DOSSIER SPÉCIAL

LA FRANCE : CIBLE DE L'HACKTIVISME GÉOPOLITIQUE

cert By xmco

Tous concernés !

Alors que Paris accueille les Jeux Olympiques cet été, les équipes d'XMCO publient ce dossier consacré à l'hacktivisme géopolitique.

Un document, établi sur les observations effectuées par nos analystes au cours des années 2023 et 2024.

Depuis plusieurs mois, la conjoncture, qui mêle instabilité politique nationale et dégradation de la situation géopolitique mondiale, donne une dimension stratégique particulière au contexte sécuritaire français.

C'est pourquoi, dans cette période si particulière, le CERT-XMCO s'est intéressé aux modes opératoires qui ont ciblé notre pays afin de comprendre comment ils fonctionnent, qui ils sont, et qui ils ciblent.

Voici notre état des lieux de la menace hacktiviste en France.

Marc Behar
PDG- Fondateur

Sommaire

Direction de la publication : XMCO
Date de publication : Août 2024

Avant-propos

L'expression « hacktivisme » est une contraction de « hacker » et « activisme ». Elle désigne un mode opératoire choisi par des individus ou des groupes plus ou moins structurés, pour mener des cyberattaques dont les finalités sont politiques (promouvoir des messages, encourager des changements, influencer des opinions publiques, menacer des organisations, etc.). Il y a différents types d'hacktivistes (religieux, sociaux, etc.), mais ce dossier traitera de l'hacktivisme géopolitique qui cible la France de manière accrue depuis 2022.

En 2023, la France a été ciblée par plusieurs centaines d'attaques de type hacktiviste (319 revendications), dans la continuité de 2022. Cette situation s'explique par une situation géopolitique mondiale de plus en plus tendue dans laquelle la France occupe encore une place de premier plan. Les premiers mois de l'année 2024 et les tensions géopolitiques croissantes n'indiquent aucun ralentissement de cette tendance à court terme.

En 2023, le CERT-XMCO a observé la prolifération des acteurs et la multiplication des opérations hacktivistes s'appuyant sur les dynamiques internes de la société française pour justifier leur passage à l'acte, notamment celles entourant le débat sur le port de l'abaya dans l'espace public, la condition des agriculteurs ou encore les émeutes ayant suivi la mort de Nahel M.

Les groupes hacktivistes ont aussi ciblé la France en marge des prises de position du gouvernement sur des conflits régionaux, notamment en Ukraine, dans la bande de Gaza et au Haut-Karabakh. Ces groupes continueront probablement de s'impliquer dans les attaques ciblant la France en 2024.

L'organisation des Jeux Olympiques et des jeux Paralympiques de Paris 2024 pourrait offrir une visibilité médiatique accrue aux groupes hacktivistes ciblant les entreprises privées et organismes publics français. En parallèle, des tentatives d'ingérence pourraient être observées sur les réseaux sociaux.

Les groupes pro-russes constituent le gros des bataillons qui s'attaquent à des entités françaises. Cependant, il est impossible d'estimer leur réel niveau d'affiliation avec des gouvernements étrangers. Aussi la visibilité des groupes pro-russe ne doit pas cacher d'autres acteurs aux motivations diverses, parfois même basés en France ou en Europe.

Les opérations hacktivistes observées en 2023 sont le plus souvent des attaques par déni de service distribué (DDoS, 289 revendications), suivies sporadiquement par des actions de défiguration (défacement). Ces dernières ont donc eu un impact opérationnel limité[1], hormis pour les entités dont l'activité commerciale dépendait de la disponibilité de leurs services en ligne. Une grande partie des attaques DDoS ont touché des entités de moindre envergure (TPE), telles que des commerces locaux et des petits sites de e-commerce.

(1) Si l'impact opérationnel est souvent limité, les impacts médiatiques et/ou réputationnels peuvent être considérables. Par exemple, les attaques DDoS contre des sites de l'Etat français, en mars 2024 avaient beaucoup fait parler d'elles https://www.bfmtv.com/tech/cybersecurite/cyberattaque-inedite-contre-la-france-c-est-quoi-l-attaque-ddos-par-deni-de-services_AV-202403110825.html

1. FAIRE FACE À LA MENACE

1. Faire face à la menace

COMME NOUS ALLONS LE VOIR, LA MENACE HACKTIVISTE PEUT PRENDRE PLUSIEURS FORMES ET ÊTRE INCARNÉE PAR DES ACTEURS PLUS OU MOINS SOPHISTIQUÉS. POUR S'EN PRÉMUNIR, IL EST POSSIBLE D'ADOPTER DES POSTURES DE SÉCURITÉ EN AMONT ET EN AVAL DES CYBERATTAQUES POUR LES EMPÊCHER OU RÉDUIRE LEUR IMPACT LORSQU'ELLES ONT LIEU.

Pour endiguer la menace, **le CERT-XMCO recommande d'abord de ne pas faire d'écho à chaud et sans analyse aux revendications d'attaques**, car l'objectif des hacktivistes est généralement triple :

- Donner le plus de visibilité à leurs messages politiques au travers de leurs opérations.
- Pousser l'opinion publique et les décideurs adverses à exagérer leur potentiel de nuisance.
- Favoriser un état de confusion chez la partie adverse.

Ainsi, se faire le relais de leurs attaques, sans recul, et renforcer le bruit médiatique autour de leurs actions revient à leur rendre service, à amoindrir les capacités de remédiations des victimes, et à potentiellement propager de fausses nouvelles (revendications d'attaques qui n'auraient pas eu lieu ou aux impacts exagérés, partage de messages inexacts, etc.).

Il est aussi important de **comprendre que des attaques en apparence hacktivistes de types DDoS (déni de service distribué) par exemple, constituent parfois une méthode de diversion populaire pour détourner l'attention des équipes de sécurité informatique** afin de distribuer des codes malveillants ou bien de s'introduire sur un réseau [30]. En d'autres termes, une attaque DDoS peut servir de diversion pour cacher une attaque plus sophistiquée et ciblée, à des fins de collecte de renseignements, de distribution de wiper ou de ransomware.

En termes de surveillance et de veille, le CERT-XMCO recommande de :

- Mener une surveillance complète et approfondie de son exposition numérique, susceptible d'être utilisée comme surface d'attaque, pour corriger les vulnérabilités et les défauts de configuration identifiés.
- Mener une veille cyber sur les groupes hacktivistes, leurs modes opératoires et leurs victimologies (géographie, taille et secteur des victimes) ainsi que sur leurs canaux de revendication d'attaques.
- Mettre en place une surveillance des acteurs de la menace connus pour diffuser des données volées et des plateformes sur lesquelles ils les publient pour être en mesure de réagir rapidement.
- Adapter sa posture de défense grâce au profilage des cybermenaces (cyber threat profiling).

Pour faire face à la menace hacktiviste et aider ses clients à mettre en place ces mesures, le CERT-XMCO propose les services Yuno et Serenety.

2. 2023 : LA FRANCE PRISE POUR CIBLE

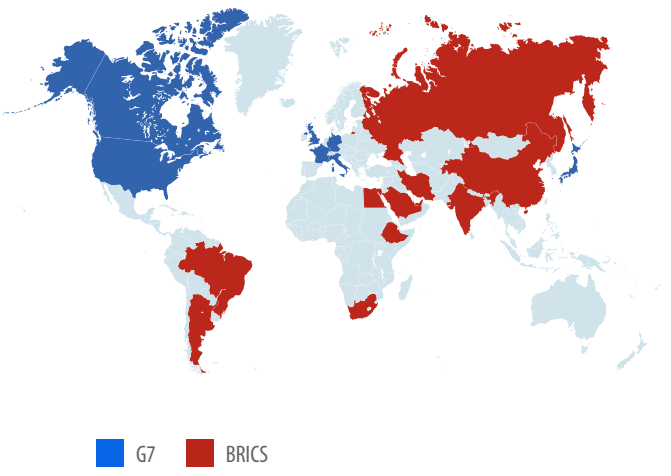
2.1

La France : acteur international visé par le retour de l'hacktivisme géopolitique

Le CERT-XMCO surveille en continu les revendications d'attaques par les groupes hacktivistes et a voulu dresser un bilan de l'année 2023 afin de disposer d'une vision claire de la menace, et en tirer des enseignements pour les années à venir. En cela, nos analystes ont recensé les attaques revendiquées sur Telegram, une plateforme initialement populaire chez les utilisateurs russophones, facile d'accès pour les audiences européennes, et qui permet de publier toutes sortes de contenus potentiellement illégaux tout en offrant certaines garanties en matière de sécurité opérationnelle aux acteurs hacktivistes qui l'emploient[2].

Dans un contexte de regain de tensions géopolitiques, la France est une cible de choix pour de nombreux acteurs de la menace. Elle est membre de l'OTAN, du G7, soutien militaire et financier de l'Ukraine, mais elle est aussi, de manière structurelle, une puissance majeure au sein de l'Union Européenne, membre du Conseil de sécurité de l'ONU et reste une puissance diplomatique de premier plan. Enfin, la France est de plus en plus traversée par des crises internes qui minent sa cohésion sociale et sa capacité à projeter sa puissance à l'international (ex. gilets jaunes, manifestations sociales d'ampleur, émeutes). Les puissances hostiles à la France sont donc tentées d'exploiter ces fractures en exacerbant les tensions sociales existantes à travers des campagnes d'influence et d'hacktivisme[3].

L'invasion de l'Ukraine par la Russie en février 2022 a entrainé une forte dégradation des relations internationales entre puissances géopolitiques. L'impression réelle ou supposée d'une accélération des conflits semble avoir suivi « l'opération militaire spéciale » russe : Gaza, Taiwan, Haut-Karabakh. Ces évènements ont contribué au renforcement d'une polarisation entre 2 camps dont les contours demeurent flous, car ils regroupent des réalités locales, régionales et nationales complexes.



Pays membres du G7 et des BRICS (en date du 1er janvier 2024)
Source : Statista en date du 29 août 2023

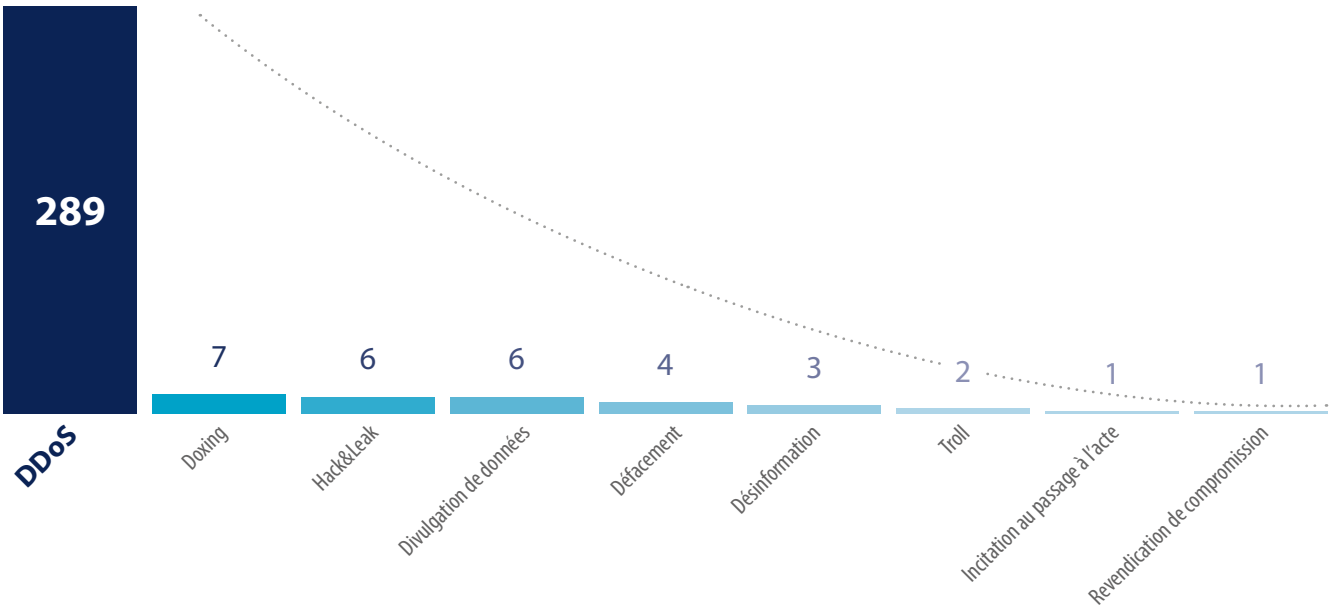
Les tensions observées, concrétisées ou non par des opérations militaires, sont accompagnées d'une myriade de modes d'action menés par des acteurs divers. Parmi ceux-là, les hacktivistes occupent une place considérable, car ils choisissent de mener des cyberattaques à fort impact médiatique pour donner de l'écho à leurs revendications. A travers son statut international et son positionnement au sein du bloc occidental, la France est visée par de nombreux groupes hacktivistes.

(2) Cf. ActuSécu #61 de février 2024, Hors-Série spécial Dark Web [46]
(3) Cf. partie « Les crises françaises : des vulnérabilités à exploiter »

2.2 Plus de 300 attaques revendiquées contre des organisations françaises en 2023

Sur l'ensemble de l'année 2023, les consultants du CERT-XMCO ont recensé **319 revendications d'attaques** contre des entités publiques ou privées françaises, sur Telegram. D'un point de vue quantitatif, ce chiffre est important et confirme que la France est largement prise pour cible par des hacktivistes qui lui sont hostiles. Disposant d'un niveau de sophistication hétérogène, ces attaques ont essentiellement pris la forme de déni de service distribué (DDoS) ayant pour objectif de rendre temporairement indisponibles les services en ligne des entités françaises ciblées et empêcher leurs clients d'y accéder (**289**).

Nombre d'attaques hacktivistes observées par le CERT-XMCO en 2023



DES ATTAQUES VARIÉES :

DDoS : Une attaque par déni de service distribué (DDoS) a pour objectif de rendre temporairement indisponible un service, en empêchant ses utilisateurs de l'utiliser. Il s'agit le plus souvent de bloquer l'accès à un serveur web et d'empêcher la consultation d'un site.

Hack&Leak et **Divulgation de données** : Une attaque de type «Hack&Leak» implique une compromission des données et leur divulgation publique. Ce type d'attaque est utilisé par les groupes hacktivistes pour discréditer des pratiques, des informations ou des individus.

La **désinformation** : Également connue sous le nom de lutte informationnelle offensive, elle fait référence à la propagation intentionnelle d'informations trompeuses ou fausses sur Internet, visant à influencer des opinions publiques, en manipulant les perceptions d'un évènement.

Le **doxing** (parfois orthographié «doxxing») : Une pratique consistant à rechercher, collecter et divulguer publiquement des informations privées sur une personne ou une organisation sur Internet, le plus souvent dans le but de les intimider ou de les discréditer.

Défacement et **Troll** : Une attaque lors de laquelle un hacktiviste modifie volontairement le contenu d'un site web pour y afficher ses revendications politiques en démontrant ses compétences techniques. En complément, le **trolling** correspond à une attitude de dénigrement ou provocatrice à l'encontre de personnalités et/ou d'institutions françaises, via la publication de contenus moqueurs.

Les chiffres présentés dans ce dossier ont vocation à représenter fidèlement la menace hacktiviste. Cependant, les acteurs surveillés ont recouru à des techniques visant à surestimer les conséquences de

leurs attaques et complexifier leurs suivis : création intempestive de chaines secondaires, changement du statut du canal Telegram (public, privé), annonces ponctuelles de coalition entre plusieurs groupes et multiples publications d'une même attaque. Pour cette raison, il est possible que les chiffres proposés par le CERT-XMCO ne couvrent pas l'intégralité des attaques revendiquées.

Les opérations hacktivistes qui ont ciblé la France en 2023 ont eu un impact globalement mineur malgré la popularisation du modèle Malware-as-a-Service, offrant aux acteurs de la menace la possibilité de mener des attaques par déni de service distribué (DDoS) avec des ressources «clés en main».

Perturbatrices sur une période relativement courte, les conséquences de certaines attaques par DDoS ne doivent néanmoins pas être sous-estimées, car elles peuvent parfois coïncider avec un incident de sécurité d'un autre type, impliquant par exemple une distribution de code malveillant ou bien une intrusion réseau plus sophistiquée.

LES OPÉRATIONS DE TYPE HACK&LEAK : PLUS RARES, MAIS PLUS DANGEREUSES

EN 2023, les consultants du CERT-XMCO ont recensé **6 opérations** de type Hack&Leak revendiquées sur Telegram, et l'une d'entre elles sur YouTube. Bien que largement sous-représentées en termes quantitatifs par rapport aux activités de DDoS, les attaques impliquant la divulgation publique de données confidentielles peuvent être très dommageables pour les entités ciblées et leurs clients.

En effet, l'analyse qualitative de l'ensemble des attaques révèle que la plupart de celles impliquant du DDoS n'ont eu que peu, ou pas d'impact, tandis que celles impliquant du Hack&Leak se sont révélées bien plus dommageables et ont été opérées par des acteurs disposant d'un mode opératoire plus sophistiqué.

R00TK1T ATTAQUE DES MULTINATIONALES FRANÇAISES (12/2023)

Le groupe hacktiviste R00TK1T s'est particulièrement illustré en la matière, en annonçant la compromission de multinationales françaises du CAC 40 pendant les vacances de Noël 2023. L'une d'entre elles a été accusée par R00TK1T de mener des « expériences sur des humains », détériorant inévitablement son image de marque. Au-delà du dénigrement médiatique de la multinationale, les opérateurs du canal Telegram avaient annoncé disposer de données confidentielles et vouloir nuire à la stabilité économique du groupe.

En 2024, R00TK1T a poursuivi ses activités de Hack&Leak en divulguant les données de 3 victimes en janvier 2024, dont une grande entreprise de sous-traitance alimentaire et une préfecture publique, incluant les coordonnées des employés concernés, des projets internes et des contrats commerciaux.

Le positionnement revendiqué du groupe reste flou et oscille entre soutien à Israël et messages anti-système. Les opérateurs du groupe R00TK1T avaient mené diverses opérations de type Hack&Leak contre l'Iran en réaction à l'attaque du Hamas en Israël le 7 octobre 2023.

2.3

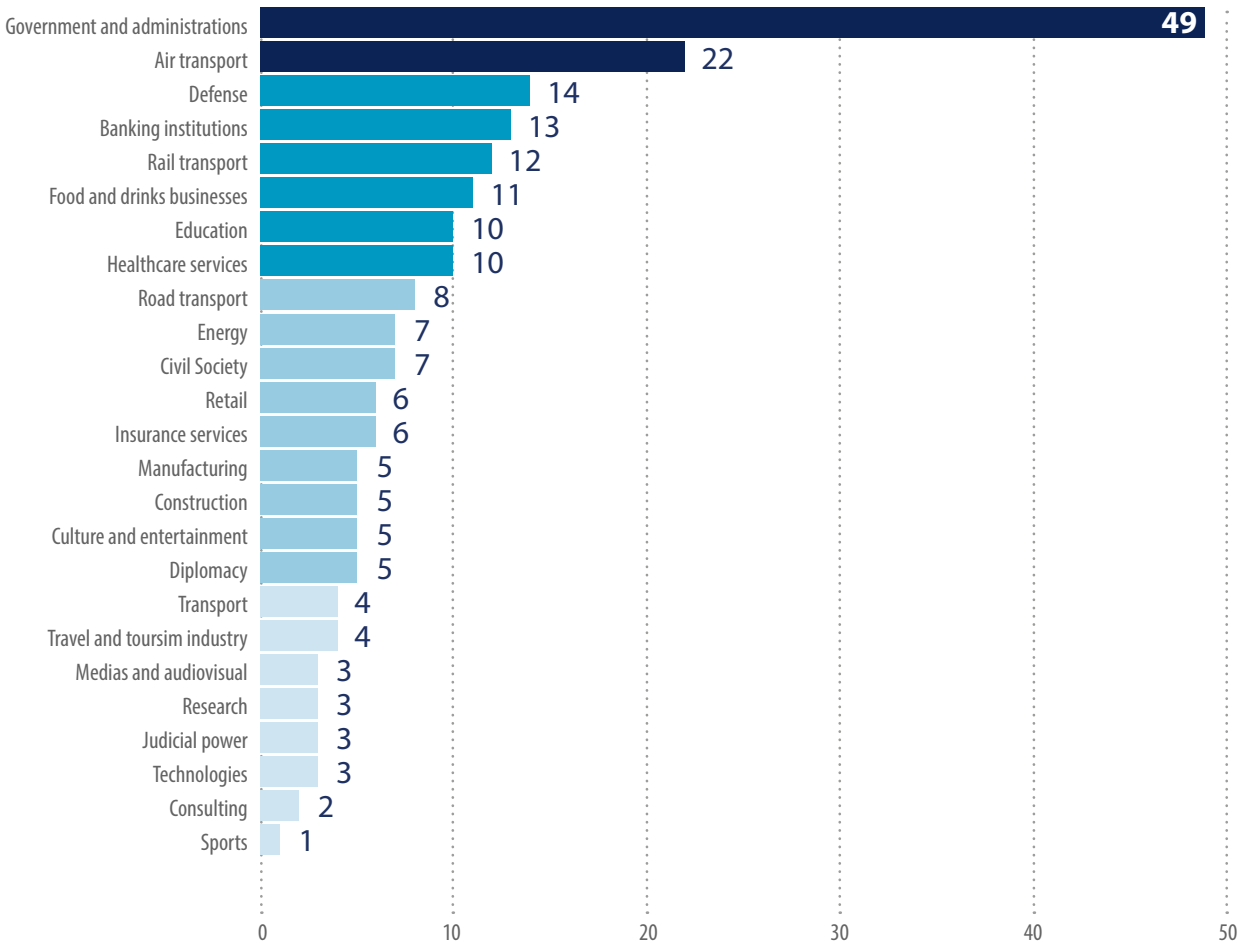
Les secteurs d'activité qui ont la plus forte visibilité sont les premières victimes d'attaques

Les opérations des hacktivistes visent à la fois des entités privées et publiques car tous les moyens sont bons pour atteindre la France :

- Attaquer des grands groupes qui représentent la France dans le monde.
- Attaquer des services publics qui font fonctionner la société et représentent l'État.
- Attaquer de manière opportuniste des entités de moindre importance dès lors qu'elles seraient basées en France.

L'analyse sectorielle révèle que le ciblage des victimes est largement influencé par l'importance du secteur auquel elles appartiennent. En effet, les secteurs qui assurent la continuité des activités économiques et sociales d'un pays, souvent stratégiques et catégorisés « opérateur d'importance vitale » (OIV) ou « opérateurs de services essentiels » (OSE), sont surreprésentés parmi les victimes.

Nombre d'attaques hacktivistes observées par le CERT-XMCO en 2023, par secteur
(les attques les plus négligeables et/ou menées sur des TPE ont été retirées pour obtenir une meilleure représentation de la menace)



Ainsi, les principaux secteurs ciblés sont :

L'ADMINISTRATION

(23% des attaques observées)

- Les organisations gouvernementales, leurs représentants, et les entités opérant dans le secteur public sont inévitablement exposées aux attaques hacktivistes.

LES TRANSPORTS

(21,5% des attaques observées)

- Les transports aériens, et plus précisément les sites des aéroports français (à 18 reprises).
- Les transports ferroviaires, et en particulier les services en ligne liés à la RATP et à la SNCF.
- Les transports routiers, notamment les compagnies de cars.
- Les transports publics (« Transport » dans le graphique plus haut), le plus souvent locaux.

LES SERVICES DE SANTÉ ET D'ÉDUCATION

(9,5% des attaques observées) :

- Pour le secteur de la santé, le groupe Anonymous Sudan a, à lui seul, ciblé 4 hôpitaux le 22 mars 2023.
- En ce qui concerne l'éducation, 4 universités françaises ont par exemple subi des attaques DDoS menées par des groupes hacktivistes dénonçant le principe de laïcité dans les écoles[4] à la veille des rentrées scolaires, le 31 août 2023.

LA DÉFENSE

(6,5% des attaques observées)

- L'industrie de défense et les forces armées ont été les cibles de groupes hacktivistes russophones, en réaction à l'aide apportée à l'Ukraine depuis février 2022. Au-delà des attaques par DDoS, le CERT-XMCO a identifié le leak d'un document sensible et le doxing de personnels travaillant au profit du secteur de la Défense.

LES SERVICES BANCAIRES ET FINANCIERS

(6% des attaques observées)

- À titre d'exemple, la même grande banque française a été victime à 9 occasions en 2023 d'attaques DDoS. Aussi, certaines attaques ayant affecté les services bancaires et financiers auraient été motivées par les sanctions économiques européennes imposées à la Russie.

Le ciblage massif et systématique de ces services est cohérent avec les objectifs des groupes hacktivistes ayant visé la France en 2023 :

- Perturber les institutions de l'État et les empêcher d'avoir un fonctionnement optimal.
- Renforcer l'écart entre les autorités publiques et la population.
- Exploiter la lassitude des citoyens français dans l'aide militaire et financière apportée à l'Ukraine.
- Alimenter la division entre les pays occidentaux et le sentiment d'instabilité économique et sociale.

(4) Cf. Chapitre « Les crises françaises : des vulnérabilités à exploiter »

2.4
Les crises françaises : des vulnérabilités à exploiter

En 2023, les groupes hacktivistes ont également exploité les difficultés rencontrées par la France tant sur le plan national qu'international pour attiser les tensions sociales et justifier leurs actions malveillantes auprès de leurs audiences sur Telegram.

NAHEL ET LES ÉMEUTES DE L'ÉTÉ (07/2023)

Le 3 juillet 2023, KromSec a publié une liste contenant les informations personnelles de 1 122 magistrats et avocats sur son canal Telegram fermé depuis. L'action a eu lieu au moment où se déroulaient des émeutes partout en France en réaction à la mort du jeune Nahel dans le cadre d'une intervention de police. Sur Twitter, KromSec dénonçait le « racisme de la police française » et apportait un soutien aux émeutiers.

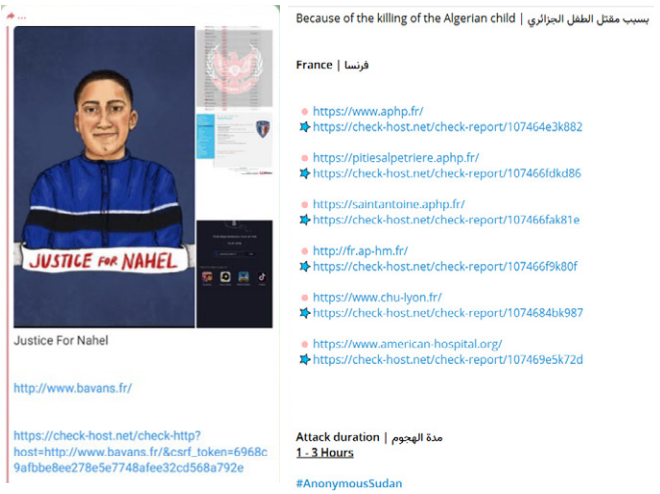
Publication de KromSec sur Twitter

Les données fuitées concernaient de nombreuses informations personnelles de victimes travaillant notamment au Palais de l'Élysée, à la mairie de Paris, à la Cour d'appel de Paris, au ministère de la Justice, à Tracfin, au ministère des Affaires étrangères et de l'Europe et à la Cour des comptes[18].

Les opérateurs de KromSec ont affirmé avoir obtenu ces données à partir d'une vulnérabilité exploitée au sein du CMS Drupal du ministère de la Justice sans préciser la CVE associée. Le ministère de la Justice a cependant nié avoir été victime d'une cyberattaque. En effet, les données en question auraient été anciennes et auraient pu être obtenues à partir de recoupements d'autres opérations de scraping de données.

Observé pour la première fois en 2022, le collectif KromSec revendique appartenir à la mouvance Anonymous. Il a articulé la majorité de ses activités perturbatrices contre des régimes autoritaires – Russie, Biélorussie, Iran en tête. D'autres opérations avaient également été effectuées par le groupe en Europe, notamment en Suède, pour donner suite à l'extradition du demandeur d'asile politique Mahmut Tat vers la Turquie[19].

Publication de KromSec sur la compromission du ministère de la Justice



D'autres groupes hacktivistes ont ciblé les sites d'entités françaises en soutien aux émeutes ayant suivi la mort de Nahel M. (à gauche : Infinite Insight, à droite Anonymous Sudan)

L'EXPULSION DES FORCES FRANÇAISES HORS D'AFRIQUE FRANCOPHONE

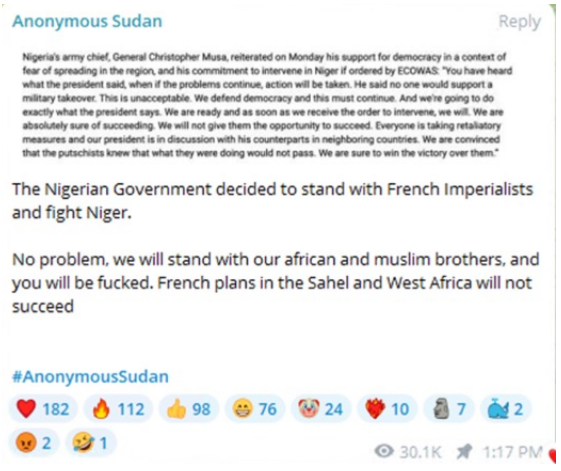
Face aux sanctions économiques européennes à la suite de l'annexion de la Crimée en 2014 et à l'isolement qui en a découlé, la Russie a progressivement réinvesti le continent africain à travers l'exportation d'armes et le déploiement de forces mercenaires (WAGNER), agissant officiellement de manière indépendante, en échange d'accès à des ressources naturelles abondantes.

De surcroit, les actions menées par la Russie pour accélérer la décomposition de la présence française en Afrique peuvent être vues comme une réponse aux actions françaises en Ukraine que la Russie perçoit à la fois comme son glacis géopolitique et son pré carré historique.

Le rapprochement des autorités russes avec différents États africains s'est notamment appuyé sur les difficultés rencontrées par les forces armées françaises dans la lutte contre le terrorisme (AQMI) et en dénonçant l'héritage colonialiste français.

Différentes campagnes de désinformation ont été menées par les groupes hacktivistes prorusses au cours des dernières années en exploitant les limites rencontrées par la France dans sa coopération avec le Mali et la Centrafrique [20]. Les autorités russes ont profité d'un contexte qui leur était favorable pour désigner Paris comme responsable des problèmes rencontrés par le continent africain. Le retrait progressif des forces armées françaises a débuté en février 2022 avec la fin de l'opération Barkhane au Mali et la rétrocession de la base de Gao en août 2022.

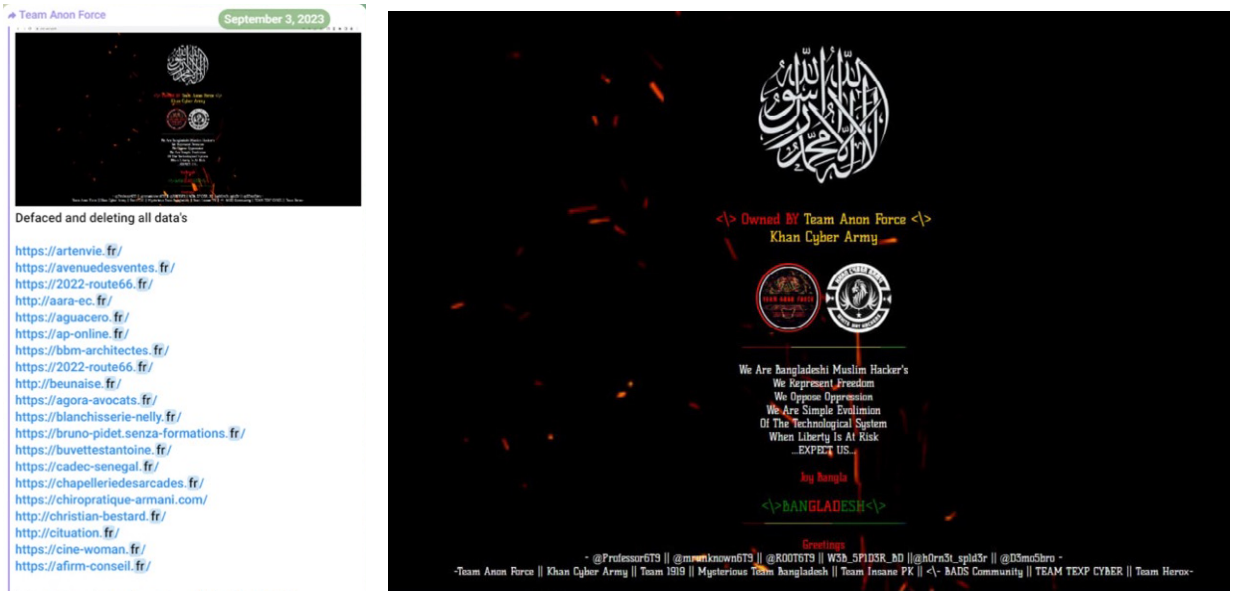
Le départ français du continent africain s'est ensuite accéléré en 2023 avec la fin de l'opération Sabre au Burkina Faso en février, suivie par le retrait complet des troupes françaises du pays en août 2023. En août 2023, à la suite d'un coup d'État au Niger, la France a retiré ses troupes après une demande de la junte militaire putschiste, malgré les accords signés avec les autorités légitimes jusque-là en place. Les forces françaises quittent définitivement le Niger en décembre 2023, avec la rétrocession de la base aérienne projetée de Niamey aux autorités nigériennes. Plusieurs groupes hacktivistes comme Killnet et Anonymous ont donc appuyé sur ces évènements pour accompagner leurs revendications d'attaques et accentuer leur ciblage de la France.



Déclaration d'Anonymous Sudan sur la présence française au Niger

L'INTERDICTION DE L'ABAYA DANS LES ÉCOLES (AOÛT ET SEPTEMBRE 2023)

Mysterious Team Bangladesh (MTB) s'est distingué en août 2023 par une série de cyberattaques par déni de service (DDoS) à l'encontre de plusieurs aéroports et services publics français, dont l'Université Paris Cité[21]. Le groupe hacktiviste a justifié ses attaques sur Telegram par l'interdiction du port l'abaya dans les écoles publiques françaises et par la position de la France sur le coup d'État au Niger. Sur sa chaîne Telegram, MTB se revendique comme étant un groupe hacktiviste musulman d'origine bangladaise.



Revendication d'attaques DDoS (à gauche) puis défacement (à droite) de PME françaises par les groupes MTB et Team Anon Force

Les actions et motivations de MTB rappellent celles du groupe Anonymous Sudan qui se revendique également comme étant un groupe hacktiviste musulman soudanais dont le positionnement géopolitique est résolument pro-russe.

3. 2024 : UNE MENACE CROISSANTE, TANT SUR LE VOLET INTERNATIONAL QU'INTERIEUR

3.1 Des configurations internationales et nationales qui favorisent le ciblage de la France

Les chapitres précédents nous ont permis de faire deux observations :

1. Les activités des groupes hacktivistes sont fortement liées aux tensions géopolitiques en cours.
2. Les groupes hacktivistes prennent appui sur des évènements nationaux (ex. les émeutes de l'été 2023) pour justifier ou faire passer leurs messages.

Or, le fort regain de tensions géopolitiques observé depuis début 2022 semble tendre vers l'escalade continue. En outre, les affrontements armés dans la bande de Gaza entre le Hamas et Israël et au Haut-Karabakh entre l'Arménie et l'Azerbaïdjan pourraient avoir des répercussions sur les Jeux Olympiques de Paris en fonction de la position diplomatique de la France sur ces dossiers. Le 13 novembre 2023, Paris avait déjà dénoncé une opération de désinformation sur les réseaux sociaux, attribuée à l'Azerbaïdjan. Cette campagne visait à ternir la réputation de la France quant à sa capacité à organiser les Jeux olympiques[23].

« Plus de 1 600 publications accompagnées de ces visuels ou des hashtags BoycottParis2024 ont ainsi été publiées sur la plateforme X/Twitter » entre le 26 et le 27 juillet, selon Viginum[50][51].

À cela s'ajoute une accumulation de plus en plus rapprochée de crises nationales connues par la France (sécuritaire, financière, politique, etc.) qui sont autant d'angles d'attaque potentiels des hacktivistes.

En effet, l'évolution du paysage politique français est susceptible d'être exploitée par les groupes hacktivistes afin de légitimer leurs actions contre la France et d'exacerber les fractures internes, comme en témoignent les récentes attaques DDoS menées par NoName057(16) en « soutien » aux manifestations menées par les agriculteurs français[24]. Face à ces constats, la menace hacktiviste semble s'intégrer durablement au paysage de la menace cyber qui pèse sur les entités françaises.

NoName057(16) revendique une série d'attaques DDoS contre la France (site de la ville de Bordeaux, du Havre, de Poitiers et des départements de l'Eure et de l'Aude) en soutien aux agriculteurs français.

3.2 Une attention toute particulière sur les JO de Paris 2024

L'organisation des Jeux Olympiques et Paralympiques de Paris 2024 pourrait offrir une visibilité médiatique accrue aux groupes hacktivistes ciblant des organisations françaises.

À titre d'exemple, le soutien apporté à l'Ukraine par la France ou les questions liées à l'exclusion d'athlètes de nationalités russe et biélorusse sont susceptibles d'être des motivations de passage à l'acte pour les acteurs de la menace hacktiviste partisans de la Russie qui chercheraient à perturber la compétition sportive et nuire à la réputation de la France.

D'autres groupes aux motivations différentes ont déjà annoncé leur intention de cibler les JO2024.

C'est notamment le cas des opérateurs du groupe hacktiviste LulzSec qui, en février 2024, avaient clairement indiqué sur X et Telegram leur volonté de cibler l'évènement.

Le groupe LulzSec annonce une campagne d'attaques contre le site des Jeux olympiques 2024 (source : CERT-XMCO)

LulzSec est un collectif hacktiviste similaire à Anonymous, qui se caractérise par le fait que différents groupes d'attaquants peuvent s'en revendiquer et conduire des attaques en utilisant son nom. C'est le cas par exemple de LulzSec Indonesia, qui avait revendiqué la compromission du site web d'Orano le 9 février dernier, ou de LulzSec France qui avait annoncé en janvier 2024 sa collaboration avec le groupe hacktiviste marocain Moroccan Black Cyber Army (MBCA) pour cibler le Danemark.

En 2024, les consultants du CERT-XMCO portent une attention particulière à LulzSec qui s'est déjà fait connaître suite à la revendication, le 12 février 2024, du piratage de 600 000 comptes de la Caisse d'Allocations familiales (CAF), menaçant de mener d'autres perturbations à l'encontre des organismes français[25]. Une revendication qui reste à nuancer, malgré l'emballement médiatique d'alors, car sur 600 000 comptes compromis de la Caisse d'Allocations Familiales (CAF), seuls 4 comptes auraient été réellement compromis. Dans la même veine, CyberKnow avait également souligné la revendication abusive d'une attaque par LulzSec Indonesia (un groupe associé à LulzSec) contre le gouvernement australien, qui n'avait, en réalité, partagé que des documents déjà publics.

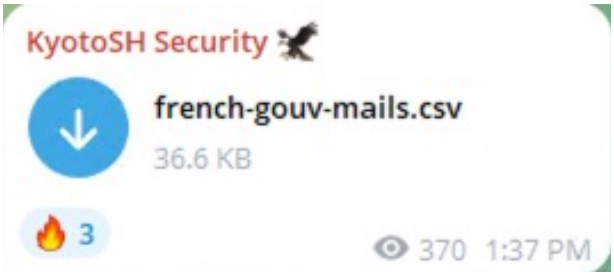
3.3 L'apparition de groupes hacktivistes francophones

Entre le 29 février et le 4 mars 2024, plusieurs groupes hacktivistes vraisemblablement francophones (notamment KyotoSH, Alixsec, GLORIAMIST et Athena) ont revendiqué des attaques contre des entités françaises. Certaines d'entre elles ont subi des attaques par déni de service distribué (DDoS) quand d'autres auraient été victimes d'un vol de données présumé.

- Un vol de données du site web du Parti de Gauche le 29 février, revendiqué par **KyotoSH** ;
- Des attaques DDoS contre le site web de l'INRAE et contre le site de recrutement de l'Armée de Terre le 1er mars, revendiquées par **Alixsec** ;
- Le vol de données à la Banque de France, également revendiqué par **Alixsec** le 2 mars ;
- Le vol de données appartenant au CNED, revendiqué par **Alixsec** le 3 mars ;
- Une attaque DDoS contre l'ESF revendiquée par **GLORIAMIST** le 3 mars ;
- Le vol de données personnelles d'étudiants de la Faculté des Sciences et Techniques (FST) de l'Université Haute-Alsace, revendiqué par **Athena** le 3 mars ;
- Le détournement de comptes EduConnect le 3 mars revendiqué par **KyotoSH**.

D'autres revendications relatives à des attaques ciblant des entités de moindre envergure ont également été constatées, par les groupes **Athena** et **Team 1916** notamment. Ces groupes, qui avaient annoncé leur association à la fin du mois de février, comprennent des membres vraisemblablement francophones. Il est probable qu'une partie significative de leur cible soit des entités localisées dans l'Hexagone à l'avenir.

Enfin, le groupe **Lapsus$** France, sur lequel encore peu d'informations sont connues, a revendiqué une série d'attaques, dont celle contre le site web de la DGSI le 10 février 2024, le site web Kiwisocial, et environ 30 000 autres sites web français le 11 février 2024.



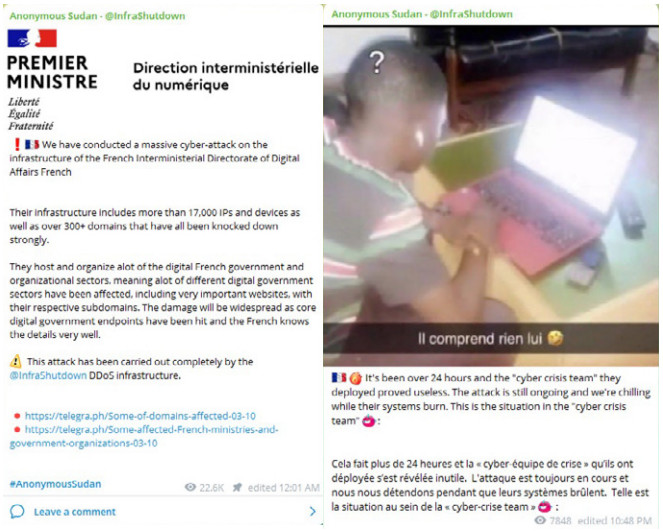
KyotoSH divulgue un dump contenant les identifiants de fonctionnaires français

3.4 La poursuite d'opérations d'envergure par les groupes hacktivistes pro-russes

Dans la journée du 10 mars 2024, les services de l'État ont été visés par une campagne d'attaques DDoS sans précédent, revendiquée sur Telegram par Anonymous Sudan[26]. D'après les déclarations du groupe, différents ministères français avaient été perturbés, dont :

- Ministère de la Culture,
- Ministère de la Santé,
- Ministère des Affaires sociales,
- Ministère de l'Économie et des Finances,
- Ministère de la Transition écologique,
- Et enfin les services du Premier ministre.

L'ampleur de l'incident, débouchant sur la médiatisation exceptionnelle de cette campagne, serait en partie liée au ciblage du réseau interministériel de l'État (RIE), responsable de l'interconnexion de plus d'un million d'agents de la fonction publique et de 14 000 sites étatiques[27].



Anonymous Sudan revendique les attaques contre la France

Au lendemain, de cette campagne, le 11 mars 2024, les groupes hacktivistes prorusses UserSec, Narodnaya CyberArmia (en russe : Народная CyberАрмия), NoName057(16), et 22C avaient collectivement revendiqué une série d'attaques DDoS contre de nouvelles cibles françaises :

- L'Agence France Presse,
- Orano,
- Électricité de France,
- La ville de Bordeaux,
- La région Normandie,
- Le Conseil Régional de Guadeloupe.

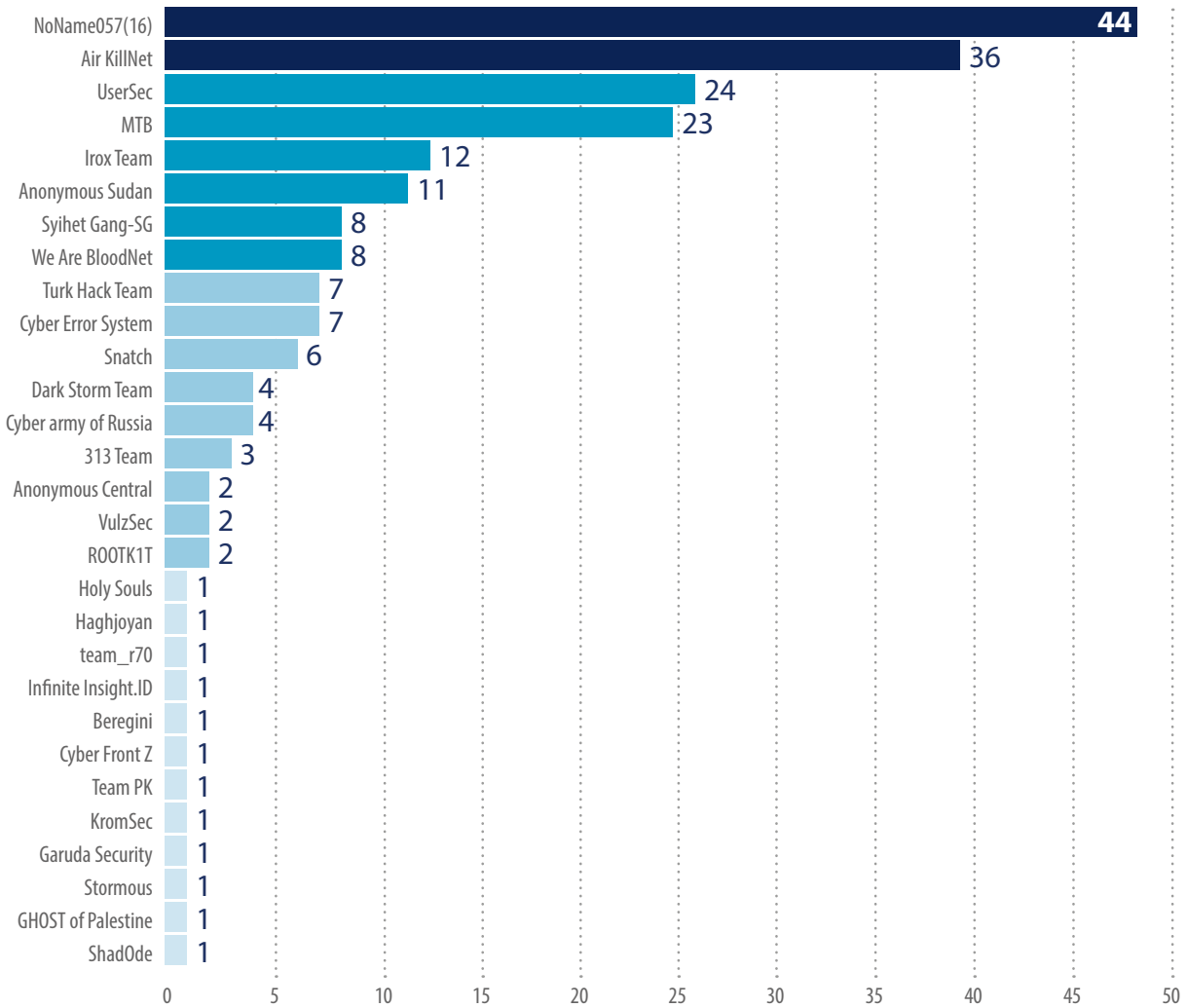
Annonce de la coalition entre les quatre opérateurs hacktivistes prorusses

4. QUI VISE LA FRANCE ?

4.1 Des acteurs aux profils variés

Si la France est désormais perçue à travers le monde comme une puissance moyenne, elle continue néanmoins de peser dans les relations diplomatiques internationales à travers ses nombreuses prises de position, son rôle européen de premier plan, son siège au Conseil de Sécurité de l'ONU et sa capacité de dissuasion nucléaire. À cet égard, elle est ciblée par une multitude d'acteurs aux prises de position géopolitiques variées. **En 2023, la France a été visée par plus de 30 organisations hacktivistes.** Ces organisations sont le plus souvent pro-russes, mais peuvent aussi porter des messages pro-Israël, de soutien à Gaza, parfois pro-Ukrainiens, ou simplement anti-français et antisystème.

Revendications d'attaques contre la France recensées en 2023, par groupe hacktiviste
(les attques les plus négligeables et/ou menées sur des TPE ont été retirées pour obtenir une meilleure représentation de la menace)

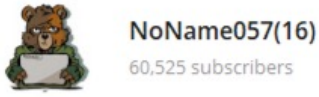


Beaucoup d'entre eux ont revendiqué leurs attaques en y associant tout au long de l'année le hashtag « #OPFrance » ou « #OP_France ». Ce dernier agit comme une bannière permettant d'élargir la visibilité des attaques et participe à l'installation d'un climat anxiogène. **Il avait déjà été utilisé en 2015, dans le cadre des attaques terroristes du 7 janvier 2015 ayant ciblé Charlie Hebdo.** À l'époque, des milliers de sites français avaient été touchés par des groupes partisans de la cause djihadiste (AnonGhost en tête), collectivement revendiqués sous la bannière #OpFrance[2]. La campagne a cependant pris une autre dimension en 2023. Les actions menées sous cette bannière ont pu varier dans leur nature et leurs intentions politiques : dénonciation du racisme dans la police, politique étrangère française vis-à-vis de Gaza, etc. En utilisant la bannière #OpFrance lors de leurs attaques, les groupes hacktivistes tentent d'augmenter la portée médiatique de leurs campagnes auprès du grand public et des médias, afin de faciliter la diffusion de leurs revendications politiques.

Présentation des principaux groupes hacktivistes qui ont ciblé la france en 2023

NoName057(16)

Date de création : **mars 2022**
Allégeance : **Pro-Russe**
Mode opératoire : **DDoS**



En 2023, NoName057(16) a été l'un des groupes hacktivistes pro-russes les plus actifs. Ses actions s'alignent avec les intérêts du Kremlin, comme l'a notamment illustré sa campagne d'attaque visant la Société Militaire Privée (SMP) russe WAGNER en juin 2023, en réaction à sa rébellion contre le ministre de la Défense Sergueï Choïgou.

NoName057(16) a revendiqué 44 attaques par déni de service distribué (DDoS) contre des organisations publiques françaises des entreprises privées du secteur des transports, de la banque et de l'énergie.

Le 27 septembre 2023, les opérateurs avaient ciblé des entités liées au ministère de l'Économie et des Finances français en réponse aux déclarations du Président de la République concernant la violation présumée du territoire arménien par l'Azerbaïdjan, et affirmant de nouveau son soutien à l'Ukraine.

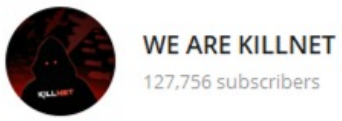
Ces attaques avaient coïncidé avec les prélèvements d'impôt sur le revenu effectué par impots.gouv.fr. En bloquant temporairement l'accès à cette plateforme gouvernementale, les opérateurs du groupe hacktiviste augmentent la visibilité de leurs revendications politiques auprès de la population française.

Le 9 novembre 2023, le secteur des transports (site de la RATP, le portail de gestion du régime spécial de sécurité sociale des personnels de la RATP et les transports publics de la ville de Rennes) a été ciblé par le groupe hacktiviste prorusse, en réponse à l'abondement de 200 millions d'euros par Paris au fonds de soutien à l'Ukraine, survenu le même jour[3].

Au cours de l'année, les opérateurs de NoName057(16) se sont appuyés sur leur projet collaboratif DDoSia, permettant à leurs partisans d'ajouter leurs machines au botnet, en échange d'une rétribution financière [4]. En complément, il est à noter que le groupe a annoncé le 4 septembre 2023 s'être associé à un collectif hacktiviste pro-russe comprenant notamment les groupes Killnet, Beregini ou encore XakNet Team pour coordonner leurs attaques.

Killnet

Date de création : **mars 2022**
Allégeance : **Pro-Russe**
Mode opératoire : **DDoS, désinformation, incitation au passage à l'acte**



Actif depuis le début du conflit en Ukraine, le groupe s'est positionné ouvertement en faveur de la Russie menant 36 attaques DDoS contre la France. Dirigé jusqu'en décembre 2023 par un acteur connu sous le nom de KillMilk (de son vrai nom Nikolai Nikolayevich Serafimov[5]), le collectif hacktiviste a principalement ciblé des entités aux États-Unis et en Europe, avec plus de 500 victimes identifiées par Mandiant entre janvier et juin 2023 dans le monde[6].

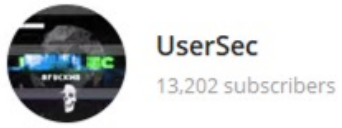
En juin 2023, Killnet avait également participé avec NoName057(16) et Anonymous Sudan à la campagne d'attaques contre les institutions bancaires françaises, pour dénoncer l'exclusion des banques russes du système bancaire SWIFT[7].

Killnet a occupé une position de leader dans l'écosystème hacktiviste prorusse. Cela étant, il a connu de fortes dissensions internes. Le responsable du canal Telegram, connu sous le nom de KillMilk, a fait l'objet d'un doxing en novembre 2023 (dévoilant publiquement son identité) à la suite de divergences internes au sein du groupe, l'accusant de fraude après le détournement d'un million de roubles à l'administrateur du forum RuTor. Le leadership avait été ensuite transféré en décembre 2023 à un autre opérateur connu sous le nom de Deanon Club[8].

Au-delà des tensions internes, le groupe hacktiviste s'est manifesté par des revendications d'attaques médiatiques, dont l'attribution reste encore incertaine. En décembre 2023, le groupe a notamment revendiqué le sabotage du principal opérateur mobile ukrainien « Kyïvstar », finalement associé au groupe hacktiviste Solntsepyok[9][10].

UserSec

Date de création : **janvier 2023**
Allégeance : **Pro-Russe**
Mode opératoire : **DDoS et divulgation de données**

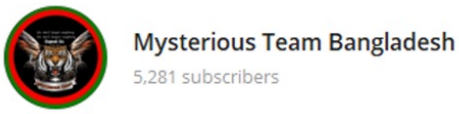


Le canal du groupe a été créé en janvier 2023 et appelle ses abonnés à la lutte contre l'Occident et au soutien à la Russie. Jusqu'au 8 octobre 2023, les attaques DDoS du groupe étaient essentiellement motivées par le soutien à la Russie, avant d'orienter son soutien à la cause palestinienne. Dès le 11 octobre, les opérateurs du groupe hacktiviste ont ciblé des aéroports français via des attaques DDoS, revendiquées également par KillNet le même jour.

Le 29 octobre, UserSec réitérait sa volonté de cibler l'Europe[11]. Par ailleurs, le groupe a aussi collaboré avec NoName057(16), qui a revendiqué une série d'attaques DDoS contre les banques centrales de plusieurs pays européens. UserSec est le troisième groupe ayant le plus ciblé la France au cours de l'année 2023, avec 23 attaques par déni de service et une divulgation de données. Malgré quelques attaques DDoS médiatisées contre les services publics français (les sites des France Visa ou d'Economie.gouv.fr), le groupe a essentiellement ciblé des petites et moyennes entreprises, issues de divers secteurs d'activités.

Mysterious Team Bangladesh

Date de création : **juillet 2020**
Allégeance : **Pro-Russe** (Se pose aussi en défenseur de la religion musulmane contre l'Israël et l'Inde)
Mode opératoire : **DDoS**



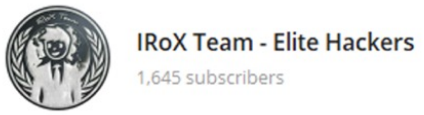
Le collectif, apparu en 2020 selon ses fondateurs, mais s'étant réellement fait connaître à partir de 2022, a mené plus de 750 attaques DDoS et 78 défacements de sites web depuis juin 2022 selon Group-IB [12]. En 2023, le CERT-XMCO a recensé 23 attaques DDoS de MTB contre la France. MTB est soupçonné par Group-IB d'avoir exploité des serveurs et des panneaux d'administration exposés, avec des outils open-source et des versions vulnérables de PHPMyAdmin et WordPress pour mener ses attaques[12].

En mars et en août 2023, MTB a ciblé des aéroports (Paris, Calvi, Lille, Toulon-Hyères et Strasbourg) et des organismes publics français avec des attaques DDoS, dont l'Université Paris-Cité, motivant ses actions par des motifs religieux et politiques. Les acteurs malveillants justifient leurs attaques par l'interdiction de porter l'abaya dans les écoles et par la position de la France en réaction au coup d'État au Niger.

Cette stratégie pourrait être une tentative de dissimuler leurs véritables origines et de susciter une sympathie du monde arabo-musulman. En effet, il est possible que MTB soit en partie un groupe russe, qui, comme Anonymous Sudan, prétend être un groupe de culture musulmane pour dissimuler ses activités. Un autre groupe russe sponsorisé par le Kremlin, APT28, aurait également employé cette stratégie lors de la compromission de TV5 Monde, qui avait été revendiquée par « Cyber Califat », un groupe hacktiviste jusque-là inconnu[13].

IRoX Team

Date de création : **septembre 2023**
Allégeance : **Pro-Palestine**
Mode opératoire : **DDoS**



IRoX Team a proclamé son soutien à la Palestine et a annoncé son intention de cibler plusieurs pays occidentaux soutenant Israël, dont la France, le 30 octobre 2023 sur Telegram[14]. Dès le 28 octobre, le groupe hacktiviste avait déjà lancé des attaques DDoS contre plusieurs sites web français.

Les revendications du groupe sont généralement publiées en anglais, mais l'administrateur d'IRoX Team prétend être un acteur de la menace originaire du Bangladesh. Il reste difficile de déterminer la crédibilité de cette menace, d'autant plus que les revendications d'attaques contre la France ont essentiellement concerné des petites ou moyennes entreprises spécialisées dans la restauration rapide et le BTP.

La victimologie du groupe, essentiellement centrée sur des petites et moyennes entreprises françaises au rayonnement local (TPE/PME), amène le CERT-XMCO à penser que ces attaques seraient en réalité opportunistes. Les conséquences de ces dernières sont largement exagérées et amplifiées par d'autres groupes hacktivistes anti-Israël (tels que Sylhet Gang-SG, Garuda Security et Ganosec Team) afin d'atteindre une audience plus large.

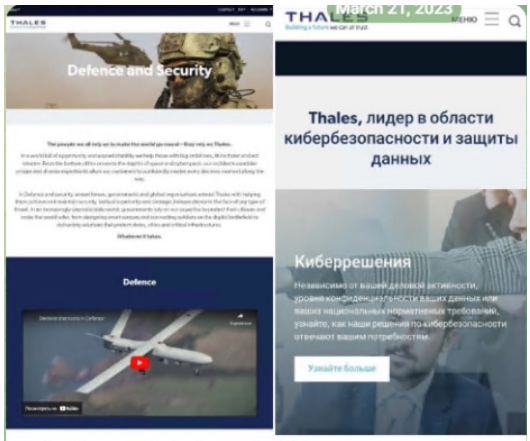
4.2 Des acteurs aux motivations politiques bien établies

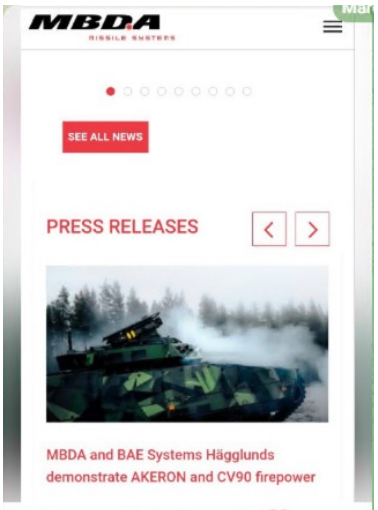
Après s'être intéressés aux profils des principaux hacktivistes qui ont visé la France, tentons maintenant de mieux comprendre leurs motivations à travers trois exemples.

DES « HACKTEURS » PRO-RUSSE ALIGNÉS SUR L'AGENDA POLITIQUE DU KREMLIN

Narodnaya CyberArmia (en russe : Народная CyberАрмия), a revendiqué une série d'attaques DDoS contre Nexter (05 janvier 2023), MBDA (11 mars 2023) et Thales (21 mars 2023). Ces trois organisations sont des acteurs majeurs de l'industrie de la Défense française et européenne et ont vraisemblablement été ciblées par leur implication directe ou indirecte dans le soutien à l'effort de guerre ukrainien et le renforcement du dispositif de défense européen. Le canal Telegram de ce groupe hacktiviste a été créé le 1er avril 2022 en réaction à la « guerre informationnelle américaine » menée en Ukraine. Les opérateurs du groupe ajoutent dans leur premier message qu'aucune menace liée à la sécurité nationale russe ne serait tolérée.

Narodnaya CyberArmia revendique des attaques DDoS contre les acteurs de l'industrie française de la défense





Depuis le début de la guerre en Ukraine, les analystes de Mandiant ont identifié trois chaînes Telegram promouvant les intérêts russes, dont Narodnaya CyberArmia. Deux hypothèses principales ressortent : Narodnaya CyberArmia pourrait être directement contrôlé par le GRU ; ou bien par des civils russes qui coordonneraient leurs activités directement avec le GRU[15]. En tout état de cause, le degré d'affiliation du groupe avec les services de renseignement militaire russes reste encore incertain.

Le groupe hacktiviste s'appuie sur la figure controversée de Stepan Bandera pour soutenir la thèse que l'Ukraine serait nazie et appuyer l'objectif souvent présenté par Vladimir Poutine dans ses discours de *dénazifier* l'Ukraine. En effet, Stepan Bandera, est une

Le groupe revendique une attaque contre un site ukrainien

figure centrale du nationalisme ukrainien et un collaborateur nazi durant la Seconde Guerre mondiale.

Via leurs attaques DDoS, les groupes hacktivistes pro-russes participent à la mise en place d'une atmosphère de « peur, d'incertitude et de discorde » autour du soutien apporté par la France à l'Ukraine. Ce prisme de lecture contribue à l'évolution cognitive du champ de bataille.

Les conséquences des attaques hacktivistes ne seraient donc pas tant liées à l'effet perturbateur qu'elles entrainent, ni même à la nature des données compromises, mais plutôt à l'impact émotionnel qu'elles entrainent sur leurs cibles, en les incitant à revoir leurs postures et/ou leurs certitudes.

CHARLIE HEBDO, VISÉ PAR LE RÉGIME IRANIEN

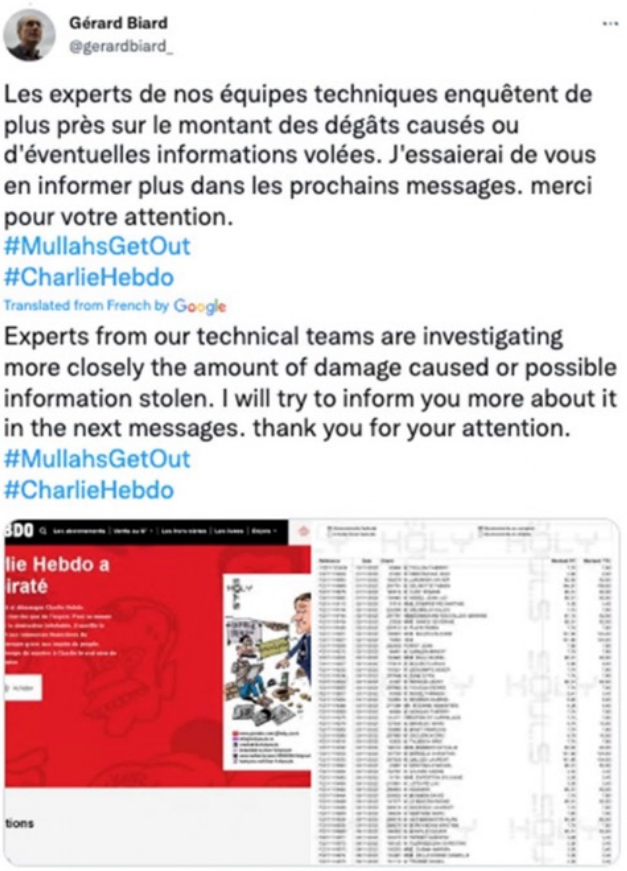
D'autres États, comme l'Iran, ont recours aux groupes hacktivistes pour revendiquer leurs opérations cyber et diffuser un message à leurs adversaires. Le 4 janvier 2023, les activités de monitoring sur le Deep/Dark Web du CERT-XMCO ont permis d'identifier la vente d'une base de données associée à Charlie Hebdo sur le forum criminel Breached Forums, incluant les données personnelles des 230 000 lecteurs du journal satirique français. Cette attaque, en parallèle revendiquée sur YouTube et en apparence motivée par la recherche de gains financiers, était intervenue juste après la publication par Charlie Hebdo de caricatures moquant le guide suprême iranien Ali Khamenei[16].

Mise en vente des données de Charlie Hebdo par Holy Souls sur Breach Forums (source : CERT-XMCO)

Un rapport publié par les équipes de Microsoft DTAC[17] avait permis d'établir que cette opération visait avant tout à discréditer Charlie Hebdo et ses publications. En plus de la mise en vente d'une base de données interne, un défacement du site de Charlie Hebdo avait été observé par Microsoft, revendiqué par le groupe hacktiviste Holy Souls, rattaché à la société de cybersécurité Emennet Pasargad, elle-même affiliée au Corps des Gardiens de la Révolution islamique (IRGC).

Défacement du site de Charlie Hebdo par le groupe Holy Souls

Le défacement du site de Charlie Hebdo avait été accompagné d'une campagne de trolling sur les réseaux sociaux à travers des comptes usurpant l'identité de personnels du journal satirique pour relayer la position de Téhéran et élargir la portée de l'attaque initiale.



Holy Souls usurpe l'identité d'un journaliste de Charlie Hebdo pour élargir l'audience de l'attaque

Carricatures publiées sur YouTube par les opérateurs du groupe Holy Souls pour revendiquer la compromission de Charlie Hebdo

UN CIBLAGE INTENSE DES SERVICES PUBLICS EN MARGE DU CONFLIT ISRAÉLO-PALESTINIEN

Depuis l'attaque lancée par le Hamas contre Israël depuis la bande de Gaza le 7 octobre 2023 et le lancement de l'opération militaire israélienne Sabre de fer le lendemain, de nombreux groupes hacktivistes ont lancé des opérations ciblant les deux parties en conflit ainsi que leurs soutiens. Parmi les groupes impliqués, des hacktivistes propalestiniens ont notamment réalisé ou annoncé des attaques visant la France, accusée d'apporter son soutien à l'État hébreu :

UserSec et **KillNet** : le 8 octobre, UserSec annonçait son ralliement à la cause palestinienne. Dès le 11 octobre, il revendiquait des attaques par déni de service distribué (DDoS) contre des aéroports français, que le groupe KillNet revendiquait également le même jour, les deux groupes ayant vraisemblablement collaboré dans la réalisation de ces attaques.

Sylhet Gang-Sg : après avoir annoncé le 8 octobre vouloir cibler des entités en France, le groupe a revendiqué une attaque DDoS contre le site web du département français de l'Eure le 12 octobre 2023 et une autre contre le secteur de la santé en Europe le 18 octobre, dont un hôpital en France. Le groupe hacktiviste explique avoir ciblé la France pour sa politique étrangère, jugée pro-israélienne et pro-indienne. Les actions menées par le Sylhet Gang-Sg sont ponctuellement revendiquées sous la bannière #Op_France et l'opérateur invite les hacktivistes musulmans à cibler la France.

Infinite Insight.ID : il a déclaré le 16 octobre le ciblage de la France pour son soutien à Israël et revendiquait le lendemain une attaque DDoS contre le site web de la banque Banorient France, annonçant avoir collaboré avec plusieurs autres groupes hacktivistes tels que Garuda Security, Hizbullah Cyb3r Team ou encore Ganosec Team.

IRoX Team : il a proclamé le 19 octobre son intention de cibler plusieurs pays occidentaux soutenant Israël, dont la France qui a commencé à faire l'objet d'attaques le 28 octobre. Le groupe adopte la cause palestinienne et fustige Tel-Aviv et la communauté internationale pour le soutien apporté à l'État juif.

Anonymous Sudan : il a invoqué le motif des «caricatures offensantes du prophète Mahomet» pour cibler la France. En 2023, Anonymous Sudan a été le 6ème groupe le plus proactif avec 11 attaques DDoS recensées par le CERT-XMCO contre l'hexagone. Au-delà de leurs positionnements prorusse, pro-Islam et antifrançais, les opérateurs du groupe affichaient notamment le message suivant « Anonymous Sudan and KILLNET are standing against Israel and anyone who supports the Zionist Entity ».

Cyb3r Drag0nz : le 27 octobre, l'opérateur du groupe Telegram a annoncé des attaques ultérieures contre la France. Le 29 octobre, il revendiquait la défiguration de plusieurs sites web français. Certaines revendications s'accompagnaient d'illustration mettant en avant le drapeau palestinien.

Bibliographie

(1) KELA, «The Stormous Extortion Group Strikes Back,» 25 07 2023. [En ligne].
Available: https://www.kelacyber.com/stormous-extortion-group-strikes-back-blog/.
(2) V. Rieß-Marchive, «#OpFrance : plus qu'une menace, une opportunité,» Le MagIT, 15 01 2015. [En ligne].
Available: https://www.lemagit.fr/actualites/2240238214/OpFrance-plus-quune-menace-une-opportunite.
(3) M. d. Armées, « Ukraine : le fonds de soutien de la France réabondé de 200 millions,» 09 11 2023. [En ligne].
Available: https://www.defense.gouv.fr/actualites/ukraine-fonds-soutien-france-reabonde-200-millions.
(4) Avast.io, «DDosia Project: How NoName057(16) is trying to improve the efficiency of DDoS attacks,» 18 04 2023. [En ligne].
Available: https://decoded.avast.io/martinchlumecky/ddosia-project-how-noname05716-is-trying-to-improve-the-efficiency-of-ddos-attacks/.
(5) Gazeta.ru, «Раскрыта личность лидера хактивистской группировки Killnet,» Gazeta.ru, 21 11 2023. [En ligne].
Available: https://www.gazeta.ru/tech/news/2023/11/21/21757105.shtml.
(6) Mandiant, «KillNet Showcases New Capabilities While Repeating Older Tactics,» Mandiant, 20 07 2023. [En ligne].
Available: https://www.mandiant.com/resources/blog/killnet-new-capabilities-older-tactics.
(7) D. Reading, «Killnet Threatens Imminent SWIFT, World Banking Attacks,» Dark Reading, 16 06 2023. [En ligne].
Available: https://www.darkreading.com/cyber-risk/killnet-threatens-imminent-swift-world-banking-attacks.
(8) R. Media, «Leader of Russian hacktivist group Killnet 'retires,' appoints new head,» Recorded Media, 08 12 2023. [En ligne].
Available: https://therecord.media/killnet-killmilk-announces-retirement.
(9) S. -. СБУ, « СБУ відкрила кримінальне провадження за фактом кібератаки на «Київстар»,» SBU - СБУ, 12 12 2023. [En ligne].
Available: https://ssu.gov.ua/novyny/sbu-vidkryla-kryminalne-provadzhennia-za-faktom-kiberataky-na-kyivstar.
(10) B. Computer, «Russian hackers wiped thousands of systems in KyivStar attack,» Bleeping Computer, 04 01 2024. [En ligne].
Available: https://www.bleepingcomputer.com/news/security/russian-hackers-wiped-thousands-of-systems-in-kyivstar-attack/.
(11) FalconFeeds.io, «Usersec to likely target Europe in the coming week.,» FalconFeeds.io, 29 10 2023. [En ligne].
Available: https://twitter.com/FalconFeedsio/status/1718569013528436890.
(12) Group-IB, «Demystifying Mysterious Team Bangladesh,» Group-IB, 03 08 2923. [En ligne].
Available: https://www.group-ib.com/blog/mysterious-team-bangladesh/.
(13) L. m. informatique, «Piratage de TV5 Monde, la piste russe se précise,» Le monde informatique, 10 06 2015. [En ligne].
Available: https://www.lemondeinformatique.fr/actualites/lire-piratage-de-tv5-monde-la-piste-russe-se-precise-61430.html.
(14) FalconFeeds.io, «Twitter/X,» FalconFeeds.io, 19 10 2023. [En ligne].
Available: https://twitter.com/FalconFeedsio/status/1714942526086644204?lang=fr.
(15) Mandiant, «Hacktivists Collaborate with GRU-sponsored APT28,» Mandiant, 23 09 2022. [En ligne].
Available: https://www.mandiant.com/resources/blog/gru-rise-telegram-minions.
(16) H. Souls, «Les esprits saints ont retiré le masque de Charlie Hebdo,» Holy Souls, 04 01 2023. [En ligne].
Available: https://web.archive.org/web/20230106154746/https://youtube.com/@holy_souls.
(17) Microsoft, «Iran responsible for Charlie Hebdo attacks,» 03 02 2023. [En ligne].
Available: https://blogs.microsoft.com/on-the-issues/2023/02/03/dtac-charlie-hebdo-hack-iran-neptunium/.
(18) 0. Net, « Après les émeutes, des pirates ont divulgué les données de 1000 magistrats français,» 04 07 2023. [En ligne].
Available: https://www.01net.com/actualites/apres-emeutes-pirates-divulgue-donnees-1000-magistrats-avocats.html.
(19) C. international, «Adhésion à l'Otan : la Suède accepte de remettre un Kurde à la Turquie,» Courrier international, 06 12 2022. [En ligne].
Available: https://www.courrierinternational.com/article/concession-adhesion-a-l-otan-la-suede-accepte-de-remettre-un-kurde-a-la-turquie.
(20) T. Insider, «Sowing discord: How Russia engages in African revolts to cement its influence,» The Insider, 13 03 2024. [En ligne].
Available: https://theins.ru/en/politics/269926.
(21) Numerama, « Cyberattaque liée à l'interdiction de l'abaya à l'école : le site d'une université à Paris en panne,» 31 08 2023. [En ligne].
Available: https://www.numerama.com/cyberguerre/1488614-le-site-dune-universite-a-paris-en-panne-la-cyberattaque-serait-liee-a-linterdiction-de-labaya-a-lecole.html.
(22) Group-IB, «Demystifying Mysterious Team Bangladesh,» Group-IB, 03 08 2023. [En ligne].
Available: https://www.group-ib.com/blog/mysterious-team-bangladesh/.
(23) F. T. Info, «Paris 2024 : une campagne de désinformation liée à l'Azerbaïdjan a ciblé les Jeux olympiques, selon un rapport,» France TV Info, 13 11 2023. [En ligne].
Available: https://www.francetvinfo.fr/les-jeux-olympiques/les-francais/jo-de-paris-2024-une-campagne-de-desinformation-liee-a-l-azerbaidjan-a-cible-la-competition-selon-un-rapport_6181863.html.

Bibliographie

(24) FalconFeeds.io, «NoName targets multiple websites in France.,» 25 01 2024. [En ligne].
Available: https://twitter.com/FalconFeedsio/status/1750466040700772520.

(25) F. Info, « Ce que l'on sait du possible piratage de 600 000 comptes de la CAF, revendiqué par un groupe de hackers mais démenti par l'organisme,» France Info, 14 02 2024. [En ligne].
Available: https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/ce-que-l-on-sait-du-pretendu-piratage-de-600-000-comptes-de-la-caf-revendique-par-un-groupe-de-hackers-mais-dementi-par-l-organisme_6365002.html.

(26) D. D. Web, «#France - Anonymous Sudan allegedly conducted a cyber attack on the infrastructure of the French Interministerial Directorate of Digital Affairs,» Daily Dark Web, 11 03 2024. [En ligne].
Available: https://twitter.com/DailyDarkWeb/status/1767188776474833354.

(27) F. Info, « Plusieurs services de l'Etat sont visés par des attaques informatiques d'une «intensité inédite», signale le gouvernement,» France Info, 11 03 2024. [En ligne].
Available: https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/plusieurs-services-de-l-etat-sont-vises-par-des-attaques-informatiques-d-une-intensite-inedite-signale-le-gouvernement_6417997.html.

(28) E. 1, «Cyberattaques russes : renforcement de la sécurité dans les armées françaises,» Europe 1, 20 02 2024. [En ligne].
Available: https://www.europe1.fr/societe/cyberattaques-russes-renforcement-de-la-securite-dans-les-armees-francaises-4231720.

(29) V. Rieß-Marchive, «Le DDoS, de plus en plus un écran de fumée,» LeMagIT, 09 10 2015. [En ligne].
Available: https://www.lemagit.fr/actualites/4500255205/Le-DDoS-de-plus-en-plus-un-ecran-de-fumee.

(30) Kaspersky, «Worse than it Seems: DDoS Attacks Often Coincide With Other Threats, Kaspersky Lab Survey Shows,» Kaspersky, 02 10 2015. [En ligne].
Available: https://www.kaspersky.com/about/press-releases/2015_worse-than-it-seems-ddos-attacks-often-coincide-with-other-threats-kaspersky-lab-survey-shows.

(31) Avast, «Beware of DDosia, a botnet created to facilitate DDoS attacks,» 16 08 2023. [En ligne].
Available: https://blog.avast.com/ddosia-project.

(32) FalconFeeds.io, «Twitter Account,» 09 11 2023. [En ligne].
Available: https://twitter.com/FalconFeedsio/status/1722553741948399801.

(33) Reuters, «Exclusive: Russian hackers were inside Ukraine telecoms giant for months,» 05 01 2024. [En ligne].
Available: https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/.

(34) Mandiant, «Hacktivists Collaborate with GRU-sponsored APT28,» 23 09 2022. [En ligne].
Available: https://www.mandiant.com/resources/blog/gru-rise-telegram-minions.

(35) Radware, « Radware Report Ranks Top 15 Most Active Political and Religious Hacktivists,» 26 04 2023. [En ligne].
Available: https://www.radware.com/newsevent/pressreleases/2023/radware-report-ranks-top-15-most-active-political-and-religious-hacktivists/.

(36) L. MagIT, «Rançongiciel : le réveil en fanfare de l'énigmatique Stormous,» 05 04 2023. [En ligne].
Available: https://www.lemagit.fr/news/365534859/Rancongiciel-le-reveil-en-fanfare-de-lenigmatique-Stormous.

(37) V. -. SGDSN, «RRN : une campagne numérique de manipulation de l'information complexe et persistante,» 13 06 2023. [En ligne].
Available: https://www.sgdsn.gouv.fr/publications/maj-19062023-rrn-une-campagne-numerique-de-manipulation-de-linformation-complexe-et.

(38) Cyfirma, «Evolution of KILLNET from Hacktivism to Private Hackers Company and the Role of Sub-groups,» 12 05 2023. [En ligne].
Available: https://www.cyfirma.com/outofband/evolution-of-killnet-from-hacktivism-to-private-hackers-company-and-the-role-of-sub-groups/.

(39) LCI, ««La Russie liquide son or pour acheter des drones Shahed» : que sait-on de cette fuite de documents iraniens ?,» 07 02 2024. [En ligne].
Available: https://www.tf1info.fr/international/la-russie-liquide-son-or-pour-acheter-des-drones-shahed-que-sait-on-de-cette-fuite-de-documents-iraniens-1287-2285432.html.

(40) S. Affairs, «Snatch group claims to have hacked military provider HENSOLDT France,» 31 10 2022. [En ligne].
Available: https://securityaffairs.com/137886/cyber-crime/snatch-hensoldt-france-ransomware.html.

(41) Sekoia, « Securing Gold: Assessing Cyber Threats on Paris 2024,» 04 01 2024. [En ligne].
Available: https://blog.sekoia.io/securing-gold-assessing-cyber-threats-on-paris-2024/.

(42) L. m. informatique, «Des centaines de milliers de comptes CAF piratés ? (MAJ),» 13 02 2024. [En ligne].
Available: https://www.lemondeinformatique.fr/actualites/lire-des-centaines-de-milliers-de-comptes-caf-pirates-maj-92955.html.

Bibliographie

(43) Microsoft, « Rapport de défense numérique Microsoft 2023,» Microsoft, 09 10 2023. [En ligne].
Available: https://www.microsoft.com/fr-fr/security/security-insider/microsoft-digital-defense-report-2023.

(44) L. Figaro, ««Kremlin Leaks» : les révélations inédites sur l'ampleur de la propagande et du contrôle de l'information en Russie,» Le Figaro, 28 02 2024. [En ligne].
Available: https://www.lefigaro.fr/international/kremlin-leaks-les-revelations-inedites-sur-l-ampleur-de-la-propagande-et-du-controle-de-l-information-en-russie-20240228.

(45) FlashPoint, «Killnet: Inside the World's Most Prominent Pro-Kremlin Hacktivist Collective,» [En ligne].
Available: https://flashpoint.io/intelligence-101/killnet/.

(46) CERT-XMCO, «ActuSécu #61 de février 2024, Hors-Série Dark Web,» XMCO, 02 2024. [En ligne].
Available: https://www.xmco.fr/wp-content/uploads/2024/02/XMCO-ActuSecu-61-Dark-Web-Spyware.pdf.

(47) Truesec, «Anonymous Sudan - Threat Intelligence Report,» Truesec, 23 02 2023. [En ligne].
Available: https://files.truesec.com/hubfs/Reports/Anonymous%20Sudan%20-%20Publish%201.2%20-%20a%20Truesec%20Report.pdf.

(48) L. Monde, «Européennes 2024 : en France, le scrutin représente une « cible considérable » de manipulations étrangères, selon la sécurité nationale,» Le Monde, 06 03 2024. [En ligne].
Available: https://www.lemonde.fr/international/article/2024/03/06/europeennes-2024-en-france-le-scrutin-represente-une-cible-considerable-de-manipulations-etrangeres-selon-la-securite-nationale_6220471_3210.html.

(49) L. Monde, «Européennes 2024 : en France, le scrutin représente une « cible considérable » de manipulations étrangères, selon la sécurité nationale,» Le Monde, 06 03 2024. [En ligne].
Available: https://www.lemonde.fr/international/article/2024/03/06/europeennes-2024-en-france-le-scrutin-represente-une-cible-considerable-de-manipulations-etrangeres-selon-la-securite-nationale_6220471_3210.html.

(50) L. Monde, «Des acteurs proches de l'Azerbaïdjan derrière une campagne de boycott des JO de Paris,» Le Monde, 14 11 2023. [En ligne].
Available: https://www.lemonde.fr/international/article/2023/11/14/des-acteurs-proches-de-l-azerbaidjan-derriere-une-campagne-de-boycott-des-jo-de-paris_6200083_3210.html.

(51) F. 24, «How France became the target of Azerbaijan's smear campaign,» France 24, 20 02 2024. [En ligne].
Available: https://www.france24.com/en/europe/20240220-how-france-became-target-azerbaijan-smear-campaign.

À propos du cert By xmco

Le CERT-XMCO met à votre disposition son équipe d'experts, afin de vous aider à protéger votre entreprise, en maitrisant votre exposition et en facilitant le maintien de votre niveau de sécurité.

Le CERT-XMCO est le CSIRT de la société XMCO. Il est reconnu par le CERT gouvernemental français (le CERT-FR), ainsi que par la TF-CSIRT et le Trusted Introducer, ce qui lui permet d'obtenir les informations et de collaborer avec les autres CERT français et européens.

Le CERT-XMCO protège votre entreprise, en maitrisant votre exposition et en facilitant le maintien de votre niveau de sécurité (veille en vulnérabilités, Cyber Threat-Intelligence, Réponse à Incident, Accompagnement à la remédiation, etc.).

xmco

Cabinet de conseil indépendant en cybersécurité, XMCO a à coeur d'accompagner ses clients, de toute taille et de tous secteurs, dans l'anticipation des vulnérabilités, la détection des failles et la réponse à incidents. XMCO est qualifié PASSI sur l'ensemble des portées, ce qui confirme le coeur de métier historique : l'audit et les tests d'intrusion.

Date de création :	2002
Effectif salariés :	+100
Qualifications :	PASSI, QSA et CERT officiel
Clients actifs :	+450
dont clients CERT :	+100
Secteurs :	Banque, Assurances, Industrie, Institutions, Transports, Médias, Luxe, etc.

Retrouvez-nous

Sur notre site :

www.xmco.fr

Sur les réseaux sociaux :

Envie d'échanger ?

info@xmco.fr

01 79 35 29 30