

# SEN: Laboratoire 1, Maltego

## Table des matières

### SEN: Laboratoire 1, Maltego

Table des matières

Reconnaissance du réseau

Première recherche

Analyse d'une personne du réseau

Recherche d'une personne

Via son nom

Via son adresse mail

Nouvelles transformations

Virus Total

Shodan

PassiveTotal

Test de transformations supplémentaires

Résumé des recherches

Scamadviser

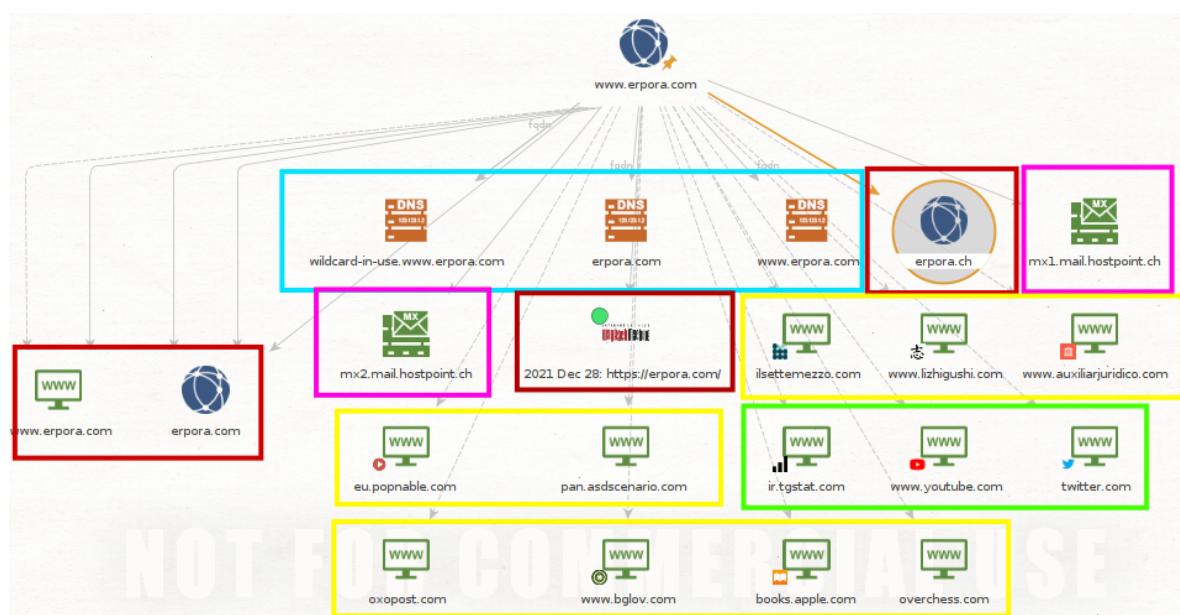
Have I Been pwned

Full contact

Résultat final de la recherche

## Reconnaissance du réseau

### Première recherche

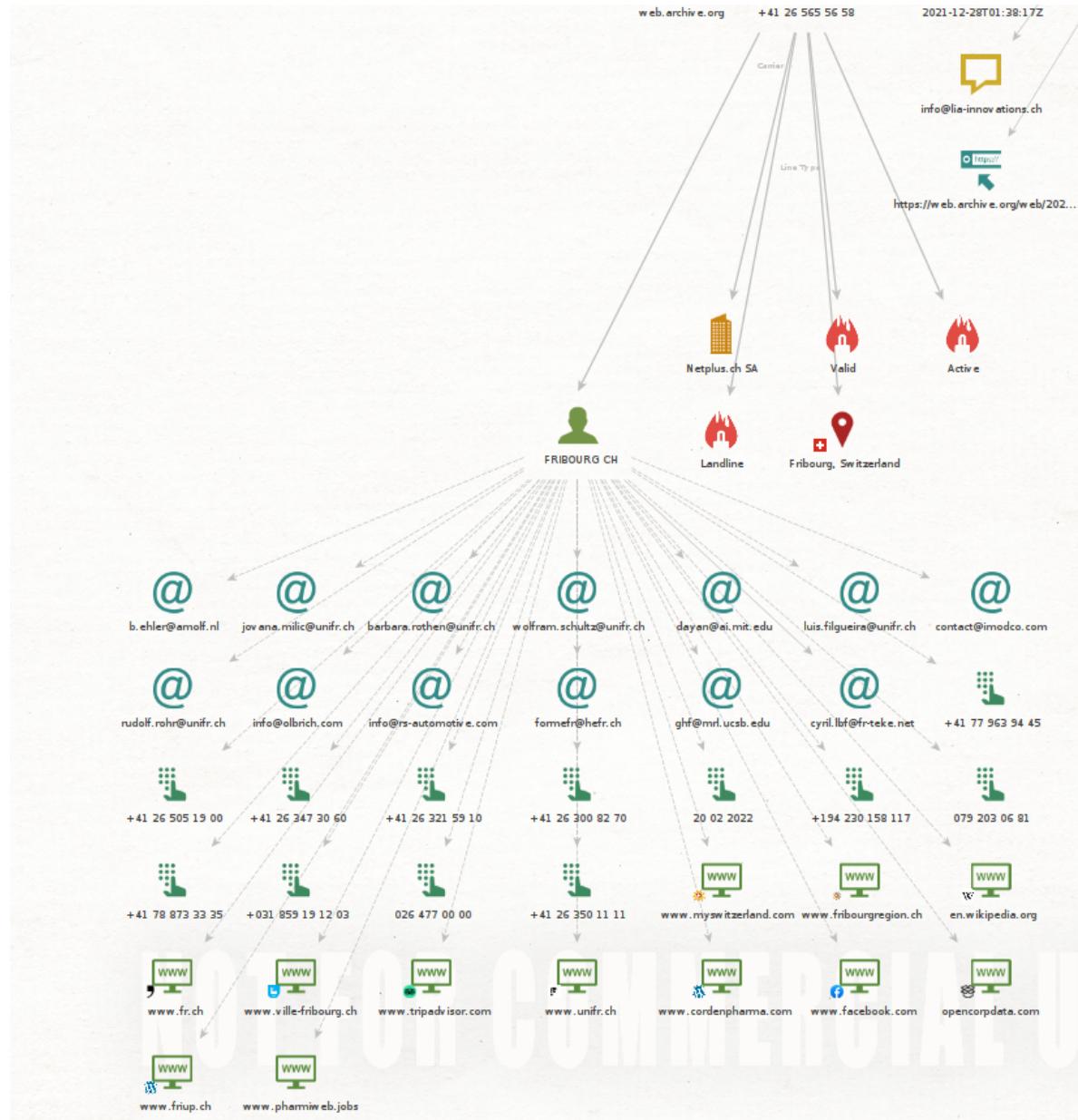


Voici ci-dessus le résultat de la reconnaissance du réseau. Les différents nœuds sont catégorisés par couleur.

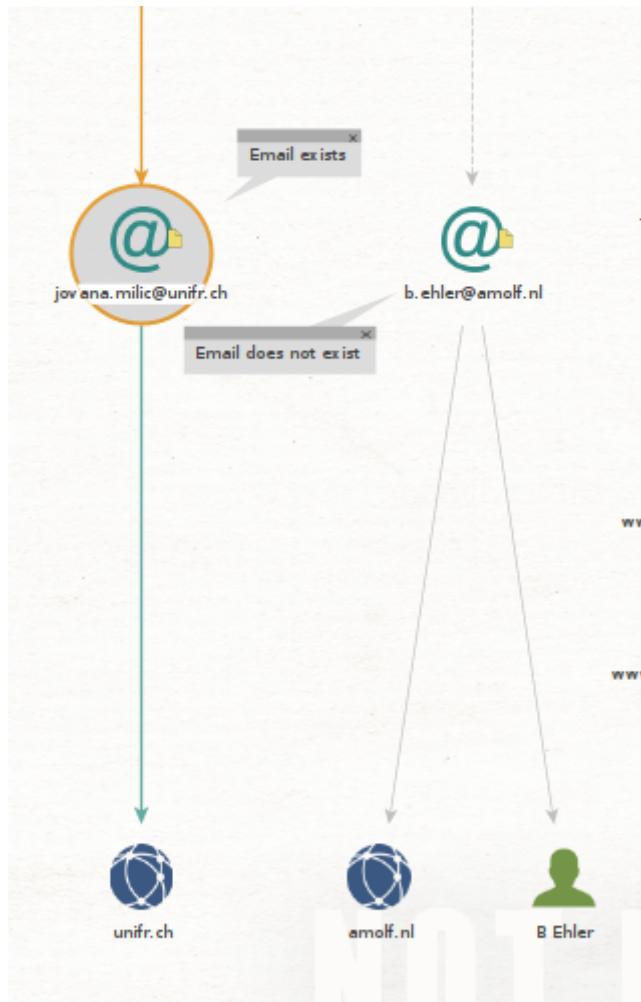
- **Bleu:** ce sont les serveurs DNS relatifs au site `erpora.com`

- **Rouge:** Ici ce sont les différents point d'accès à erpora, à savoir, erpora.com, [www.erpora.com](http://www.erpora.com), <https://erpora.com>, erpora.ch. Concernant ce dernier, ce n'est pas du tout la même plateforme que erpora.com, même si elle est hébergée sur le même serveur
- **Rose:** Les serveurs SMTP
- **Jaune:** Ce sont principalement des erreurs d'interprétation de l'outil. En effet, en se rendant sur les dits sites, on ne trouve aucun lien vers erpora, et inversement.
- **Vert:** Ici ce sont de simple liens vers les réseaux sociaux de la plateforme.

## Analyse d'une personne du réseau



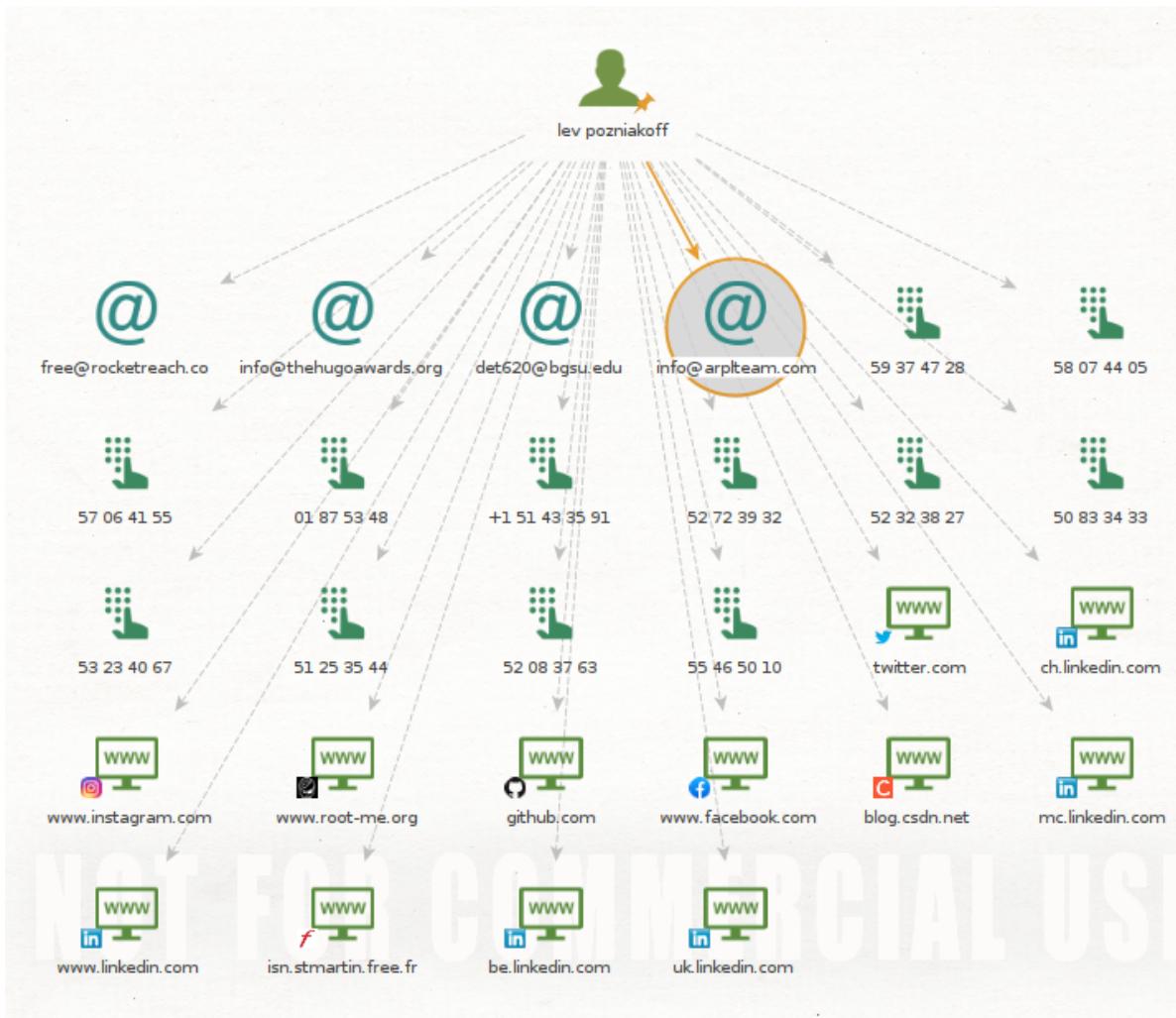
J'ai du creuser avant de trouver une identité. En l'occurrence FRIBOURG CH. Cette identité dérive d'un numéro de téléphone (page contact de l'application), il y a donc peu de chance que cette personne ait un quelconque lien avec erpora.com. Toutefois, nous utiliserons cela pour les besoins du laboratoire



En utilisant des transformations sur 2 personnes du réseaux, j'ai pu apprendre que l'une d'entre-elles avaient une adresse mail fonctionnelle alors que l'autre non.

## Recherche d'une personne

### Via son nom



J'ai fait une recherche avec mon identité, je n'ai toutefois trouvé aucune adresse mail m'appartenant. Toutefois, sur rocketreach.co, mon nom apparaît ainsi qu'un de mes postes dans une association. Ceci permet aisément de trouver l'adresse mail associé:

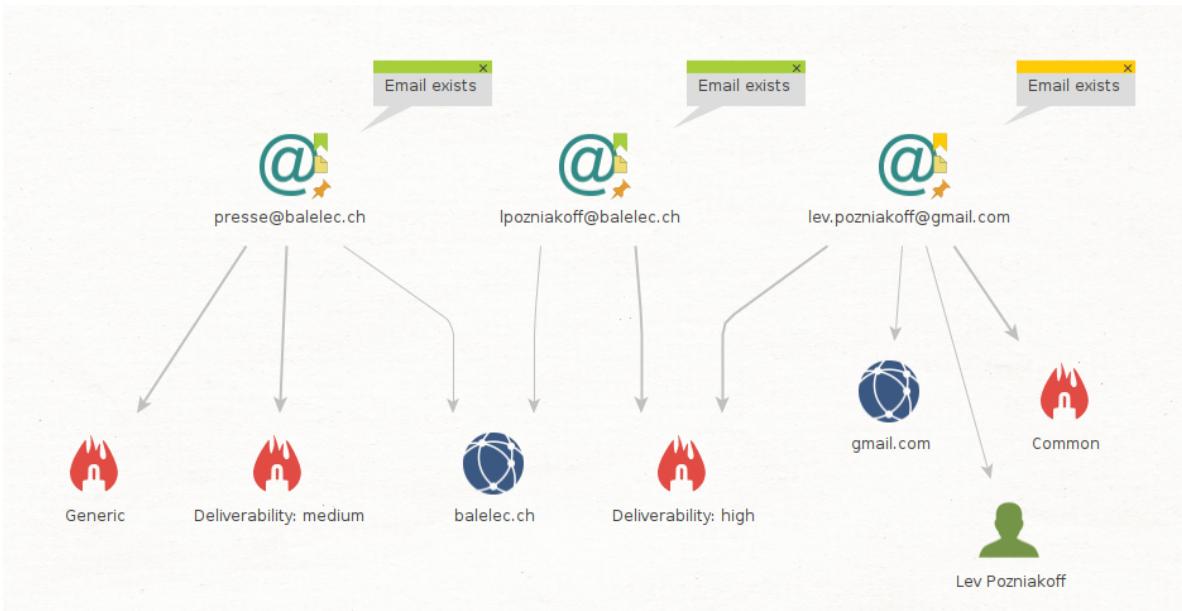
10 results found. <a href="#">Save this search</a>				
<input type="checkbox"/>	Name	Company	Location	Contact Info
<input type="checkbox"/>	Jean-Yves Gloor Attaché De Presse <a href="#">in</a>	Attaché De Presse	Lausanne, Vaud, Switzerland	<a href="#">jyg@terrasse.ch</a> <small>BEST PROFESSIONAL</small> <a href="#">+41 79 210 98 21</a> <small>1 more phone</small> <a href="#">Improve Results</a>
<hr/>				
Profiles like Jean-Yves Gloor				
<input type="checkbox"/>	Lev Pozniakoff Attaché De Presse <a href="#">in</a>	Festival Balelec	Lausanne, Vaud, Switzerland	No verified emails found <a href="#">Improve Results</a>
<hr/>				

Si je devais essayer de trouver, je ferais: lev.pozniakoff@festival-balelec.ch puis lev.pozniakoff@balelec.ch (bonne réponse). Il est donc assez facile de retrouver l'email.

J'ai pu également trouvé un traReconnaissance du réseau vaill que j'avais rendu il y a de cela plus de 7 ans dans mon lycée en France (lien isn.stmartin.free.fr). Prouvant que Maltego fais des associations qui peuvent être plutôt précises.

J'ai été confronté à plusieurs erreurs obscures qui, après recherches, semblent liées à un problème de licence expirées. Maltego manque en tout cas clairement de clarté sur son lancement d'erreur.

## Via son adresse mail



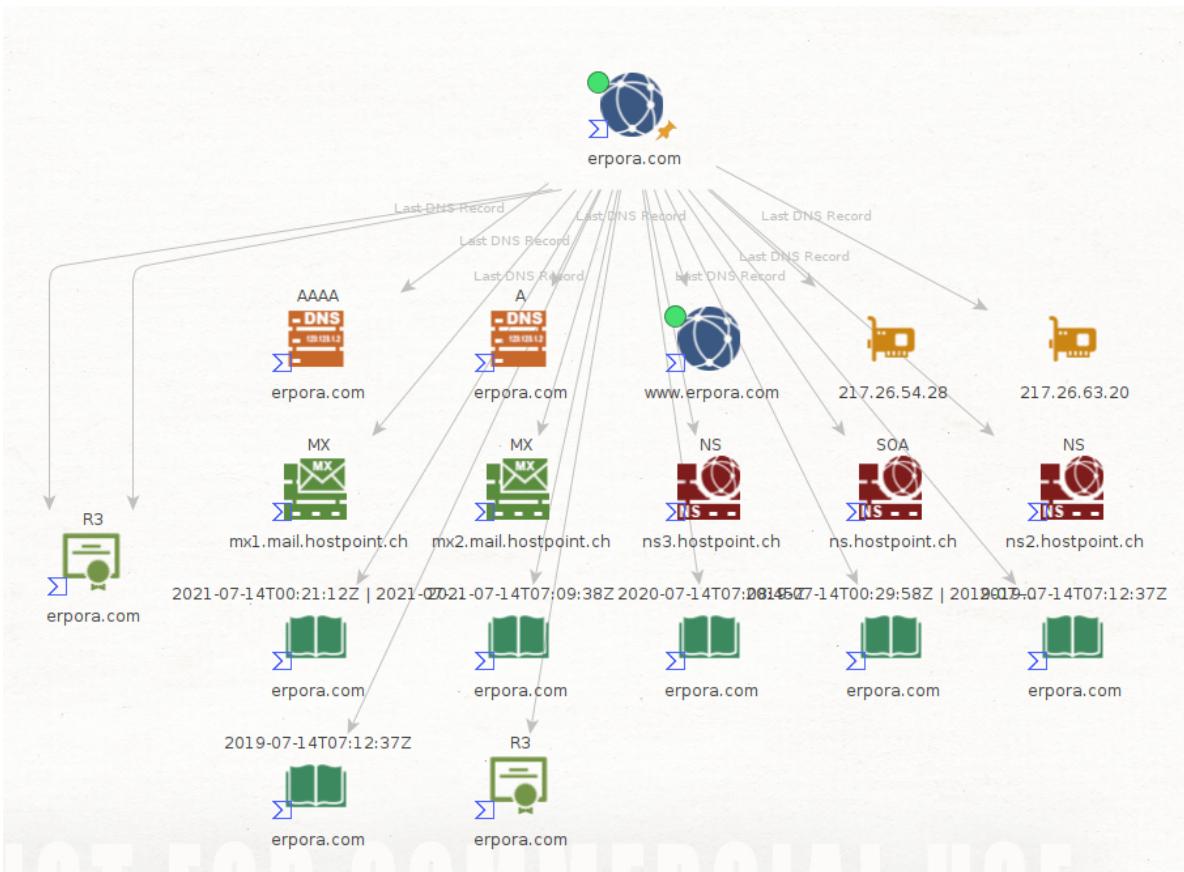
J'ai fait une recherche ici sur 3 adresses mail m'appartenant. Nous pouvons constater que la 3e nous permet de retomber sur mon nom qui donnerait exactement la même recherche que la partie précédente.

Les 2 premières m'ont en revanche permis de retomber sur le site [www.balelec.ch](http://www.balelec.ch) qui est l'organisation auxquelles sont rattachées les 2 premières adresse. Pour l'adresse presse@balelec.ch, maltego est même capable de reconnaître que celle-ci est un alias (mention de generic) indiquant ainsi que l'adresse est probablement plus une mailing list qu'une personne directement.

Les icônes rouge sont des tag IPQS indiquant la disponibilité du serveur mail. Nous pouvons voir que la réactivité dépend de l'adresse bien que les 2 adresses balélec dépendent du même serveur mail.

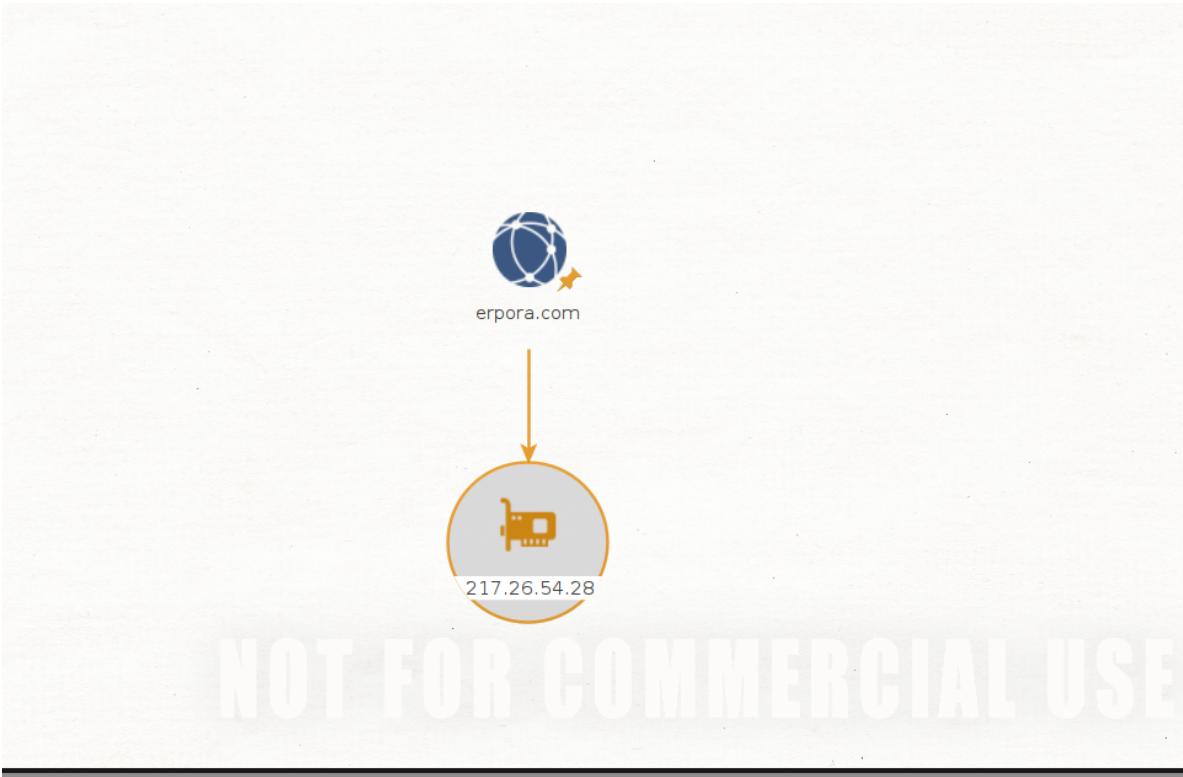
## Nouvelles transformations

### Virus Total



Le résultat de la recherche nous montre les certificats du site. Les icônes de livre indique le résultat d'un WHOIS. La pastille verte au dessus de `erpora.com` indique son score sur VirusTotal, à savoir 81/90, qui le catégorise en *harmless*.

## Shodan



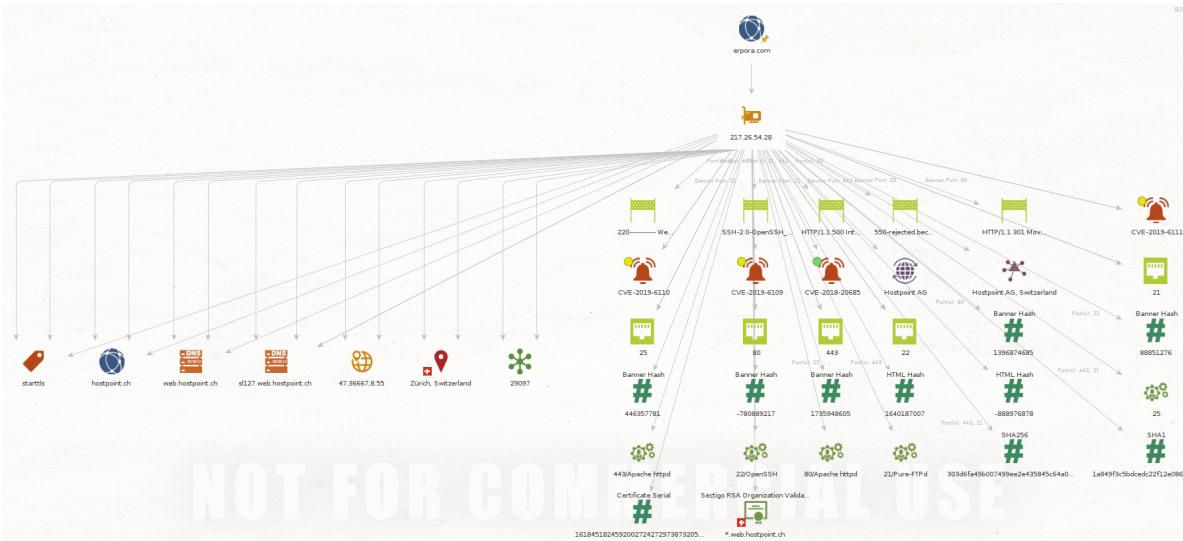
#### t - Transform Output

```

Transform To Tags [Shodan] done (from entity "erpora.com")
Transform To IP Addresses [Shodan] returned with 1 entities (from entity "erpora.com")
Transform To IP Addresses [Shodan] done (from entity "erpora.com")
[401] Insufficient query credits, please upgrade your API plan or wait for the monthly limit to reset (from entity "erpora.com")
Transform To Subdomains (+ Historical) [Shodan] returned with 0 entities (from entity "erpora.com")
Transform To Subdomains (+ Historical) [Shodan] done (from entity "erpora.com")
[401] Insufficient query credits, please upgrade your API plan or wait for the monthly limit to reset (from entity "erpora.com")
Transform To DNS Records [Shodan] returned with 0 entities (from entity "erpora.com")
Transform To DNS Records [Shodan] done (from entity "erpora.com")
[401] Please upgrade your API plan to use filters or paging (from entity "erpora.com")
Transform To IP Addresses on hostname [Shodan] returned with 0 entities (from entity "erpora.com")
Transform To IP Addresses on hostname [Shodan] done (from entity "erpora.com")

```

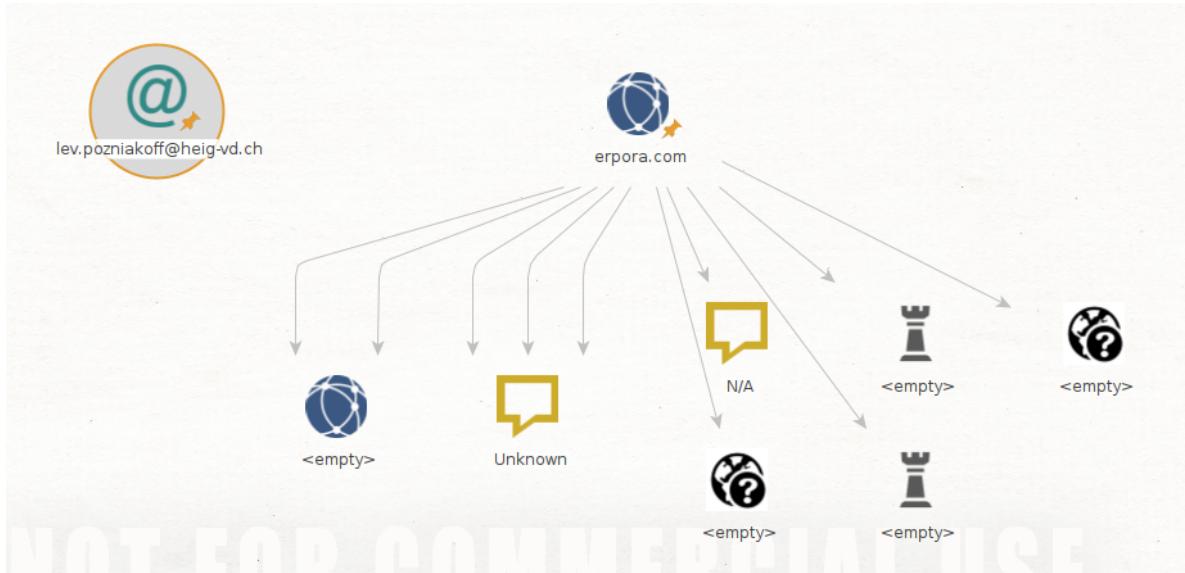
Nous pouvons voir que Shodan permet de trouver l'adresse IPv4 correspondante à erpora. Toutefois, nous pouvons aussi constater que la licence gratuite est très limité. J'ai ensuite refait un scan sur la dite adresse avec shodan et voici le résultat:



Nous y trouvons notamment des certificats SSL (les icônes #) mais aussi des codes http notamment des codes Apache httpd nous renseignant sur le serveur applicatif utilisé. Shodan réalise aussi un banner grabing et relève enfin des failles de sécurité répertoriées (icônes de cloche).

Les ports ouverts sont également affichés

# PassiveTotal



Passive total ne semble rien trouver de particulier. J'ai donc réessayé avec l'adresse mail aussi ce qui n'a rajouté aucun résultat supplémentaire.

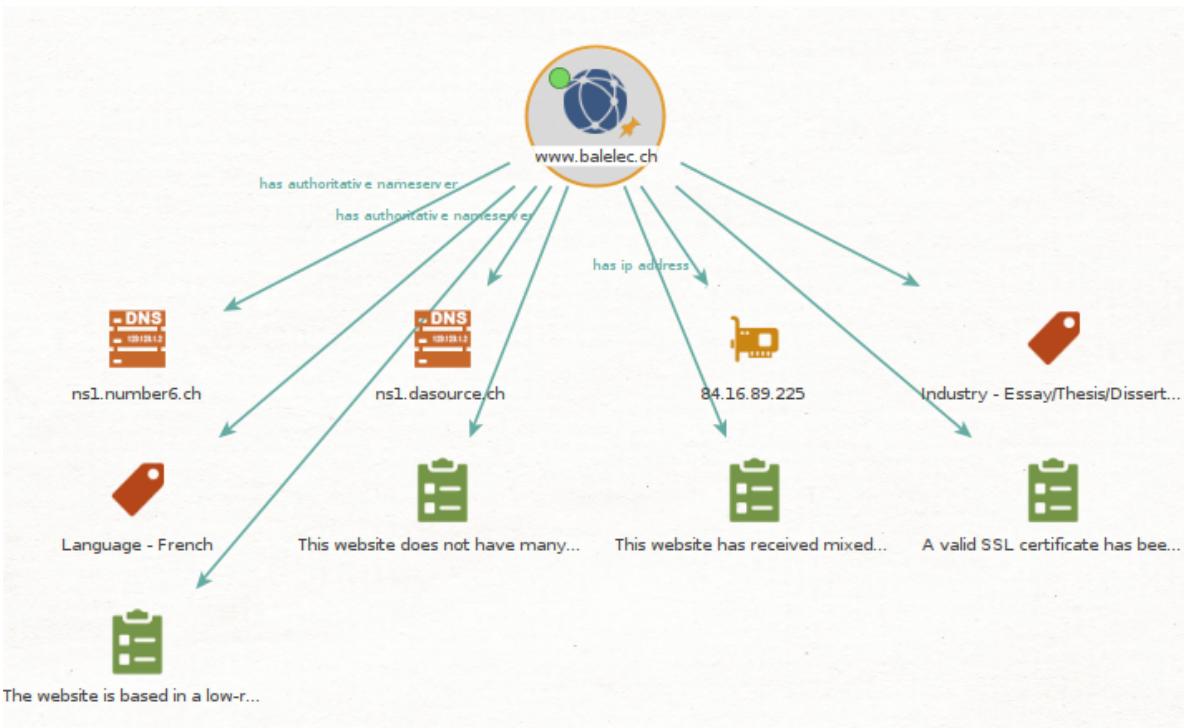
## Test de transformations supplémentaires

### Résumé des recherches

Je n'ai pas trouvé dataprovider alors j'en ai essayé une autre à savoir: scamadviser

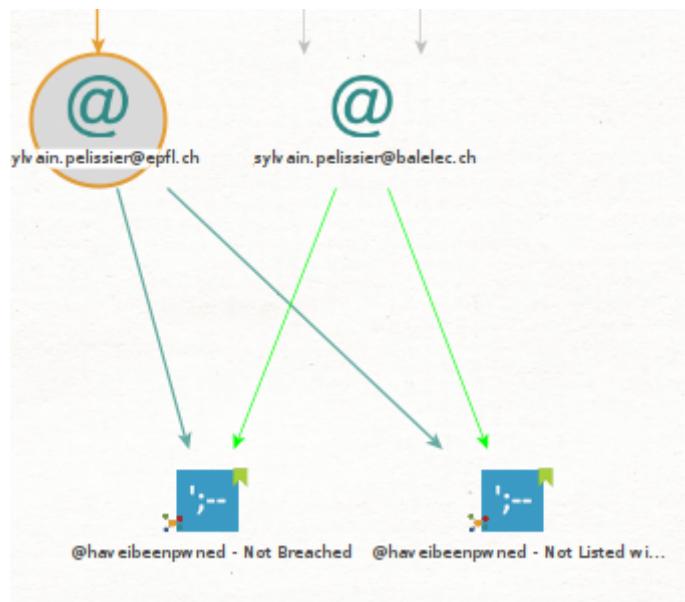
Transformation	Fonction
Have I been Pwned ?	Vérifie que l'information testée (no téléphone, mail, mot de passe) n'a pas été rendu publique.
Scamadviser	Vérifie qu'un site n'est pas frauduleux (scam, phishing)
Farsight DNSDB	Enrichi le résultat de la recherche grâce à une base de données DNS
FullContact	Enrichi la recherche avec des adresses mails, no de téléphone, liens vers les réseaux sociaux, etc ...

### Scamadviser



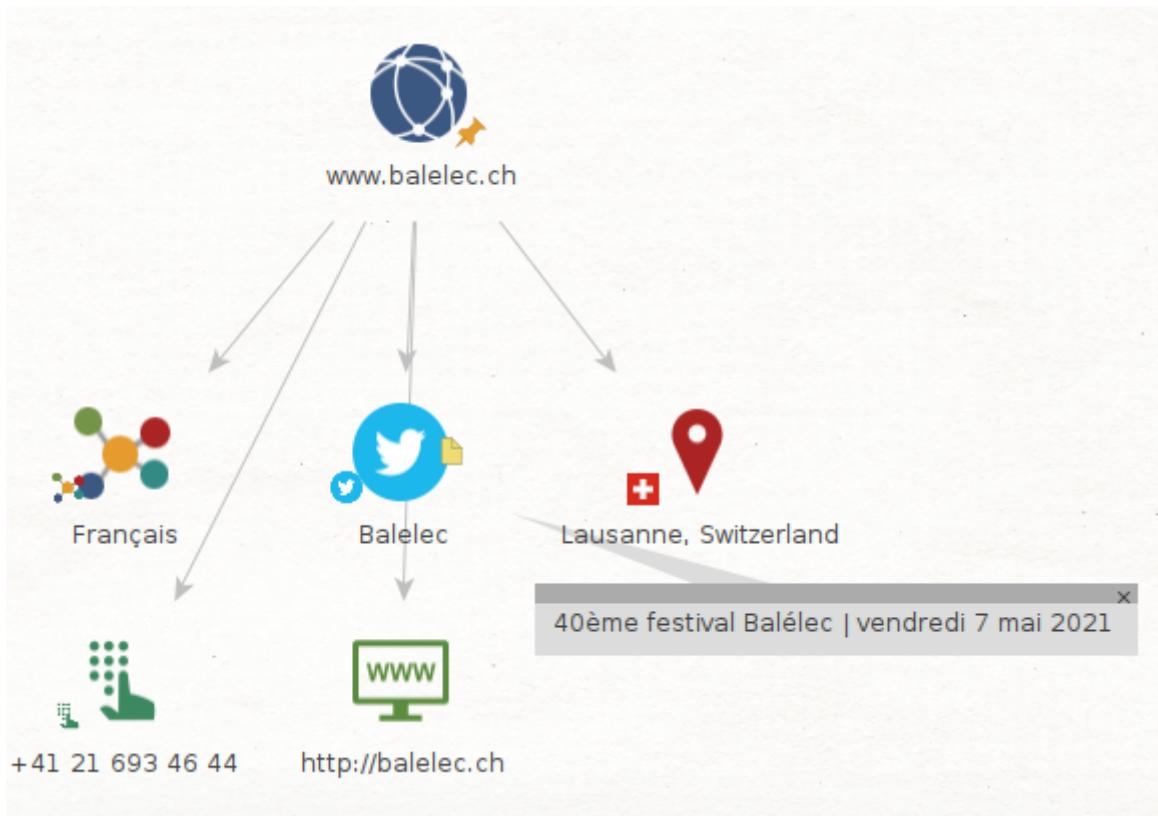
Voici le résultat de la transformation scam adviser indiquant que le site en question n'est pas une escroquerie.

## Have I Been pwned



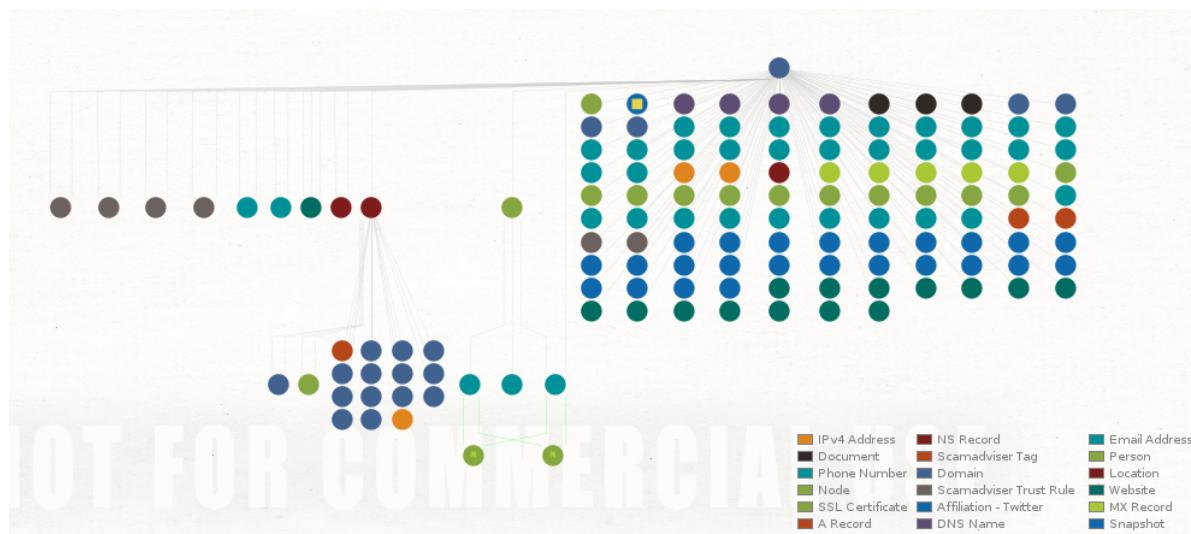
Voici le résultat de have I been pwned sur une des adresses trouvées lors de la recherche nous indiquant que celle-ci n'a pas été rendu publique.

## Full contact



Voici le résultat de full contact. Certaines informations sont dépréciées (date du festival), le site n'a pas dû être mis à jour.

## Résultat final de la recherche



Comme vous pouvez le constater, la recherche a donné des résultats conséquents. Le problème de ces résultats, est, à mon sens, qu'il ne peuvent pas être triés par transformation, rendant le filtrage de l'information très complexe. De plus, certains résultats n'ont strictement aucun rapport avec le site originel. Maltego a tendance à faire des liens qui sont parfois obscures.

Ajouté à cela, le logiciel est soumis à de **très** nombreuses licences (une par transformation), et les erreurs générées en cas d'invalidité sont excessivement obscures et ne permettent pas un debugage efficace. Ceci est probablement dû au fait que maltego fait des requêtes sur des API (probablement REST) et qu'il ne gère pas les erreurs.

Enfin, je dirais que les transformations de base de maltego peuvent être réalisées à la main (recherche google, whois, etc...) très facilement et l'outil basique n'apporte pas grand chose à ce niveau.

