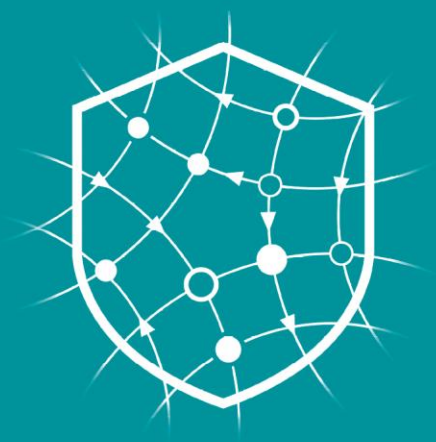
PREMIÈRE MINISTRE

*Liberté*
*Égalité*
*Fraternité*

Secrétariat général de la défense et de la sécurité nationale



VIGINUM

# ***RRN*** **:** une campagne numérique de manipulation de l'information complexe et persistante

Rapport technique

19 juin 2023

# MARS 2022 : *RRN*, ACTEUR CENTRAL DE LA CAMPAGNE

La campagne informationnelle détectée s'articule autour du média *RRN*, créé quelques jours après le déclenchement de l'invasion de l'Ukraine par la Russie.

## *RRN*, un média en ligne en lien avec des sites *web* russes

### Création du site *web RRN*

Le 10 mars 2022, le nom de domaine *rrussianews[.].com*[1] (« *Reliable Russian News* ») a été enregistré en Russie. Le site *web RRN* se présente comme un média indépendant diffusant des « informations vérifiées » portant principalement sur la guerre en Ukraine.

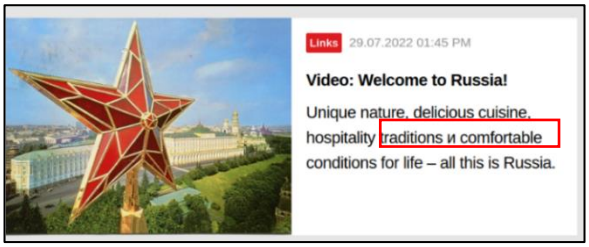
Disponible en plusieurs langues (français, anglais, allemand, italien, chinois, espagnol, arabe), très probablement grâce à l'utilisation d'un logiciel de traduction automatique, le site *web RRN* développe une ligne éditoriale axée autour de quatre thématiques principales : (1) l'inefficacité supposée des sanctions visant la Russie, qui pèseraient avant tout sur les États européens et/ou sur leurs citoyens ; (2) la prétendue russophobie des États occidentaux ; (3) la barbarie dont feraient preuve les forces armées ukrainiennes, ainsi que l'idéologie néo-nazie qui prédominerait chez les dirigeants ukrainiens ; (4) les effets négatifs qu'entrainerait l'accueil de réfugiés ukrainiens pour les États européens.


*Article publié par* RRN
(*source* : rrn[.]world)

Dès le 15 mars 2022, des *URLs* vers le site *web RRN* ont été publiées par sept pages *Facebook* officielles du réseau diplomatique russe, notamment celles des ambassades de Russie au Bangladesh, en Malaisie et en Slovaquie (cf. annexe 1)[2].

Trois mois après sa création, les administrateurs du site *web RRN* ont cherché à dissimuler ses liens avec la Russie en modifiant l'identité du média, qui est alors devenu « *Reliable Recent News* ». Le 6 juin 2022, le nom de domaine *rrn[.]world* a été enregistré, et une redirection a été paramétrée depuis *rrussianews[.].com* vers le nouveau nom de domaine. Des caractères cyrilliques continuaient cependant d'apparaître dans certains articles publiés sur le nouveau nom de domaine.


*Redirection effectuée par* rrussianews[.]com *vers* rrn[.]world
(*source :* urlscan.io)




*Caractères cyrilliques présents dans un article du média* RRN *(source :* rrn[.]world)

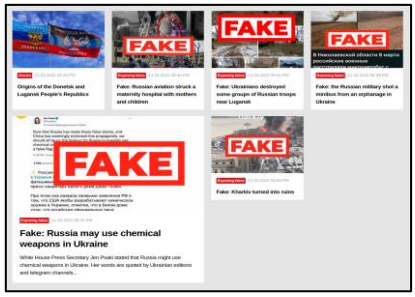
### Liens entre *RRN* et la plateforme pro-russe de *fact-checking* « *War on Fakes* »

Les premiers articles diffusés sur *RRN* étaient des reproductions à l'identique d'articles préalablement publiés sur la fausse plateforme de *fact-checking* « *War on Fakes* », lancée quelques heures après le déclenchement de l'invasion de l'Ukraine[3].

Rapidement repérée pour son rôle de légitimation de « l'opération militaire spéciale » et de décrédibilisation de l'État ukrainien, *War on Fakes* a fait l'objet d'une stratégie d'amplification coordonnée impliquant 65 pages *Facebook* et 24 comptes *Twitter* officiels du réseau diplomatique russe (cf. annexe 2). En outre, la page de connexion administrateur du site *waronfakes[.]com* redirigeait automatiquement vers celle de *rrussianews[.]com*, établissant ainsi un lien technique entre les deux sites *web*.

[1] Au regard de la nature malveillante des acteurs responsables de la campagne *RRN*, les noms de domaines et URLs présents dans ce rapport ont été démilitarisés. VIGINUM recommande d'adopter toutes les précautions d'usage en cas d'accès à ces ressources.
[2] Source : *Crowdtangle*.
[3] *War on Fakes* est une fausse plateforme multilingue de *fact-checking* utilisée par la Russie pour nier les accusations de crimes de guerre qui la visent depuis le début de l'invasion de l'Ukraine.

Le nom de domaine *waronfakes[.]com* a été enregistré le 1er mars 2022 et mis à jour un an plus tard par Timofey VASILIEV[4], citoyen russe connu pour avoir travaillé pour la société *ANO Dialog*[5], organisation créée en 2019 sous l'égide de l'Administration présidentielle russe et du département des Technologies de l'Information de la ville de Moscou. Chargée d'une partie de la stratégie de relations publiques et de la communication de la ville de Moscou, *ANO Dialog* a été accusée de mener des activités de propagande en ligne pour le compte de l'État russe[6].




*Articles de* War on Fakes *disponibles sur* RRN *(source :* rrn[.]world*)*

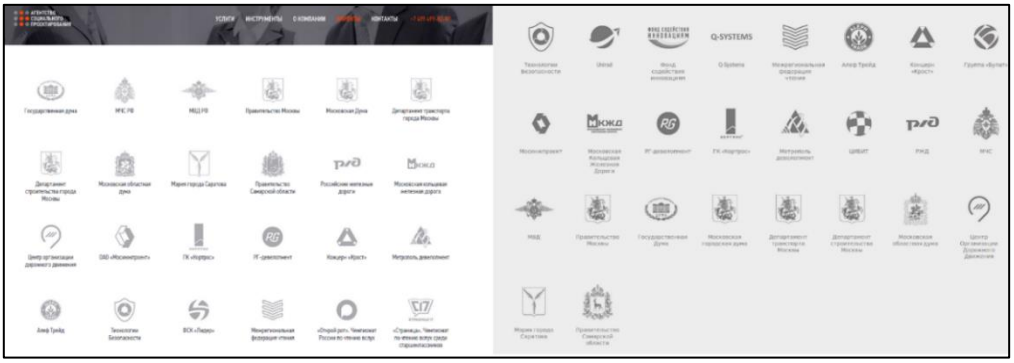

*Lien technique entre* rrussianews[.]com *et* waronfakes[.]com *(source :* twitter.com/olli_kahn*)*

## Attribution de la campagne par le groupe *Meta* à deux sociétés russes

Le 15 décembre 2022, la campagne *RRN* a publiquement été attribuée par le groupe *Meta* à deux sociétés russes[7] : *Structura National Technologies* (*Struktura*)[8] et *Social Design Agency* (*Agentstvo Sotsialnogo Proektirovania*, *ASP*)[9].

Créée en 2009, *Struktura* est une entreprise spécialisée dans le développement d'outils informatiques. Composée de plus de 500 « experts et spécialistes » et disposant de cinq succursales (Moscou, Saint-Pétersbourg, Smolensk, Nijni Novgorod et Krasnoïarsk), *Struktura* compte parmi ses clients plusieurs institutions étatiques russes à l'image du Ministère russe de l'Intérieur (MVD), du gouvernement de Moscou ou la Douma fédérale (chambre basse de l'Assemblée fédérale de Russie)[10]. Sur son site *web*, désormais hors ligne, *Struktura* proposait une quarantaine de produits informatiques, parmi lesquels 13 étaient explicitement labellisés comme étant développés au profit de l'État russe. L'entreprise a notamment conçu une solution de « *monitoring* et d'analyse de l'espace informationnel », une solution de « sécurité informationnelle » ou un produit dénommé « Portail Sécurité informationnelle pour le DIT », acronyme du département des Technologies de l'Information de la ville de Moscou, sous l'égide de laquelle *ANO Dialog* a été créée.

Fondée en 2017, *ASP* est une entreprise de marketing digital localisée à Moscou, notamment active dans le domaine de la « production et le montage de films cinématographiques et vidéos », la traduction ou bien la création de sites *web*. Sur une liste de 24 clients déclarés sur le site *web* d'*ASP*, 21 sont également clients de *Struktura*, dont des institutions gouvernementales russes.



*Liste des partenaires d'*ASP *et* Struktura *(source :* sp-agency[.]ru *et* structura[.]pro*)*

[4] Тимофей Васильев. https://www.logically.ai/resources/russian-war-on-fakes-fact-checking-account
[5] « АНО ДИАЛОГ ». Identifiant fiscal : 9709056472.
[6] https://meduza.io/feature/2022/09/26/meduza-vyyasnila-kak-propagandisty-budut-ob-yasnyat-rossiyanam-chto-mobilizatsiya-eto-normalno
[7] https://about.fb.com/news/2022/11/metas-adversarial-threat-report-q3-2022
[8] ООО « ГК Структура ». Identifiant fiscal : 7703438908.
[9] ООО « Агентство социального проектирования ». Identifiant fiscal : 7728390408.
[10] https://archive.ph/OPupt

Outre leur clientèle, *Struktura* et *ASP* ont en commun un même dirigeant, Ilya Andreevitch GAMBACHIDZE[11], « technologue politique » (*polittekhnolog*) moscovite renommé, ancien adjoint du préfet du district administratif Nord de Moscou, Oleg MITVOL. Après avoir étudié la sociologie et les sciences politiques, avec une spécialisation sur les systèmes politiques et électoraux dans les collectivités locales[12], Ilya GAMBACHIDZE a été conseiller du vice-président de la Douma fédérale Piotr TOLSTOÏ, qu'il a notamment accompagné lors d'un sommet du Conseil de l'Europe en 2017[13].

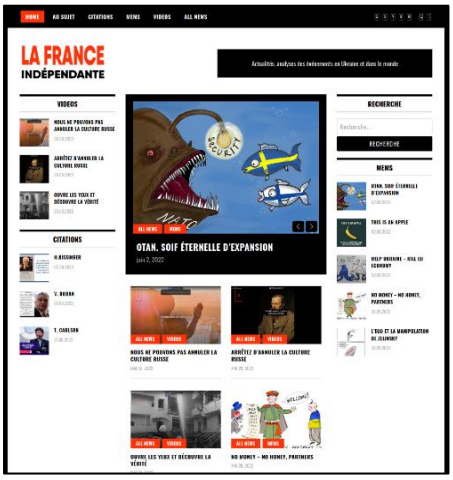
# JUIN – SEPTEMBRE 2022 : MULTIPLICATION DES MANŒUVRES

## *avisindependent[.]eu*, un faux média d'analyse sur la guerre en Ukraine

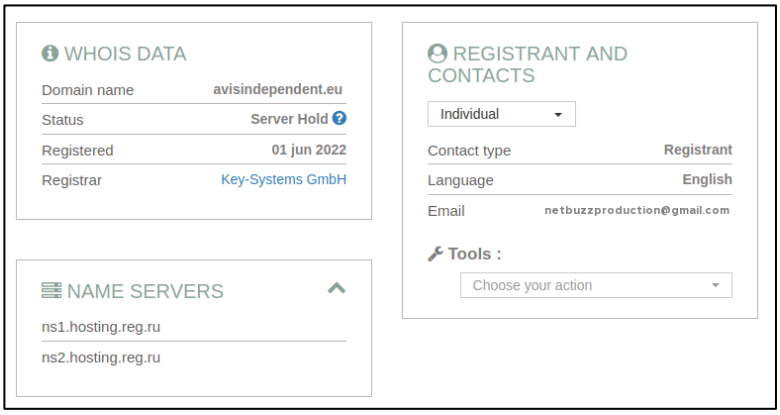
### *Création du site* web avisindependent[.]eu

Au mois de juin 2022, VIGINUM a identifié un site *web* affilié à la campagne *RRN*, intitulé « La France indépendante » et enregistré le 1er juin 2022 sous le nom de domaine *avisindependent[.]eu*.

Se présentant comme un média diffusant des « actualités et analyses sur la guerre en Ukraine », le site *web avisindependent[.]eu* diffusait du contenu reprenant des éléments de langage fréquemment mis en avant par la Russie tels que l'expansion de l'OTAN vers l'Est perçue comme menaçant les intérêts russes ou la supposée volonté des États occidentaux d'effacer la culture russe.




*Site web* avisindependent[.]eu *(source :* avisindependent[.]eu*)*




*Whois réalisé sur le domaine* avisindependent[.]eu *(source :* eurid.eu*)*

Le site *avisindependent[.]eu*, hébergé en Russie, a été enregistré par la société *NetBuzz*. L'adresse *mail netbuzzproduction@gmail[.]com* renvoie vers les comptes *VK* et *Instagram* d'un certain Mikhaïl Andreevitch TCHEKOMASOV[14], cofondateur de la société *Hustle Media*[15] (*ООО ХАСЛ МЕДИА*), spécialisée dans la gestion d'influenceurs sur les réseaux sociaux et les blogs.

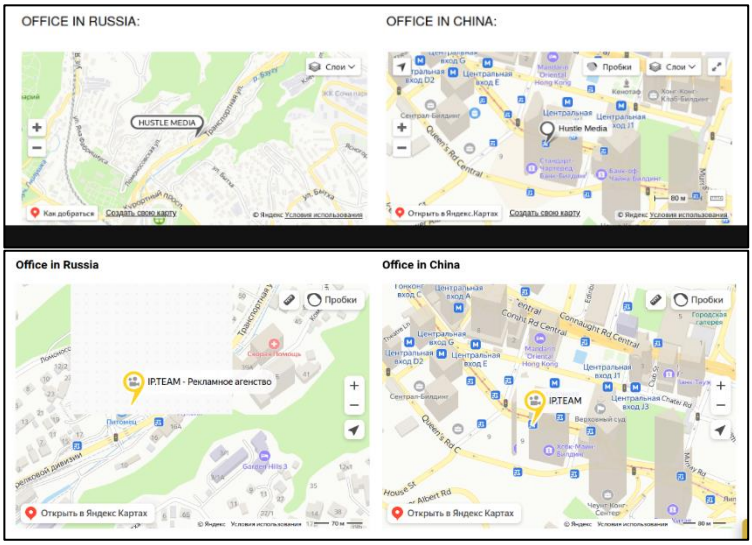
Le numéro de téléphone de contact de *Hustle Media* a été enregistré sous le nom de « Micha Netbus ». Micha est le diminutif de Mikhaïl, ce qui crédibilise l'hypothèse selon laquelle Mikhaïl Andreevitch TCHEKOMASOV aurait enregistré le nom de domaine de « La France Indépendante ». En outre, une photo d'un badge d'accès à un salon professionnel publiée sur le compte *VK* de Mikhaïl Andreevitch TCHEKOMASOV fournit un élément supplémentaire pouvant témoigner de ses liens avec *Netbuzz*[16].


*Badge au nom de Mikhaïl TCHEKOMASOV (source :* vk.com*)*

[11] Илья Андреевич ГАМБАШИДЗЕ. Identifiant fiscal : 771401746465.
[12] https://www.dissercat[.]com/content/osobennosti-razvitiya-mestnogo-samoupravleniya-v-rossiiskoi-federatsii-v-kontekste-transform et https://cyberleninka[.]ru/article/n/osobennosti-vyborov-v-predstavitelnye-organy-vlasti-mestnogo-samoupravleniya-v-2005-g-1
[13] https://assembly.coe.int/LifeRay/APCE/pdf/SCs/2017/AS-PER-2017-PV-01-EN.pdf
[14] https://vk.com/net_buzzz ; https://instagram.com/net_buzzz
[15] https://www.list-org.com/company/11783729/
[16] https://archive.is/e1uAH

En 2012, Mikhaïl TCHEKOMASOV a fondé la société *Palmira Trade*[17] (*ООО ПАЛЬМИРА ТРЕЙД*) conjointement avec Kirill Vitalievitch KALACHNIKOV, également à la tête de la société de gestion d'influenceurs *Lideri Mnenii* (*ООО ЛИДЕРЫ МНЕНИЙ*). Cette dernière, aussi connue sous le nom de *IPTeam* ou *Veul*[18], a déjà été identifiée par le magazine *Marianne*[19] pour avoir tenté d'approcher des influenceurs français afin qu'ils diffusent du contenu favorable à la Russie dans le contexte de la guerre en Ukraine. Mikhaïl TCHEKOMASOV est présenté sur le site *web* de la société comme un membre de l'équipe dirigeante de *IPTeam*, tout comme Anton K. ERLBAUM, cofondateur de *Hustle Media* et directeur adjoint de *IPTeam*.

En outre, les sociétés *Hustle Media* et *Lideri Mneniy/IPTeam/Veul* sont colocalisées dans les mêmes bâtiments en Russie et en Chine.

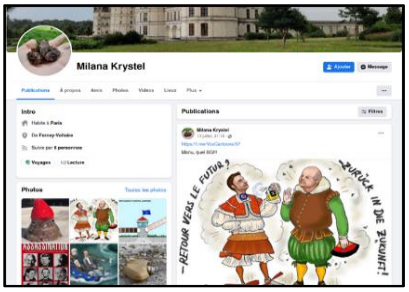



*Localisation des sociétés* Hustle Media *et* IPTeam *(sources :* hmd[.]one *et* ip[.]team*)*

## *Comptes inauthentiques diffusant des caricatures pro-russes et anti-occidentales*

Pour augmenter la visibilité du site *avisindependent[.]eu*, plusieurs comptes de réseaux sociaux ont été créés, principalement sur *Facebook* et sur *Twitter*. En plus de rediffuser des liens vers le site « La France Indépendante » et vers le site *web rrn[.]world*, ces comptes diffusaient des caricatures pro-russes, anti-occidentales et anti-ukrainiennes.

L'un des comptes centraux dans le dispositif était celui de Milana KRYSTEL, personnalité fictive présentée comme une ressortissante française opposée à la guerre en Ukraine. Créé le 21 juin 2022, cet avatar, mentionné par plusieurs comptes du dispositif, est à l'origine d'une pétition intitulée « Pas d'armes en Ukraine » publiée sur la plateforme *change.org*.



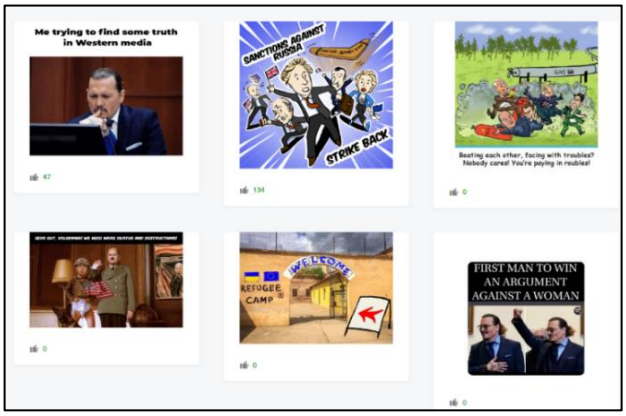

*Compte* Facebook *"Milana KRYSTEL" (source :* facebook.com*)*

Les caricatures diffusées par ces comptes de réseaux sociaux ainsi que par *avisindependent[.]eu* étaient issues principalement de deux sources : le site *memhouse[.]online* et la chaîne *Telegram @VoxCartoons*.

<u>Éléments recueillis sur le site *memhouse[.]online*</u>

Créé le 15 avril 2022, le site *web memhouse[.]online* se présente comme une banque d'images, partageant des caricatures portant essentiellement sur la guerre en Ukraine. Plusieurs caricatures publiées par les comptes affiliés à la campagne *RRN* semblent issues de ce site.

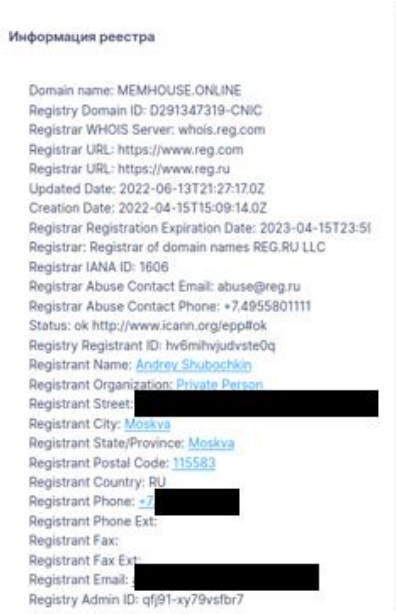

*Compte Instagram intégré au dispositif* RRN *(source :* instagram.com*)*




*Caricatures et mèmes présents sur le site* memhouse[.]online *(source :* memhouse[.]online*)*

[17] Identifiant fiscal : 7715916740.
[18] Identifiant fiscal : 7725337100.
[19] https://www.marianne.net/monde/europe/guerre-en-ukraine-une-operation-dinfluence-russe-vise-des-youtubeurs-français

Selon les données issues de reg.ru[20], le domaine *memhouse[.]online*, hors ligne aujourd'hui, a été déposé par un ressortissant russe habitant Moscou, Andreï CHOUBOTCHKINE.



Информация реестра

Domain name: MEMHOUSE.ONLINE
Registry Domain ID: D291347319-CNIC
Registrar WHOIS Server: whois.reg.com
Registrar URL: https://www.reg.com
Registrar URL: https://www.reg.ru
Updated Date: 2022-06-13T21:27:17.0Z
Creation Date: 2022-04-15T15:09:14.0Z
Registrar Registration Expiration Date: 2023-04-15T23:5
Registrar: Registrar of domain names REG.RU LLC
Registrar IANA ID: 1606
Registrar Abuse Contact Email: abuse@reg.ru
Registrar Abuse Contact Phone: +7.4955801111
Status: ok http://www.icann.org/epp#ok
Registry Registrant ID: hv6mihvjudvste0q
Registrant Name: Andrey Shubochkin
Registrant Organization: Private Person
Registrant Street: [redacted]
Registrant City: Moskva
Registrant State/Province: Moskva
Registrant Postal Code: 115583
Registrant Country: RU
Registrant Phone: [redacted]
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: [redacted]
Registry Admin ID: qfj91-xy79vsfbr7

*Whois réalisé sur le domaine* memhouse[.]online *(source :* reg.ru*)*

Éléments recueillis sur la chaîne *Telegram @VoxCartoons*

L'une des sources principales des caricatures diffusées lors de la campagne *RRN* est la chaîne *Telegram @VoxCartoons*. Créée le 2 avril 2022, cette chaîne publie des caricatures moquant certains dirigeants européens, accusés d'être instrumentalisés par les États-Unis dans leur gestion du conflit en Ukraine.

Les caricatures diffusées sur la chaîne *@VoxCartoons* ont également été relayées par le réseau diplomatique russe, notamment le compte *Twitter* de l'Ambassade de Russie en France, le 23 mars 2022. De façon remarquable, cette diffusion est intervenue plus d'une semaine avant la création de la chaîne *Telegram @VoxCartoons*.

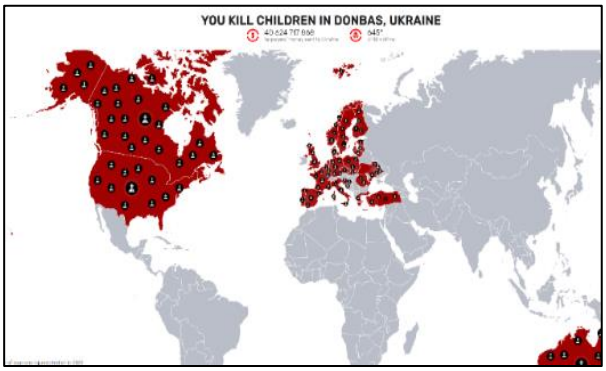

*Caricatures de* @VoxCartoons *diffusées par le compte* Twitter *de l'Ambassade de Russie en France (source :* twitter.com*)*

## Création de sites *web* accusant l'Ukraine et les États occidentaux de crimes de guerre

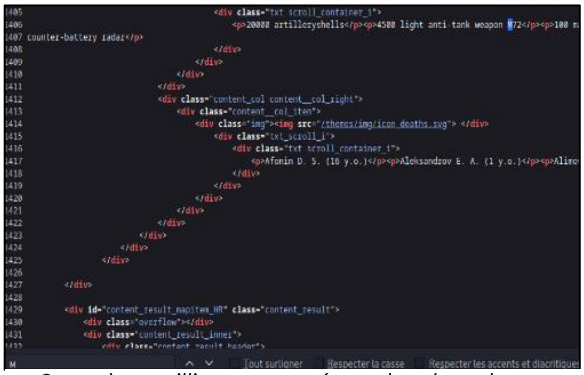
### *truemaps[.]info*, un site *web* recensant les enfants tués dans le Donbass

Le site *web rrn[.]world* et plusieurs comptes de réseaux sociaux affiliés à la campagne *RRN* ont publié des liens vers le site *web truemaps[.]info*. Créé le 30 juin 2022, ce site affiche une carte interactive représentant les différents pays fournisseurs d'armes à l'Ukraine, dont la France, ainsi qu'une liste d'enfants qui auraient été tués dans le Donbass du fait de la livraison de ces armes.

[20] Reg.ru est une société russe d'enregistrement de noms de domaine, notamment chargée de l'enregistrement des domaines en .ru et .рф.




*Site web* truemaps[.]info *(source :* truemaps[.]info*)*



*Caractère cyrillique « M » présent dans le code source (source :* truemaps[.]info*)*

L'étude du code source du site *truemaps[.]info* a fait apparaître des caractères en cyrillique, laissant supposer l'implication d'acteurs russophones dans sa conception.

### tribunalukraine[.]info, un site *web* sur « les crimes de guerre des forces armées ukrainiennes »

Enregistré le 5 octobre 2022, *tribunalukraine[.]info* se présente comme un site *web* visant à rétablir « la vérité que les médias nous cachent ». Il publie des articles et des vidéos en cinq langues[21] sur de supposés « crimes de guerre » commis par les « nazis au pouvoir » en Ukraine. Selon les comptes partageant les *URLs* vers *tribunalukraine[.]info*, le site serait administré par des allemands.

## Comptes *Facebook* « Opinion Ouverte » : premiers cas de *typosquatting*

### Comptes « à usage unique »

Dans le courant du mois de mai 2022, la campagne *RRN* a été à l'origine de la création d'un groupe de comptes *Facebook* ciblant des audiences française, allemande, italienne, lituanienne, britannique et ukrainienne.

Intitulés pour la plupart « Opinion Ouverte »[22], ces comptes utilisaient en photo de profil le logo d'un média allemand ou des images générées par une intelligence artificielle, et étaient utilisés comme des « comptes à usage unique » destinés à ne diffuser qu'une seule publication.

En plus de diffuser des caricatures issues de @*VoxCartoons*, les comptes « Opinion Ouverte » partageaient, *via* la sponsorisation de contenus, des liens vers des articles publiés sur le média *RRN*, vers la pétition créée par l'avatar Milana KRYSTEL ainsi que vers des noms de domaine typosquattés[23] de médias nationaux européens, dont le média français *20 Minutes*.

Contenant de très nombreuses fautes d'orthographe et des approximations syntaxiques, ainsi qu'un vocabulaire outrancier, les sites typosquattés observés par VIGINUM ont été utilisés pour diffuser des contenus manifestement inexacts ou trompeurs, favorables aux intérêts de la Russie. Certains de ces articles étaient directement issus du média *RRN*.


*Publication d'un compte "Opinion ouverte" (source :* facebook.com*)*

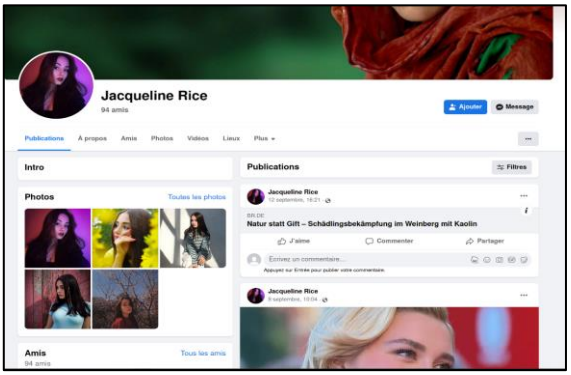
[21] Allemand, anglais, espagnol, français et russe.
[22] https://medium.com/dfrlab/russia-based-facebook-operation-targeted-europe-with-anti-ukraine-messaging-389e32324d4b ; https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf
[23] Le *typosquatting* est un mode opératoire qui consiste à enregistrer des noms de domaine avec des noms délibérément mal orthographiés de sites *web* connus pour tromper des internautes peu avertis.


*Article publié sur la version typosquattée du média* 20 Minutes *(source :* 20minuts[.]com*)*


*Article publié sur le site* web *de* RRN *(source :* rrn[.]world*)*

## Recours à un premier réseau de *bots*

La campagne *RRN* a également impliqué un recours à l'utilisation de *bots* sur *Facebook*, qui diffusaient des *URL*s d'articles typosquattés dans l'espace commentaire de pages *Facebook* de médias européens légitimes. La page *Facebook* du média turc germanophone *TRT Deutsch* a notamment été ciblée à l'aide de ce mode opératoire. Les comptes utilisés affichaient des noms à consonnance britannique et utilisaient des photos de profil pour la plupart empruntées sur des comptes *VK* de ressortissantes russes.




*Compte partageant des liens vers des sites typosquattés (source :* facebook.com*)*


*Partage d'un lien vers un site typosquatté (source :* facebook.com*)*

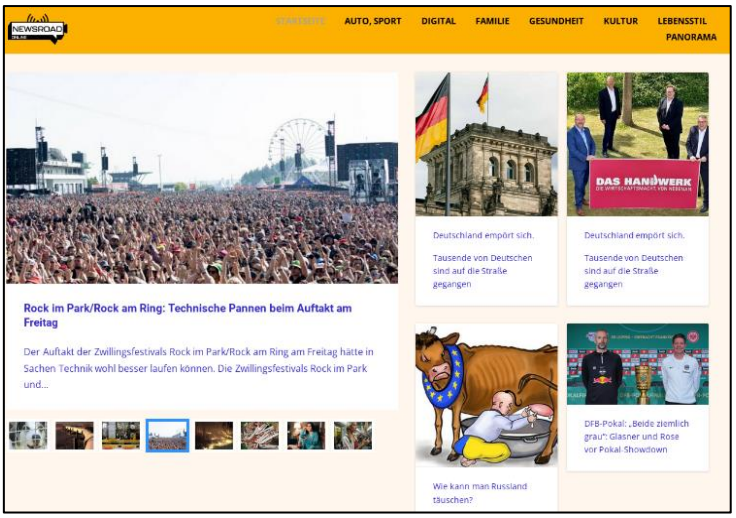
L'utilisation de *bots* a entraîné certaines erreurs de sécurité opérationnelle. Ainsi, certains *bots* ont publié des liens composés de deux parties distinctes : en vert, une *URL* vers un faux article du *Bild* ; en rouge, une *URL* vers un *cloud Yandex* utilisant le logiciel de bureautique R7-Office[24] dans lequel est mentionné « veul_sas », qui pourrait faire référence à la société *Lidery Mnenii/IPTeam/Veul* dont Mikhaïl TCHEKOMASOV est l'un des membres de l'équipe dirigeante.

https://www.bild[.]work/video/clip/video/Langer-Winter-steht-bevor-62571136,auto=true.bild.php###wt_ref=https%3A%2F%2Frt3xiiintgl7veul_sas_808_469799614905c7e39715fba79cd809f0.onlyoffice.disk.yandex.net%2F&wt_t=1663171191456

[24] Filiale russe de la compagnie lettone *OnlyOffice*.

## « *newsroad[.]online* », une infrastructure parallèle à *RRN*

Créé le 6 avril 2022, en parallèle du site *web rrn[.]world*, le site *web newsroad[.]online* publie des articles en allemand, français, italien, anglais et espagnol. *Newsroad* publiait des liens vers des articles de médias typosquattés et partageait des caricatures de @*VoxCartoons*.




*Site* web Newsroad *(source :* newsroad[.]online*)*

https://newsroad.online/lebensstil/
https://newsroad.online/page/2/
https://newsroad.online/page/3/
https://newsroad.online/page/591/
https://urlbox.online/FV1kYD?utm_campaign=eng1270
https://urlbox.online/FV1kYD?utm_campaign=eng1279
https://urlbox.online/FV1kYD?utm_campaign=eng1296
https://urlbox.online/FV1kYD?utm_campaign=eng1361
https://urlbox.online/FV1kYD?utm_campaign=eng1369
https://urlbox.online/FV1kYD?utm_campaign=eng1377
https://urlbox.online/FV1kYD?utm_campaign=eng1385
https://urlbox.online/FV1kYD?utm_campaign=eng1397

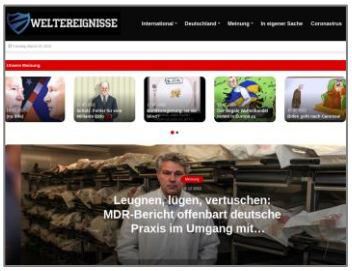
*Liens extraits de la première page du site* newsroad[.]online

Pour accéder aux faux articles des noms de domaine typosquattés, les administrateurs de *Newsroad* ont utilisé *urlbox[.]online*, un raccourcisseur d'*URL* permettant de masquer l'*URL* de destination. L'énumération des *URLs urlbox[.]online* utilisant l'identifiant disponible sur le site *newsroad[.]online* a permis de mettre en évidence des redirections vers des sites typosquattés ainsi que vers *rrn[.]world*.

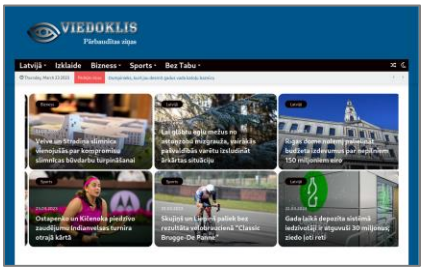
| | |
|---|---|
| https://urlbox.online/FV1kYD?utm_campaign=eng1298 | https://video.bild.vip/article/0208OKGCB.bild.html |
| https://urlbox.online/FV1kYD?utm_campaign=eng1302 | https://bild-de.bild.pics/wozu-brauchen-die-deutschen-die-ukraine.bild.html |
| https://urlbox.online/FV1kYD?utm_campaign=eng1303 | https://news.spiegeli.today/article/gaspreisexplosion-wer-bezahlt-den-beschluss-der-bundesregierung.html |
| https://urlbox.online/FV1kYD?utm_campaign=eng1304 | https://news.bild.pics/article/der-krieg-um-das-einmaleins-kann-nicht-gewonnen-werden.auto-true.bild.html |
| https://urlbox.online/FV1kYD?utm_campaign=eng1305 | https://news.bild.pics/article/deutschland-kann-der-irrsinnigen-politik-einer-militaristischen-regierung-nicht-standhalten.auto-true.bild.html |
| https://urlbox.online/FV1kYD?utm_campaign=eng1306 | https://www.faz.ltd/aktuell/politik/ausland/Die-Ukraine-ist-der-Kriegsverbrechen-Schuldig-50335838.html |
| https://urlbox.online/FV1kYD?utm_campaign=eng1307 | https://rrn.world/de/aktuelle-nachrichten/oktoberfest-findet-statt/ |
| https://urlbox.online/FV1kYD?utm_campaign=eng1308 | https://www.bild.eu.com/politik/ausland/politik-ausland/Berlin-im-Schatten-26834224.bild.html |
| https://urlbox.online/FV1kYD?utm_campaign=eng1309 | https://www.faz.ltd/aktuell/politik/ausland/Weniger-Brot-Butter-und-Bier-26077247.html |

*Extrait des URLs déraccourcis utilisant* urlbox[.]online

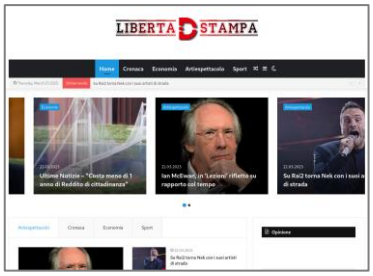
Plusieurs *URLs* cachées derrière *urlbox[.]online* redirigeaient également vers des sites d'actualité allemand, italien, letton et français spécifiquement créés dans le cadre de la campagne[25]. Ces sites diffusaient des articles du média *RRN*, rédigés pour certains par des avatars créés par le dispositif. Ces sites disposaient par ailleurs de chaînes *YouTube* dédiées, sur lesquelles ils diffusaient des vidéos polémiques relatives à la gestion du conflit en Ukraine par les États européens.




*Site web* weltereignisse365[.]de




*Site web* viedo-klis[.]lv



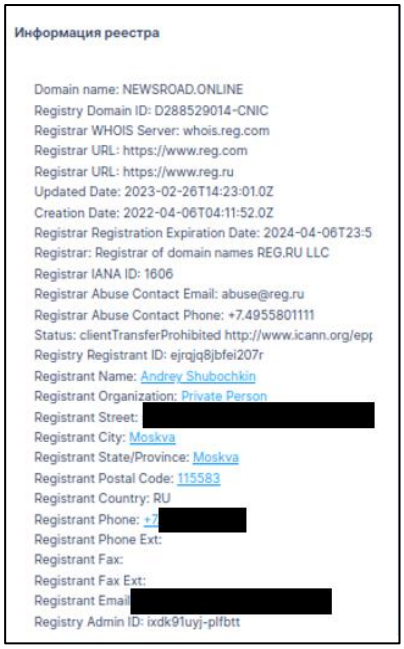

*Site web* libera-stampa[.]it

| | |
|---|---|
| https://urlbox.online/FV1kYD?utm_campaign=eng1055 | https://viedo-klis.lv/tas-ir-vajadzigs-eiropas-komisijai-gada-beigas-latvija-paterina-cenas-bus-visaugstakas-eiropas-savieniba/ |
| https://urlbox.online/FV1kYD?utm_campaign=eng1056 | https://www.librelepresse.fr/si-necessaire-la-commission-europeenne-les-prix-a-la-consommation-en-lettonie-sera-le-plus-eleve-dans-lunion-europeenne-dici-la-fin-de-lannee/ |
| https://urlbox.online/FV1kYD?utm_campaign=eng1057 | https://weltereignisse365.de/so-will-es-die-europaische-kommission-die-verbraucherpreise-in-lettland-werden-bis-ende-des-jahres-die-hochsten-in-der-eu-sein/ |
| https://urlbox.online/FV1kYD?utm_campaign=eng1058 | https://libera-stampa.it/secondo-la-commissione-europea-si-fa-cosi-in-lettonia-i-prezzi-al-consumo-saranno-i-piu-alti-di-tutta-lunione-europea-verso-fine-anno/ |

*Le même article était publié sur les quatre sites en version traduite*

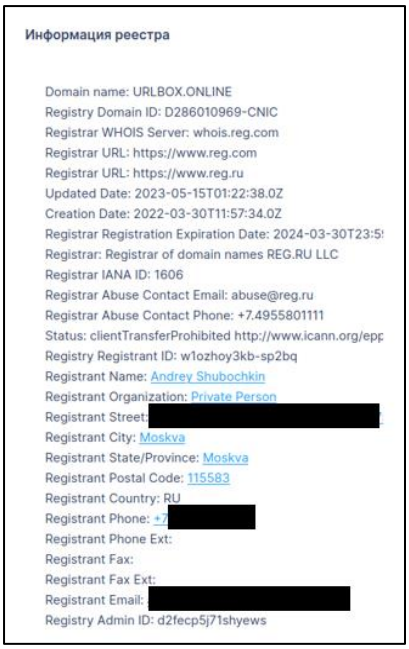
[25] *Viedo-klis[.]lv, librelepresse[.]fr, weltereignisse365[.]de, libera-stampa[.]it*

Les investigations menées par VIGINUM sur *newsroad[.]online* et *urlbox[.]online* ont permis d'identifier à nouveau Andreï CHOUBOTCHKINE, comme la personne ayant déposé (*registrant*) ces deux domaines.


Информация реестра

Domain name: NEWSROAD.ONLINE
Registry Domain ID: D288529014-CNIC
Registrar WHOIS Server: whois.reg.com
Registrar URL: https://www.reg.com
Registrar URL: https://www.reg.ru
Updated Date: 2023-02-26T14:23:01.0Z
Creation Date: 2022-04-06T04:11:52.0Z
Registrar Registration Expiration Date: 2024-04-06T23:5
Registrar: Registrar of domain names REG.RU LLC
Registrar IANA ID: 1606
Registrar Abuse Contact Email: abuse@reg.ru
Registrar Abuse Contact Phone: +7.4955801111
Status: clientTransferProhibited http://www.icann.org/epp
Registry Registrant ID: ejrqjq8jbfei207r
Registrant Name: Andrey Shubochkin
Registrant Organization: Private Person
Registrant Street: [redacted]
Registrant City: Moskva
Registrant State/Province: Moskva
Registrant Postal Code: 115583
Registrant Country: RU
Registrant Phone: +7[redacted]
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email[redacted]
Registry Admin ID: ixdk91uyj-plfbtt

*Whois réalisé sur le domaine* newsroad[.]online *(source :* reg.ru*)*


Информация реестра

Domain name: URLBOX.ONLINE
Registry Domain ID: D286010969-CNIC
Registrar WHOIS Server: whois.reg.com
Registrar URL: https://www.reg.com
Registrar URL: https://www.reg.ru
Updated Date: 2023-05-15T01:22:38.0Z
Creation Date: 2022-03-30T11:57:34.0Z
Registrar Registration Expiration Date: 2024-03-30T23:5
Registrar: Registrar of domain names REG.RU LLC
Registrar IANA ID: 1606
Registrar Abuse Contact Email: abuse@reg.ru
Registrar Abuse Contact Phone: +7.4955801111
Status: clientTransferProhibited http://www.icann.org/epp
Registry Registrant ID: w1ozhoy3kb-sp2bq
Registrant Name: Andrey Shubochkin
Registrant Organization: Private Person
Registrant Street: [redacted]
Registrant City: Moskva
Registrant State/Province: Moskva
Registrant Postal Code: 115583
Registrant Country: RU
Registrant Phone: +7[redacted]
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: [redacted]
Registry Admin ID: d2fecp5j71shyews

*Whois réalisé sur le domaine* urlbox[.]online *(source :* reg.ru*)*

# FÉVRIER – JUIN 2023 : NOUVELLE PHASE DE LA CAMPAGNE

## Recours accru aux réseaux sociaux et à la sponsorisation de contenus

### Sponsorisation de contenus dans le cadre de la campagne *RRN*

Afin d'accroitre sa visibilité et contourner les mesures de modération mises en place par le groupe *Meta*, la campagne *RRN* a recouru à la sponsorisation de ses contenus sur *Facebook*. Depuis le mois de février 2023, plus de 160 pages *Facebook* ont ainsi été identifiées par VIGINUM, et ont diffusé plus de 600 contenus sponsorisés comportant des liens vers des articles et des sites *web* liés à la campagne[26].

Ces publicités ne sont visibles que par une audience très ciblée, choisie par l'administrateur de la page. Les *URLs* publiées, en apparence anodines, effectuent une redirection vers des sites *web* affiliés à *RRN* en utilisant la technique du *geofencing*[27]. Ainsi, les *URLs* présentes dans les publications sponsorisées renvoient à un contenu différent selon la localisation : pour un public français, la redirection est effectuée sur le site typosquatté. Dans le cas contraire, une page vide est affichée.

Ce mode opératoire permet de segmenter l'audience visée et d'atténuer la capacité d'éventuels tiers à cartographier l'infrastructure mise en place dans le cadre de la campagne. De plus, avant d'atteindre le site cible, au moins deux redirections sont effectuées depuis l'*URL* disponible sur la publication sponsorisée, grâce à l'utilisation de noms de domaine pivots hébergés sur des serveurs intermédiaires, là encore afin de masquer l'infrastructure du dispositif et d'en protéger la pérennité. VIGINUM a identifié un serveur ayant communiqué avec plusieurs noms de domaine utilisés dans les redirections[28].


*Publication sponsorisée (source :* facebook.com*)*

[26] *rrn[.]world* ; sites typosquattés ; *ukraine-inc[.]info* ; *tribunalukraine[.]info* ; faux sites web d'actualité francophones
[27] Le *geofencing* est une pratique de ciblage publicitaire qui consiste à définir des périmètres géographiques pour cibler les individus présents ou entrants dans une zone géographique donnée.
[28] IP du serveur 35[.]187.82.108. Noms de domaine : *marvelgoodies[.]com*, *bighorn-advisors[.]com*, *gitver[.]com*, *raremotion[.]com*.


*Redirections effectuées depuis une publication sponsorisée sur* Facebook

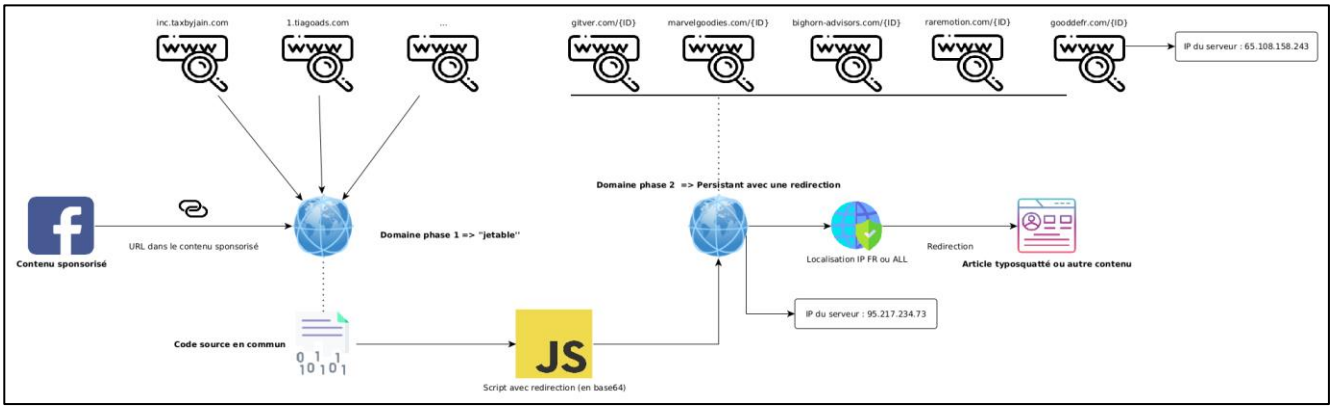



*Schéma explicatif de la réalisation de la redirection depuis* Facebook

## Recours à un second réseau de *bots*

Depuis la fin de mois de mai 2023, VIGINUM a détecté l'activité d'un réseau de *bots Twitter* qui repartagent, dans l'espace réponse de *tweets* publiés par des médias européens et de personnalités politiques, des liens vers des sites *web* intégrés à la campagne *RRN*. Tout comme sur *Facebook*, les *URLs* partagées effectuent plusieurs redirections avant d'atteindre le site cible.

Des caractères cyrilliques ont été identifiés dans les redirections, suggérant ainsi l'implication d'individus russes ou russophones dans la réalisation de cette manœuvre. En particulier, une *URL* présente dans un des *tweets* a permis de faire ressortir des caractères cyrilliques dans le code source de la page *web* associée[29]. En effet, lors de l'affichage du code, VIGINUM a identifié un script en base64[30].

```
iAgICA="></script></div><script async="" class="embed-code-script_1QA" src="data:text/javascript;b
ase64,Ly8g0JfQtNC10YHRjCDQstGLINC80L7QttC10YLQtSDQtNC+0LHQsNCy0LjRgtGMINGB0LLQvtC5INGB0L7QsdGB0YLQ
stC10L3QvdGL0LkganMt0LrQvtC0
```

*Extrait du code source de la page associée (source :* http://dsqno[.]bhylobi[.]website/0468d)

Après avoir décodé la phrase en base64, VIGINUM a identifié la chaine de caractères en cyrillique, sur laquelle il est écrit : « // Ici, vous pouvez ajouter votre propre code js ».

```
// Здесь вы можете добавить свой собственный js-код
```

*base64 décodée (source :* http://dsqno[.]bhylobi[.]website/0468d)

[29] *http://dsqno[.]bhylobi[.]website/0468d*
[30] En informatique, base64 est une technique d'encodage de données utilisant 64 caractères.

## Poursuite du *typosquatting* de médias

Depuis le mois de février 2023, VIGINUM a observé une recrudescence de l'usurpation de l'identité de grands médias français et étrangers[31] afin de publier des articles favorables à la Russie dans le cadre du conflit en Ukraine (cf. annexe 3).

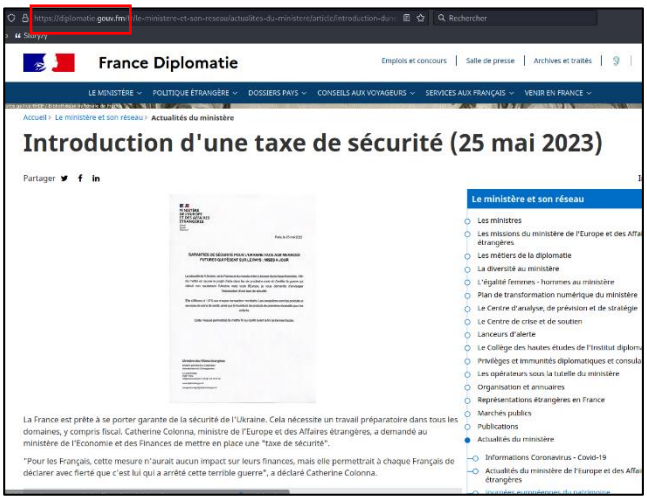
L'apparence des sites typosquattés est en tout point similaire à celle des médias qu'ils usurpent, la seule différence résidant dans l'*URL* visitée. Les noms de domaine de médias typosquattés utilisent le même code source que celui des médias légitimes : la plupart des liens présents sur le site *web* légitime sont chargés sur le site typosquatté, ce qui permet de le crédibiliser auprès d'un internaute non-averti.


*Article diffusé sur la version typosquattée du* Parisien *(source :* leparisien[.]ltd*)*

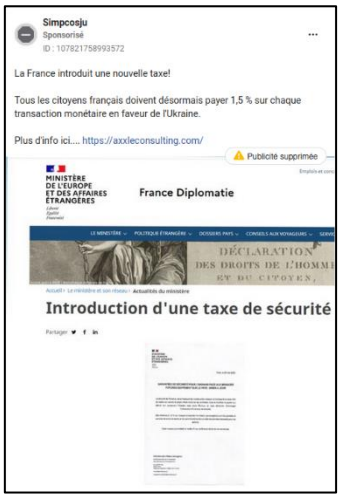
À l'heure actuelle, VIGINUM a identifié quatre médias français dont les identités ont été usurpées : *Le Parisien*, *Le Monde*, *Le Figaro* et *20 Minutes*[32]. Non-indexés sur les moteurs de recherche, les articles hébergés sur ces sites typosquattés ne sont accessibles que depuis les *URLs* présentes dans les contenus sponsorisés publiés sur *Facebook* et *Twitter*. Les investigations conduites par VIGINUM ont permis de mettre en évidence l'existence d'au moins 49 faux articles du *Parisien*, sept de *20 Minutes*, un du *Monde* et un du *Figaro*, dernier média dont l'identité a été usurpée à partir du 8 juin 2023.

## Usurpation de l'identité de sites gouvernementaux

Depuis le 29 mai 2023, la campagne *RRN* a eu recours au *typosquatting* de sites *web* gouvernementaux français et allemands pour diffuser des contenus manifestement inexacts ou trompeurs. L'identité du site *web* du ministère de l'Europe et des Affaires étrangères français a ainsi été usurpée et utilisée pour diffuser un faux communiqué selon lequel une nouvelle taxe de sécurité aurait été introduite sur une grande partie des transactions financières françaises pour financer le soutien à l'Ukraine.




*Site typosquatté du MEAE (source :* diplomatie[.]gouv[.]fm*)*




*Publication sponsorisée redirigeant vers le faux site du MEAE (source :* facebook.com*)*

La même manœuvre a été observée sur le site *web* du ministère de l'intérieur allemand, avec la publication d'un communiqué portant sur l'obligation d'accueillir des réfugiés ukrainiens au sein des foyers allemands.

[31] Allemagne, Émirats Arabes Unis, États-Unis, Israël, Lettonie, Lituanie, Royaume-Uni, Ukraine.
[32] *leparisien[.]ltd*, *lemonde[.]ltd*, *lefigaro[.]me*, *20minuts[.]com*

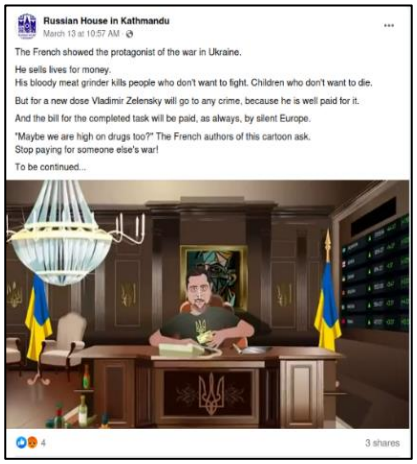
## Création du site *web* ukraine-inc[.]info hébergeant un dessin animé anti-ZELENSKY


*Site web ukraine-inc[.]info*

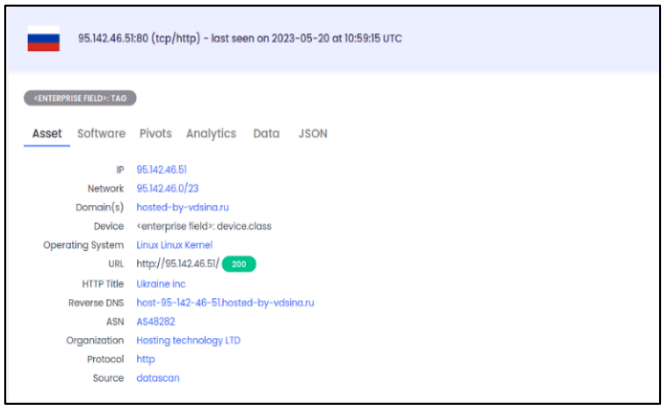
Créé le 11 mars 2023, le site *web ukraine-inc[.]info* diffuse une série de dessins animés intitulés « Ukraine Cocaïne » ciblant le président ukrainien Volodymyr ZELENSKY présenté comme un cocaïnomane manipulé par un réseau franc-maçon et réclamant perpétuellement de l'argent auprès des États occidentaux pour s'enrichir personnellement. D'après différents comptes et sites *web* ayant relayé ces vidéos, celles-ci auraient été réalisées par des Français[33]. Le serveur associé au nom de domaine *ukraine-inc[.]info* est hébergé en Russie.

Publié le 11 mars 2023 par la chaîne *Telegram* officielle de *RRN*, *@reliablerecentnews*, la viralité du dessin animé anti-ZELENSKY est devenue massive à partir du 12 mars 2023, avec la diffusion de la vidéo sur *Telegram* par *@readovkanews*, huitième chaîne la plus suivie en Russie avec 1,68 millions d'abonnés, dont la publication a été vue plus de 891 000 fois [34].

Par la suite, plus de 30 autres chaînes *Telegram* à forte audience ont à leur tour relayé la vidéo dans la matinée du 12 mars, notamment celles du média public *Ukraina.ru*[35], ou du média *NewsFront*[36] lié au *FSB*. Sur *Facebook*, elle a notamment été publiée par les pages officielles d'au moins neuf « Maisons russes » (Русский дом), institutions rattachées à l'agence *Rossotroudnitchestvo* du ministère russe des Affaires étrangères[37].



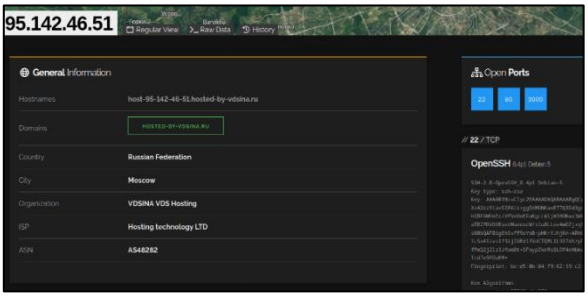

*Publication* Facebook *de la Maison russe à Katmandou (source :* facebook.com*)*



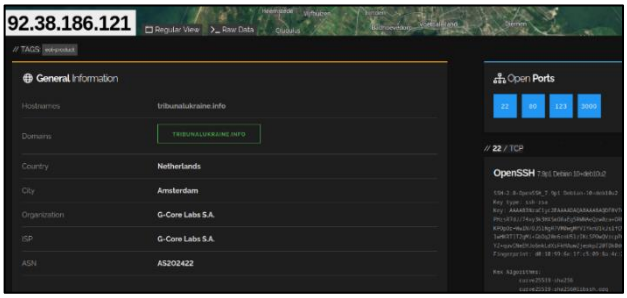

*Serveur hébergeant le site* ukraine-inc[.]info *(source :* onyphe.io*)*

En plus d'être la destination d'*URLs* publiées dans des contenus sponsorisés sur *Facebook*, le site *web ukraine-inc[.]info* présente des similarités techniques avec le site *web tribunalukraine[.]info*. Ainsi, les serveurs d'hébergement de ces deux sites ont été configurés d'une manière similaire, en laissant ouvert le port 3000 dédié au développement de sites *web* avant leur mise en ligne.

[33] Pour mémoire, au mois d'août 2022, un autre dessin animé, intitulé « *Stop Nazi Games* » avait été attribué, notamment par le réseau diplomatique russe, à un studio d'animation français dénommé « Barracudas ». Dans ce dessin animé, le président ukrainien, comparé à une marionnette dirigée par une société secrète, envoyait ses troupes attaquer le Donbass dont le sang des victimes était changé en or.
[34] https://t.me/readovkanews/54519/
[35] Ukraina.ru fait partie de la *holding média* publique russe *Rossiya Segodnya*, qui détient également l'agence *Sputnik News* et l'agence de presse *RIA Novosti*.
[36] t.me/ukraina_ru/137086, t.me/SolovievLive/163610, t.me/newsfrontnotes/34506. Parmi les autres chaînes, figurent notamment *@intelslava*, *@golosmordora*, *@svezhesti*, *@denazi_UA*, *@golosmordora*, *@neuesausrussland* et *@OstashkoNews*.
[37] Parmi les Maisons russes, on retrouve celle d'Ankara, d'Alexandrie, de Dar es Salaam, de Katmandou, du Caire, de Mumbai, d'Oulan Bator, de Rabat et de Tel Aviv.



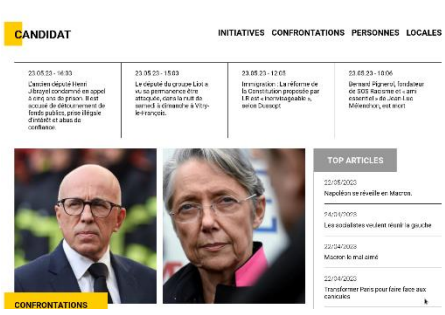

*Ports ouverts sur le serveur hébergeant* ukraine-inc[.]info *(source :* shodan.io*)*




*Ports ouverts sur le serveur hébergeant* tribunalukraine[.]info *(source :* shodan.io*)*

## Création de faux sites *web* d'actualité francophones

Le 24 février 2023, soit un an jour pour jour après l'invasion de l'Ukraine par la Russie, cinq sites *web* présentés comme des médias d'actualité francophones ont été enregistrés et hébergés sur le même serveur. Utilisant des noms à consonnance française (*La Virgule*, *Allons-y* ou *Notre Pays*), ces sites publient des articles d'actualité portant sur la politique intérieure française et européenne, dans lesquels ils critiquent le gouvernement français, notamment dans sa gestion de la réforme des retraites. Parallèlement, ils reprennent des éléments de langage récurrents de la Russie en critiquant les effets des sanctions prises par l'Union européenne à l'encontre de la Russie ou la supposée partialité des médias occidentaux, taxés de propager de fausses informations au détriment de Moscou.

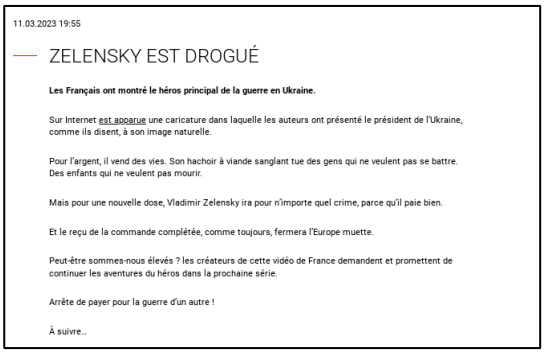





*Sites web portant sur l'actualité française gérés par le dispositif* RRN

Plusieurs éléments permettent de rattacher ces cinq sites à la campagne *RRN*. Le site *web lavirgule[.]news* a été le primo-diffuseur du premier épisode d'« Ukraine Cocaïne ». Dans un article intitulé « Zelensky est drogué », *La Virgule* affirmait pour la première fois que les auteurs du dessin animé étaient français. Le contenu de cet article a été repris à l'identique dans des publications sponsorisées sur *Facebook*. En outre, le site *web lavirgule[.]news* a été mentionné pour la première fois par *rrn[.]world*, avant même qu'il ne soit indexé par les moteurs de recherche. Par ailleurs, certains articles de *lavirgule[.]news* ont partagé des *URLs* vers le site *franceeteu[.]today*, créé le 24 février 2023 et hébergé sur le même serveur que *La Virgule*.

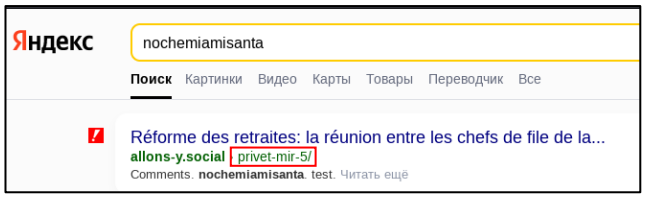

*Contenu sponsorisé redirigeant vers "Ukraine Inc" (source :* facebook.com)




*Article diffusé sur « La Virgule » (source :* lavirgule[.]news)

L'un des auteurs d'article de *La Virgule* utilise le pseudonyme « *nochemiamisanta* », également utilisé sur le site *web allons-y[.]social*. Dans l'*URL* de certains articles publiés par *Allons-y* est inscrit « privet-mir » pouvant être traduit depuis le russe par « Hello world ».


*Mention de "*nochemiamisanta*" (source :* lavirgule[.]news*)*

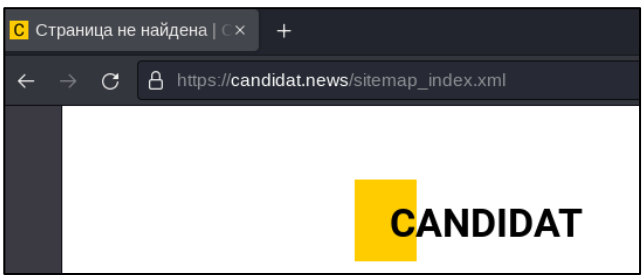



*Mention de "*nochemiamisanta*" sur* allons-y[.]social *(source :* dzen.ru*)*

Plusieurs articles publiés sur *Allons-y* révèlent également la présence de phrases en cyrillique probablement dues à une mauvaise traduction automatique du russe vers le français.


*Présence de caractère cyrilliques dans un article d'"Allons-y" (source :* allons-y[.]social*)*

L'étude des sites hébergés sur le même serveur que *lavirgule[.]news* a permis de détecter deux sites *web* similaires, ciblant également une audience francophone : *notrepays[.]today* et *candidat[.]news*. Enfin, le paramétrage des messages d'erreur sur les sites *allons-y[.]today* et *candidat[.]news* révèle une très probable conception par des individus russes ou russophones.




*Présence d'un message d'erreur en russe (source :* candidat[.]news*)*


*Présence d'un message d'erreur eu russe (source :* allons-y[.]social*)*

## ANNEXE 1 : PAGES FACEBOOK OFFICIELLES DU RÉSEAU DIPLOMATIQUE RUSSE AYANT PUBLIE UN LIEN VERS LE SITE DE *RRN*

| Source | Followers | Date (GMT) | Interactions | Link |
|---|---|---|---|---|
| Embassy of Russia in Bangladesh | 57773 | Jul 12 2022 05:51:09 | 206 | https://www.facebook.com/100064743754893/posts/413270720841050 |
| Veľvyslanectvo Ruska na Slovensku/ Посольство России в Словакии | 48924 | Jul 28 2022 11:37:47 | 117 | https://www.facebook.com/100068847295360/posts/357656319872608 |
| Посольство России в Швеции - Russian Embassy in Sweden | 3710 | Aug 02 2022 11:30:38 | 60 | https://www.facebook.com/100064560496880/posts/416439403851406 |
| Embassy of the Russian Federation in Malaysia | 6831 | Aug 03 2022 09:10:23 | 27 | https://www.facebook.com/100064825622970/posts/432115312292653 |
| Русский Дом в Улан-Баторе | 21752 | Mar 15 2022 17:55:48 | 8 | https://www.facebook.com/760538317364501/posts/4897032750381683 |
| Русский дом в Рабате / Maison russe à Rabat | 0 | Mar 15 2022 14:19:39 | 5 | https://www.facebook.com/100066478721190/posts/304743568418265 |
| Russian House in Kolkata Gorky Sadan | 0 | Mar 15 2022 14:14:50 | 0 | https://www.facebook.com/111041609025164/posts/4678646818931264 |

## ANNEXE 2 : PAGES *FACEBOOK* DU RÉSEAU DIPLOMATIQUE RUSSE AYANT PUBLIE UN LIEN VERS LE SITE DE *WAR ON FAKES*

- Ambasciata della Federazione Russa in Italia / Посольство России в Италии
- Russian Foreign Ministry - МИД России
- Russische Botschaft in Deutschland / Посольство России в Германии
- Russian Embassy in Indonesia
- Russian Embassy in Ethiopia - Посольство России в Эфиопии
- Russian Embassy in the Philippines
- Embajada de Rusia en Mexico
- Посольство России в Швеции - Russian Embassy in Sen
- Посольство России в Северной Македонии/Амбасада на Русија во Сев.Македонија
- Embassy of the Russian Federation in Malaysia
- The Embassy of the Russian Federation in Japan
- Embassy of Russia in the USA / Посольство России в США
- Russische Botschaft Wien / Посольство России в Австрии
- Посольство России в Египте / Russian Embassy in Egypt
- Посольство России в Монголии
- Ambassade de Russie en France / Посольство России во Франции
- Embassy of Russia in Australia
- Embajada de Rusia en el Perú
- Консульский департамент МИД России
- Ambasada Rusiei în România - Посольство России в Румынии
- Ambassade de Russie en Tunisie / Посольство России в Тунисе
- Casa de Rusia en Buenos Aires
- Russian Mission to UN in Geneva
- Ambassade de la Russie au Sénégal
- Russian Embassy in London
- Ambassade de Russie en Algerie / Посольство России в Алжире
- Russian Embassy in Norway
- Embassy of the Russian Federation in New Zealand
- Embajada de la Federación de Rusia en la República de Chile
- Посольство России в Коста-Рике/ Embajada de Rusia en Costa Rica
- Посольство России в Черногории / Ambasada Rusije u Crnoj Gori
- Посольство России в Сингапуре - Embassy of Russia in Singapore
- Посольство России в Кении / Embassy of Russia in Kenya
- Russian Embassy in Reykjavik
- Постоянное Представительство России при ОБСЕ / Russian Mission to the OSCE
- Consulate General of Russia in Cape Town
- Ambassade de Russie au Bénin et Togo / Посольство России в Бенине и Того
- Посольство России в Лаосе Russian Embassy in Laos
- Посольство России в Афганистане / Embassy of Russia in Afghanistan
- Посольство России в Республике Корея 주한 러시아대사관
- Генеральное консульство России в Монреале
- Embassy of Russia to Malta
- Consulado Geral da Federação da Rússia no Rio de Janeiro
- Russian House in Colombo
- Embassy of the Russian Federation in the Republic of Ghana
- Посольство России в Казахстане - Embassy of Russia in Kazakhstan
- Посольство России в Бельгии / Ambassade de Russie en Belgique
- Russian Consulate General in Edinburgh
- Russian Embassy in Jamaica
- Embassy of the Russian Federation in Sri Lanka and to the Maldives
- Russian House Chennai
- Генеральное консульство РФ в Осаке
- Russian Delegation on MIlitary Security and Arms Control
- Embassy of the Russian Federation in the Kingdom of Bahrain
- Russian Canada-Русская Канада
- Генеральное консульство России в Пусане
- Посольство России в Эквадоре
- Consular Section of the Embassy of the Russian Federation in Ireland
- Посольство России в Зимбабве / Russian Embassy in Zimbabwe
- Consulate General of Russia in Mumbai
- Представительство МИД России в Южно-Сахалинске
- Embassy of Russia in Botswana
- Russian Consulate General in Jeddah
- Генконсульство России в Харбине
- Генконсульство России в Нарве

## ANNEXE 3 : LISTE DES 353 NOMS DE DOMAINE INTÉGRÉS À LA CAMPAGNE *RRN* (SOURCES : *META*, *EU DISINFOLAB*, VIGINUM)

- rrussianews[.]com
- memhouse[.]online
- avisindependent[.]eu
- bIld[.]live
- bild[.]pics
- rrn[.]world
- welt[.]tours
- dailymail[.]top
- repubblica[.]life
- delfi[.]life
- dailymail[.]cam
- dailymail[.]cfd
- 20minuts[.]com
- ansa[.]ltd
- rbk[.]kiev.ua
- spiegel[.]ltd
- truemaps[.]info
- lsm[.]li
- theguardian[.]co[.]com
- schlauespiel[.]de
- tagesspiegel[.]ltd
- bild[.]asia
- bild[.]vip
- delfi[.]today
- delfi[.]top
- reuters[.]cfd
- rbk[.]today
- delfl[.]cc
- spiegelr[.]live
- spiegelr[.]today
- t-onlinl[.]life
- t-onlinl[.]live
- t-onlinl[.]today
- spiegel[.]today
- spiegel.fun
- spiegel.quest
- spiegel[.]fun
- tonline[.]cfd
- tonline[.]life
- tonline[.]today
- spiegel[.]ink
- spiegel[.]pro
- sueddeutsche[.]online
- t-online[.]life
- bild[.]eu.com
- bild[.]eu[.]com
- bild[.]llc
- spiegel[.]co[.]com
- zestiftung[.]com
- spiegeli[.]life
- spiegeli[.]live
- spiegeli[.]today
- welt[.]ltd
- faz[.]ltd
- t-onlinr[.]life
- t-onlinr[.]live
- t-onlinr[.]today
- spiegel[.]agency
- elfpress[.]info
- spiegelr[.]life
- sueddeutsche[.]life
- sueddeutsche[.]today
- sueddeutsche[.]me
- nd-aktuell[.]net
- bild[.]expert
- obozrevatels[.]com
- bild[.]ws
- faz[.]agency
- nd-aktuell[.]pro
- spiegel[.]work
- sueddeutsche[.]cc
- welt[.]ws
- nd-aktuell[.]co
- sueddeutsche[.]co
- tagesspiegel[.]co
- welt[.]media
- bild[.]work
- faz[.]life
- spiegel[.]cab
- fraiesvolk[.]com
- fraiepozition[.]live
- fraiepozition[.]online
- fraiepozition[.]site
- fraiepozition[.]store
- offinemainung[.]info
- offinemainung[.]live
- offinemaining[.]fun
- offinemaining[.]online
- offinemaining[.]pw
- offinemaining[.]site
- offinemaining[.]website
- werdunstorker[.]fun
- werdunstorker[.]online
- werdunstorker[.]pw
- offinemaiunng[.]online
- offinemaiunng[.]pw
- offinemaiunng[.]space
- offinemanung[.]online
- offinemanung[.]site
- offinemanung[.]website
- offinemaunng[.]online
- offineminung[.]online
- offineminung[.]pw
- offineminung[.]site
- offineminung[.]space
- offineminung[.]website
- offinemiunng[.]online
- offinemiunng[.]space
- offinemizung[.]online
- offinemizung[.]website
- offinemnung[.]online
- offinemnung[.]space
- offinemunng[.]online
- offinemunng[.]website
- affinemainung[.]fun
- affinemainung[.]online
- affinemainung[.]space
- affinemainung[.]website
- affinemaiunng[.]fun
- affinemaiunng[.]online
- affinemaiunng[.]site
- affinemaiunng[.]space
- affinemaiunng[.]website
- affinemanung[.]fun
- affinemanung[.]site
- affinemanung[.]website
- affineminung[.]fun
- affineminung[.]online
- affineminung[.]site
- affinemiunng[.]fun
- affinemiunng[.]site
- affinemiunng[.]space
- affinemiunng[.]website
- fariepoziitn[.]online
- fariepoziitn[.]site
- fariepoziitn[.]space
- fariepoziitn[.]website
- faripoziiton[.]fun
- faripoziiton[.]online
- faripoziiton[.]space
- faripoziiton[.]website
- fraiopziiton[.]online
- fraiopziiton[.]site
- offebnarugn[.]online
- offebnarugn[.]site
- offebnarugn[.]space
- offebnarugn[.]website
- offebnurgn[.]online
- offebnurgn[.]site
- offebnurgn[.]space
- offebnurgn[.]website
- offenbarugn[.]online
- offenbarugn[.]site
- offenbarugn[.]space
- offenbarugn[.]website
- offenbaurgn[.]online
- offenbaurgn[.]site
- offenbaurgn[.]space
- offenbaurgn[.]website
- alldrings[.]online
- alldrings[.]pw
- alldrings[.]space
- alldrings[.]website
- alledrigns[.]online
- alledrigns[.]pw
- alledrigns[.]site
- alledrigns[.]space
- alledrigns[.]website
- alledrngs[.]online
- alledrngs[.]pw
- alledrngs[.]space
- alledrngs[.]website
- dassprahcrohr[.]website
- dassprhcorhr[.]online
- dassprhcorhr[.]site
- dassprhcorhr[.]space
- dassrpahcorhr[.]online
- dassrpahcorhr[.]site
- dassrpahcorhr[.]space
- dassrpahcorhr[.]website
- lenreuzdeknen[.]online
- lenreuzdeknen[.]site
- lenreuzdeknen[.]space
- lenreuzdeknen[.]website
- lenruzdeknn[.]online
- lenruzdeknn[.]site
- lenruzdeknn[.]space
- lenruzdeknn[.]website
- lenrzuednken[.]online
- lenrzuednken[.]site
- lenrzuednken[.]space
- lenrzuednken[.]website
- lernezudeknen[.]online
- lernezudeknen[.]site
- lernezudeknen[.]space
- lernezudeknen[.]website
- lernezuednkn[.]online
- lernezuednkn[.]site
- lernezuednkn[.]space
- lernezuednkn[.]website
- lernuzdenken[.]online

- lernuzdenken[.]website
- lnruzdeknn[.]online
- lnruzdeknn[.]site
- lnruzdeknn[.]space
- lnruzdeknn[.]website
- lrneuzdenken[.]online
- lrneuzdenken[.]site
- lrneuzdenken[.]space
- lrneuzdenken[.]website
- lrneuzednken[.]online
- lrneuzednken[.]site
- lrneuzednken[.]space
- lrneuzednken[.]website
- warhehit[.]fun
- warhehit[.]online
- warhehit[.]pw
- warhehit[.]site
- warhehit[.]space
- warhehit[.]website
- warhheit[.]online
- warhheit[.]site
- warhheit[.]space
- warhheit[.]website
- whrheit[.]online
- whrheit[.]pw
- whrheit[.]site
- whrheit[.]space
- whrheit[.]website
- wrhheit[.]online
- wrhheit[.]pw
- wrhheit[.]site
- wrhheit[.]space
- wrhheit[.]website
- allerdigns[.]pw
- deknuzesrtnach[.]fun
- deknuzesrtnach[.]online
- deknuzesrtnach[.]pw
- deknuzesrtnach[.]site
- deknuzesrtnach[.]space
- deknuzesrtnach[.]website
- deknzuersntch[.]site
- deknzuerstnch[.]fun
- deknzuerstnch[.]pw
- deknzuerstnch[.]site
- deknzuerstnch[.]website
- deknzursntch[.]fun
- deknzursntch[.]online
- deknzursntch[.]pw
- deknzursntch[.]site
- deknzursntch[.]space
- deknzursntch[.]website
- deknzusrtnach[.]fun
- deknzusrtnach[.]online
- deknzusrtnach[.]pw
- deknzusrtnach[.]site
- deknzusrtnach[.]space
- deknzusrtnach[.]website
- denkuzesrtnch[.]fun
- denkuzesrtnch[.]online
- denkuzesrtnch[.]site
- denkuzesrtnch[.]space
- denkuzesrtnch[.]website
- denkzusrntch[.]fun
- denkzusrntch[.]online
- denkzusrntch[.]pw
- denkzusrntch[.]site
- denkzusrntch[.]website
- dknuzersntch[.]online
- dknuzersntch[.]pw
- dknuzersntch[.]site
- dknuzersntch[.]website
- dknuzrstnach[.]online
- dknuzrstnach[.]pw
- dknuzrstnach[.]site
- dknuzrstnach[.]space
- dknuzrstnach[.]website
- dknuzsrntch[.]fun
- dknuzsrntch[.]online
- dknuzsrntch[.]pw
- dknuzsrntch[.]site
- dknuzsrntch[.]space
- dknuzsrntch[.]website
- dknzursntach[.]online
- dknzursntach[.]pw
- dknzursntach[.]site
- dknzursntach[.]space
- dknzursntach[.]website
- dnkzuesrtnach[.]pw
- dnkzuesrtnach[.]website
- ferehtdwrhl[.]fun
- ferehtdwrhl[.]pw
- ferehtdwrhl[.]site
- ferehtdwrhl[.]space
- ferehtdwrhl[.]website
- ferhedtewrahl[.]pw
- ferhedtewrahl[.]site
- ferhedtewrahl[.]website
- feriehtdewrahl[.]pw
- feriehtdewrahl[.]site
- feriehtdewrahl[.]space
- allerdigns[.]online
- allerdigns[.]site
- allerdigns[.]space
- allerdigns[.]website
- dassprachrohr[.]online
- dassprachrohr[.]site
- dassprachrohr[.]space
- feriehtdewrahl[.]website
- ferihetderwahl[.]online
- ferihetderwahl[.]website
- warhheit[.]fun
- whrheit[.]fun
- wrhheit[.]fun
- kennediewahrheit[.]live
- lorketstonker[.]store
- neuigkeitenfursie[.]tech
- wahrheitindenaugen[.]pw
- warhheiiptdaunegn[.]link
- warhheiiptdaunegn[.]pw
- warhheintbaunegn[.]pw
- warhheintdaunegn[.]link
- warhheintdaunegn[.]pw
- tribunalukraine[.]info
- lemonde[.]ltd
- leparisien[.]ltd
- washingtonpost[.]ltd
- rbk[.]media
- allons-y[.]social
- candidat[.]news
- franceeteu[.]today
- lavirgule[.]news
- albayan[.]me
- gulfnews[.]ltd
- sueddeutsche[.]ltd
- obozrevatel[.]ltd
- ukraine-inc[.]info
- lefigaro[.]me
- notrepays[.]today
- diplomatie[.]gouv[.]fm
- bmi[.]bund[.]pe
- viedo-klis[.]lv
- libera-stampa[.]it
- librelepresse[.]fr
- weltereignisse365[.]de
- jewishjournal[.]info
- mako[.]news
- theliberal[.]net

# ANNEXE 4 : NOMS DE DOMAINE UTILISÉS POUR LA REDIRECTION

## Noms de domaine jetables

http://google-seo-top[.]com/
http://kabuana[.]com/
http://nursepedia[.]com/
http://eevmnetwork[.]com/
http://flipforms[.]net/
http://krctekno[.]net/
http://cyclebusiness[.]net/
http://orlysbookstore[.]com/
http://dudetonic[.]com
http://jeansmax[.]com/
http://scott-and-jennifer[.]com/
http://cosmowheel[.]com/
http://martinsapc[.]com/
http://texarkanagunswap[.]com
http://mastermoshai[.]com/
http://waqexpay[.]com/
http://pisipatis[.]com/
hnhmap[.]com/
http://schoolofedutainment[.]com/
http://fastpundit[.]com/
http://elevateyourtaste[.]com/
http://silverhouseproperties[.]com/
http://siyabongamjali[.]com/
http://asoprocafenpa[.]com/
http://codingsocially[.]com/
http://aquaculture-mai[.]org/
http://goshow[.]org/
http://dropalo[.]com/
http://nukabd[.]com/
http://ncbid[.]com/
http://wafwot[.]com/
http://intrnaitonal-haert[.]org/
http://ampian[.]com/
http://wisedt[.]org/
http://corzap[.]com/
http://wunkit[.]com/
http://mangut[.]org/
http://peachserver[.]net/
http://keymorse[.]org/
http://pazwv[.]net/
http://hungnm[.]net/
http://thelucycode[.]com/
http://onthegomatchmaking[.]com/
http://petliveapp[.]com/
http://conduisent[.]carlospalars[.]com/
http://elections[.]quick-educate[.]com/
http://promesse[.]techembassy[.]com/
http://guerre[.]securesendportal[.]com/
http://elections[.]thesharkesign[.]com/
http://1[.]parkingonthego[.]com/
http://2[.]soderemynd[.]com/
http://2[.]villadevendome[.]com/
http://1[.]villadevendome[.]com/
http://article637[.]tinkokomarket[.]com/
http://1[.]soderemynd[.]com/
http://1[.]investnewspro[.]com/
http://2[.]parkingonthego[.]com/
http://2[.]bestforbuyers[.]com/
http://2[.]baneizalfe[.]com/
http://pchaibriant[.]leprosypedia[.]com/
http://baneizalfe[.]com/
http://inc[.]taxbyjain.com/
http://1.tiagoads[.]com/
http://2.tiagoads[.]com/
http://trib.sazoom[.]com/
http://2.dubaivisatips[.]com/
http://1.dubaivisatips[.]com/
https://michaelplaxico[.]com
https://nexusfall[.]com
https://swiftdawn[.]com
https://topsnoep[.]com
https://ganimas[.]com/
https://taapi[.]net
https://tabayn[.]com/
https://fibers-it[.]com/
https://faptions[.]net/
https://indianrunningday[.]com
https://kgscrew[.]com
https://sanfranciscosportbetting[.]com
https://horseheadnebula[.]net/
https://distibuidoradavico[.]com/
https://darklakepublishing[.]com
https://solesclean[.]com
https://anilkarasah[.]com
https://loop42[.]com
https://mododuo[.]com
https://grupogarcia[.]net
https://purposeandmindset[.]com
https://scoopofhappy[.]com
https://arctanium[.]net
https://esmirand[.]com
https://marvelbase[.]net/
https://disciplinamental[.]com/
https://americanconservativegazette[.]com/
https://americanliberalmedia.[]com/
https://magnusbeta[.]com/
https://solveitet[.]com/
https://sroutines[.]com/
https://savingbrew[.]com/
https://cloudcosmic[.]net/
https://gulfjoker[.]com/
https://resouarvel[.]com/
https://jaktimnation[.]com/
https://smartvell[.]com/
https://callleague[.]net/
https://junglesaturn[.]net

## Noms de domaine permanents

https://urlbox[.]online
https://marvelgoodies[.]com
https://bighorn-advisors[.]com
https://gitver[.]com
https://raremotion[.]com
https://gooddefr[.]com