La récente annonce en décembre 2022 de la création d'un consortium mené par la société Whalebone a sonné le coup d'envoi du projet de résolveur européen « DNS4EU ». Ce projet aura pour objectif de fournir aux citoyens, sociétés et institutions de l'Union européenne, un service de résolution de nom sécurisé et respectueux de la vie privée. La Commission européenne prévoit ainsi à terme jusqu'à 100 millions d'utilisateurs.

« DNS4EU » : projet européen pour un internet sécurisé

Fig.1

Pour mieux comprendre les origines de ce projet, il convient dans un premier temps de remonter en décembre 2020 quand l'Union européenne (UE) présentait [1] sa nouvelle stratégie de cybersécurité où figurait parmi d'autres projets, celui de sécurisation d'internet. C'est donc dans la lignée de cette stratégie qu'en découla naturellement le projet de résolveur européen intitulé « *DNS4EU* » (entendre « DNS pour l'UE »). Il est actuellement porté par la société tchèque *Whalebone* [2], spécialiste de la cyber sécurité et de la protection de l'identité numérique, conjointement à 12 autres organisations membres de 9 pays européens : Italie, Allemagne, Pologne, Roumanie, Hongrie, Belgique, Portugal, Bulgarie et Finlande.

Mais avant tout, qu'est-ce qu'un résolveur ? Pour mieux comprendre cette question, il est possible d'assimiler un résolveur à un annuaire de type « Pages Jaunes ». En effet, à partir d'une information donnée (par exemple un nom d'entreprise), ce dernier permet d'obtenir un complément d'informations sur l'entreprise recherchée (adresse postale, téléphone, email…). De fait, un résolveur internet agit de la même façon et permet de « traduire » une requête pour un nom de domaine (ex : www.europa.eu) en une adresse IP (147.67.34.45) qui sera ensuite contactée par l'émetteur de la requête (ex : un ordinateur, un smartphone…) afin d'atteindre le domaine souhaité. On en conviendra d'ailleurs que la mémoration d'une adresse IP n'est pas une tâche aisée et c'est pourquoi l'introduction de ce système de résolution de nom dans les années 80[3] fut nécessaire.

De nos jours, l'usage de cette résolution de nom est assuré par le protocole « *DNS* » (« *Domain Network System* ») dont l'utilisation est omniprésente voire quasi-indispensable dans l'ensemble de nos échanges quotidiens. Ce service est assuré par de nombreuses sociétés ou organisations disposant chacune de plusieurs serveurs placés à des points d'échanges stratégiques. Pour fournir un service de qualité ou mettre en valeur leurs services, certaines entreprises

[1] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

[2] https://www.whalebone.io/post/press-release-dns4eu.

[3] https://www.bortzmeyer.org/bind-dns-history.pdf.

Par **Michel de Crevoisier**, membre du comité Cyber.
Analyste Senior en détection des cybermenaces.

n'hésitent pas à privilégier leurs propres résolveurs au détriment d'autres résolveurs alternatifs. C'est le cas par exemple des fournisseurs d'accès à internet dont toute requête sera par défaut acheminée via leurs propres résolveurs. Dans d'autres cas, les résolveurs les plus utilisés seront directement configurés par certains fabricants de matériel afin de s'abstenir de la configuration distribuée par ces opérateurs. Au total, il existe plusieurs centaines de résolveurs publics à travers le monde, et cela sans compter ceux propres à chaque fournisseur d'accès à internet. À titre d'information, une liste non exhaustive des principaux résolveurs [4] mondiaux classés par origine est proposée à la fin de cet article. On remarquera qu'aucune de ces organisations n'est implantée dans un pays membre de l'Union européenne, d'où l'intérêt justifié de ce projet.

Afin de se présenter comme une alternative sérieuse face aux résolveurs actuels, le projet s'est doté d'objectifs [5] ambitieux, à savoir :

- Offrir une alternative aux leaders de ce domaine via un service de résolution résiliant et sécurisé ;
- S'affranchir des services de résolution de nom établis en dehors de l'Union européenne en fournissant un service autonome tout en réduisant le risque d'exposition aux pannes liées aux résolveurs non européens ;
- S'assurer que les données et la vie privée des citoyens européens restent protégés par les textes et lois régies par l'Union européenne, et notamment celui du Règlement Général pour la Protection des Données (« RGPD »).

Par ailleurs, l'analyse de l'appel d'offres[6] nous révèle un aspect très important de ce projet : la sécurité. On apprend ainsi que ce projet devra :

- Fournir différents services de sécurité tels que le « *DNS over HTTPS* » (« DoH »), le « *DNS over TLS* » (« DoT »), le DNSSEC ou encore le support du format d'IP en version 6 (IPv6) ;
- Disposer d'un service premium avec des fonctionnalités avancées de filtrage, de contrôle parental et de support ;
- Bloquer les menaces les plus récentes, notamment à partir de l'échange de données avec des « *Computer Emergency Response Team* » (« *CERT*[7] » - au total quatre sont à dénombrer dans ce consortium) et être en mesure de filtrer les contenus illégaux sur la base de recours juridiques.

S'il n'existe aucun doute en ce qu'un service sécurisé, résiliant et respectueux de la vie privée puisse être délivré, il convient tout de même de rappeler que la résolution de nom n'est qu'une étape parmi tant d'autres venant baliser le parcours de la navigation internet. Or un des points majeurs qu'il convient de mentionner est que de nombreux sites web font de nos jours appel à des réseaux de diffusion (« *CDN* » ou « *Content Delivery Network* ») qui sont pour la plupart non-européens afin de fluidifier leur trafic. On citera pour les plus connus : Akamai, Cloudflare, Fastly et d'autres fournisseurs de service dans le nuage tels que Google, Amazon et Microsoft Azure. Or les pannes de ces derniers ont été fréquentes ces dernières années. Ce fut par exemple le cas de Fastly en 2021 (qui rendit

[4] https://www.lifewire.com/free-and-public-dns-servers-2626062.
[5] https://www.aic.fel.cvut.cz/projects/dns4eu.
[6] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/cef/wp-call/2021/call-fiche_cef-dig-2021-cloud_en.pdf.
[7] https://fr.wikipedia.org/wiki/Computer_emergency_response_team.

Par **Michel de Crevoisier**, membre du comité Cyber.
Analyste Senior en détection des cybermenaces.

inaccessible, entre autres, le site Le Monde[8]) et de Cloudflare en 2022[9]. Par ailleurs il est nécessaire de rappeler que ce projet ne vise en aucun cas à créer un « internet européen parallèle » (comme l'a entamé la Russie en 2019[10]) mais bien à offrir un service de résolution de nom sécurisé et respectueux de la vie privée.

On évoquera pour terminer un des points cruciaux de ce projet qui est celui de son utilisation. En effet, une fois le service de résolution en place, il sera nécessaire de modifier la configuration technique des différents équipements réseau afin de pouvoir bénéficier de ses services. Est-ce que cette étape sera à la portée des utilisateurs finaux ? Disposera-t-il d'une ou plusieurs adresses IP facilement mémorables (telles que celles de Cloudflare, Google ou Quad) afin de faciliter son utilisation ?

Quoiqu'il en soit, les utilisateurs européens ont désormais la possibilité de bénéficier d'un tout autre résolveur français en attendant que « DNS4EU » voit le jour. Il pourront pour cela utiliser le résolveur français nommé « DNS0.eu[11] » qui a vu le jour[12] le 7 février 2023 et qui viendra compléter la dizaine de résolveurs DNS européen[13] déjà présents sur le marché.

Société	Date de lancement	Adresse IP	Origine	Maison mère / partenaires
Cloudflare	2018	1.1.1.1	USA	
Quad9	2017	9.9.9.9	Suisse	IBM X-Force, Packet Clearing House, and Global Cyber Alliance
Google	2009	8.8.8.8	USA	Alphabet
OpenDNS	2006	208.67.222.222	USA	Cisco

[8] https://www.lemonde.fr/pixels/article/2021/06/08/fastly-l-entreprise-dont-la-panne-a-mis-hors-ligne-des-dizaines-de-sites-web-majeurs_6083378_4408996.html.
[9] https://www.zdnet.com/article/cloudflare-service-hit-by-widespread-issues/.
[10] https://www.bfmtv.com/tech/vie-numerique/la-russie-teste-son-propre-internet-pour-resister-en-cas-de-cyberguerre_AN-201912230020.html.
[11] https://www.dns0.eu/fr.
[12] https://twitter.com/dns0eu/status/1622912939501010945.
[13] https://european-alternatives.eu/category/public-dns.

Par **Michel de Crevoisier**, membre du comité Cyber.
Analyste Senior en détection des cybermenaces.