

CONTENTS

Un test simple sur le domaine d'un projet de groupe	2
Un domaine un peu plus professionnel Gammadia	3
Recherche d'une identité Bastien potet	4
Transformation additionnelles Gammadia	5
Virus total	5
passive total	7
Shodan	7
Transformation supplémentaires	8
Have i been powned	8
Social links	8
Les différentes informations apportées par maltégo(Transformations standard)	9
Conclusion	9

SEN LABO 1: MALTEGO

UN TEST SIMPLE SUR LE DOMAINE D'UN PROJET DE GROUPE

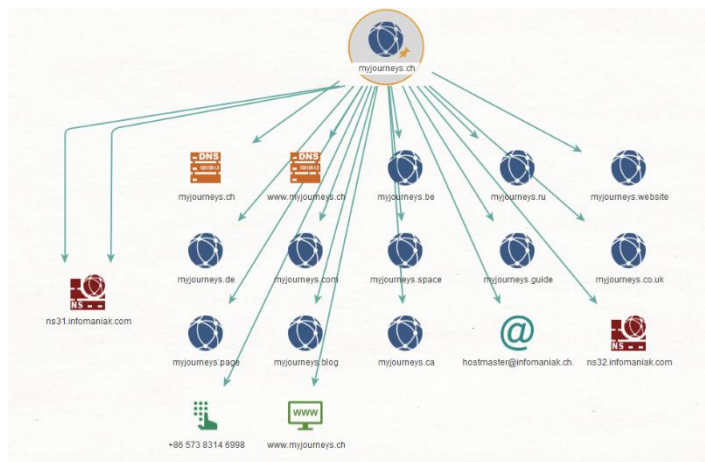
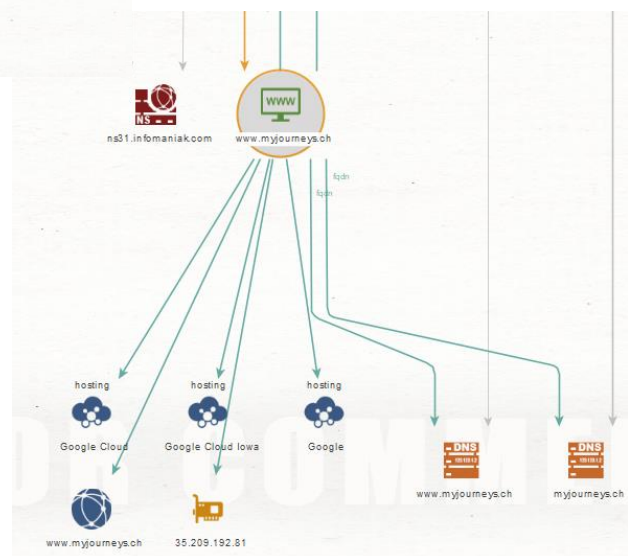


Figure 1 journeys basic CE Transforms

Bien que simple notre domaine qu'on a mis en place pour notre projet de groupe montre des données intéressante relevant les serveurs DNS utilisé et chez qui on a acheté notre nom de domaine. Ainsi que divers nom de domaine potentiellement lié à notre cible

En allant plus loin on peut retrouver que notre site web est en effet déployé sur la plateforme de google cloud, l'adresse IP donnée correspond effectivement à l'IP assigné à notre load balancer.



En inspectant cette adresse IP on peut encore trouve plus d'information tel que la localisation (Pays) il est hébergé

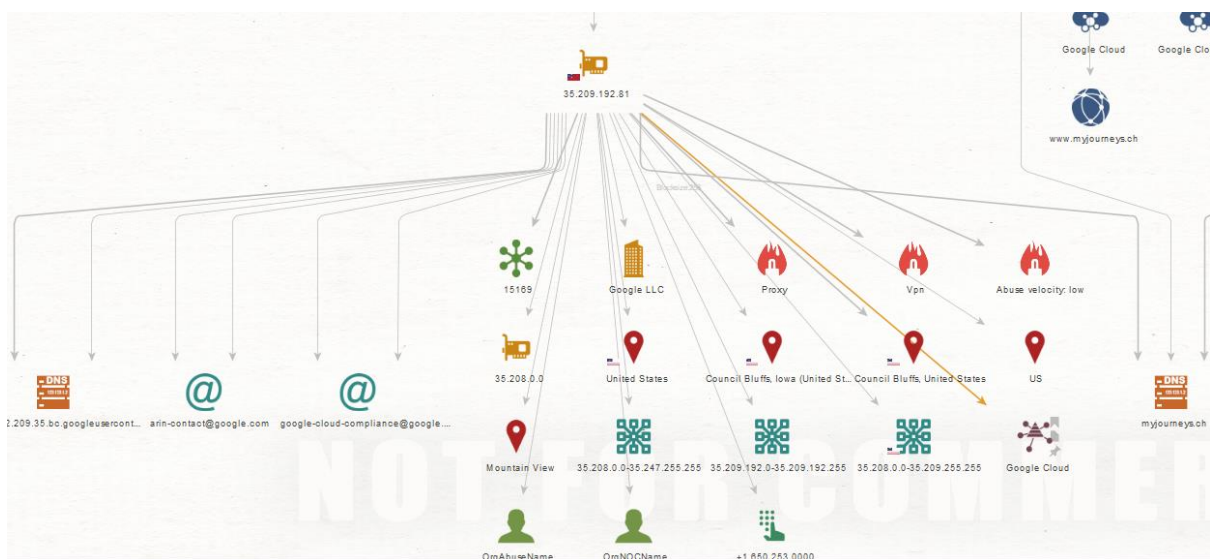
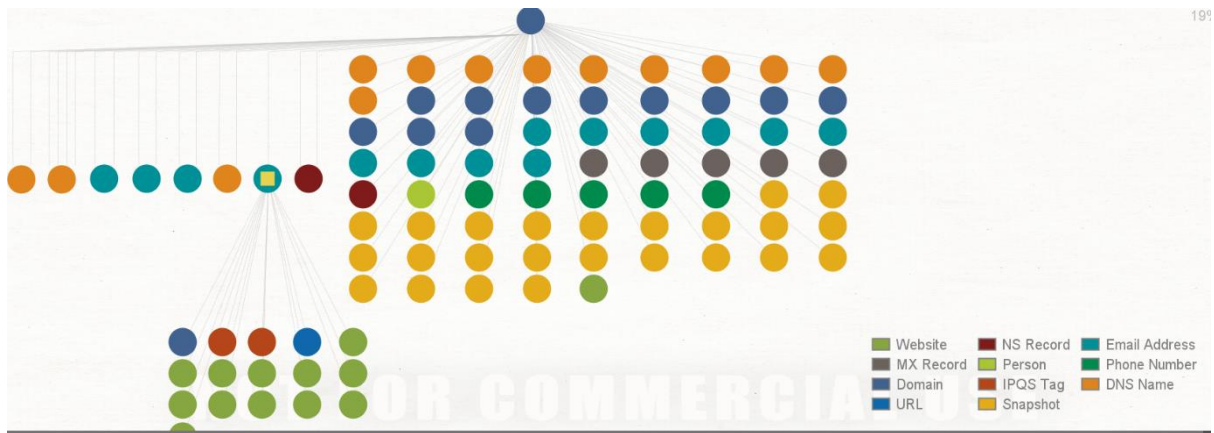


Figure 2 gcp

UN DOMAINE UN PEU PLUS PROFESSIONNEL GAMMADIA



Gammadia est une entreprise ou un amis à été engagé cette année, elle mes en avances divers solution informatique tel que tipeg. Cette information est récupérée après les transformation basique et on obtient une adresse email liée à ce produit(Figure 3 tipeg).

On peut également trouver un grand nombre de backup/snapshot du site web ainsi que des numéros de téléphones et d'autres informations diverses.

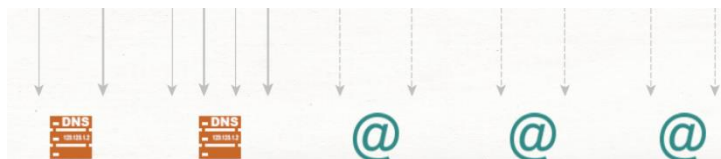
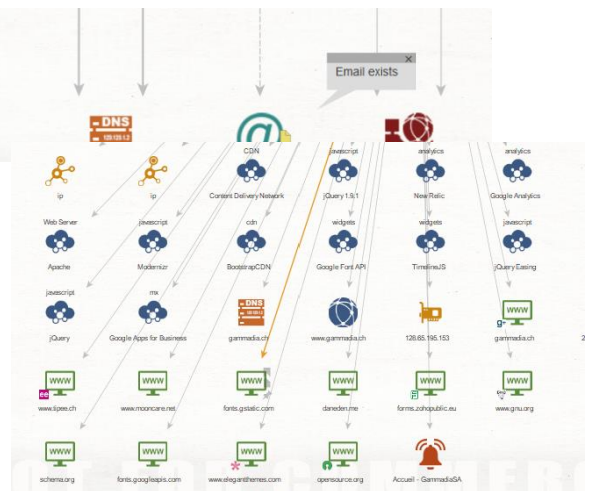


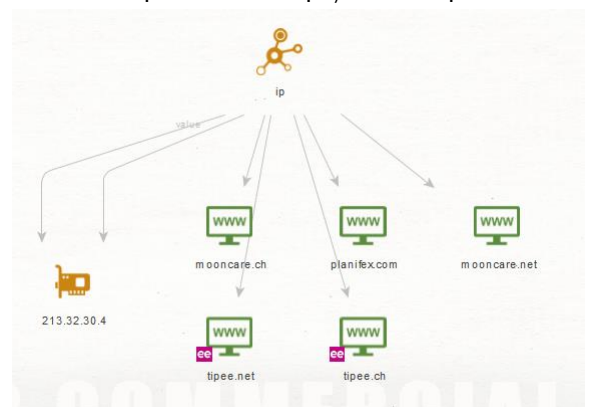
Figure 3 tipeg

En inspectant le site web de gammadia.ch on peut retrouver divers informations tels que la stack technologique utilisée



En effectuant des transformations sur l'adresse IP on peut retrouver les différents produit développé/maintenu par gammadia

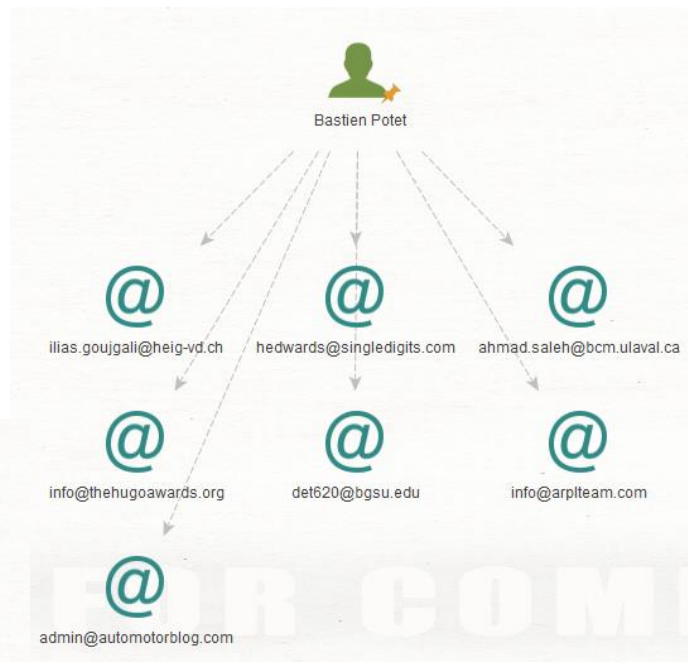
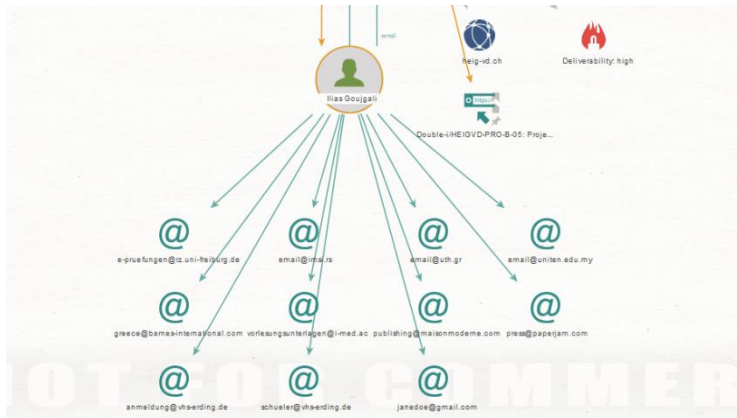
- Mooncare
- Planiflex
- Tipeg



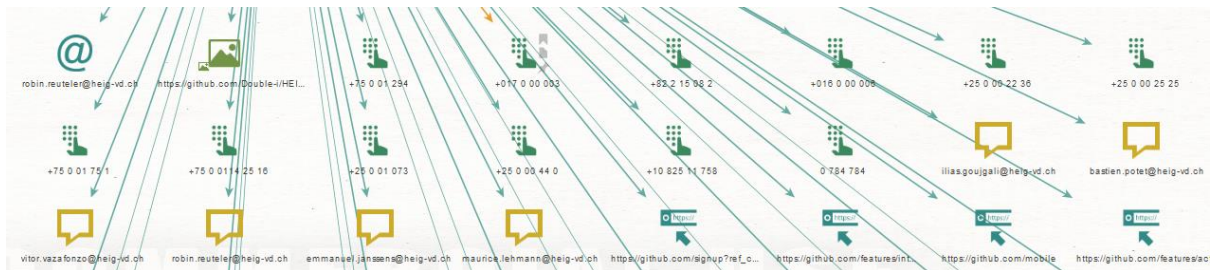
RECHERCHE D'UNE IDENTITÉ BASTIEN POTET

Bastien potet était un étudiant à l'HEIG-VD, Il à reçu son diplôme en début d'année et n'est donc plus présent dans le système de l'HEIG, par contre on peut voir qu'il est encore lié à un autre étudiant qui est un amis en commun et qui est actuellement encore étudiant.

En inspectant cette adresse E-mail on peut retrouver une identité liée à ce dernier ainsi que une information qui est surement l'élément clé qui relie ces deux personne.

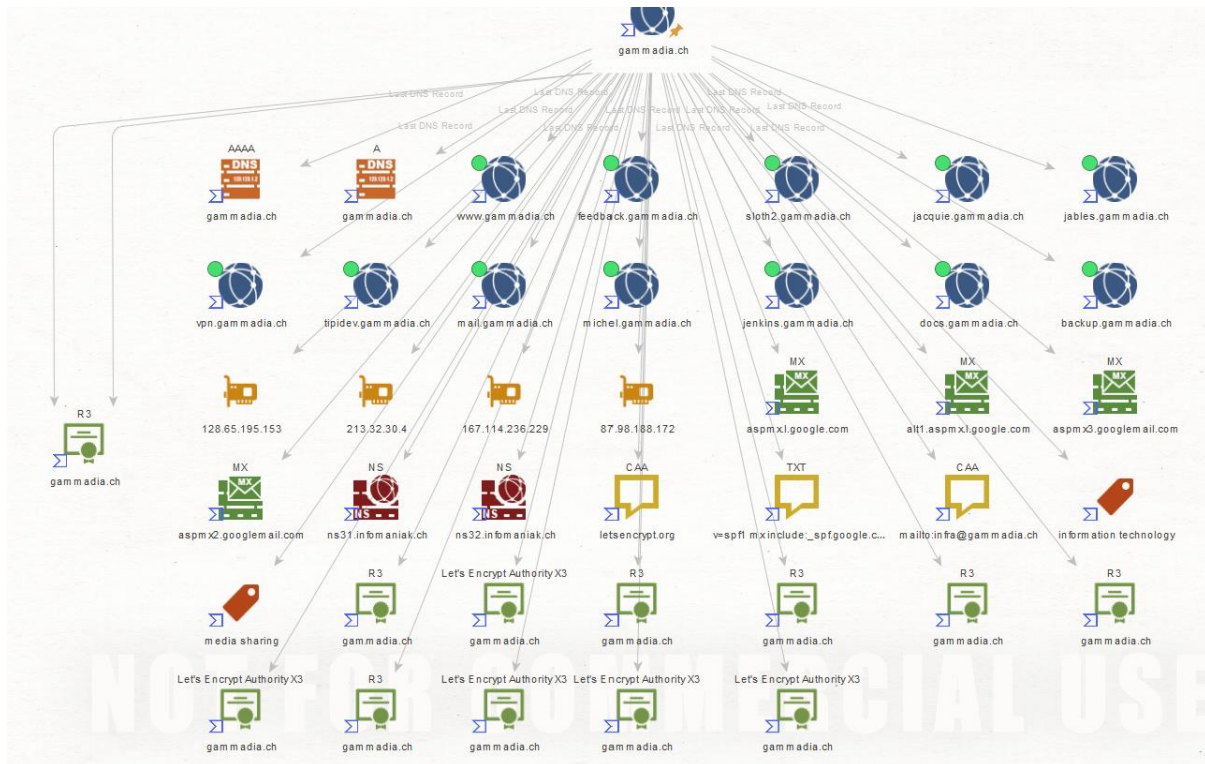


Un lien vers un projet qui à été réalisé il y a deux ans dans le cadre du cours de PRO(Je faisais partie du même groupe) permet de retrouver l'adresse e-mail de tout les collaborateurs ayant participé au projet



TRANSFORMATION ADDITIONELLES GAMMADIA

VIRUS TOTAL



















































DESCRIPTION GÉNÉRALE

On peut retrouver des entrées DNS, des sous domaine éventuellement liées, des adresses IP, quel type de « buissness » c'est ainsi que les différents certificats

CERTIFICATS

On peut voir quelques informations en plus tels que les certificats. Ces derniers sont issue par des autorités reconnues et ne posent donc pas de problème au site. La liste de certificats permet de détecter des certificats issues à des DNS compromettante, des nom de domaines expirées. Aucun des certificats listées représentent une vulnérabilité.

 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				1	0	0
 maltego.X509Certificate	gammadia.ch				2	0	0

ADRESSES IP

On peut voir que une des adresse ip est effectivement liée à gammadia.

Concernant les autres adresses IP je n'ai rien trouvé de relevant autre que ils ne sont pas atteignables, donc supposément inexistant.

```
emman> nslookup 128.65.195.153
Server: ns1.einet.ch
Address: 10.193.64.16

Name: h2web142.infomaniak.ch
Address: 128.65.195.153

emman> nslookup 87.98.188.172
Server: ns1.einet.ch
Address: 10.193.64.16

Name: sbg-app-003.proxyclick.com
Address: 87.98.188.172

emman> nslookup 167.114.236.229
Server: ns1.einet.ch
Address: 10.193.64.16

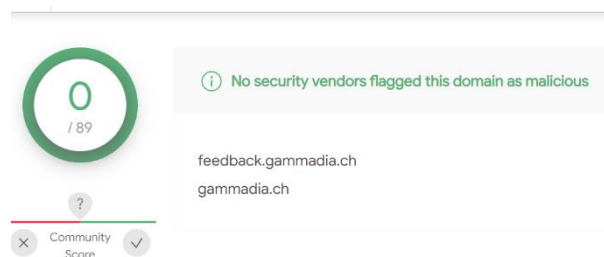
*** ns1.einet.ch can't find 167.114.236.229: Non-existent domain
emman> nslookup 213.32.30.4
Server: ns1.einet.ch
Address: 10.193.64.16

*** ns1.einet.ch can't find 213.32.30.4: Non-existent domain
emman> nslookup gammadia.ch
Server: ns1.einet.ch
Address: 10.193.64.16

Non-authoritative answer:
Name: gammadia.ch
Addresses: 2001:1600:4:b:4ed9:8fff:fe45:b77f
          128.65.195.153
```

DOMAINES

En inspectant les domaines on peut cliquer dessus et cela nous mène vers un site web de virus total. Aucun des sous-domaines sont soumis à des risques dans cet exemple j'ai pris feedback.gammadia.ch.

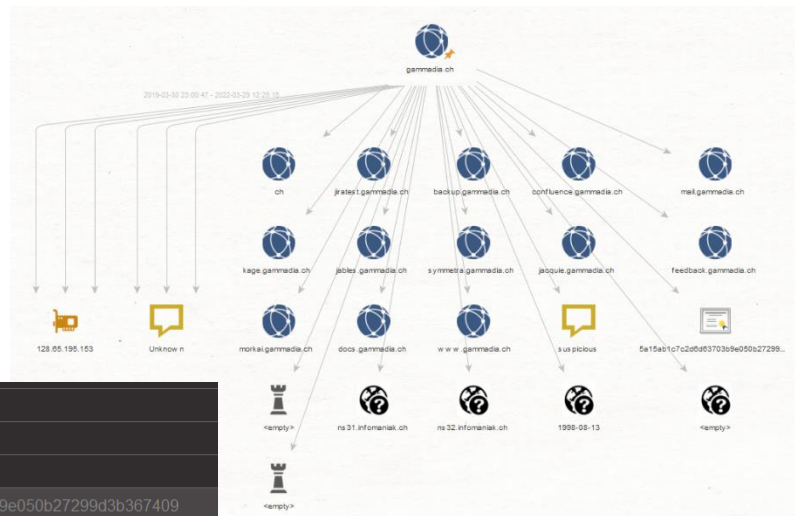


Pour finir plusieurs badge de couleurs sont identifiable pour des échantillons

- Rouge : échantillons considéré comme malicieux par les « vendors »
- Jaune : quelque un des « vendors » détectent échantillons comme malicieux
- Vert : échantillons Sans risque
- Gris : échantillons Non trouvé

PASSIVE TOTAL

Autre que les domaines on obtient pas plus d'information que les transformations de virus total



maltego.IPv4Address	128.65.195.153
maltego.Phrase	Unknown
maltego.Phrase	suspicious
pt.SSLCertificate	5a15ab1c7c2d6d63703b9e050b27299d3b367409
pt.whoisExpiresAt	
pt.whoisNameserver	ns32.infomaniak.ch
pt.whoisNameserver	ns31.infomaniak.ch
pt.whoisRegistered	1998-08-13
pt.whoisRegistrar	
pt.whoisRegistryUpdatedAt	

SHODAN

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



Figure 4 exécution de shodan

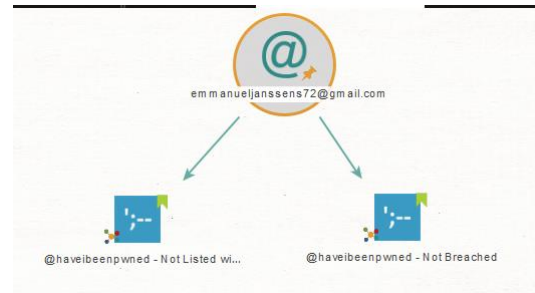
Hormis l'adresse IP déjà retrouvé par les transformation basique rien d'autre est retourné du au fait que la clé API ne met pas à disposition toute les transformations à moins d'upgrade.

TRANSFORMATION SUPPLÉMENTAIRES

HAVE I BEEN POWNED

En faisant des transformation sur mon adresse e-mail privé deux informations sont retrouvées

- Not listed in pastes : Elle n'est pas présente dans une « liste » d'adresses récupérée par un attaquant
- Not breached : exposée inintentionnellement au public



Dans mon cas je n'ais pas grand-chose à me soucier pour l'instant

Figure 5 est ce que mon adresse privée est compromise

SOCIAL LINKS

Ce dernier permet de retrouver des informations liées à une identité dans ce graphe on retrouve trois type d'objet

- CompaniesHouse

« identifier for an officer (natural person or legal person) of companies registered with Companies House in the United Kingdom » [Companies House](#)

[officer ID - Wikidata](#)

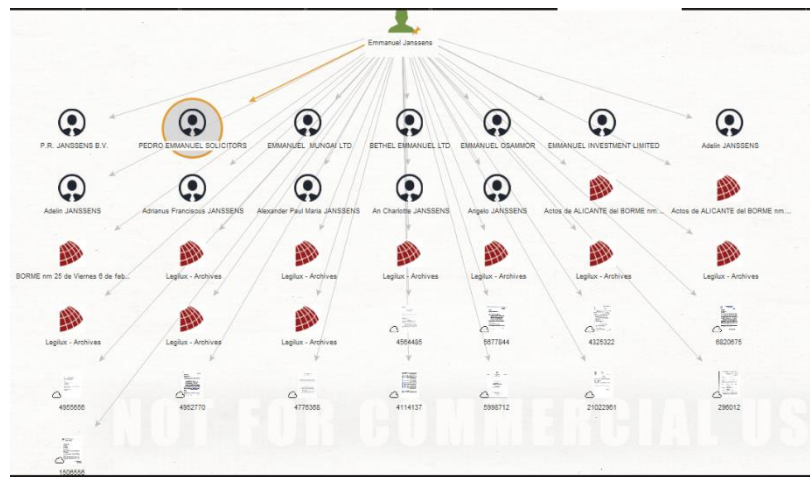


Figure 6 social links sur moi même

- Documents OCCRP : organized crime and corruption reporting project, heureusement il y a rien fortement lié à moi-même. Ce sont des données qui peuvent en effet être utilisée contre une cible potentielle.
- DocumentCloud : registre de document publique mis à disposition en ligne

Sinon aucune autre données me concernant ont été trouvé tel que les réseaux sociaux,...

LES DIFFÉRENTES INFORMATIONS APPORTÉES PAR MALTÉGO (TRANSFORMATIONS STANDARD)

Have I Been pwned	Permet de vérifier si une adresse e-mail a été trouvée dans un registre public et est donc compromis.
FullContact	Récupère des informations plus précises sur une identité tel que l'adresse mail, twitter, entreprise, alias et numéro de téléphone
Google maps geocoding	Permet de récupérer des informations plus détaillées sur des adresses
Farsight DNSDB	Une plus grande base de données DNS, permet de récupérer des entrées IP, NX, MX, AAAA, SOA, etc
Google programmable search engine	Utilise la plateforme google pour mesurer son empreinte en ligne (réseaux sociaux,...)
Scamadviser	Permet de détecter si un site web est frauduleux, infecté par des malwares ou effectue des activités malicieuses.

CONCLUSION

On peut en effet trouver énormément d'informations mais malheureusement pas forcément liées directement à notre cible. Un seul bémol est de devoir créer un compte pour la majorité des transformations pour récupérer une clé d'API.

Exécuter toutes les transformations (de base et extensions) retourne en effet beaucoup d'entités et il faut passer pas mal de temps à retrouver l'information correcte que l'on veut utiliser. Ces actions sont rendues assez simples dans Maltego où on peut juste créer un nouveau graphe à partir d'un nœud et effectuer des transformations dessus jusqu'à trouver l'information désirée.

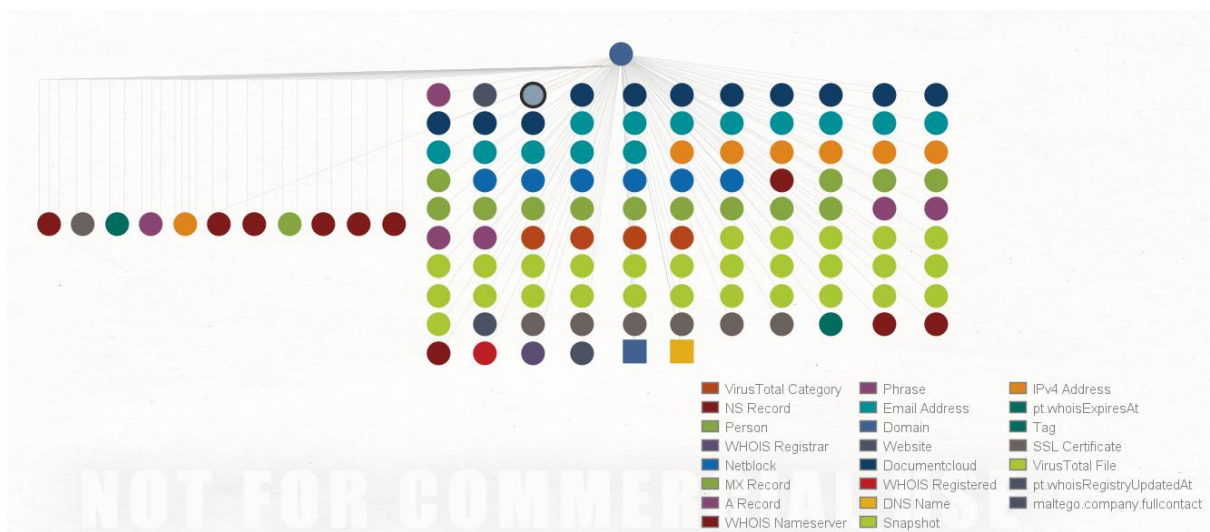


Figure 7 exécution de toutes les transformations sur le domaine heig-vd.ch