LA LETTRE AFNIC

N°1

afnic
Internet made in France

ÉDITO

Pour ce premier numéro de « La Lettre Afnic » dédiée à la gouvernance technique de l'internet, et alors que le RGPD a fêté ses 4 ans le 25 mai 2022 et que le cadre juridique européen a été largement rénové par l'adoption des législations sur les services et marchés numériques, nous avons voulu partager avec vous une synthèse de ce qui se dit et se débat sur trois sujets majeurs : les abus sur et par les noms de domaine, la sécurisation de l'internet des objets, et enfin, la sécurisation et le chiffrage au niveau des protocoles d'internet. Ces trois thématiques, d'apparence distinctes, évoquent des questions qui sont communes à la plupart des débats qui ont cours aujourd'hui au niveau national autour des « régulations » d'internet : responsabilité des acteurs, efficacité des mesures techniques, confidentialité des échanges, sécurité des protocoles.

Vastes questions qui ne sont ici qu'effleurées, mais dont nous espérons que le traitement dans ce nouveau format sera perçu comme une invitation à approfondir, ensemble, le débat. Bonne lecture !

Pierre Bonis
Directeur général de l'Afnic

SOMMAIRE

LUTTE CONTRE LES ABUS EN LIGNE : LE RÔLE DES REGISTRES
P.2

LA SÉCURITÉ DES OBJETS CONNECTÉS AU CŒUR DE LA SÉCURITÉ SUR INTERNET
P.5

LA SÉCURISATION DES REQUÊTES DNS : ÉTAT DES TRAVAUX EN COURS
P.7

LES PROCHAINS ÉVÉNEMENTS AUXQUELS L'AFNIC PARTICIPE
P.10

LUTTE CONTRE LES ABUS EN LIGNE : LE RÔLE DES REGISTRES

LES PRATIQUES DES OPÉRATEURS DNS DANS LA LUTTE CONTRE LES ABUS

Dans un contexte de baisse générale de tolérance face au spam, au hameçonnage et aux autres menaces courantes en ligne, la lutte contre les abus prend une place croissante dans les discussions de l'écosystème de gestion de l'infrastructure internet. Les opérateurs DNS (*Domain Name System*) sont un des leviers identifiés par des acteurs comme l'Union Européenne ou le gouvernement français[1], pour s'attaquer à certains des abus spécifiques au monde numérique.

Mais comment lutter, exactement ? Qui piloterait la lutte ? Quels outils mettre en place ? À quelle étape ? Le succès d'internet tient à son architecture en réseau de réseaux donc en la possibilité de chacun de ses acteurs de prendre ses propres décisions, rappelle l'ICANN[2] (*Internet Corporation for Assigned Names and Numbers*). Pour cette organisation, la lutte contre les abus DNS pourrait donc être organisée de la même manière : avec des protocoles techniques et des règles opérationnelles qui permettent la coopération, mais sans système de contrôle centralisé.

La perspective est intéressante, mais quelles que soient les modalités de gestion adoptées, un premier problème de définition se pose. Si une bonne partie des opérateurs DNS s'intéressent désormais aux moyens de lutte contre certains types d'abus techniques, il n'existe aucun consensus, au sein de cette communauté ni de celle de la standardisation de l'internet en général, sur la définition exacte des abus DNS.

Pistes de définition

Pour évoquer les méthodes de lutte contre les abus DNS, il est nécéssaire de bien connaitre en premier lieu la nature des abus en question. Plusieurs typologies de classement des abus DNS existent.

Le *Security and Stability Advisory Committee* de l'ICANN propose une approche des abus DNS en trois catégories :

- abus de protocole ;
- abus d'infrastructure (utiliser les services DNS comme support pour créer d'autres abus) ;
- abus des noms de domaine eux-mêmes.

Cette dernière catégorie peut être re-divisée entre les abus par création de domaines

1 - https://www.nextinpact.com/article/68658/comment-fonctionnera-filtre-anti-arnaque-en-ligne-promis-par-emmanuel-macron
2 - https://www.icann.org/en/system/files/files/sac-115-en.pdf

directement malveillants et la corruption de domaines légitimes, aux dépens de leur propriétaire.

La Commission Européenne adopte de son côté une définition relativement large : selon son étude dédiée[3], un abus DNS correspond à « n'importe quelle activité utilisant un nom de domaine ou les protocoles DNS pour réaliser des activités illégales ou malveillantes ». De fait, elle classe les abus en trois catégories :

- abus par noms de domaine enregistrés à des fins malveillantes ;
- abus liés au fonctionnement technique du DNS et des noms de domaine ;
- abus liés à la distribution de contenu malveillant par le DNS.

Chaque occurrence donne lieu à une prise en charge par un ou des acteurs différents.

Sous une apparence technique, cette approche pose problème dans la mesure où elle cherche à effectuer une classification de tous les abus en ligne. En effet, comme près de la totalité des échanges sur internet s'appuient sur le DNS, indiquer que toutes les activités malveillantes qui l'utilisent constituent des abus DNS, revient, dans les faits, à viser toutes les activités malveillantes sur internet. La mention du DNS est ici trompeuse, car ce protocole ne peut, par construction, évoluer pour prendre en charge la lutte contre de tous les abus.

« Le protocole DNS ne peut prendre en charge la lutte contre tous les abus. »

Si cette lutte contre les abus en ligne est nécessaire, cette approche pseudo-technique ne permettra pas de la mener de manière efficace. Par comparaison, personne n'a eu l'idée jusqu'à ce jour de modifier profondément le système postal pour lutter contre les lettres de corbeaux anonymes.

Menée en avril et mai 2022 par le Centr (*Council of European National Top-Level Domain Registries*, Association des registres européens des domaines nationaux) auprès d'opérateurs DNS européens, l'étude « *Measuring Abuse* » donne une approche beaucoup plus terre à terre des problèmes à gérer. En soumettant une série de problématiques à ses interrogés, elle rapporte que les abus les plus fréquemment cités (parce que rencontrés) par les répondants sont les suivants :

- le hameçonnage ;
- les logiciels malveillants ;
- les faux sites (ou *fake webshops* - sites dont le nom de domaine peut imiter un nom de domaine existant ou utiliser un nom de domaine déjà bien référencé par le passé) ;
- la contrefaçon ;
- le *pharming* (qui détourne directement une requête DNS vers un site frauduleux) ;
- les *botnets* ;
- et le spam.

Si la définition des abus DNS est si complexe, c'est que certaines sous-catégories embarquent de vrais défis politiques, dont l'appréciation varie selon les cadres légaux, politiques et culturels. En effet, une partie des éléments considérés comme des abus DNS par la Commission Européenne concernent les contenus diffusés grâce aux noms de domaine associés. Cela

3 - https://op.europa.eu/en/publication-detail/-/publication/7d16c267-7f1f-11ec-8c40-01aa75ed71a1

soulève des questions de liberté d'expression et de neutralité.

À défaut de trancher le débat, de son côté, le *Security and Stability Advisory Committee* de l'ICANN recommande que le suivi et la définition des abus DNS adoptés par chaque acteur évoluent au fil du temps et des cas constatés sur le terrain.

Pratiques de lutte contre les abus

En s'appuyant sur les différents documents mentionnés précédemment, on peut dessiner un récapitulatif des principales pratiques de lutte contre les abus DNS constatées chez différents opérateurs de domaines de premier niveau.

- **Politique d'usage acceptable** ou **politique anti-abus**. Qu'elle soit documentée dans le sens des autorisations ou dans celui des interdictions, la politique du registre fixe un cadre clair des actions possibles et des cas dans lesquels ce dernier réagit, le plus souvent à sa seule discrétion.
- **Point de contact**. Les opérateurs affichent les étapes de leurs processus de réaction et fournissent un point de contact clair pour les signalements et réclamations (par exemple https://www.afnic.fr/noms-de-domaine/resoudre-un-litige/).
- **Collaboration**. Au fil des réunions (organisées par l'IETF, RIPE, etc.), un grand nombre d'opérateurs se déclarent intéressés par la possibilité de travailler ensemble, et avec d'autres entités, pour améliorer la lutte contre les abus.

L'ICANN encourage la création de « programmes de notification » avec des entités de confiance (représentants des forces de l'ordre dans la zone concernée, Interpol et autres agences internationales, CERTs, etc.). L'initiative « *Internet and Jurisdiction* », créée par l'ancien ambassadeur français pour le numérique Bertrand de la Chapelle, travaille également sur le concept de tiers de confiance à même de signaler aux registres des abus sur lesquels ces derniers pourraient avoir une action. L'ICANN suggère aussi la création d'un *Common Abuse Response Facilitator*, entité indépendante qui permettrait de mettre les savoirs et les techniques en commun et de trouver des appuis.

« Imposer des règles applicables à tous faciliterait le travail des escrocs. »

Pour autant, il ne faut pas confondre collaboration et harmonisation forcée. Les échanges de bonnes pratiques et les comparaisons de taux d'abus entre registres internet relèvent de l'exercice du métier : ils sont nécessaires. Ces échanges permettent de piloter les politiques de lutte contre les abus, au niveau des extensions internet, en prenant en compte le contexte, les habitudes, le cadre juridique et réglementaire applicable. C'est d'ailleurs une constante chez les gestionnaires de ccTLD (*Country code Top Level Domain*) européens, dont les extensions sont reconnues, y compris dans le rapport de la Commission Européenne cité précédemment, comme portant le moins d'abus au monde, de militer pour une approche différenciée. « *One size doesn't fit all* » est une recette qui a fait ses preuves chez chacune des extensions européennes, dont le .fr. Au-delà de l'effet de communication, imposer de nouvelles règles applicables à tous serait le meilleur cadeau à faire aux escrocs, qui n'auraient dès lors à se concentrer que sur le contournement d'un seul mécanisme de protection.

LA SÉCURITÉ DES OBJETS CONNECTÉS AU CŒUR DE LA SÉCURITÉ SUR INTERNET

Par la mise en réseau d'objets allant du thermostat au vêtement, en passant par le téléphone portable ou l'habitat, l'Internet des Objets (IdO) a un impact croissant sur la vie quotidienne des Français comme des entreprises. Alors que leur usage se développe, ces objets créent de nouveaux risques, tant en termes de protection des données personnelles, que de cybersécurité. L'exemple de la santé connectée, dont les données sont par nature sensibles, illustre l'importance de concevoir un IdO sobre et respectueux des utilisateurs.

Lors du RIPE 84[1], où l'Afnic était présente, Tommy Haga de l'Helse Vest IKT (en charge de la gestion du système d'information de l'agence de santé de l'ouest norvégien) a réalisé une présentation[2] éloquente sur les questions que soulève l'IdO en matière de sécurité. Il est parti de l'exemple avec lequel lui-même doit se débrouiller au quotidien : les 60 000 outils connectés de l'hôpital public norvégien.

À l'occasion de cette présentation, l'ingénieur a souligné que l'IdO connecte sur le réseau des ressources qui, comme dans les hôpitaux, n'étaient pas connectées auparavant. Résultat, les administrateurs systèmes se retrouvent forcés de composer avec des ressources très hétéroclites :

- des machines connectées au système mais impossibles à identifier (on sait qu'elles sont là, mais on ne sait pas ce qu'elles font) ;
- des objets (ex : un réfrigérateur dédié à garder des virus biologiques, un distributeur d'uniformes médicaux) tournant sous Windows XP ou Windows NT et infectés par des virus informatiques. Les constructeurs ont refusé d'installer les patchs de sécurité nécessaires, de peur que ceux-ci bloquent le bon fonctionnement des machines ;
- des machines impossibles à authentifier parce qu'elles n'envoient pas de données.

Tommy Haga a attiré l'attention sur le besoin de réfléchir à l'intégration de chaque outil, quelle que soit sa configuration, dans l'architecture globale. Ce qui, dans un contexte hospitalier, nécessite de ne pas prendre en compte seulement la fonction médicale d'un objet, mais aussi son enveloppe technique.

ENJEUX SPÉCIFIQUES AUX OBJETS CONNECTÉS

Parmi les enjeux à intégrer : la taille, souvent minimale, des objets connectés. Celle-ci implique d'imaginer des méthodes de sécurisation adaptées.

1 https://ripe84.ripe.net/
2 https://ripe84.ripe.net/archives/video/780/

L'IETF (RFC 7228[3]) a classé les objets connectés contraints en trois catégories :

- ceux de classe 0 disposent d'une RAM de moins de 10 kiloctets et d'une mémoire flash de moins de 100 ko ;
- ceux de classe 1, d'une RAM d'environ 10 ko et d'une mémoire flash jusqu'à 100 ko ;
- ceux de classe 2, d'une RAM jusqu'à 50 ko et d'une mémoire flash jusqu'à 250 ko.

Tous ont donc des capacités bien plus limitées que l'ordinateur ou le smartphone le plus basique. Pour ces objets à faible capacité de mémoire et de calcul, cela implique de créer des mécanismes spécifiques de sécurité, afin d'intégrer des éléments comme des certificats. Il reste donc encore à concevoir des protocoles de communication et des architectures de sécurisation adaptés. Citons notamment le projet Franco-Allemand PIVOT[4] qui travaille sur l'amélioration de la sécurité et de la confidentialité au sein de ces architectures contraintes.

Une autre problématique est celle de l'interopérabilité. Établir une connexion entre le stimulateur cardiaque d'un patient et le système informatique d'un hôpital pour échanger des données requiert le plus souvent, pour le moment, d'utiliser le protocole propriétaire de l'objet. Il faut donc que celui-ci fonctionne avec le système de l'hôpital, et qu'il soit sécurisé.

MULTIPLICITÉ DES TRAVAUX

Pour répondre à ces enjeux, les groupes de travail se multiplient, à l'IETF et au sein d'autres organisations. Lors de l'IETF 115[5], le groupe *IoT Operations* a d'ailleurs mis l'accent sur la nécessité d'avoir une base de référence pour pointer vers différents travaux liés à la sécurité de l'IdO, qu'il s'agisse de ceux de l'IETF, de l'Agence de l'Union Européenne pour la cybersécurité (ENISA), de l'Institut Européen des Normes de Télécommunications (ETSI), du *National Institute of Standards and Technology* (NIST), américain, ou encore de l'Union Internationale des Télécommunications (IUT[6]).

« Minimale, la taille des objets connectés implique d'imaginer des méthodes de sécurisation adaptées. »

La question du passage à l'échelle de certaines architectures d'IdO, conçues pour être plus silotées ou « verticales », est essentielle. En attendant, le nombre de connexions aux réseaux augmente avec celui des objets connectés, générant ainsi une pression sur les gestionnaires de systèmes IdO. Ces derniers doivent assurer l'intégrité globale de leur système et des connexions, entre réseaux connus et réseaux inconnus, sur internet ou sur des réseaux dédiés comme LoRa ou Sigfox.

Sans une capacité d'authentification et de vérification de ces objets ou ressources spécifiques sur un réseau, le risque principal est celui d'un accès non autorisé à l'objet. Cela peut par exemple le rendre visible sur un réseau privé à des personnes non autorisées ou

3 https://www.rfc-editor.org/rfc/rfc7228
4 https://www.afnic.fr/observatoire-ressources/papier-expert/respect-de-la-vie-privee-dans-lido-un-point-detape-sur-le-projet-pivot-et-les-travaux-de-lafnic/
5 https://www.ietf.org/how/meetings/115/
6 https://www.itu.int/fr/ITU-T/studygroups/2017-2020/20/Pages/default.aspx

sur un réseau public, permettre d'en perturber le fonctionnement, ou encore de le détourner pour des finalités malveillantes (ex : *botnet*).

Pour répondre à ces questions, une partie des recherches en matière de sécurisation se concentrent sur les infrastructures à clés publiques. Un autre pan de recherche s'intéresse également à l'intégration d'ancres de confiance et de clés privées dans les dispositifs dès leur fabrication. L'Afnic participe activement à l'ensemble de ces travaux.

LA SÉCURISATION DES REQUÊTES DNS : ÉTAT DES TRAVAUX EN COURS

Dès 2013, la défiance créée par les révélations d'Edward Snowden a eu pour conséquence la relance des travaux de normalisation visant à renforcer la confidentialité des échanges. L'IETF (*Internet Engineering Task Force*, le regroupement à l'origine des standards et protocoles internet) a clairement pris position, définissant dès lors la surveillance de masse comme une attaque contre internet. Depuis, le renforcement de la confidentialité et de la sécurité des requêtes DNS est devenu un enjeu pris en charge par l'IETF qui mène des travaux d'évolution des protocoles[1].

Rappelons qu'initialement, les protocoles sous-jacents d'internet n'ont pas été pensés pour assurer un haut niveau de confidentialité, mais pour garantir un haut niveau de résilience. Au sein des couches applicatives, ce sont d'autres protocoles tels que TLS ou HTTPS, qui ont historiquement été utilisés pour assurer la confidentialité des échanges. Le DNS, lui, était vu comme portant des données essentiellement techniques, nécessaires à l'adressage et à la résolution des noms de domaine.

AMÉLIORER LA CONFIDENTIALITÉ DES REQUÊTES DNS : DOT, DOH, DOQ

Plusieurs leviers permettent d'améliorer la sécurité des échanges :

- la minimisation des données qui transitent sur le réseau[2], c'est-à-dire la réduction de la quantité de données envoyées et leur exploitabilité par un tiers ayant accès à ces informations. Dans le cas du DNS, on cesse de transmettre la requête complète à tous les serveurs, y compris ceux de la racine ;

1 https://www.rfc-editor.org/rfc/rfc7258
2 https://www.afnic.fr/observatoire-ressources/papier-expert/vers-un-dns-moins-indiscret/

- le chiffrement des échanges et du trafic des applications et services sur internet. Dans ce domaine, le changement le plus connu du grand public est le passage de HTTP à HTTPS. Du côté du DNS, toutes les étapes du parcours d'une requête et d'une réponse sur le réseau ne sont pas intégralement sécurisées. Des travaux sont encore nécessaires. Trois protocoles de chiffrement existent pour le DNS : DoH (DNS over HTTPS), DoT (DNS over TLS) et le plus récent, DoQ (DNS over QUIC).

Une histoire de protocoles

Do53, ou DNS over TCP/UDP, est le protocole classiquement utilisé pour les requêtes DNS. Il s'agit d'un standard d'échange non chiffré, ce qui rend les requêtes DNS et leur contenu visibles sur le réseau et vulnérables à différents types d'attaques. Une attaque permettrait à un acteur tiers d'intercepter l'échange et de l'écouter ou de le rediriger vers un autre serveur que celui recherché. Pour résoudre ces problèmes, plusieurs solutions de chiffrement existent déjà :

« Pour protéger les requêtes DNS entre l'utilisateur et le résolveur, le chiffrement est indispensable. »

- **DoT, DNS over TLS,** protocole le plus ancien, chiffre la communication entre l'utilisateur et le résolveur en utilisant le traditionnel TLS (*Transport Layer Security*, le même que celui utilisé par HTTPS). Il a été normalisé en 2016 ;
- **DoH, DNS over HTTPS**, chiffre également la communication entre l'utilisateur et le résolveur DNS mais en intercalant le protocole HTTP entre TLS et DNS.

Les deux fonctionnent correctement depuis plusieurs années. Un nouveau protocole est apparu depuis : **DNS over QUIC**. Il a été élaboré par les ingénieurs de Google (à l'initiative de Jim Roskind) et repris par l'IETF dès 2015.

Dernier arrivé aux résultats prometteurs : DoQ

QUIC intéresse beaucoup l'écosystème des opérateurs DNS de résolveurs dans la mesure où il promet des performances améliorées, en permettant une protection de la confidentialité des requêtes et une moindre latence.

DNS over QUIC[3] n'ayant été normalisé[4] qu'en mai 2021, les études se multiplient pour estimer ses avantages et ses éventuels inconvénients. Adguard[5], qui fournit entre autres un résolveur DNS public, a détaillé certains atouts de DoQ dans une présentation faite lors de l'OARC 38[6] (le *DNS Operations, Analysis and Research Center*, DNS-OARC, organise régulièrement des réunions pour l'écosystème). Selon les auteurs de l'étude, DNS over QUIC augmente le nombre de requêtes possibles par connexion, améliore globalement la rapidité, la stabilité et offre une plus grande durabilité des connexions. En revanche, QUIC demande davantage de puissance de calcul que DoT ou DoH.

Menée par l'Université technique de Munich et présentée au RIPE 85[7] (*RIPE Network Coordination Center*, le registre régional d'adresses IP qui dessert l'Europe, une partie de l'Asie

3 https://www.afnic.fr/wp-media/uploads/2021/09/afnic-jcsa2021-quic-bortzmeyer.pdf
4 https://www.afnic.fr/observatoire-ressources/papier-expert/le-protocole-de-transport-quic-est-desormais-normalise/
5 https://adguard.com/fr/blog/dns-over-quic-official-standard.html
6 https://indico.dns-oarc.net/event/43/
7 https://ripe85.ripe.net/

et le Moyen-Orient), une autre étude[8] apporte un peu de nuances. Selon ses auteurs, DoQ fait légèrement ralentir le chargement d'une page web, mais représente tout de même une grosse amélioration par rapport à DoH. En revanche, DoQ est moins performant que DoH quand les requêtes augmentent. Enfin, des tests menés par CZNIC (association des principaux fournisseurs d'accès internet tchèques, également registre du .cz) montrent qu'en cas d'attaque DoS, les serveurs DoQ réagissent moins bien que DoT et DoH.

À partir de juin 2022, le Directeur scientifique du registre internet régional pour l'Asie Pacifique, APNIC (*Asia Pacific Network Information Centre*), Geoff Huston a commencé à calculer l'usage d'HTTP/3 (qui utilise QUIC) pour le comparer à celui d'HTTPS. Lors de la présentation de ses résultats à l'IETF 114, ses calculs montraient que 10 à 15 % des utilisateurs demandant un enregistrement DNS recherchaient un serveur résolveur DNS via HTTPS, tandis qu'1,5% d'entre eux seulement utilisait ensuite HTTP/3 pour récupérer la valeur de l'enregistrement DNS visé. HTTP/3 et QUIC jouissaient tout de même d'une certaine dynamique de déploiement du côté des navigateurs, tirée, en particulier, par le Safari d'Apple dans les dernières versions d'iOS. Geoff Huston a publié de nouveaux calculs sur l'usage de QUIC sur son site personnel[9] en septembre 2022.

PRINCIPAUX PROTOCOLES DE SÉCURISATION DU DNS

- **DNS over TLS** : chiffre la communication entre l'utilisateur et le résolveur via TLS
- **DNS over HTTPS** : chiffre la communication entre l'utilisateur et le résolveur DNS en intercalant le protocole HTTP entre TLS et DNS
- **DNS over QUIC** : nouveau protocole de couche transport, protège la confidentialité des requêtes tout en réduisant la latence, comparé aux deux autres

En parallèle, des membres du *Charter working group* de l'IETF « *IP Performance Measurement*[10] » travaillent sur des « Techniques de mesure de débit explicite ». Ces dernières utilisent quelques bits de marquage pour quantifier la perte et le retard. Cela permet de mesurer les performances de la connexion, et de localiser le segment de réseau où les perturbations se produisent. Des acteurs, comme Orange, utilisent ces nouvelles techniques lorsque les méthodes historiques ne permettent pas la détection des retards et des pertes sur un réseau.

Si le chiffrement des requêtes DNS est bénéfique pour les utilisateurs et la plupart des fournisseurs de services de résolution DNS, l'enjeu de déploiement est complexe pour certains exploitants. En effet, il nécessite de régler des contraintes opérationnelles, notamment sur les aspects de supervision des services. De la même manière, de grands groupes restent vigilants et proactifs quant au risque d'utilisation de services DNS tiers par rapport à des solutions qu'ils maîtrisent intégralement.

La poursuite des travaux de sécurisation des requêtes et l'accélération du déploiement des protocoles reposent donc sur une coordination et un partage des connaissances adaptés entre les acteurs impliqués.

8 https://vaibhavbajpai.com/documents/papers/proceedings/doq-imc-2022.pdf
9 https://www.potaroo.net/ispcol/2022-09/quic2.html
10 https://datatracker.ietf.org/doc/draft-ietf-ippm-explicit-flow-measurements/

LES PROCHAINS ÉVÉNEMENTS AUXQUELS L'AFNIC PARTICIPE

- **IETF 116**
  Yokohama, Japon
  25-31 mars 2023
- **ICANN 77 Policy Forum**
  Washington D.C., États-Unis
  12-15 juin 2023
- **Journée du Conseil scientifique de l'Afnic (JCSA)**
  Paris, France
  5 juillet 2023
- **FGI France**
  Paris, France
  6 juillet 2023
- **IGF Monde**
  Kyoto, Japon
  8-12 octobre 2023

afnic
Internet made in France

VOTRE CONTACT

lalettre@afnic.fr

Directeur de publication : Pierre Bonis

Afnic | www.afnic.fr
Immeuble Stephenson, 1 rue Stephenson,
78180 Montigny-le-Bretonneux