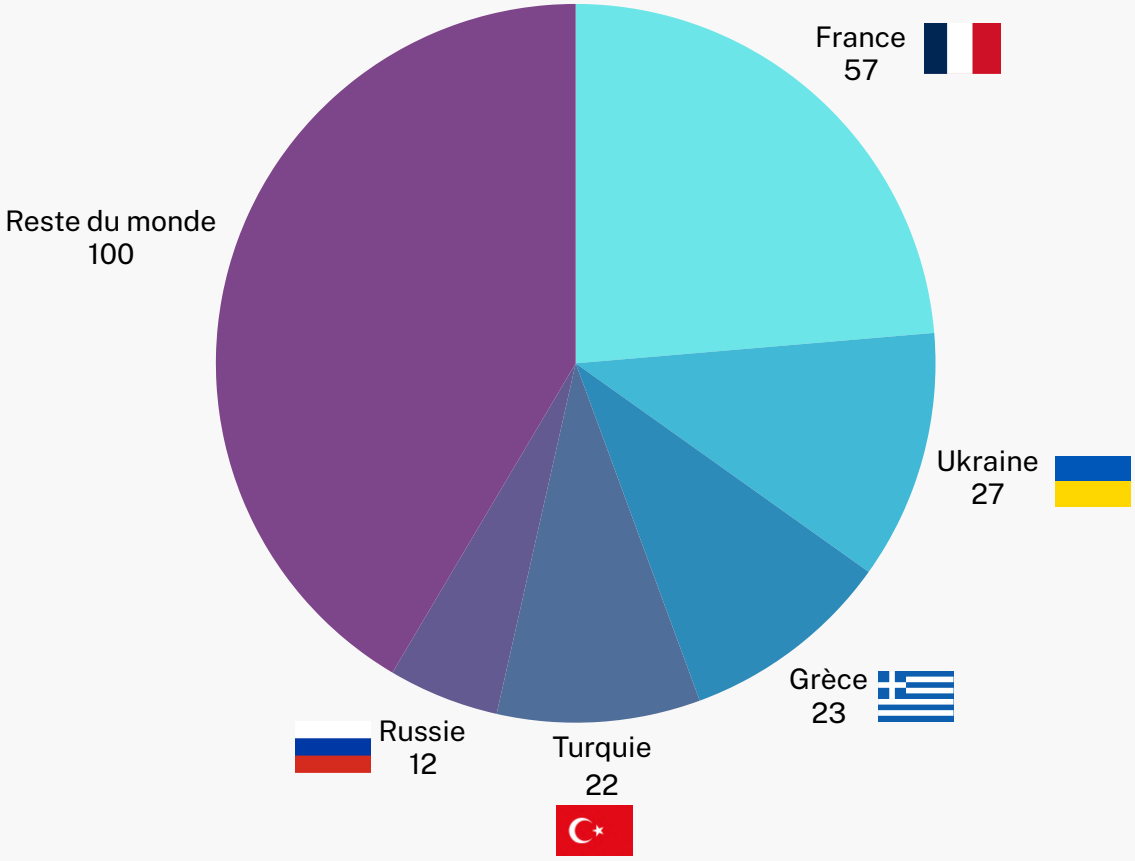
27 juillet 2025, 14h01

Première confirmation que tous les liens menant aux extraits des leaks ne fonctionnent plus.



PRESSE INTERNATIONALE

Nombre d'articles publiés sur le sujet par pays entre le 23 juillet et le 2 aout 2025



Il est également pertinent d'analyser la manière dont la nouvelle du leak s'est diffusée dans le monde, en particulier au regard des appels d'offres potentiels évoqués précédemment.

En Norvège, un seul article traitant du sujet a été identifié, publié le 29 juillet.

En Indonésie, en revanche, nous n'avons trouvé aucune mention du leak, ce qui peut surprendre. Durant toute la période concernée, de nombreux médias indonésiens ont évoqué *Naval Group*, mais uniquement dans le cadre du contrat récemment signé : son organisation, ses retombées positives pour le pays, etc. Aucun de ces articles ne fait allusion à la fuite d'informations.

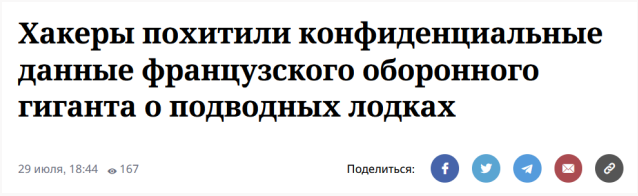
La situation est très différente en Grèce. De nombreux articles ont été publiés tout au long de la période étudiée, et ce dès le 26 juillet, ce qui est relativement tôt comparé aux autres pays (à l'exception de la France). Le contenu de ces articles traduit une forte inquiétude côté grec, notamment en raison de l'annonce de l'achat de nouvelles frégates à *Naval Group* et des nombreuses acquisitions effectuées au cours des cinq dernières années (classes Belharra et Kimon). Les médias grecs expriment aussi la crainte que la Turquie puisse accéder à des informations sensibles sur ces bâtiments.

"Cyberattaque contre Naval Group sous surveillance – Risque de fuite de données pour les frégates Belharra ?"

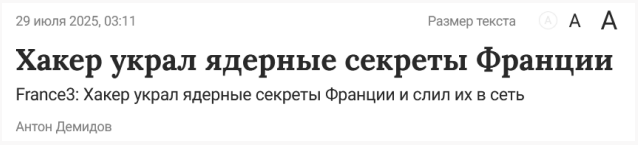
"Divulgation - Des pirates informatiques russes ont attaqué Naval Group et obtenu des données secrètes - Vont-ils les vendre aux Turcs ?"

Concernant la Russie et l'Ukraine, l'intérêt pour le sujet est apparu plus tardivement, la majorité des publications datant du 29 juillet ou après. Leur intérêt peut s'expliquer par la forte culture du cyberespace et du hacking dans ces deux pays, ce qui rend ce type d'incident particulièrement attractif pour leurs médias. Dans le cas de l'Ukraine la majorité des articles identifiés sont purement descriptifs, sans analyse poussée. Dans le cas de la Russie, ceux-ci tendent plus à mettre en avant le fait que les codes de l'arme nucléaire auraient été volés.

En ce qui concerne la Turquie, aucune explication particulière ne ressort quant à l'intérêt pour le sujet. Là encore, la majorité des articles se contentent de relater les faits, sans commentaire ni analyse approfondie.



"Des pirates informatiques volent des données confidentielles sur les sous-marins du géant français de la défense"



Un pirate informatique a volé les secrets nucléaires de la France

"L'entreprise de défense française Naval Group aurait subi une cyberattaque"

Dans l'ensemble, ces éléments suggèrent que la diffusion de la nouvelle du leak a été relativement lente et limitée à l'échelle mondiale. Il faut attendre le 29 juillet pour que d'autres pays prennent véritablement le relais de la France dans la couverture médiatique de cette affaire. Avant cette date, très peu de pays publiaient plus de deux articles par jour sur le sujet, à l'exception notable de la Grèce.

GESTION DE CRISE DE NAVAL GROUP

Dans ce cadre, la stratégie de *Naval Group* a consisté à ne pas réagir publiquement pendant toute la phase active des publications. Cette absence de réaction a probablement contribué à éviter de renforcer l'effet viral recherché. Ce n'est qu'après le dernier message de l'auteur que l'entreprise a publié un communiqué officiel, indiquant qu'aucune intrusion n'avait été détectée dans ses systèmes.

Ce choix de temporisation, combiné à la communication sobre et tardive, s'inscrit dans une logique de maîtrise du rythme et de contrôle de l'exposition médiatique. L'entreprise semble avoir misé sur l'essoufflement naturel de l'opération, et les erreurs de l'attaquant ont renforcé la pertinence de cette stratégie.

À court terme, la stratégie de *Naval Group* apparait efficace.

La publication de leur communiqué a ravivé l'attention médiatique, mais selon ses termes et son narratif et non ceux imposés par la crise. Si aucune nouvelle information ne refait surface, cette attention devrait progressivement diminuer en laissant dans l'opinion les éléments transmis par *Naval Group*.

D'autant que la plus grande partie de la communication des médias s'est faite avec leur narratif. Durant la grande exposition médiatique des 28 et 29 juillet, le message était : *Naval Group* n'a pas trouvé de signe d'intrusion et il s'agit d'une attaque réputationnelle.

En lieu et place d'un entachement de l'image de *Naval Group*, l'entreprise apparait comme la victime d'une campagne hostile mal organisée et rapidement désamorcée, renforçant la résilience future de l'image de marque du groupe dans de futures attaques.

NAVAL GROUP

POSITION DE NAVAL GROUP

Paris, le 26 juillet 2025

Dans un contexte international, commercial et informationnel sous tension, générant une intensification des tentatives de déstabilisation, Naval Group constate être la cible d'une attaque réputationnelle, caractérisée par la revendication d'un acte de cyber malveillance.

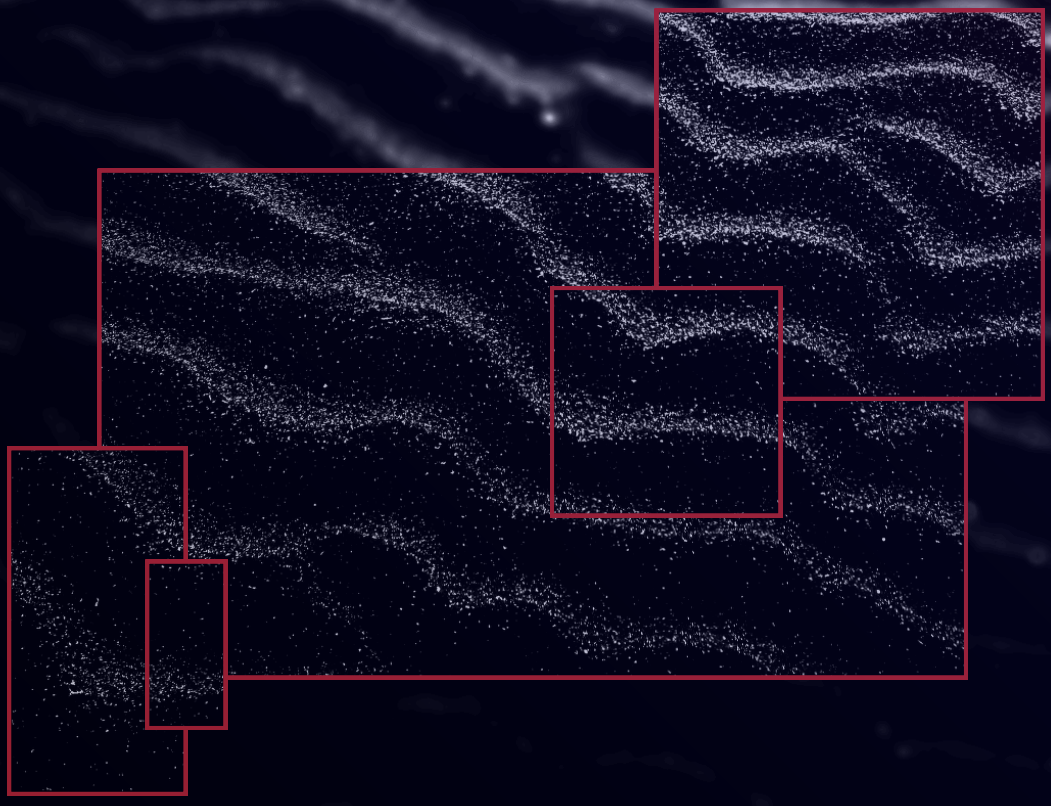
Au regard des faits constatés, des enjeux de souveraineté de Naval Group et de la nécessité de protéger les données de nos clients, une plainte a été déposée pour faire la lumière sur ces actes de malveillance.

Conformément à nos procédures de cybersécurité, nous avons immédiatement déclenché des investigations techniques, en s'appuyant sur une équipe d'experts en cybersécurité et sur le CERT Naval Group, en collaboration étroite avec les services de l'Etat.

Toutes nos équipes et tous les moyens sont actuellement mobilisés pour analyser et vérifier dans les plus brefs délais l'authenticité la provenance et l'appartenance des données concernées.

À ce stade, aucune intrusion dans nos environnements informatiques n'a été détectée et aucun impact sur nos activités n'est à signaler.

5 CONCLUSIONS



CONCLUSIONS SUR LES HYPOTHÈSES 1/2

FAITS :

Publication sur un forum annonçant détenir des informations piratées sur *Naval Group*. La publication inclut des extraits et demande à *Naval Group* de contacter le publicateur.

TYPE D'ATTAQUE :

- **Attaque pour rétribution.**
- Attaque réputationnelle.

AUTEUR :

- **Un attaquant isolé.**
- **Un groupe d'attaquants.**
- Attaque d'origine étatique.
- Attaque d'origine privée.

DÉTAIL :

- **Attaque d'un groupe pour rétribution.** — Aucune preuve substantielle n'étaye l'hypothèse. ✗
- **Attaque d'un individu pour rétribution financière.** — Aucune preuve substantielle hormis les dires de l'attaquant qui indique vouloir être contacté. ✗
- **Attaque d'un individu isolé pour rétribution réputationnelle.** — Peu probable, le hacker ayant jusqu'à preuve du contraire disparu sans laisser de traces. Celui-ci n'a pas capitalisé sur son action. ✗

CONCLUSIONS SUR LES HYPOTHÈSES 2/2

TYPE D'ATTAQUE :

- Attaque pour rétribution.
- **Attaque réputationnelle.**

AUTEUR :

- Un attaquant isolé.
- Un groupe d'attaquants.
- **Attaque d'origine étatique.**
- **Attaque d'origine privée.**

DÉTAIL :

Attaque réputationnelle d'un État hostile ou opportuniste.

Uniques indices désignent la Russie
La semaine suivante, l'Ukraine a indiqué avoir obtenu des informations sur ses sous-marins nucléaires russes.
L'attaque sur *Naval Group* semble cependant trop maladroite pour être d'origine russe.

Attaque réputationnelle d'un concurrent de Naval Group.

Correspondance du mode opératoire et attaque anonyme
Tropisme des leaks sur des frégates proposées en appels d'offres
Cumulé à un opportunisme temporel en lien avec des contrats
L'attaque cible spécifiquement un des arguments de vente de *Naval Group*, la sécurité électronique de ses systèmes.

Attaque réputationnelle d'un concurrent sur un fournisseur de Naval Group

Correspondance du mode opératoire et attaque anonyme
Contenu des leaks pouvant correspondre à un ou des sous-traitants spécifiques pour les rendre identifiables par *Naval Group*
Amateurisme correspondant aux plus faibles moyens
Hypothèse cependant complexe

Attaque réputationnelle sur le cours de Thales.

Baisse du cours de *Thales* de 3% suite au leak
Mode opératoire léger mais envisageable
Incohérences multiples (baisse de courte durée, pas de short significatif, baisse du cours stimulée par d'autres facteurs, pas de signature de l'acte…)

RÉSULTATS PROBANTS

TYPE D'ATTAQUE :

Attaque réputationnelle.
L'analyse des faits disponibles, confrontée aux hypothèses de départ, désigne cette option comme la plus vraisemblable. Cela ne signifie pas qu'il n'y a pas eu de hacking ou que les informations révélées soient fausses, mais que l'objectif final est de nuire à la réputation de la cible à travers une bombe informationelle.
Indice de confiance : 4/5

CIBLE :

***Naval Group*, l'un de ses fournisseurs ou un État.**
Il ressort de notre analyse que *Naval Group* est plus probablement la cible de l'attaque.
Indice de confiance : 4/5
Mais il ne faut pas exclure que l'un de ses fournisseurs puisse être la cible finale.
Indice de confiance : 3/5
Dans une moindre mesure, l'État pourrait aussi être cette cible.
Indice de confiance : 2/5

ATTAQUANT :

Entreprise concurrente de *Naval Group* ou d'un fournisseur.
Notre analyse tend à indiquer une attaque de la part d'un concurrent.
Indice de confiance : 4/5
Il est envisageable qu'un acteur étatique ait réalisé l'attaque, les indices pointeraient vers la Russie.
Indice de confiance : 2/5

MOYENS MIS EN PLACE :

Faibles à modérés.
Plusieurs indices, liés à la planification de l'opération et à son exécution, indiquent des erreurs et des moyens limités.
Indice de confiance : 4/5

RECHERCHES FUTURES

Les données collectées et traitées par Timour dans le cadre de cette analyse relèvent exclusivement de données disponibles en source ouverte. Afin de compléter et d'affiner cette analyse, il serait possible d'étudier les pistes suivantes :

ANALYSE TECHNIQUE DES EXTRAITS DU LEAK* :

Une analyse rigoureuse des extraits du leak peut révéler des informations importantes sur la méthode de collecte, la date et le lieu de l'intrusion, la sensibilité des informations et leur authenticité, voire permettre d'identifier l'attaquant.

VEILLE DES RÉSEAUX SOCIAUX, DU DARKWEB ET MÉDIATIQUE* :

Cela permettrait d'identifier et de qualifier un retour de l'attaquant revendiquant son action, essayant de capitaliser sur celle-ci ou diffusant de nouveaux extraits du leak nécessitant une attention particulière. Ainsi, il sera possible de confirmer ou d'infirmer des hypothèses, mais aussi de se protéger rapidement en cas de nouvelle attaque.

ANALYSE TECHNIQUE DES LOGS* :

Dans le cas où l'attaquant cherchait des informations sur l'organisation de *Naval Group*, il aurait pu commettre des erreurs et donc laisser des traces dans les logs. Nous avons enregistré son passage anonyme via DuckDuckGo sur le site de la CCI Normandie. Il est possible qu'il ait aussi consulté l'article et y ait laissé des traces.

ANALYSE INTERNE DE NAVAL GROUP ET DES SOUS-TRAITANTS:

Cette analyse, orientée par les autres éléments précédemment mentionnés, peut permettre la résolution entière de cette attaque, des méthodes d'action à l'identification de l'attaquant et donc aux objectifs détaillés.

**Nos collaborateurs disposent d'une expertise reconnue sur l'ensemble de ces prestations.*

BIBLIOGRAPHIE

BIBLIOGRAPHIE

AMF. (s. d.). BDIF - Decisions and financial disclosures database. https://bdif.amf-france.org/en?typesInformation=VAD

Cluley, G. (s. d.). Ukraine claims to have hacked secrets from Russia's newest nuclear submarine. Hot For Security. https://www.bitdefender.com/en-us/blog/hotforsecurity/ukraine-claims-to-have-hacked-secrets-from-russias-newest-nuclear-submarine

Client challenge. (s. d.). https://www.ft.com/content/ccbafbbf-6693-476d-8949-6dbf68b37ddb

Client challenge. (s. d.-b). https://www.ft.com/content/ae104fce-0576-4ff0-a7ec-a0eed7849e97

Cluley, G. (s. d.). Ukraine claims to have hacked secrets from Russia& # x27 ; s newest nuclear submarine. Hot For Security. https://www.bitdefender.com/en-us/blog/hotforsecurity/ukraine-claims-to-have-hacked-secrets-from-russias-newest-nuclear-submarine

Cookman, L. (2025, août 3). Ukraine hacks Russian submarine key to Moscow's Arctic expansion. The Times. https://www.thetimes.com/world/russia-ukraine-war/article/ukraine-hacks-russian-submarine-as-moscow-expands-arctic-presence-2tmwc8dn5

Correspondent, H. (2016, août 25). New Scorpene submarine details emerge, navy says leak not serious | Latest News India. Hindustan Times. https://www.hindustantimes.com/india-news/scorpene-submarine-leak-new-set-of-documents-on-underwater-warfare-out/story-FX3d1piQUd69prHtfkFuKN.html

Cyber leak report deals extra hit to Thales as EU-US deal shakes defence sector. (2025, 28 juillet). TradingView. https://www.tradingview.com/news/reuters.com,2025:newsml_L8N3TP0EV:0-cyber-leak-report-deals-extra-hit-to-thales-as-eu-us-deal-shakes-defence-sector/

Cybernews. (s. d.). DarkForums rushes to hide after hacker exposes user IPs. https://cybernews.com/cybercrime/darkforums-ssrf-exploit-leak/

Cybernews. (s. d.). Europe's defence giant Naval Group hit with major breach, hackers claim. https://cybernews.com/security/naval-group-france-defense-data-breach/

Elshani, N. (2025, 29 juillet). France faces largest cyberattack in history – secret defense data falls into the hands of hackers. Telegrafi. https://telegrafi.com/en/France-faces-the-largest-cyberattack-in-history--secret-defense-data-falls-into-the-hands-of-hackers/amp/

Entrée en vigueur du contrat Scorpène® Evolved pour l'Indonésie | Naval Group. (s. d.). Naval Group. https://www.naval-group.com/fr/entree-en-vigueur-du-contrat-scorpener-evolved-pour-lindonesie

Epstein, J. (2025, août 4). Ukraine says it stole intel from the Russian Navy and found weak points in its newest nuclear missile submarine. Business Insider. https://www.businessinsider.com/ukraine-found-weak-points-in-new-russian-nuclear-missile-submarine-2025-8

Express News Service. (2016, août 24). Scorpene submarine leak : Huge setback for India as 22,000 pages of secret data leaked. The Indian Express. https://indianexpress.com/article/india/india-news-india/scorpene-submarine-leak-huge-setback-india-as-22000-pages-of-secret-data-leaked/

FDI : à Oslo, Emmanuel Macron plaide pour les frégates françaises. (s. d.). Mer et Marine. https://www.meretmarine.com/fr/defense/fdi-a-oslo-emmanuel-macron-plaide-pour-les-fregates-francaises

FinAristo. (s. d.). Shorted company THALES. https://finaristo.com/short-selling/shorted-companies/thales

Fransız savunma şirketi Naval Group'un siber saldırıya uğradığı iddia edildi. (s. d.). https://www.aa.com.tr/tr/dunya/fransiz-savunma-sirketi-naval-groupun-siber-saldiriya-ugradigi-iddia-edildi/3646775

Giansiracusa, A. (2025, 20 février). Naval Group supporterà le corvette Gowind degli Emirati Arabi Uniti. Ares Osservatorio Difesa. https://aresdifesa.it/naval-group-supportera-le-corvette-gowind-degli-emirati-arabi-uniti/?fsp_sid=13778

Global operation targets NoName057(16) pro-Russian cybercrime network – The offenders targeted Ukraine and supporting countries, including many EU Member States | Europol. (s. d.). Europol. https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

Hodunova, K. (2025, août 5). Ukraine obtains classified data on Russia's newest nuclear submarine, intelligence claims. The Kyiv Independent. https://kyivindependent.com/ukrainian-intelligence-allegedly-obtains-classified-data-on-russias-newest-nuclear-submarine-cruiser/

Ikeda Scott. (s. d.). Threat Actor Claims to Have Stolen DARPA Files From GE, Data Theft Remains Unconfirmed. CPO Magazine. https://www.cpomagazine.com/cyber-security/threat-actor-claims-to-have-stolen-darpa-files-from-ge-data-theft-remains-unconfirmed/

Info, P. R. (2025, août 4). Des données secrètes dérobées ? L'Ukraine affirme avoir piraté le tout nouveau sous-marin nucléaire russe. . . . RTL Info. https://www.rtl.be/actu/monde/international/guerre-en-ukraine/des-donnees-secretes-derobees-lukraine-affirme-avoir-pirate-le-tout-nouveau-sous/2025-08-04/article/758747

Khomenko, I. (2025, août 3). Ukraine Gains Secrets of Russia's Newest Nuclear Sub "Knyaz Pozharsky"—Crew, Schematics, Combat Orders Leaked. UNITED24 Media. https://united24media.com/latest-news/ukraine-gains-secrets-of-russias-newest-nuclear-sub-knyaz-pozharsky-crew-schematics-combat-orders-leaked-10399

Lagneau, L. (2025, 17 février). Le français Naval Group devrait finalement participer à l'appel d'offres des futurs sous-marins canadiens. Zone Militaire. https://www.opex360.com/2025/02/17/le-francais-naval-group-devrait-finalement-participer-a-lappel-doffres-des-futurs-sous-marins-canadiens/

Launching of the first phase of the European Patrol Corvette project with signature of Modular and Multirole Patrol Corvette contract | Naviris. (s. d.). https://www.naviris.com/news/launching-first-phase-european-patrol-corvette-project-signature-modular-and-multirole-patrol

Naval Group [@navalgroup]. (2025, juillet 26). https://x.com/navalgroup/status/1949149936294998040

Noname05716 [@Noname05716]. (2025). https://x.com/Noname05716/status/1942187239330414922

Nova, R. A. (2024, 21 novembre). Naval Group participera à l'appel d'offres lancé par la Norvège pour de nouvelles frégates. Agenzia Nova. https://www.agenzianova.com/fr/news/groupe-naval-participera-%C3%A0-l%27appel-d%27offres-lanc%C3%A9-par-la-Norv%C3%A8ge-pour-de-nouvelles-fr%C3%A9gates/

Nouvelle organisation de Naval Group | CCI Business Normandie. (s. d.). https://normandie.ccibusiness.fr/economie-maritime/nouvelle-organisation-de-naval-group/teaser

Online, I. (2025, 24 juin). Grèce : Les groupes de défense grecs ferraillent pour s'arrimer à Naval Group - 24/06/2025 - Intelligence Online. Intelligence Online. https://www.intelligenceonline.fr/grands-contrats/2025/06/24/les-groupes-de-defense-grecs-ferraillent-pour-s-arrimer-a-naval-group,110467450-gra

Pentapostagma. (2025, août 3). Αποκάλυψη-Ρώσοι χάκερ χτύπησαν την Naval Group αποκτώντας μυστικά στοιχεία-Θα τα πουλήσουν στους Τούρκους ; Pentapostagma. https://www.pentapostagma.gr/kosmos/rosia/7319268_apokalypsi-rosoi-haker-htypisan-tin-naval-group-apoktontas-mystika-stoiheia

Petkauskas, V. (s. d.). Europe's defence giant Naval Group hit with major breach, hackers claim. Cybernews. https://cybernews.com/security/naval-group-france-defense-data-breach/

Poireault, K. (2025, août 1). Naval Group denies hack claims, alleges « Reputational attack ». Infosecurity Magazine. https://www.infosecurity-magazine.com/news/naval-group-denies-hack/

Sauveton, P. (2025, 28 juillet). Naval Group visé par une opération de déstabilisation ? OpexNews. https://opexnews.fr/cyberattaque-naval-group-2025/

SaxX [@SaxX]. (2025, juillet 23, 14:35). https://x.com/SaxX/status/1948988282894704785

SaxX [@SaxX]. (2025, juillet 24). https://x.com/SaxX/status/1948300361426464888

Singh, S. (2016, août 24). Scorpene submarine classified data is leaked, Government seeks report from Navy. The Indian Express. https://indianexpress.com/article/india/india-news-india/scorpene-submarine-secret-data-leaked-indian-navy-2994944/

Sor, J. (2024, 8 juillet). How a New York short-seller took on one of the world's richest people, wiped out $150 billion in market value, and barely made any money. Business Insider. https://www.businessinsider.com/hindenburg-research-adani-group-explained-stock-crash-short-seller-profits-2024-7

Совина, М. (2025, 28 juillet). Хакер украл ядерные секреты Франции. Lenta.RU. https://lenta.ru/news/2025/07/28/haker-ukral-yadernye-sekrety-frantsii/

Sudinfo. (2025, août). L'Ukraine affirme avoir piraté le tout nouveau sous-marin nucléaire russe, inauguré il y a quelques jours en présence de Vladimir Poutine. SUDINFO. https://www.sudinfo.be/id1024225/article/2025-08-04/lukraine-affirme-avoir-pirate-le-tout-nouveau-sous-marin-nucleaire-russe

Thales. (s. d.). Thales publie ses résultats du premier semestre 2025. Thales. https://www.thalesgroup.com/fr/group/investisseurs/press_release/thales-publie-ses-resultats-du-premier-semestre-2025

Truță, F. (s. d.). Boeing Allegedly Negotiating with LockBit Hackers Who Stole Sensitive Data from Its Servers. Hot For Security. https://www.bitdefender.com/en-us/blog/hotforsecurity/boeing-allegedly-negotiating-with-lockbit-hackers-who-stole-sensitive-data-from-its-servers

Υπό παρακολούθηση ηκυβερνοεπίθεση στη Naval Group – Κίνδυνος διαρροής στοιχείων για τις φρεγάτες Belharra ; (2025, 29 juillet). thepressroom.gr. https://www.thepressroom.gr/amyna/ypo-parakoloythisi-i-kybernoepithesi-sti-naval-group-kindynos-diarrois-stoiheion-gia-tis

Шпак, К. (2025, juillet). Хакери викрали конфіденційні дані французького оборонного гіганта про підводні човни. NV. https://nv.ua/ukr/world/countries/vitik-danih-naval-group-francuzka-oboronna-kompaniya-rozpochala-rozsliduvannya-50533280.html

L'équipe de Timour vous remercie sincèrement pour l'attention portée à ce rapport.

Nous serions reconnaissants si vous envisagiez de le partager avec toute personne que le sujet pourrait intéresser.

Si la lecture de ce rapport vous a été utile, n'hésitez pas à nous le faire savoir, nous serons heureux de lire votre retour.

Enfin, si par votre intimité avec le dossier ou grâce à vos recherches personnelles, vous souhaitez apporter un enrichissement, un erratum ou un droit de réponse, nous nous tenons également à votre disposition.

Avec Timour, dissipez le brouillard.

CYBERATTAQUE, OU OPÉRATION RÉPUTATIONNELLE ?

#OSINT
#INFLUENCE

NAVAL GROUP
EN EAUX TROUBLES

RAPPORT D'INVESTIGATION

TIMOUR.

David SALGADO co-fondateur
Mathis B. co-fondateur

Publication : 08 / 2025