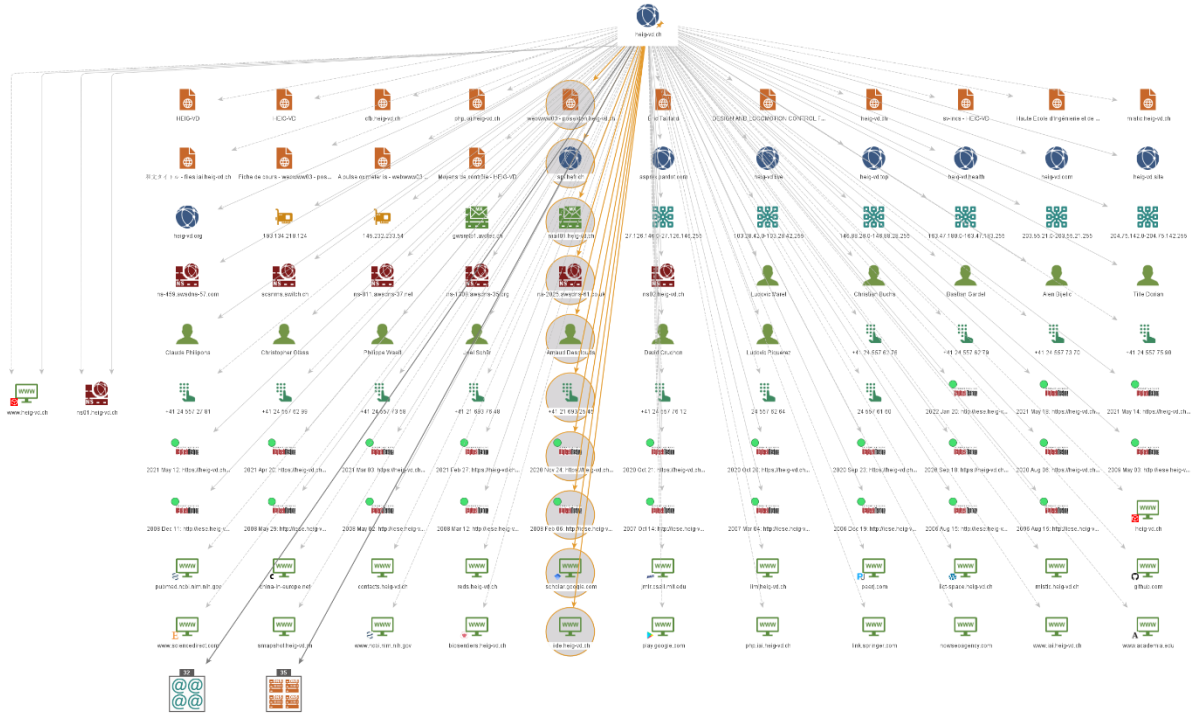
SEN – Laboratoire Maltego

Guillaume Laubscher

Table des matières

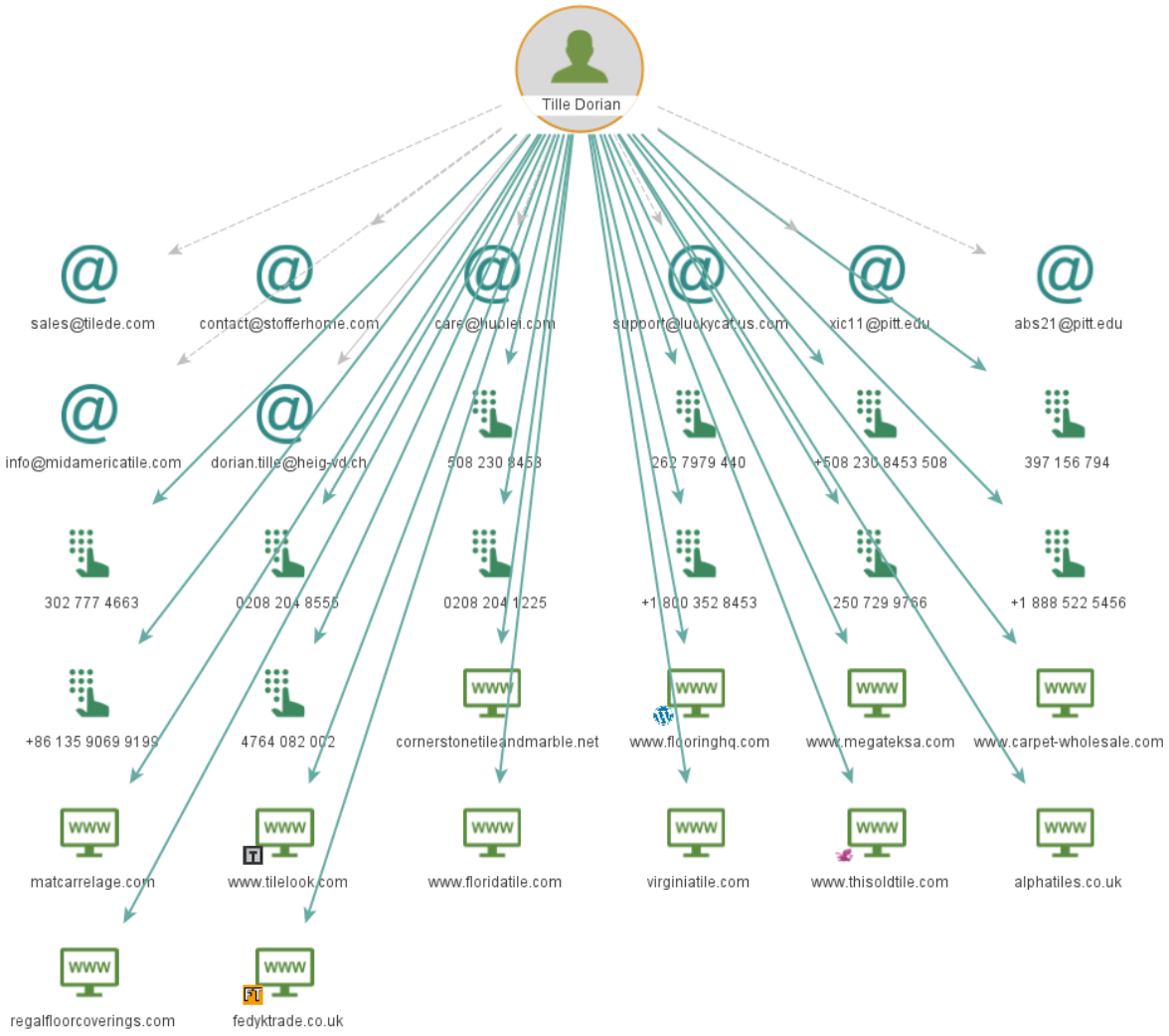
Une simple reconnaissance de réseau



En appliquant toutes les transformations disponibles de bases sur le domaine heig-vd.ch, voici les éléments qui ont été retournés :

- Des fichiers de différents types (docx, exe, mp3)
- Différents noms de domaines
- Des serveurs d'emails
- Des clef publiques PGP
- Des numéros de téléphone
- Une liste de DNS
- Une liste d'adresses emails
- Des listes d'adresses IP

La quantité d'informations retournées est assez importante, cela pourrait permettre une première analyse du domaine avec des points d'attaques.

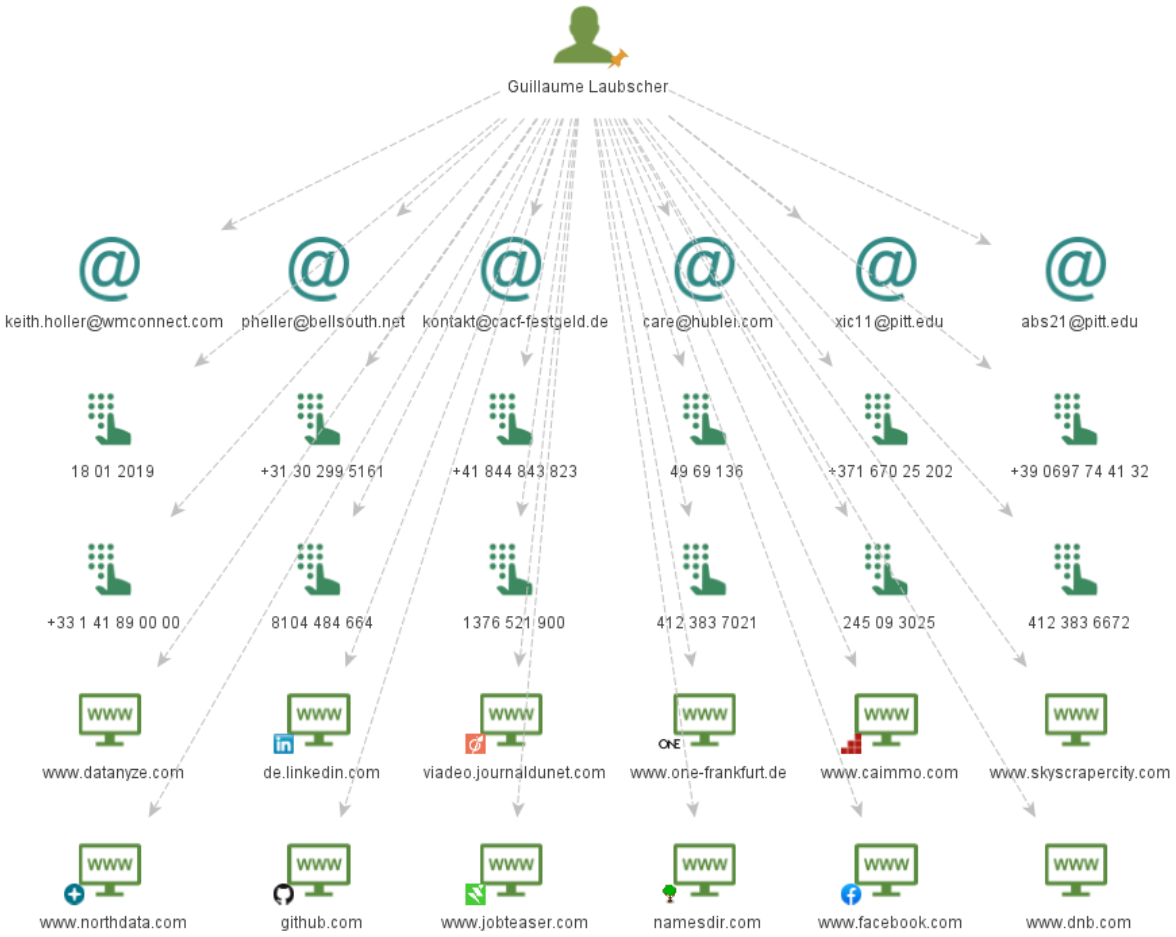


En appliquant toutes les transformations sur la personne de Tille Dorian, voici les différents éléments retournés :

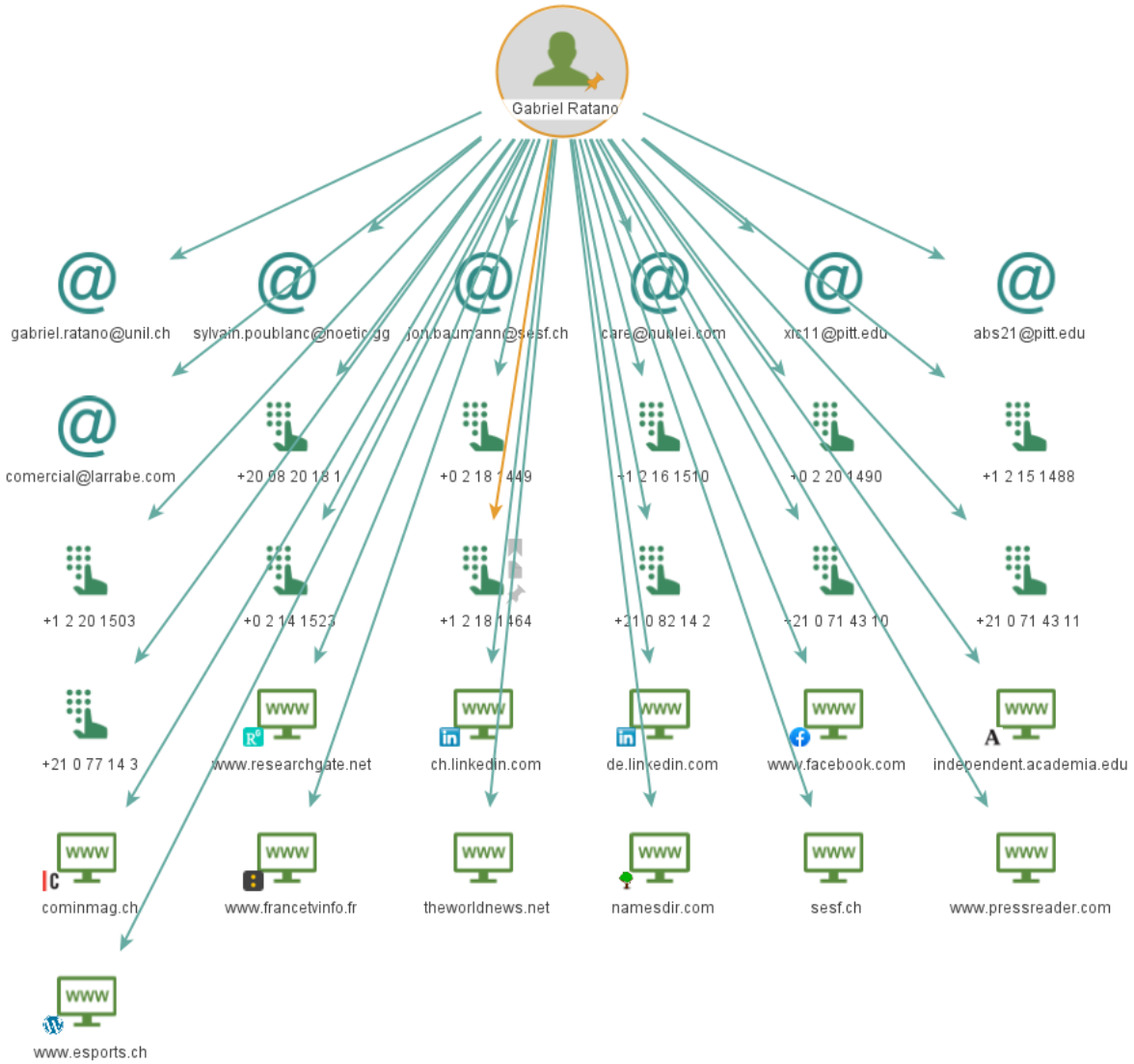
- Des adresses emails
- Des numéros de téléphones
- Des sites web

En ce qui concernes les numéros de téléphones, il est peu probable qu'ils appartiennent à cette personne parce que la plupart d'entre eux ne sont pas des numéros de particuliers.

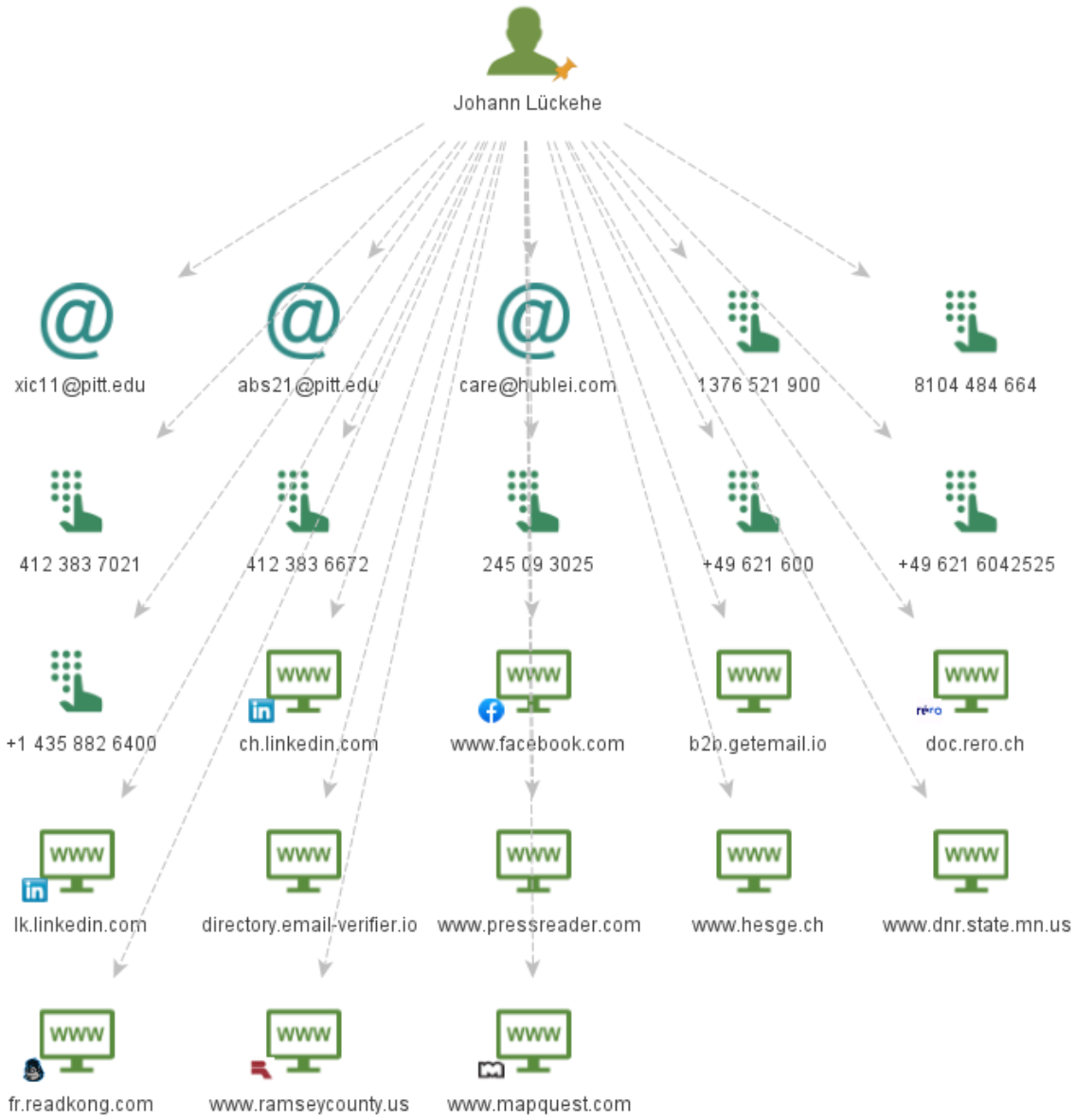
Recherche d'une identité



Lorsque je lance toutes les transformations sur ma personne, aucune des informations ne se trouve être exacte sauf une : GitHub. Le lien vers le site GitHub est effectivement un projet dans lequel j'ai participé et où mon nom apparait.

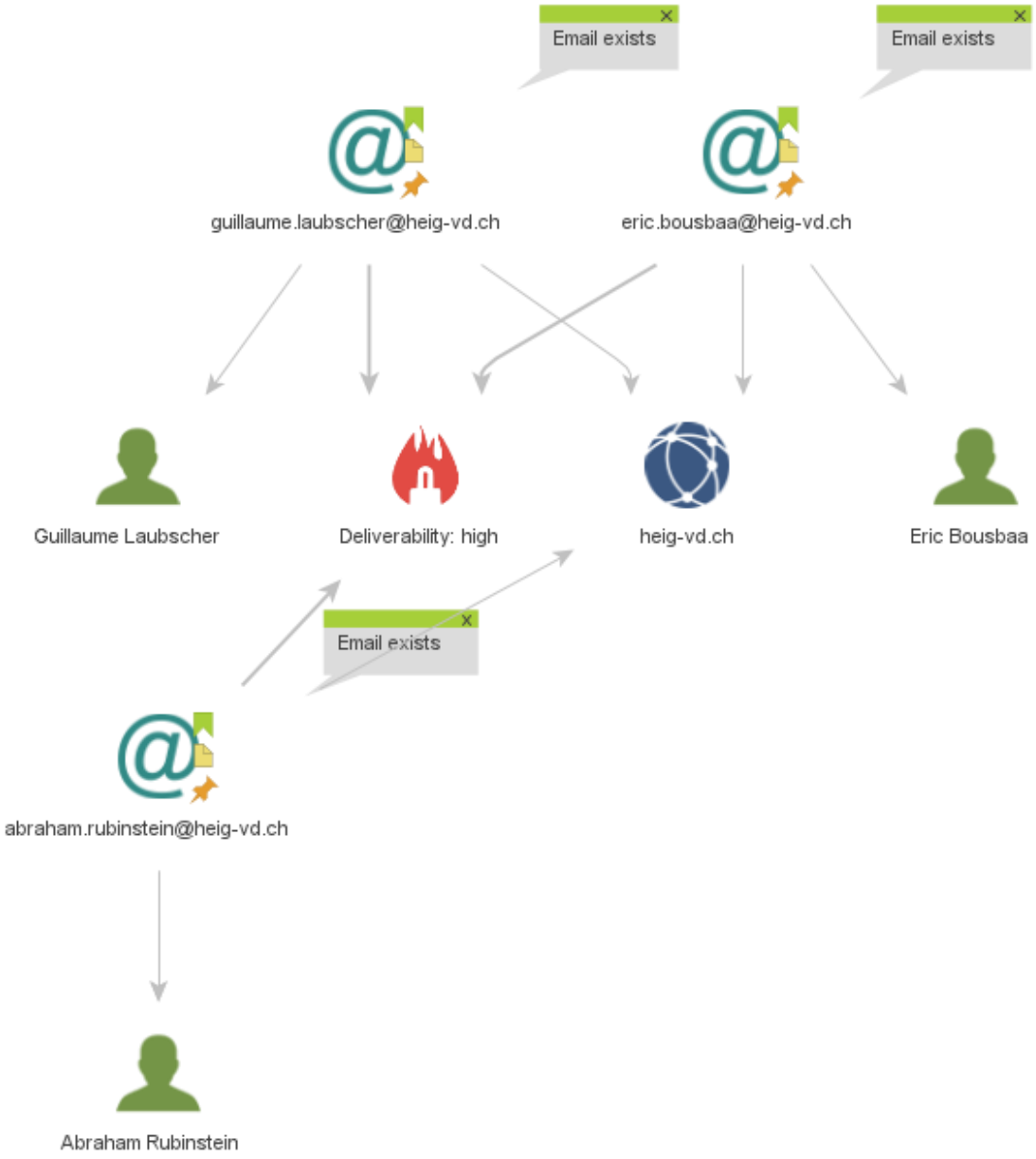


La recherche sur un de mes amis donne des résultats plus intéressants. On y trouve une adresse email qui lui appartient bien ainsi que des références à son nom sur plusieurs page web qui sont soit de lui soit qui parle de lui.



Pour un autre de mes amis, seul certaines mentions de lui peuvent être trouvées sur les pages web retournées tendis que le reste des informations ne sont pas en lien avec lui.

Recherche d'une adresse email

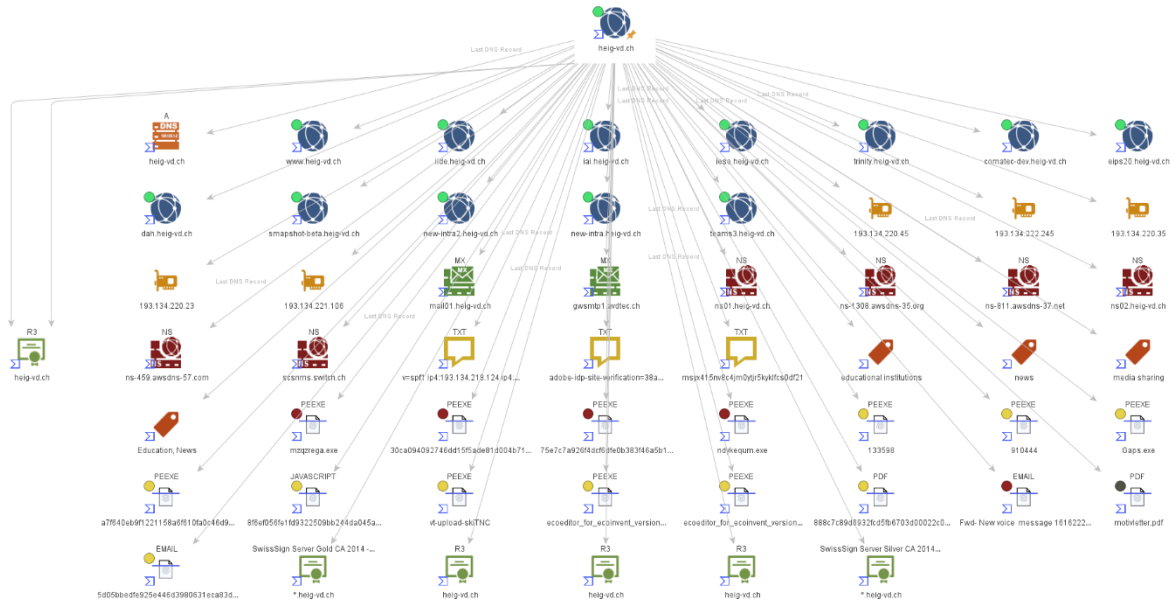


J'ai essayé d'effectuer des recherches sur trois adresses emails appartenant à la heig mais je n'ai quasiment rien trouvé comme informations. La seule information potentiellement intéressante est qu'il indique que les adresses emails existes ce qui pourrait être utile pour rechercher un email d'une personnes à cibler.

Installation et utilisation de nouvelles transformations

En effectuant à nouveau de nouvelles transformations sur le domaine heig-vd.ch, voici les résultats supplémentaires obtenus séparés par API.

VirusTotal



En effectuant la recherche avec VirusTotal, on trouve de nouveaux éléments :

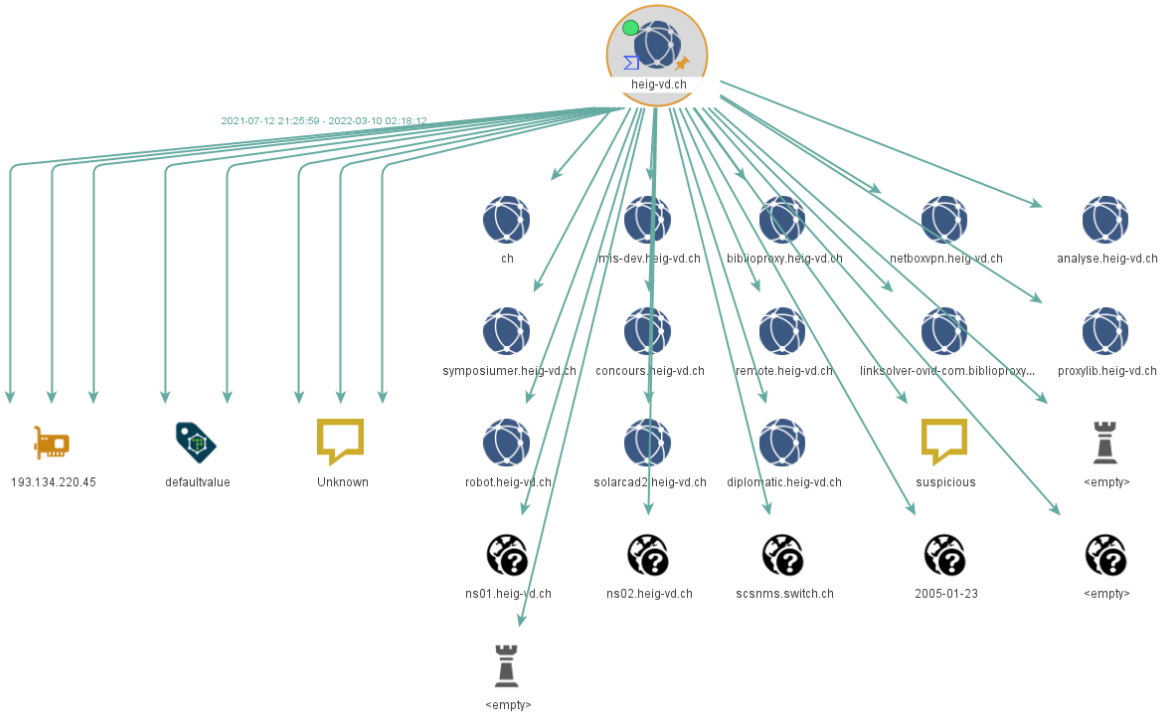
- Des adresses IP (et non des plages d'IP)
- Des fichiers txt, exe, JS et PDF
- Des certificats d'authentification SSL

Ces informations peuvent être extrêmement utiles notamment en ce qui concerne la meilleure recherche des fichiers sur le réseau. Cela pourrait permettre de trouver des points d'attaques en supposant des utilisateurs peut avisés.

Shodan

Shodan ne ressort qu'une IP et rien d'autres.

PassiveTotal



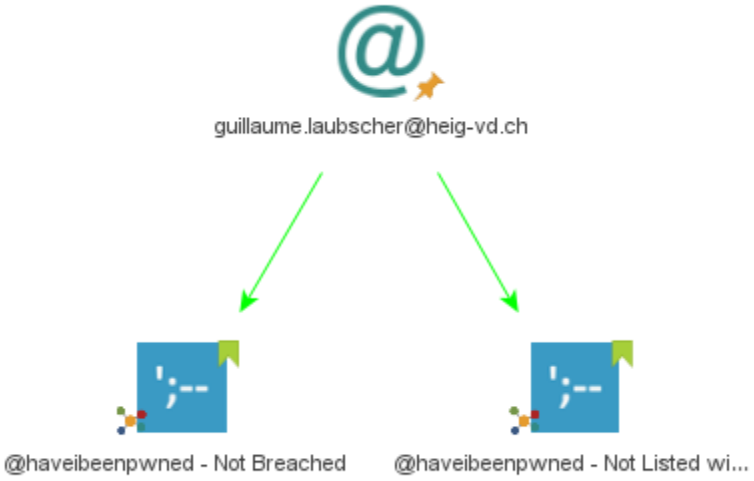
PassiveTotal trouve certains détenteurs des noms de domaines liés à la heig et d'autres liens sur d'autres sites possédés par la heig. Il retourne aussi certains éléments qui n'ont aucune propriété et je n'ai pas d'explication à cela.

Autres transformations

Ci-dessous, un tableau indiquant ce que les nouvelles transformations retournent :

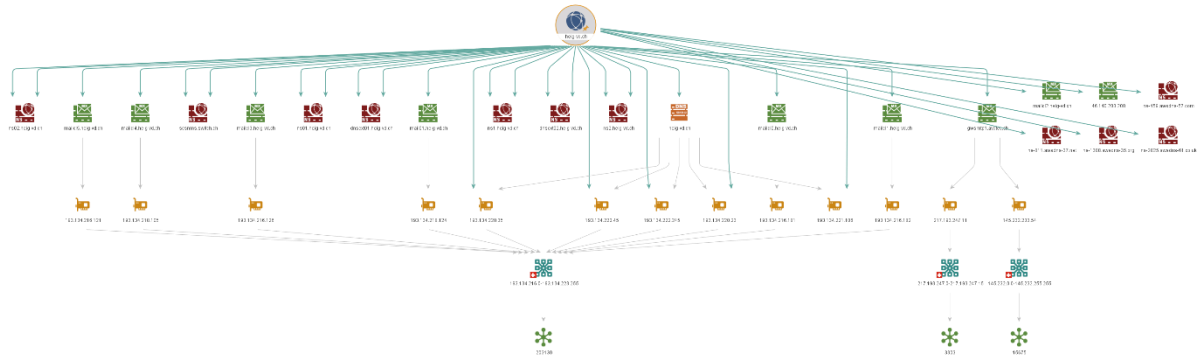
Transformation	Eléments retournés
Have I Been Pwned ?	Indique si les emails ont eu ou non une association avec leur mot de passe spécifique ou non.
Farsight DNSB	Analyse les différentes données liées à un DNS comme les domaines, les IPs, et les éléments suivants : NX, MX, AAAA, SOA
Scamadviser	Scan un nom de domaine pour y chercher des virus, des redirections douteuses et tout autres éléments indiquant une utilisation frauduleuse du domaine.

Have I Been Pwned ?



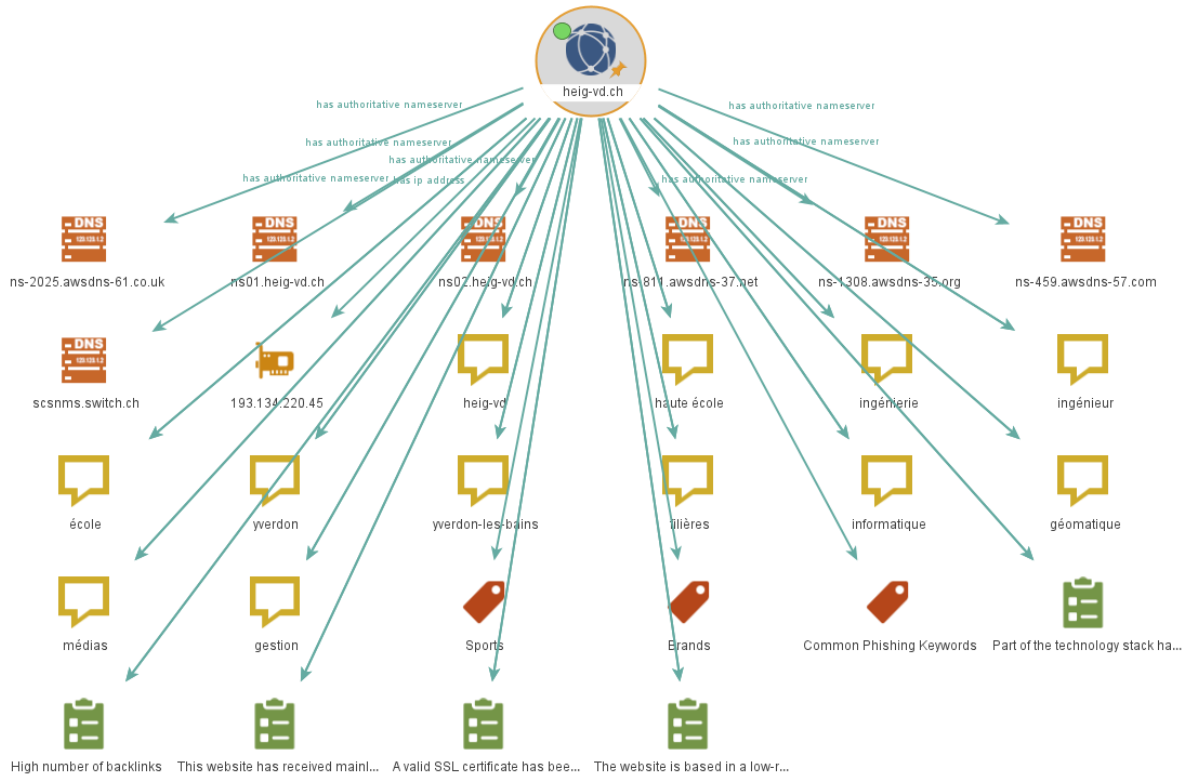
Les informations retournées sont assez simples à analyser et nous permets de savoir si nos informations ont fuité ou non.

Farsight DNSB



La quantité d'informations est importantes mais permet une bonne visualisation de ce qui se trouve dans le domaine heig-vd.ch.

Scamadviser



Une bonne quantité d'informations sont retournée mais dans l'ensemble on peut facilement analyser les différents éléments fournis. On y retrouve notamment les mots clef qui ressortes souvent dans les sites du domaine ainsi qu'une analyse des certificats SSL.