

Labo découverte Maltego

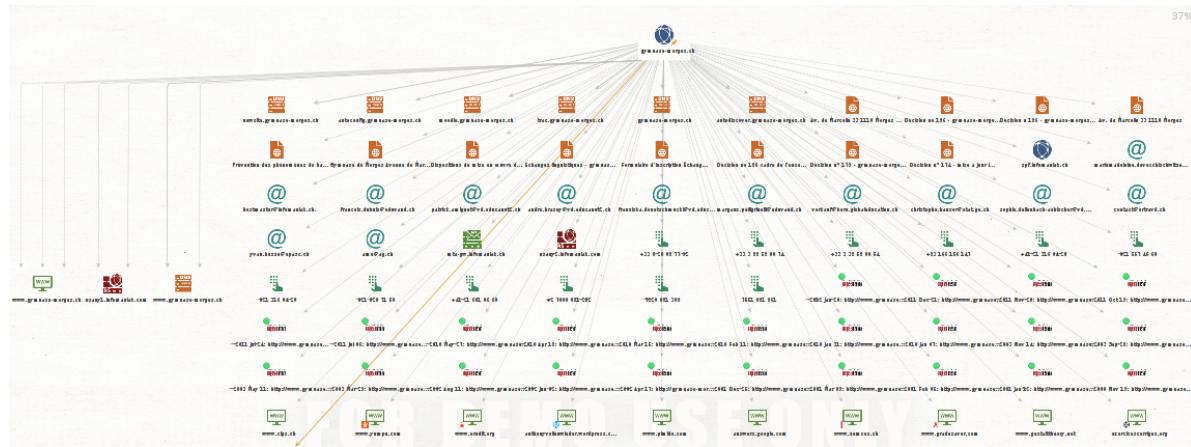
Auteur: Alexandra Cerottini

Date: 26.03.2022

Une simple reconnaissance de réseau

Domaine

J'ai choisi d'effectuer une reconnaissance de réseau sur le domaine **gymnase-morges.ch**.



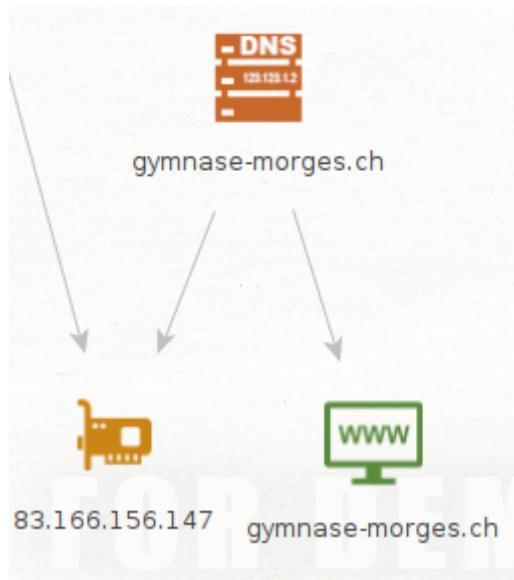
Nous pouvons voir que nous obtenons toutes sortes d'informations comme des serveurs DNS, des documents, un autre domaine, des adresses emails, un MX Record (permettant d'associer un nom de domaine à un serveur de messagerie électronique), un NS Record (permettant de gérer un sous-domaine via un autre serveur DNS), des numéros de téléphones, des anciennes versions du site internet disponibles sur Wayback Machine ainsi que des sites webs.

Serveur DNS



Nous retrouvons 6 serveurs DNS.

Nous pouvons effectuer une recherche supplémentaire sur le DNS **gymnase-morges.ch**



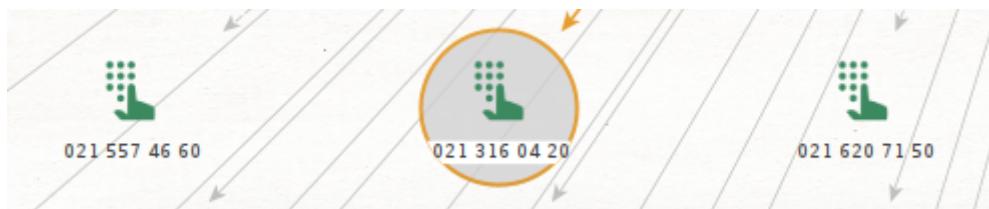
Nous retrouvons l'adresse IPV4 ainsi que le site web.

Documents



Nous retrouvons 12 documents se trouvant sur le site internet **gymnase-morges.ch** comme par exemple la brochure du gymnase, des décisions relatives au COVID-19 et des formulaires pour partir en échange.

Numéros de téléphones



Nous retrouvons le vrai numéro de téléphone du gymnase.

Avec le site [local.ch](#), nous avons la possibilité de tester les numéros Suisse pour trouver une correspondance. Un numéro appartient à une agence de communication, un autre numéro redirige sur le gymnase de Chamblaines, un autre sur l'Espace santé social Vaud et un autre sur le CIPS (Centre d'information des professions santé-social).

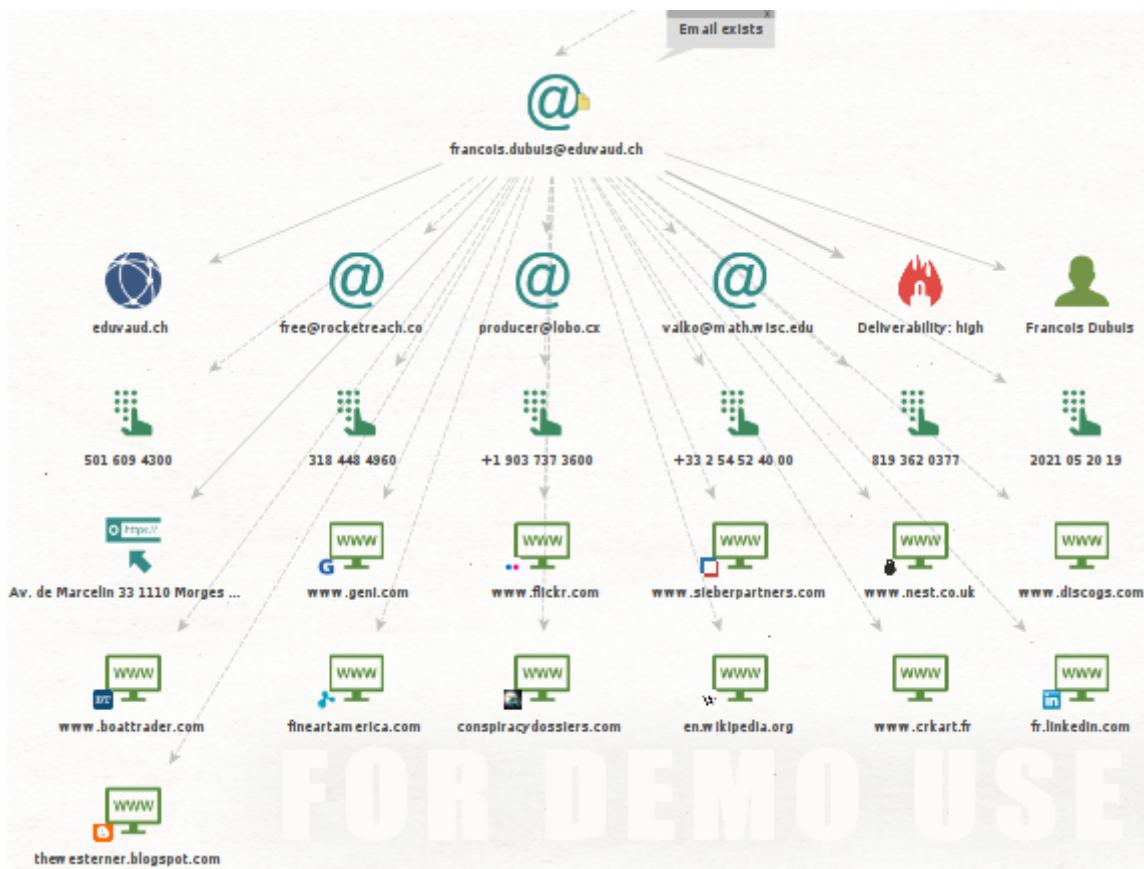
Nous remarquons ici qu'il faut bien traiter les informations retournées par **Maltego**. Elles ne sont pas toutes pertinentes pour ce que l'on recherche.

Emails



Nous retrouvons 13 adresses emails.

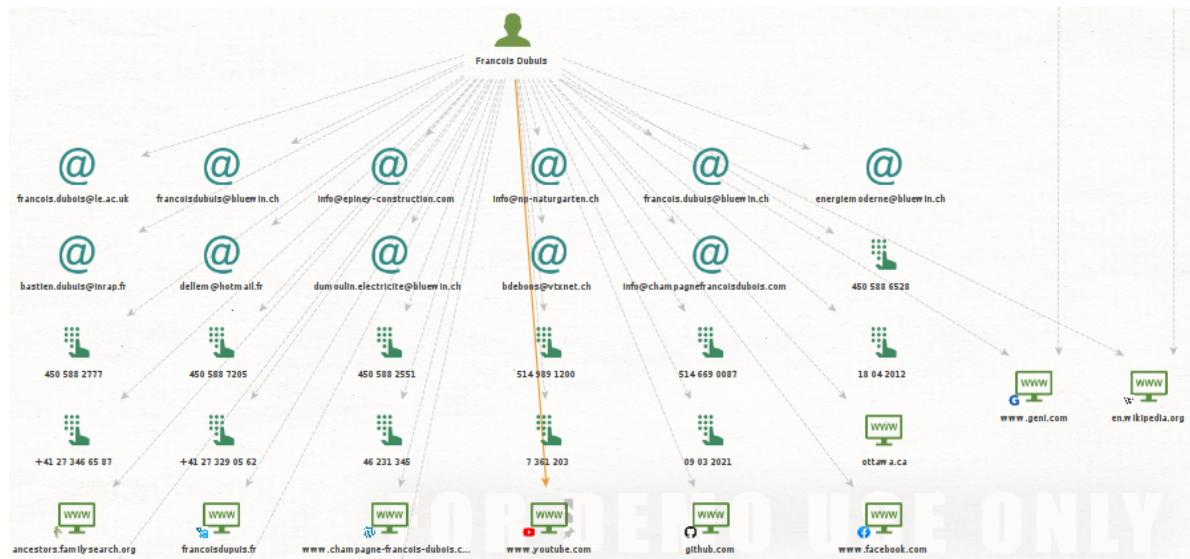
Nous pouvons effectuer une recherche sur l'email **francois.dubuis@eduvaud.ch**



Maltego nous confirme que l'email existe et trouve d'autres informations reliées à ce email. Il a également trouvé une entité personne de François Dubuis.

Personne

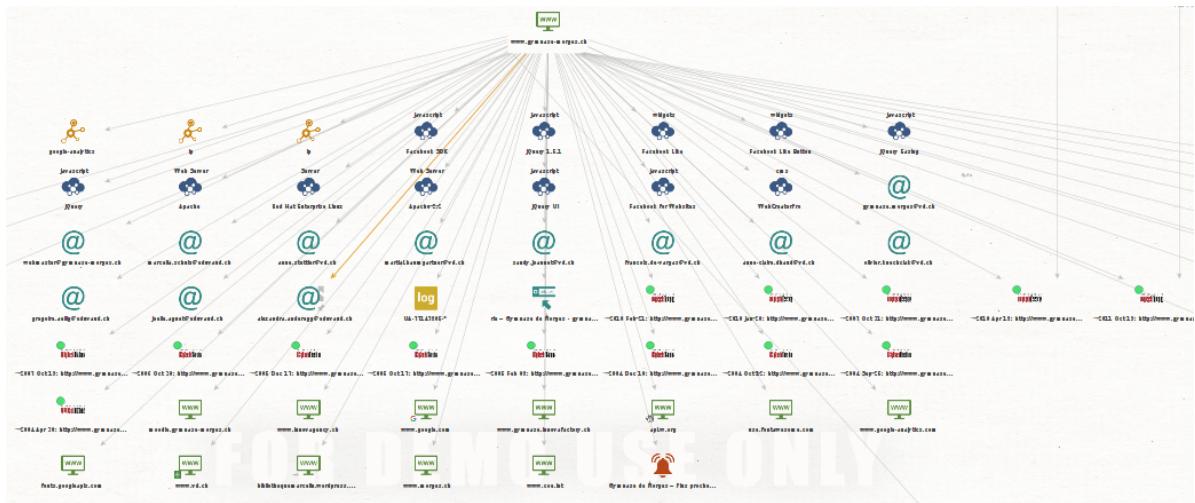
Nous allons maintenant exécuter les transformations sur la personne **François Dubuis**.



Nous avons probablement trouvé son email Bluewin. Les autres résultats ne sont pas pertinents car le nom de famille n'est pas le même (Dupuis ou Dubois).

Site web

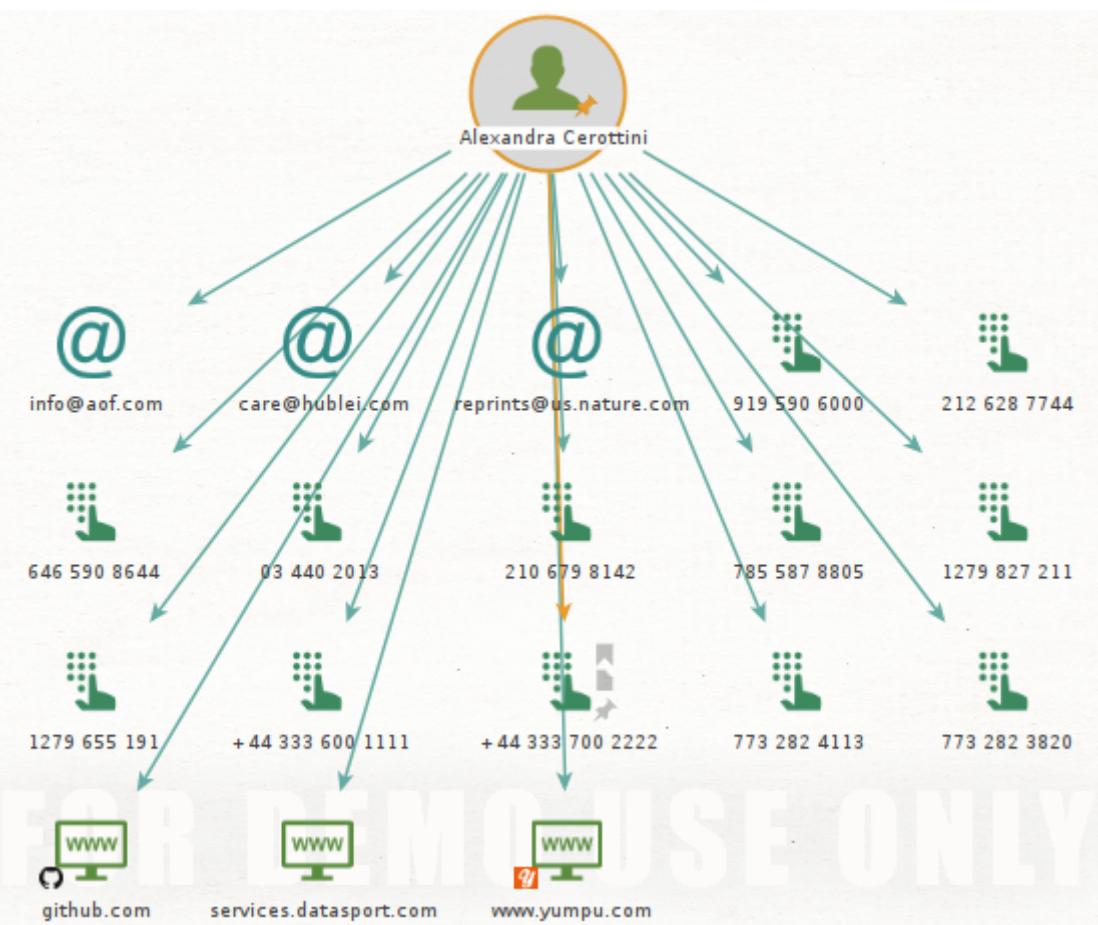
Nous pouvons prendre directement le site web du gymnase.



Nous retrouvons en plus des informations sur les technologies utilisées, d'autres adresses emails et également l'adresse IP que nous avions trouvée précédemment.

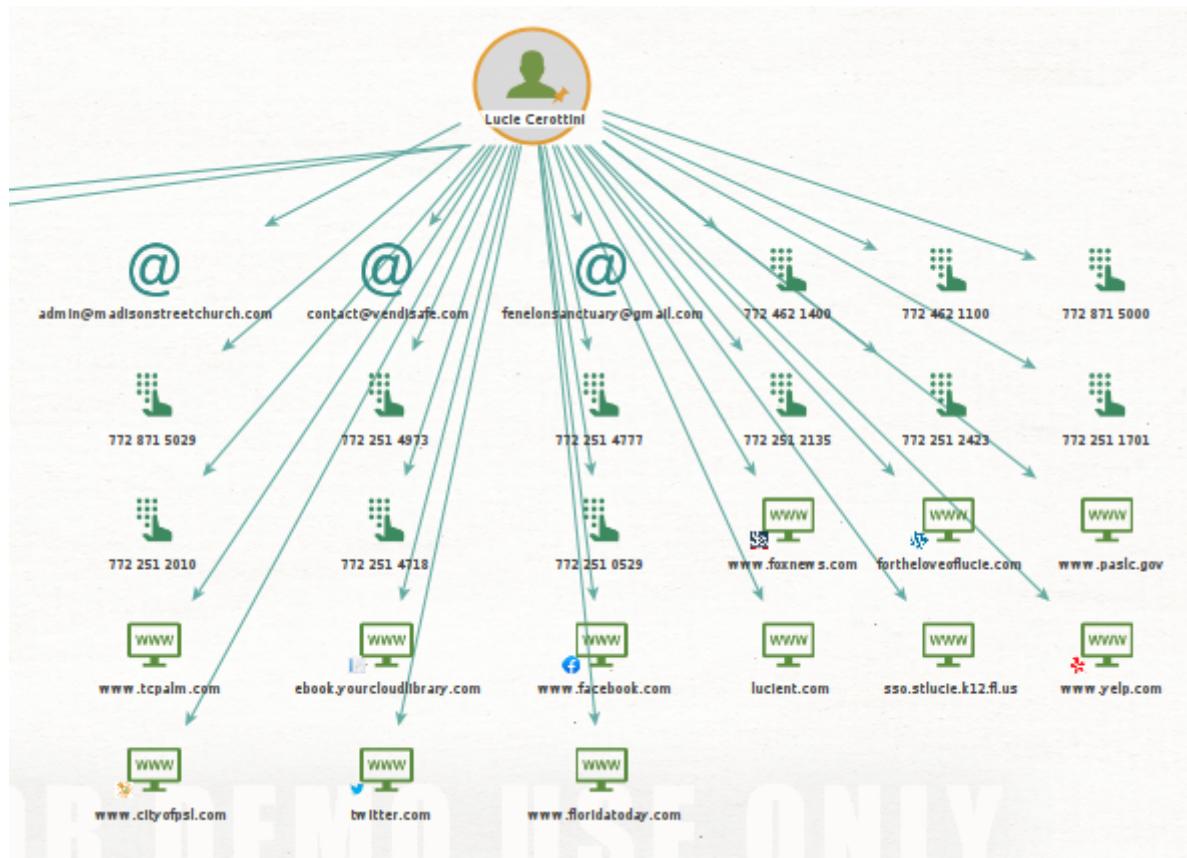
Recherche d'une identité

J'ai choisi de me rechercher moi-même.



Aucun des emails et des numéros ne m'appartiennent. Par contre, nous retrouvons mon Github ainsi que le résultat des courses à pied que j'ai effectuées sur Datasport et sur Yumpu.

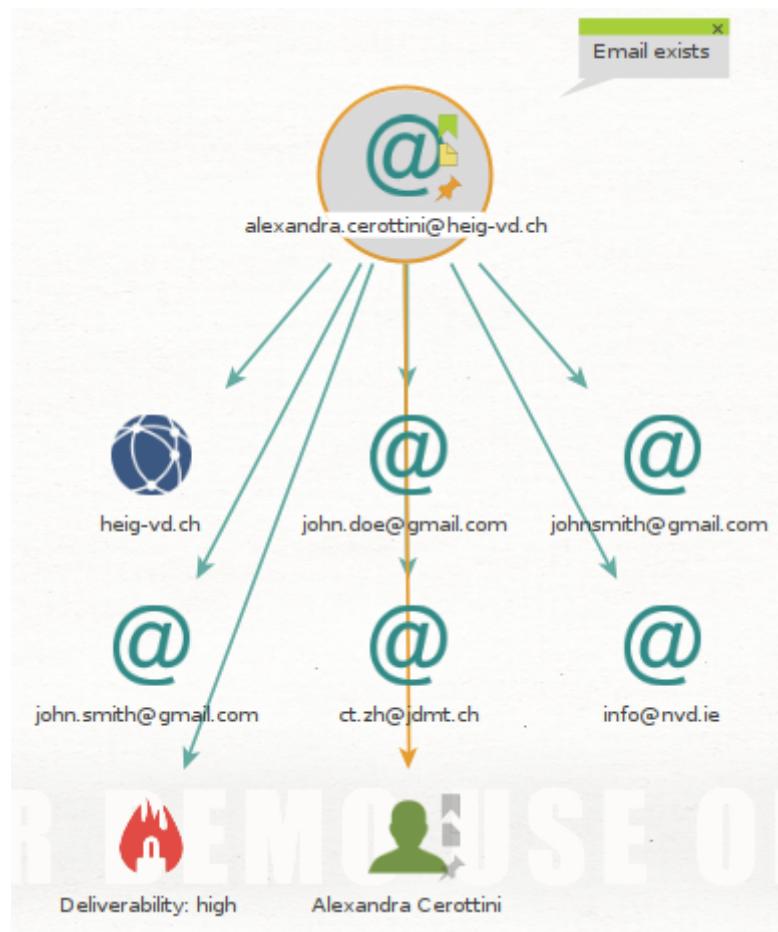
J'ai également recherché ma sœur, Lucie Cerottini.



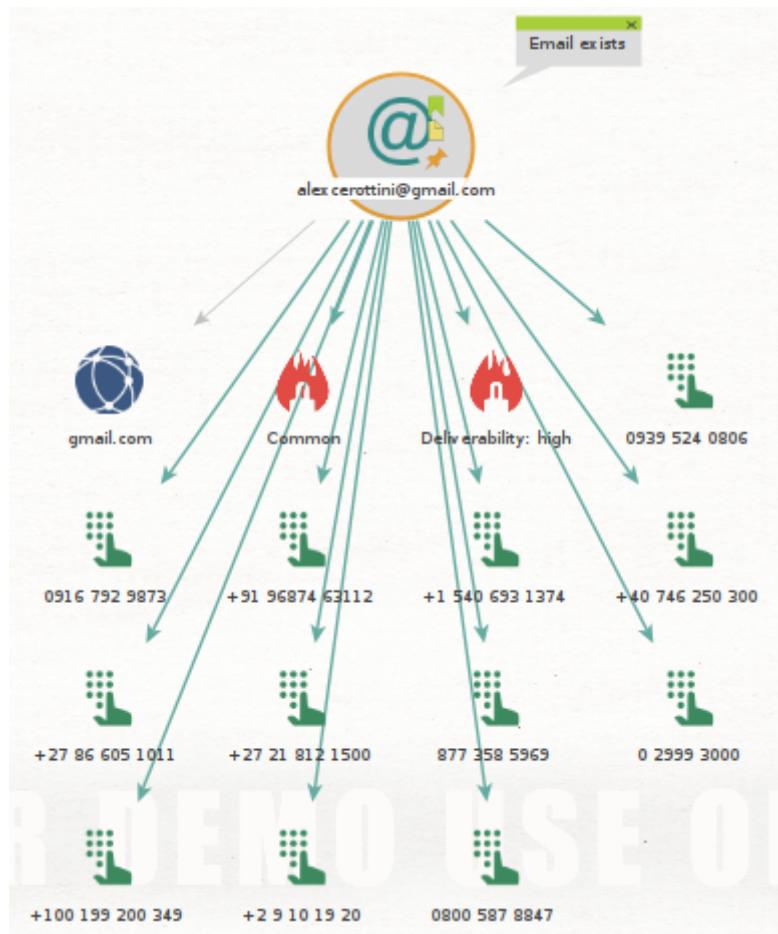
Aucun des emails et numéros ne lui appartiennent également. J'ai vérifié un à un les sites internet et aucun de ces sites ne la mentionnent. Nous ne retrouvons donc aucune information sur elle.

Recherche d'une adresse email

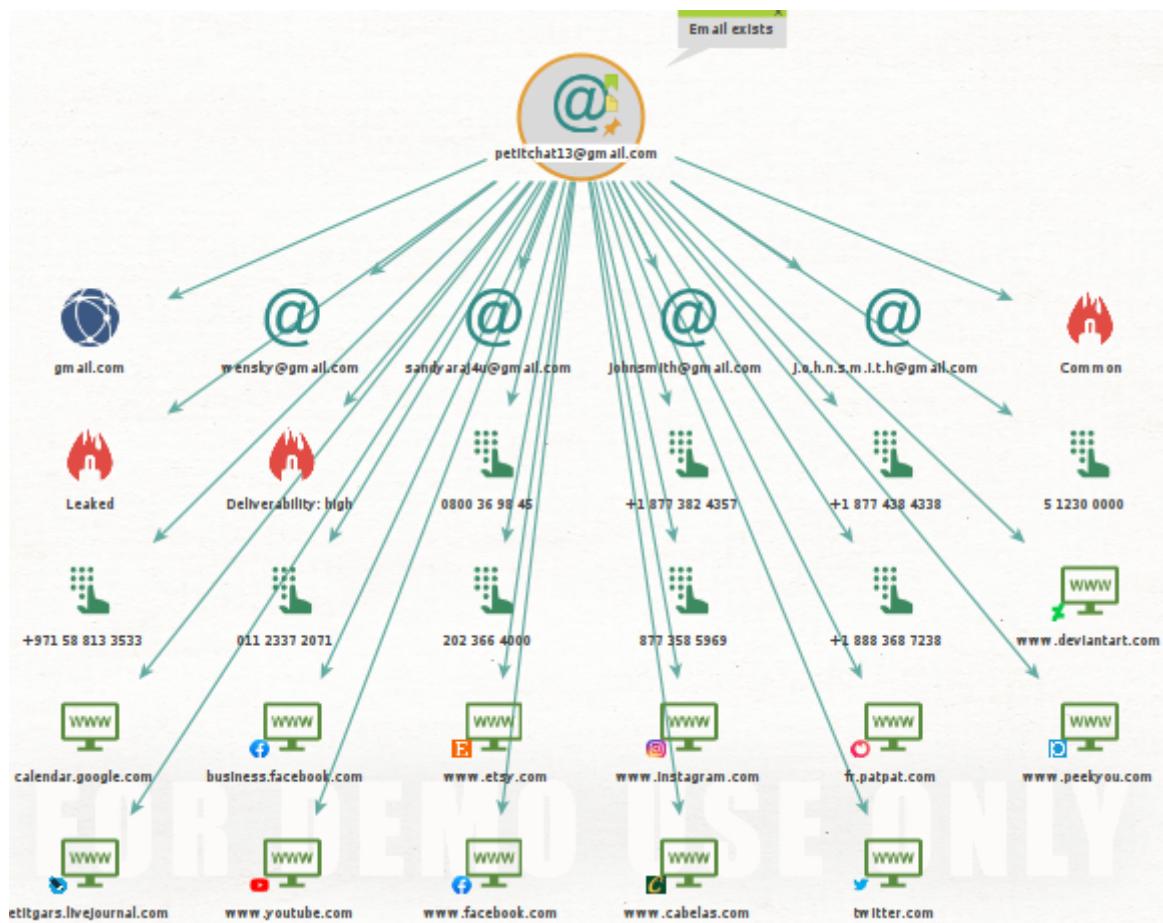
J'ai testé cette fonctionnalité avec 3 adresses emails différentes: celle de la HEIG-VD, mon adresse privée ainsi que mon adresse "poubelle".



Maltego confirme que mon adresse email existe. Il retrouve également le domaine de la HEIG-VD et il crée une entité personne en mon nom. *Deliverability: high* signifie que la capacité de l'email à atteindre la boîte de réception cette adresse email est haute.



Maltego confirme que mon adresse email existe. Il retrouve également le domaine de Gmail. Par contre, aucun de ces numéros ne m'appartiennent. Le fournisseur d'email est commun.

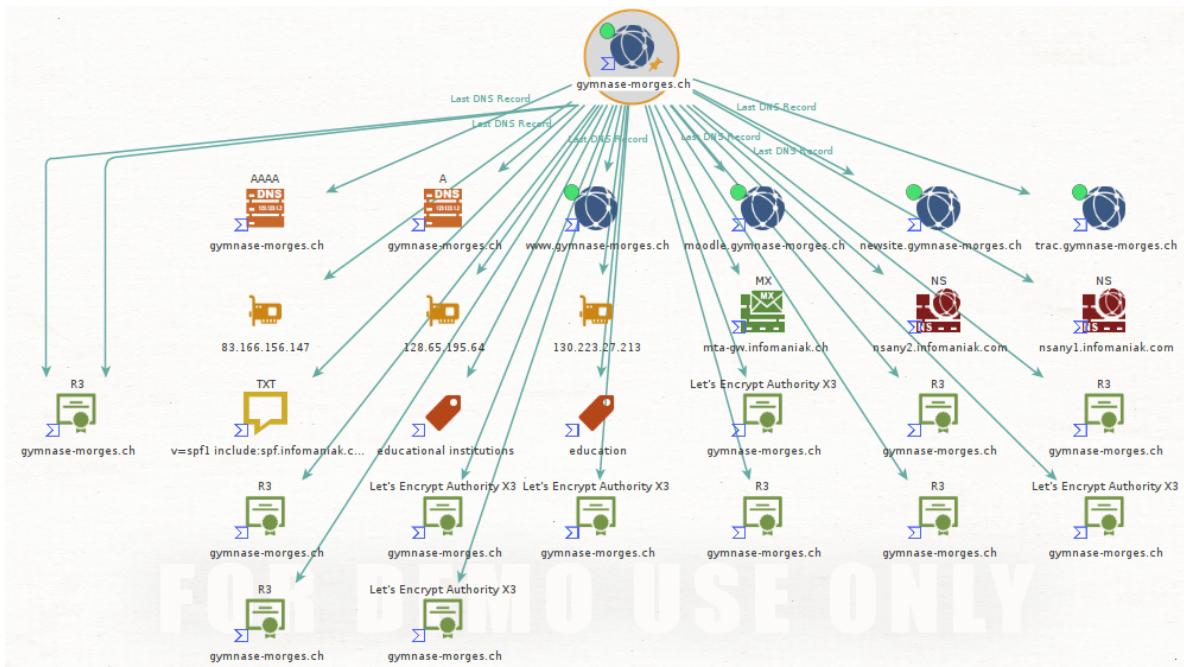


Maltego confirme que mon adresse email existe. Il retrouve également le domaine de Gmail. Concernant les numéros ainsi que les sites web, aucun ne me sont reliés. Nous voyons également que l'adresse email a été leaked. Cela ne m'étonne pas vraiment comme celle-ci est mon adresse "poubelle".

Installation et utilisation de nouvelles transformations

VirusTotal

L'exécution de VirusTotal s'est faite sur le domaine gymnase-morges.ch.



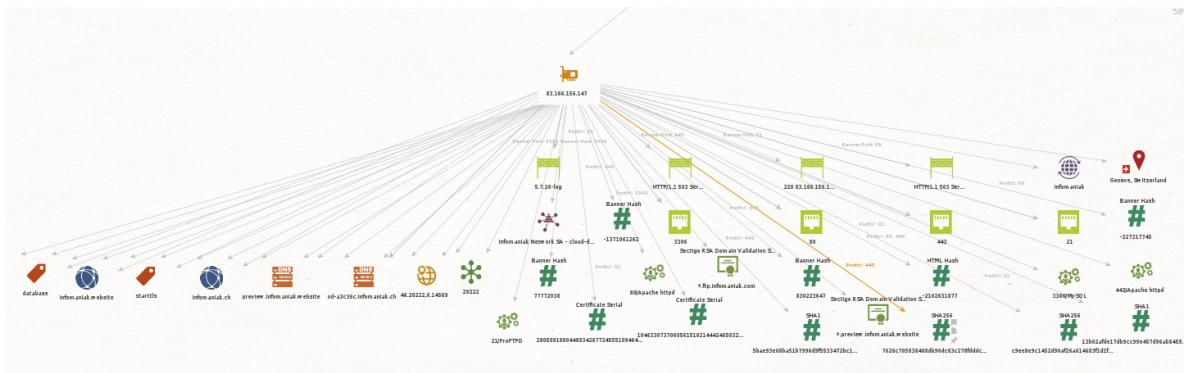
Maltego obtient de nouvelles informations comme les certificats TLS, d'autres serveurs DNS, MX Record, NS record, un txt et des catégories.

Les catégories représentent les catégories assignées à un domaine.

Les points verts au-dessus des différents domaines signifient que les résultats globaux de ceux-ci sont inoffensifs. Ils ne contiennent donc pas de malwares.

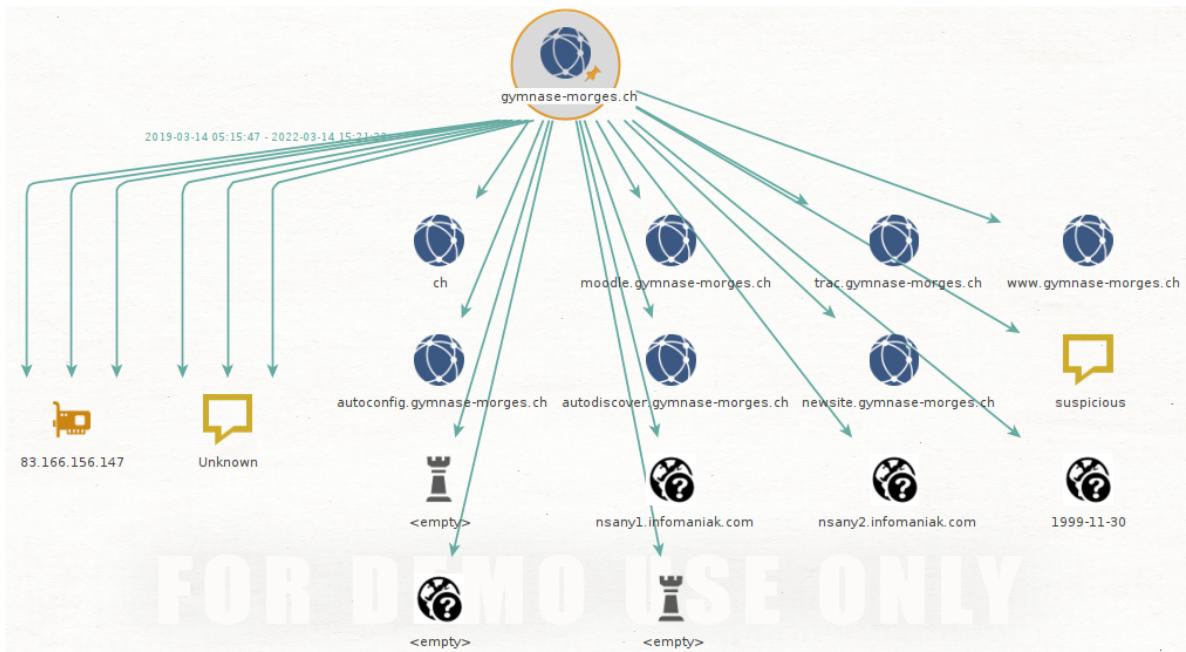
Shodan

Nous pouvons exécuter Shodan sur l'adresse IP trouvée précédemment:



Nous découvrons de nouvelles informations comme les tags (database et starttls), d'autres domaines, des DNS, des coordonnées GPS (pointant sur Genève), des bannières, un fournisseur d'accès internet (Infomaniak), une organisation (Infomaniak Network SA), des ports ouverts (3306, 80, 443 et 21), des services (MySQL, Apache httpd et ProFTPD), des certificats TLS et la localisation (Genève).

PassiveTotal



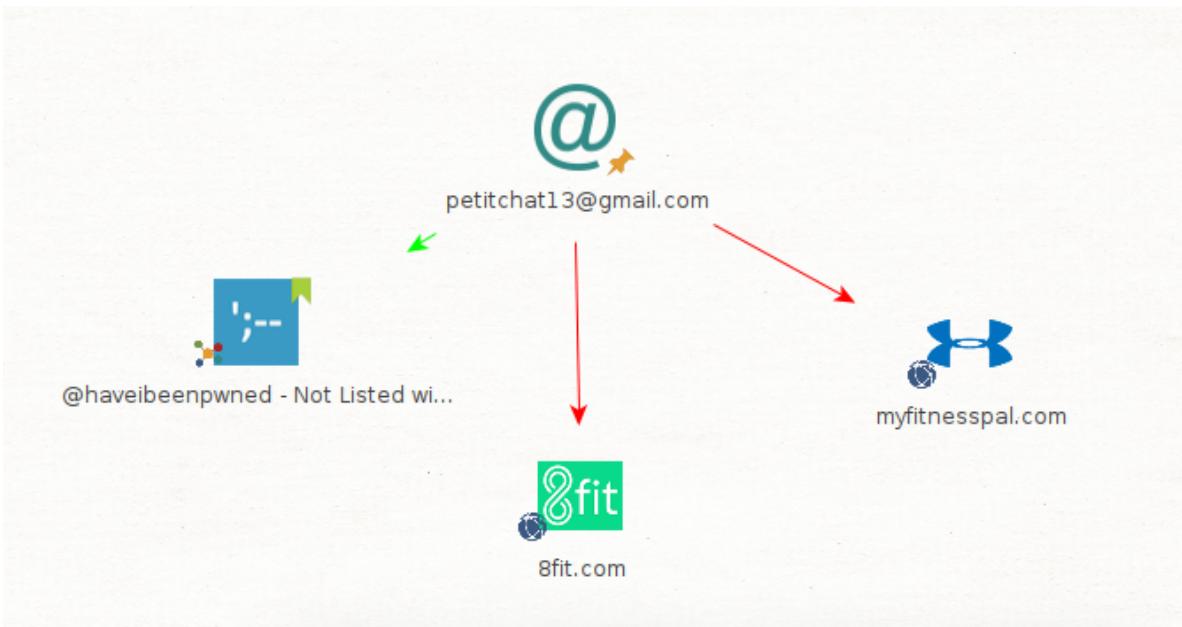
Nous découvrons de nouveaux sous-domaines, des phrases, une adresse IP, les nameservers, les registraires de nom de domaine et les expirations

Autres transformations

Dataprovider n'existe plus dans la liste des transformations.

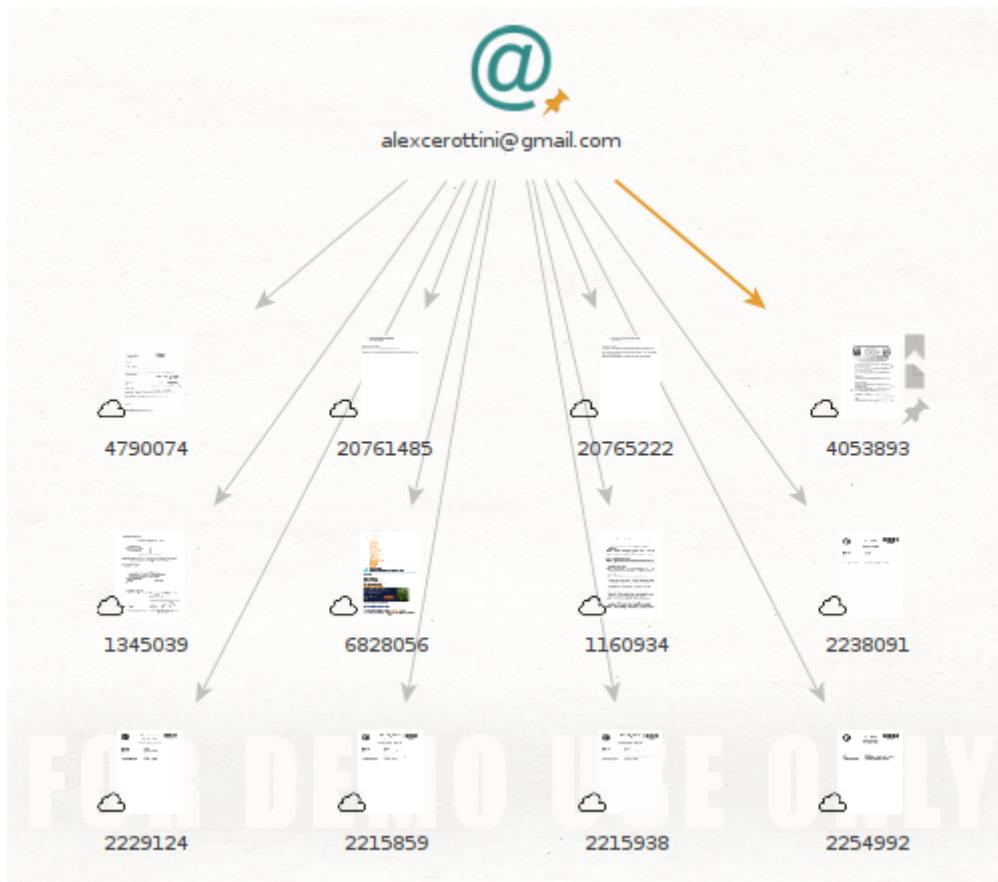
Transformations	Descriptions
Have I Been Pwned	Vérifie si des données personnelles ont été compromises suite à des violations de données.
Farsight DNSDB	Permet de contextualiser les informations DNS mais aussi exposer des noms de domaines, IPs, NX, MX, etc...
FullContact	Enrichir la recherche avec les adresses emails, les comptes Twitter, les domaines, les sociétés, les personnes et le numéro de téléphones.
Social Links CE	Recherche des données sur plusieurs sites (ZoomEye, Shodan, SecurityTrails, Censys, Rosette, Skype, Documentcloud) pour savoir s'il y a un compte associé à l'adresse email.
Wayback Machine	Permet d'avoir accès à des snapshot et contenu archivé du web
SSL Certificate Transforms	Permet de récupérer des informations sur les certificats TLS et potentiellement des activités malicieuses (par exemple: certificats issus de DNS compromis, de sous domaines abandonnés, d'une CA compromise...)

Have I Been Pwned



J'ai testé `Have I Been Pwned` sur mon adresse email qui a été identifiée comme leaked précédemment. Elle est bien associée à plusieurs sites ayant subi des fuites de données.

Social Links CE



Je n'ai pas obtenu de résultats pertinents avec `Social Links CE`. Il n'a retourné que des fichiers disponibles publiquement qui ne me sont aucunement reliés.