

Labo découverte Maltego

Dans ce laboratoire je vais découvrir l'outil de datamining « Maltego ». Je vais utiliser la version « Maltego CE (Community Edition) ».

Contents

Domaine.....	1
Données	1
Recherche plus précise	2
Encore plus loin.....	3
Personne	5
E-mail	8
Nouvelles transformations.....	9
Have I been pwned	9
VirusTotal.....	10
Scamadviser	10
Autres transformations.....	11
Conclusion.....	11

Domaine

Le nom de domaine que j'ai choisi est celui de www.bobst.com, une entreprise où j'ai pu faire un stage

En utilisant « all transforms » sur ce nom de domaine on trouve beaucoup de résultats du serveur DNS au numéro de téléphone. Je vais en préciser la plupart dans cette partie.

Données

Nous trouvons d'abord des serveurs DNS liés au nom de domaine :



Ensuite des fichiers liés à l'organisation comme par exemple des brochures :



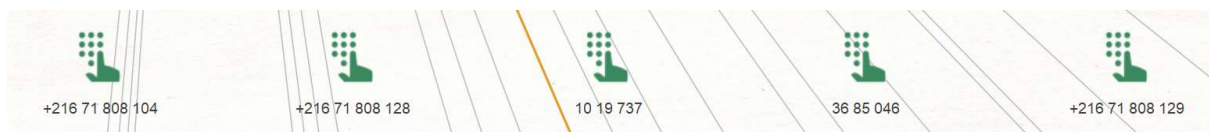
Puis des noms de domaine avec entre autres le site en français :



Ensuite beaucoup d'emails de chez bobst avec, en particulier, celui de CEO actuel de l'entreprise (tout à droite) :



Beaucoup de numéros de téléphones, mais aucun de ceux trouvé semblent être des numéros de téléphone suisses. Cela est étrange car bien qu'étant une entreprise internationale, Bobst est basé principalement en Suisse :



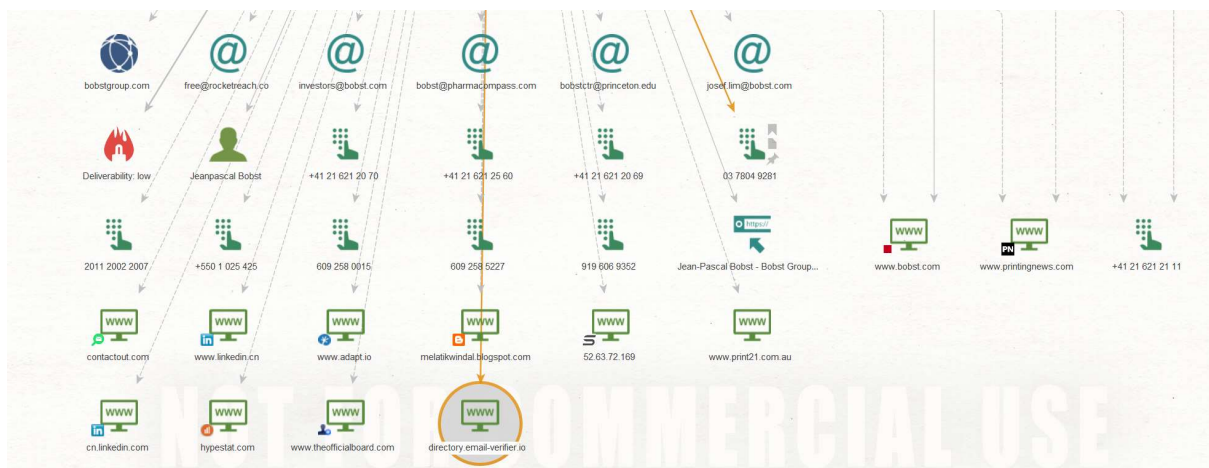
Et finalement des URLs de sites liés de près ou de loin au domaine.



Il est intéressant de voir qu'il y a beaucoup de résultats pertinents, mais aussi beaucoup qui ne le sont pas, comme des domaines ou des sites internet qui n'ont rien avoir ou des numéros de téléphone.

Recherche plus précise

J'ai décidé de me pencher sur l'e-mail du CEO de l'entreprise. En appliquant « all transforms », on peut voir apparaître plus d'information tel que son identité, ainsi que des numéros de téléphones suisses. En en cherchant un sur local.ch on remarque que ce numéro correspond effectivement à Bobst. On voit aussi un autre domaine apparaître : « bobstgroup.com ».




Bobst Mex SA

 Appareils et machines d'Emballage
 fabr. machines pour impression

Ouvert · jusqu'à 17h30

5.0 / 5



* Appeler 021 621 21 11

E-mail

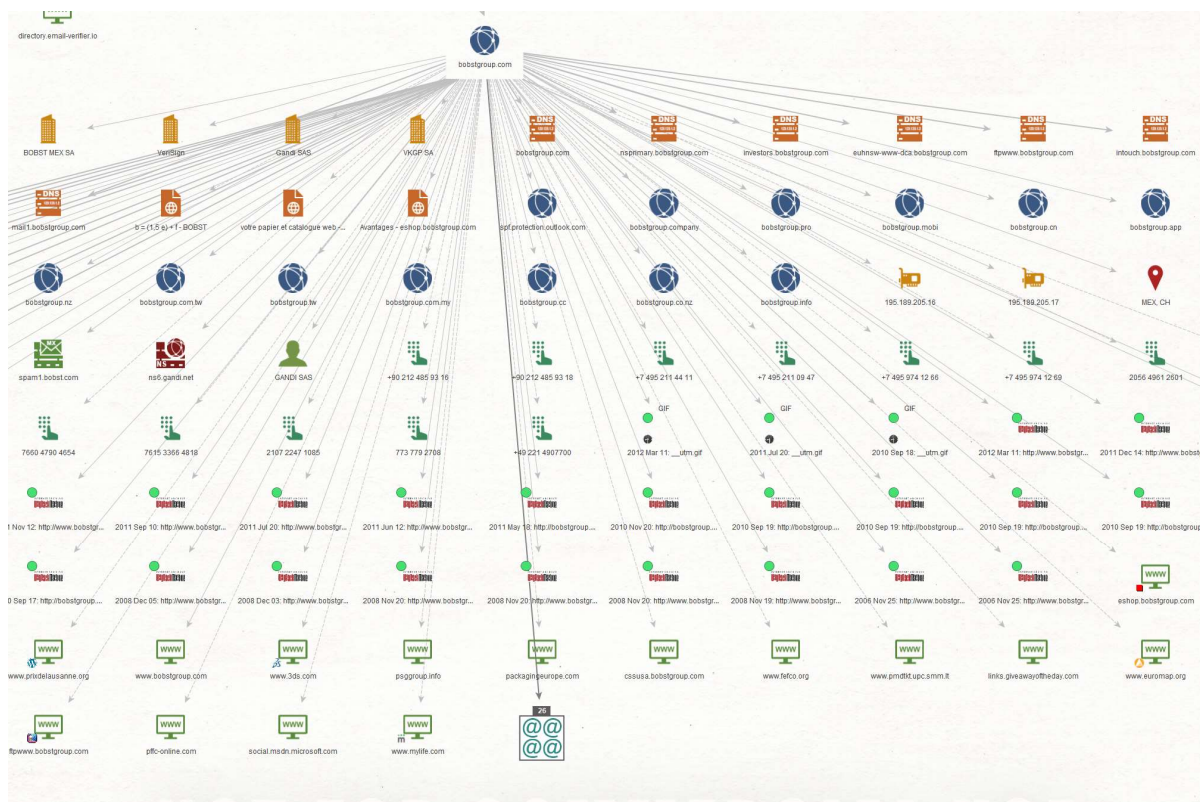
Plus



Encore plus loin

J'ai donc décider de continuer ma recherche sur le domaine « bobstgroup.com » car celui-ci me semble plus pertinent que « bobst.com » que j'avais choisis au début.

En appliquant « all transforms » sur ce domaine on se rends rapidement compte qu'il donne plus de résultats plus pertinents par rapport à Bobst.



En particulier on trouve une référence directe à l'entreprise « BOBST MEX SA » qui est celle qui nous intéresse. Mais aussi quelques entreprises partenaire comme « Gandi SAS » un fournisseur de domaines français dont les services sont surement utilisés par Bobst :



On arrive aussi à récupérer des adresses IP ainsi que l'endroit physique où la maison mère de Bobst est située :



Ainsi qu'un MXrecord, un Mail Exchange qui est donc un DNS qui dirige les e-mails vers le bon mail server. Celui-ci semble lié à la gestion du spam :



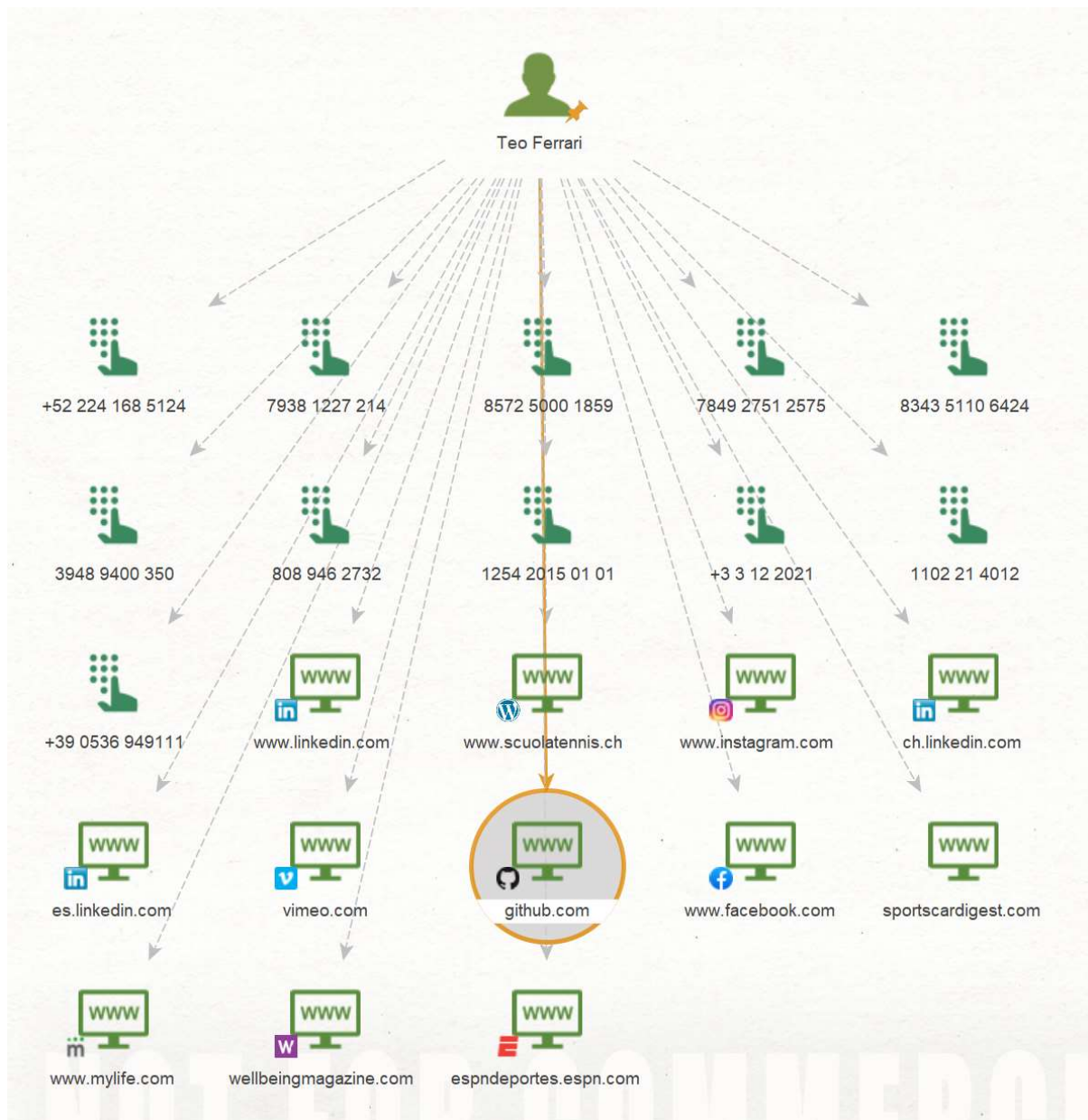
Finalement on récupère aussi beaucoup plus d'e-mails :

@Email Addre... (26)				
	Entity			
<input type="radio"/>	sales.tn@bobstgroup.com			65
<input type="radio"/>	contato@applebees.com.br			60
<input type="radio"/>	investors@bobstgroup.com			58
<input type="radio"/>	aquiarcor@arcor.com.br			54
<input type="radio"/>	steve.carey@bobstgroup.com			51
<input type="radio"/>	arpifrio@arpifrio.com.br			48
<input type="radio"/>	st.l@bobstgroup.com			44
<input type="radio"/>	atacado@atacado.com.br			42
<input type="radio"/>	last@bobstgroup.com			37
<input type="radio"/>	bebafruta@bebafruta.com.br			36
<input type="radio"/>	last.first@bobstgroup.com			30
<input type="radio"/>	michael.dangelo@bobstgroup.co			22

Personne

J'ai, pour cette partie, décidé de me chercher moi-même et voir ce sur quoi j'allais tomber.

Après avoir appliqué « all transforms » beaucoup des résultats dont peu pertinents, avec des numéros de téléphone qui n'ont rien avoir avec moi et des liens sur des site qui ne mènent à rien ou a quelque chose qui ne me concerne pas.



Pourtant il y a bien un résultat qui me concerne. C'est le lien vers le repository github de mon projet de PRO fait le semestre passé : « findyourpet.ch ». Comme on peut le voir dans les images suivantes c'est bel et bien le bon repo et mon nom est cité dans le readme ce qui est sûrement la raison pour laquelle Maltego a pu le retrouver.

The screenshot shows the GitHub repository for 'FindYourPet' by MelvynHerzig. The repository is public and has 76 branches and 0 tags. The commit history shows a recent commit 'ae2b842' on 27 Jan with 354 commits. The file list includes .github/workflows, src, .gitignore, LICENSE, and README.md. The README.md file is open, showing the project description: 'Le but de ce projet de semestre de la HEIG-VD est de développer une application web innovante. Nous avons décidé de réaliser un site d'annonces d'animaux de compagnies qui centraliserait toutes les recherches et...'. The right sidebar shows the repository's metadata: 0 stars, 0 watching, 2 forks, and 4 contributors.

Auteurs

Nous sommes une équipe de 4 étudiants de la HEIG-VD en informatique logiciel :

- Alec Berney (alecberney)
- Teo Ferrari (LordTT)
- Quentin Forestier (QuentinForestier)
- Melvyn Herzig (MelvynHerzig)

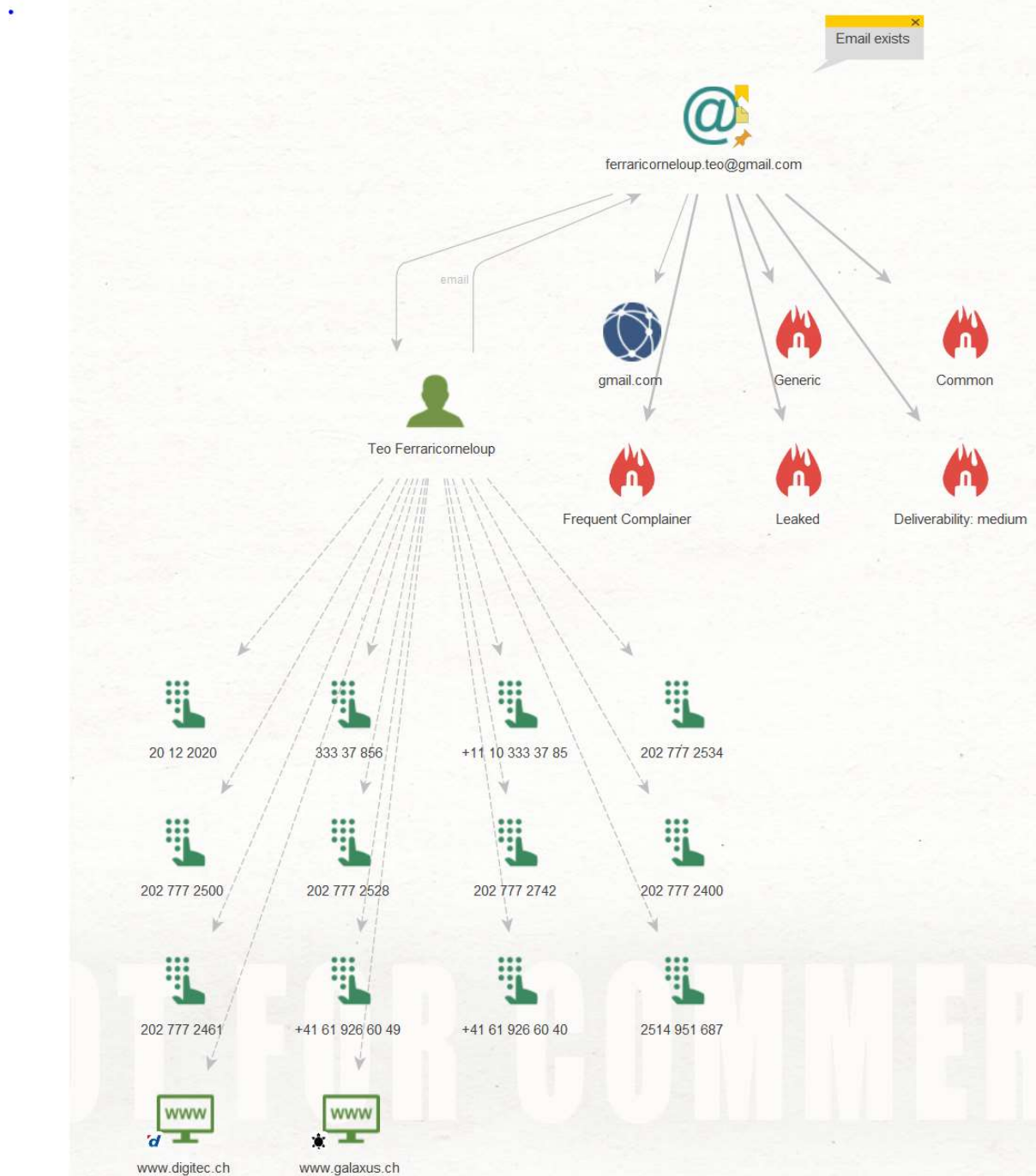
Pourtant le site lui-même, qui est en ligne, contient aussi mon nom mais n'est pas apparu dans les résultats de la recherche. J'imagine que cela est dû au fait qu'il n'est pas très utilisé et pas très référencé.

The screenshot shows the homepage of the 'Find your pet' website. The header is dark blue with a logo on the left and navigation links: 'Accueil', 'Annonces', 'Se connecter', and 'S'inscrire'. The main content area features a large image of a white cat lying down. Overlaid on the image is a white box containing the 'Find your pet' logo, the text 'Adoptez un animal de compagnie proche de chez vous maintenant !', and a subtext 'Trouvez des animaux proches de chez vous et créez des annonces pour vos animaux !'. At the bottom of the box are two buttons: 'Voir des annonces' and 'Créer des annonces'.



E-mail

Pour la recherche sur un e-mail j'ai décidé d'enquêter sur mon e-mail personnel. Maltego a donc confirmé que mon adresse existe bel et bien. Il à aussi trouvé une identité qui me correspond (Ferrari-Corneloup étant mon nom complet), qui elle-même mène vers des reviews produit que j'avais écrit sur Digitec et Galaxus.




On remarque aussi les IPQS tags liés à mon e-mail.

- Fraud score : Note la possibilité qu'une adresse e-mail soit frauduleuse, un score de 75 ou plus deviens un problème
- Generic : Indique que l'adresse semble être une adresse partagée du type contact, admin, etc... je ne comprends pas pourquoi mon adresse personnelle est concernée.

- Common : L'adresse viens d'un provider standard. Dans mon cas gmail.
- Frequent complainer : L'adresse se désabonne souvent de mailing lists et marque souvent des e-mails comme spams. Ceci est clairement vrai dans mon cas.
- Leaked : l'adresse est concernée par un data leak d'un parti tier. J'étais effectivement déjà au courant de plusieurs data leaks concernant mon adresse. Heureusement j'ai une authentification à 2 facteurs dessus.
- Deliverability : medium : La possibilité qu'un email de spam/pub attérisses dans la boîte mail.

Detail View



Email Address

maltego.EmailAddress

ferraricorneloup.teo@gmail.com

+Relationships

-Notes

Email exists

+Info

-IPQS Info

IPQS determined that this email address appears to be valid.

-IPQS Fraud Score

Fraud score: 45

This is an overall fraud score in the context of online user or customer screening (e.g. automated webshop checkout validation).

According to IPQS: 'Fraud Scores >= 75 are suspicious, but not necessarily fraudulent.' IPQS recommends 'flagging or blocking traffic with Fraud Scores >= 85.'

-IPQS Tag: Generic

Indicates this email is suspected as being a catch all or shared email for a domain ("admin@", "webmaster@", "newsletter@", "sales@", "contact@", etc.)

-IPQS Tag: Common

Indicates this email is from a common email provider ("gmail.com", "yahoo.com", "hotmail.com", etc.)

-IPQS Tag: Frequent Complainer

Indicates if this email frequently unsubscribes from marketing lists or reports email as SPAM.

-IPQS Tag: Leaked

Indicates that this email address is associated with a recent database leak from a third party. Leaked accounts pose a risk as they may have become compromised during a database breach.

-IPQS Tag: Deliverability

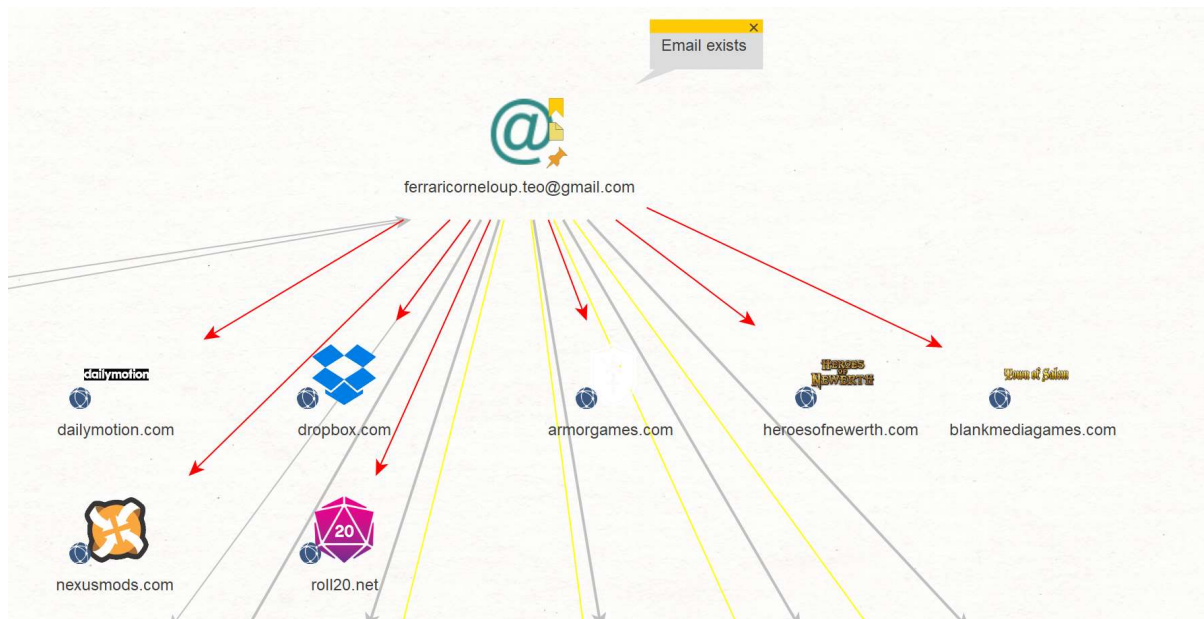
Deliverability: medium

Nouvelles transformations

J'ai pu installer et tester quelques nouvelles transformations

Have I been pwned

Contrôle si des données personnelles ont été compromises. Dans mon cas mon e-mail personnel a été compromis plusieurs fois. J'étais déjà au courant de quasi tous ces leaks avec l'exception notable de dropbox ce qui m'inquiète un peu.

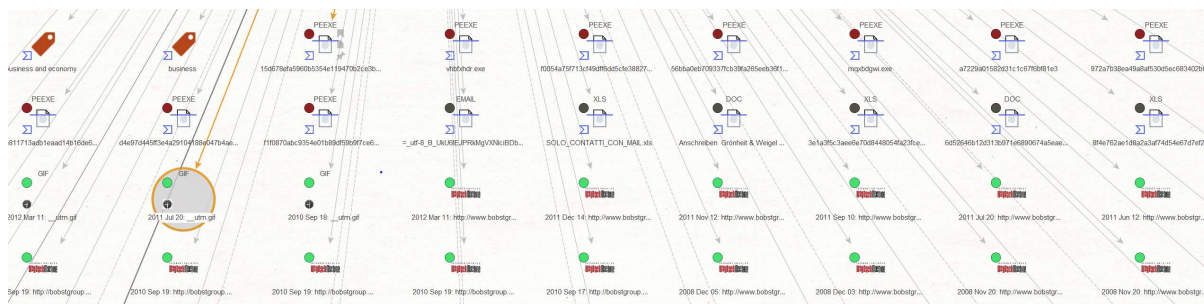


Virustotal

Permet de vérifier si des résultats trouvés sont considérés malicieux ou non. Il y a 4 couleur différente :

- Rouge : La plupart des scanners considèrent l'échantillon comme malicieux
- Jaune : Plus d'un scanner considère l'échantillon comme malicieux
- Vert : Echantillon détecté mais marque comme inoffensif
- Gris : Echantillon non détecté

Dans le cas de « bobstgroup.com » on peut voir plusieurs pastilles rouges des grises et des vertes.



Scamadviser

Vérifie si un site ou un domaine est légitime ou non en se basant sur différentes règles. Dans le cas de « bobstgroup.com » on voit que le site est très vieux, que le propriétaire montre son identité et

que aucun certificat SSL valide n'a été trouvé.



Autres transformations

Wayback Machine	Permet d'accéder à des archives et des snapshots du web
FullContact	Enrichie la recherche en essayant de récupérer le contact complet d'une personne (adresse e-mail, compte, téléphone, etc...)
Google maps geocoding	Permet de récupérer des adresses de manière standardisée et avec plus de précision
URLhaus	Collecte et traque des malwares
Google programmable search engine	Vérifie la présence d'une personne sur les réseaux sociaux
Social links CE	Recherche des données sur plusieurs sites pour vérifier si l'adresse e-mail à un compte sur ces sites.

Conclusion

Finalement on peut voir que Maltego est un outil qui permet de récolter énormément de différentes informations des différentes manières. Mais que ces informations ne sont pas toujours pertinentes et deviennent rapidement compliquées à trier.