

TP3 - Florian POMPIDOU

PS : tous les passages entre parenthèses et ENTIEREMENT en italiques (*comme ceci donc*) sont des appartés, des commentaires que je fais moi en dehors du rapport. Ils apportent précisions ou explications en dehors du rapport, comme s'ils n'existaient pas dans le rapport final.

Merci d'en tenir compte.

Demande client

Votre chef de mission a transmis votre rapport JSON d'hier au directeur technique. Retour dans la matinée :

"Bonne cartographie technique. Maintenant le client veut savoir s'il est exposé côté humain aussi — est-ce qu'on peut remonter aux admins, aux devs, identifier des patterns d'emails, des fuites de credentials ? Et si on trouve des documents internes accessibles avec des metadata exploitables, c'est un finding critique. Allez-y."

Vous définissez votre propre approche.

0. Préparation opérationnelle

Compte tenu des précédents rapports, il a été établi pour Tesla, avec son domaine principal **tesla.com** :

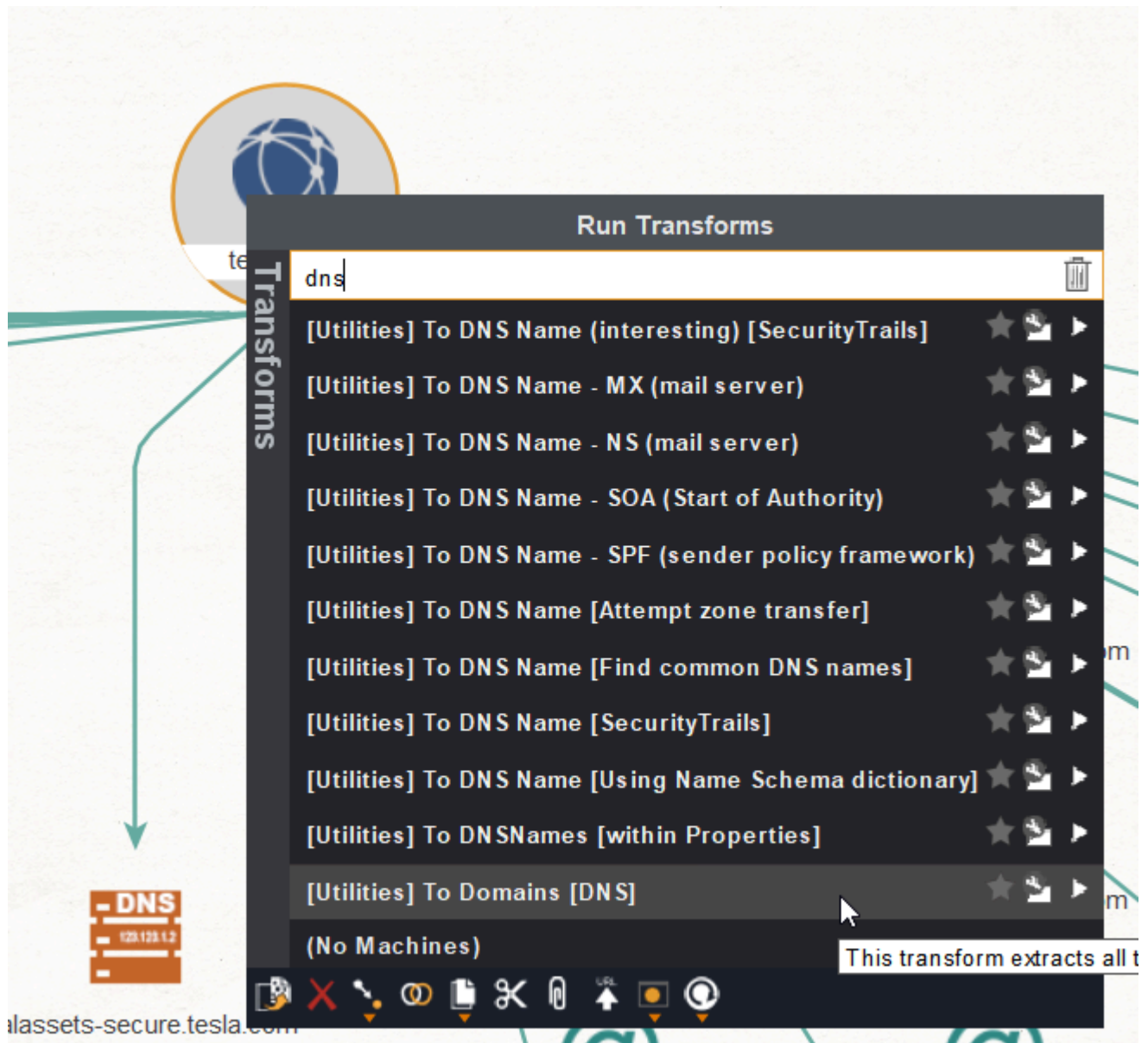
- La découverte en surface de plus de 70 sous-domaines, incluant sous-domaines commerciaux et techniques (APIs, environnements de préprod, noms NetBIOS, etc)
- La découverte de ports exposés, avec des services aux CVEs connues
- La cartographie globale de l'environnement technique

Le client demande maintenant les capacités non plus de surface d'attaque *technique* mais *sociale* : courriels exposés, noms corrélés, identifiants fuités, documents accessibles, etc.

Pour les besoins d'analyse **passive** (à la demande du client) et pour obtenir ces informations, le choix s'est porté sur la solution **Maltego** en mode **Discret** (Stealth), afin de n'utiliser que des rapports et analyses tierces, sans communication directe avec les serveurs.

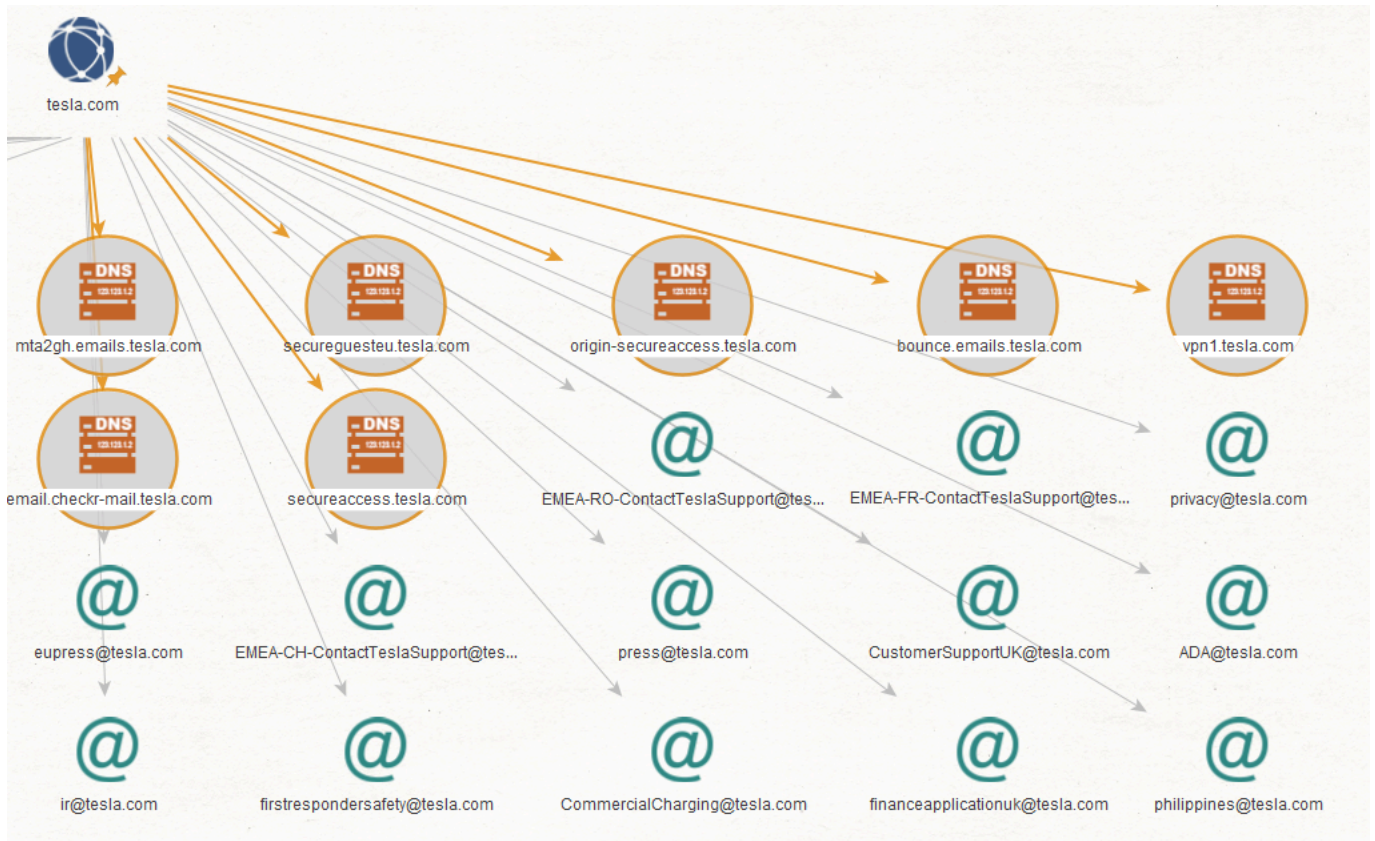
1. Première topologie

Inscrivant le domaine **tesla.com** comme élément de recherche racine, une première topologie des sous-domaines par recherche DNS s'impose :

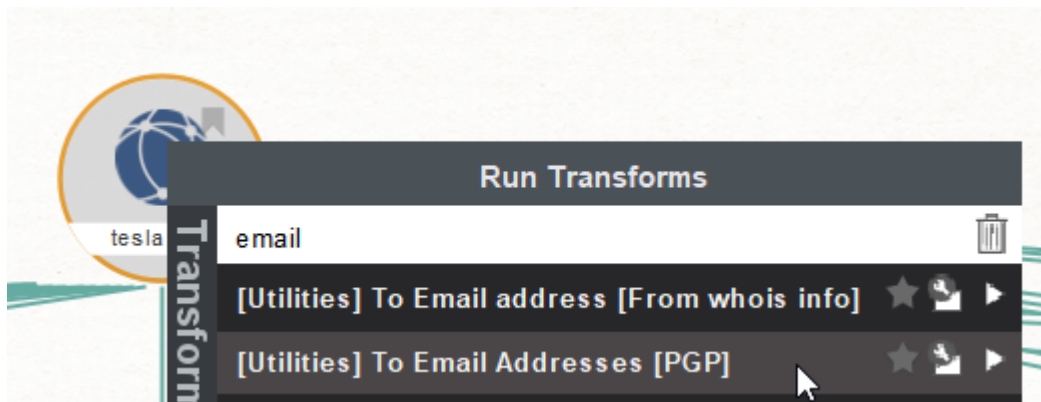


La transformation des noms DNS en adresses IP permet de retrouver la topologie extraite lors des documents précédents.

Une recherche de courriels sur la base du domaine racine permet de trouver une surface classique d'adresses accessibles depuis les pages publiques (équivalent "Contactez-nous", "Mentions Légales", etc) :



En faisant une recherche selon les signatures PGP (**Pretty Good Privacy**, protocole de chiffrement des courriels) on peut retrouver un serveur commun et tenter de recroiser les informations :



De fait, nous pouvons apercevoir des courriels signés de la même façon, et donc par le même serveur central :

Email Address
maltego.EmailAddress
37 EmailAddress entities

+		Entity						
+	@	ir@tesla.com			37	1	0	100
+	@	philippines@tesla.com			37	1	0	100
+	@	press@tesla.com			37	1	0	100
+	@	privacy@tesla.com			37	1	0	100
+	@	afaltin@tesla.com			37	1	0	0
+	@	AlexSmith@tesla.com			37	1	0	0
+	@	aweddel@tesla.com			37	1	0	0
+	@	ax-support@tesla.com			37	1	0	0
+	@	dwuentele@tesla.com			37	1	0	0
+	@	elon@tesla.com			37	1	0	0
+	@	elonmusk@tesla.com			37	1	0	0
+	@	gsachdev@tesla.com			37	1	0	0
+	@	hgrosman@tesla.com			37	1	0	0
+	@	jglenn@tesla.com			37	1	0	0
+	@	jjames@tesla.com			37	1	0	0
+	@	jkoziej@tesla.com			37	1	0	0
+	@	lbagdadi@tesla.com			37	1	0	0
+	@	mesetiawan@tesla.com			37	1	0	0
+	@	mikanderson@tesla.com			37	1	0	0
+	@	ray@tesla.com			37	1	0	0
+	@	simaddi@tesla.com			37	1	0	0
+	@	svilain@tesla.com			37	1	0	0
+	@	taedwards@tesla.com			37	1	0	0
+	@	tfortenberry@tesla.com			37	1	0	0
+	@	tigu@tesla.com			37	1	0	0
+	@	wdawson@tesla.com			37	1	0	0
+	@	ybudiono@tesla.com			37	1	0	0
+	@	yoni@tesla.com			37	1	0	0

La structure semble indiquer, exceptions faites de "AlexSmith", "elon" et "elonmusk", la première lettre du prénom suivi du nom de famille attaché, sans tiret ni point.

2. Recherche de courriels

Avec le moteur de recherche dédié hunter.io, on peut faire usage d'une recherche de courriels "égarés" (annonces d'emplois, publications sur les réseaux sociaux, cartes de visites, etc) :

Find email by company







Find email by name

Domain Search ?

Upload a list of domains to search

tesla.com

Q



 Tesla		tesla.com	559 results
 TESLA d.o.o.		tesla.com.hr	18 results
 Tesla		tesla.com.br	12 results
 Tesla		tesla.com.sa	4 results
 Tesla		tesla.com.co	30 results

Le résultat fait état de plus de 500 adresses courriels, donc une majorité génériques, mais aussi celles de personnes, dont les 4 premières révélées nous informent sur le patron de fabrication des adresses :


People · 123 **Decision makers** · 1 **Generic** · 436

▼ **IT** 5

☐


Erin Chen  | Data Engineer
echen@tesla.com  | **in**

Saved ▼




1 source ▼

☐


Patrick Glaser | Senior Staff Software Engineer
pglaser@tesla.com  | **in**

Saved ▼




5 sources ▼

☐


Yingcong Wang | Senior EMC Engineer
ywang@tesla.com  | **in**

Saved ▼




4 sources ▼

☐


Daniel Hanks | Engineer
dhanks@tesla.com 

Saved ▼






1 source ▼

☐

Ashkan P. | Senior Software Engineer
*****@tesla.com  | **in**

A noter : les trois premiers retours indiquent des profils LinkedIn et plusieurs sources externes à Tesla :

☐ **Patrick Glaser** | Senior Staff Soft Saved ▾ 

pglaser@tesla.com  |  5 sources ^

Email

<https://patchwork.ozlabs.org...> May 8, 2021

Email

<https://patchwork.ozlabs.org/...> Jan 6, 2022

Email


<https://patchwork.ozlabs.org/...> Jul 27, 2021



Removed

<https://patchwork.ozlabs:...> Jun 8, 2021

Removed

<https://patchwork.ozlab...> Aug 25, 2020

☐ **Yingcong Wang** | Senior EMC Eng Saved ▾ 

ywang@tesla.com  |  4 sources ^

Email

<https://victoriaevclub.com/te...> Apr 4, 2020

Email

<https://driveteslacanada.ca/...> Jun 26, 2020

Email

<https://driveteslacanada.ca/...> Jun 26, 2020

Removed

<https://ssiev.ca/tesla-sale...> Jul 19, 2022

La source "driveteslacanada.ca" semble être un site de fan, tandis que "patchwork.ozlabs.org" semble être un site type "Pastebin"

Conclusion rapide et croisée est faite sur le format : prénomnom@tesla.com. Nous pouvons alors reprendre une investigation avec LinkedIn et chercher des employés de haute stature directement [sur la page LinkedIn](#), section "Personnes" pour trouver une liste relativement à jour des employés actuels, et retrouver leur courriel.

3. Recherche d'individus

Prenant l'exemple de "Manal FENNIRI", Titre "Associate HR Operations and Payroll Specialist", je reprend la structure et utilise un outil ordinaire, en l'occurrence "Email Checker" de "MailMeteor" pour vérifier la validité de la structure du courriel :



VERIFY

Valid
mfenniri@tesla.com is a valid email address

Format valid

This email address is written correctly and isn't gibberish.

Professional valid

The domain isn't linked to webmail or throwaway email services.

Domain status valid

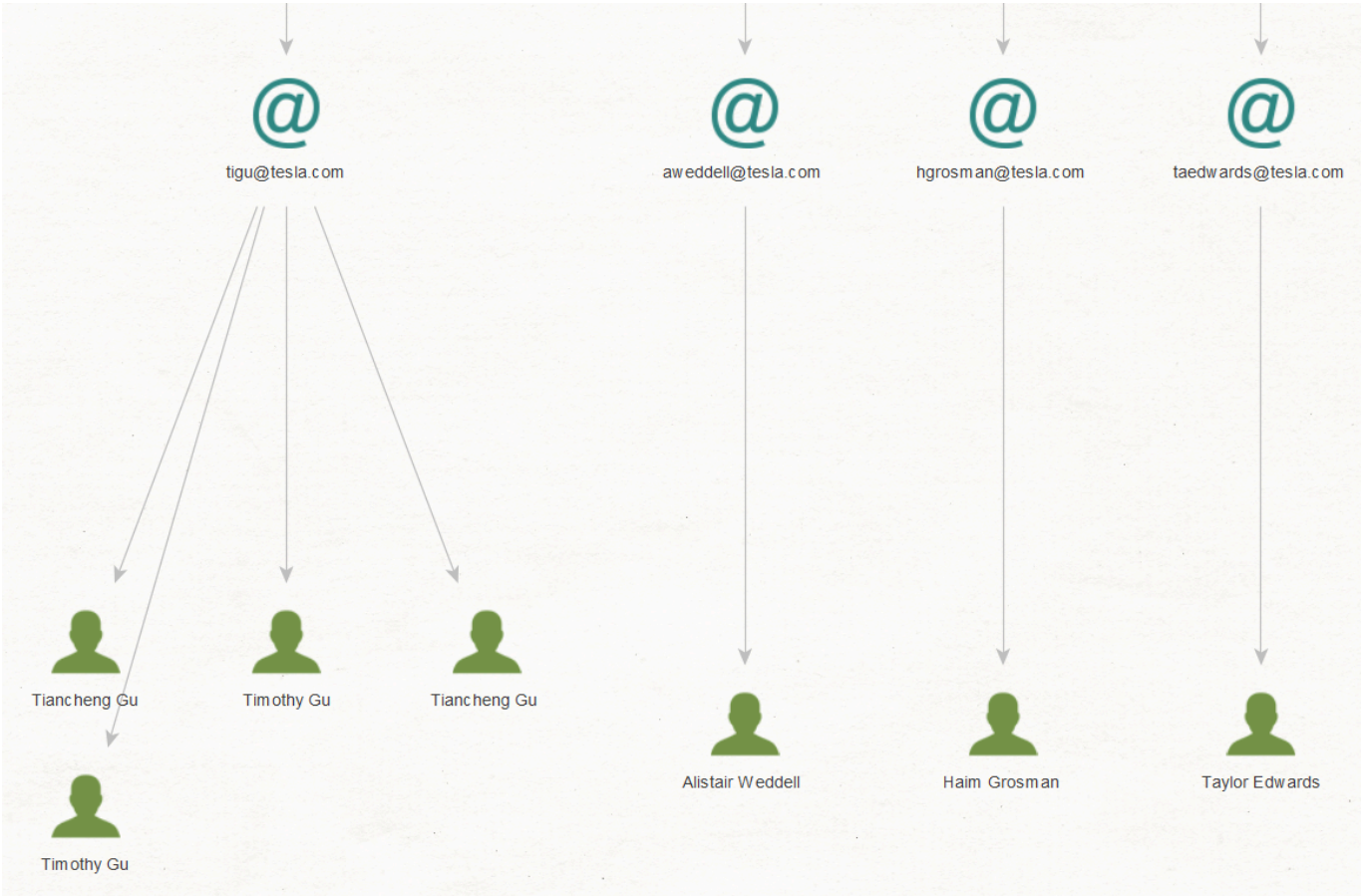
The domain name exists and has valid MX records.

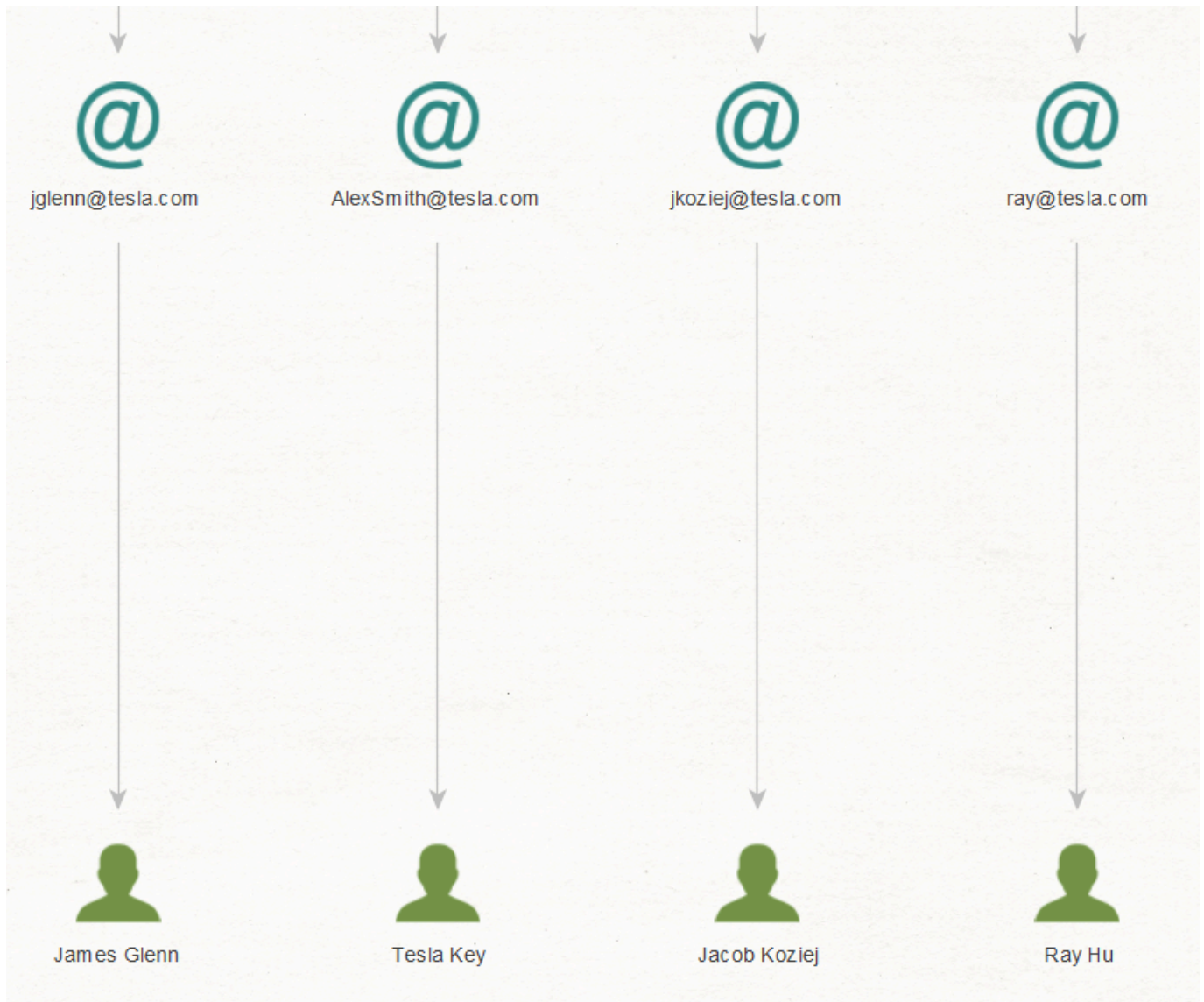
Mailbox valid

The mail server responded and confirmed that this mailbox exists.

On peut en conclure que la structure est toujours utilisée aujourd'hui.

Une contre-recherche de courriel à personne permet d'identifier les individus à partir des courriels extraits par recherche PGP, avec quelques ratés/approximations néanmoins :







4. Recherche de fuites d'identifiants

La diffusion - involontaire ou malveillante - de mots de passe, de Jetons d'accès ou de Clefs APIs est encore monnaie courante. Une recherche sur Github avec des mots clefs ciblés, à savoir en première instance `tesla.com API_KEY=` permet de cibler les croisements entre Tesla et les endroits où la variable `API_KEY=` est définie, formulation standard en base de code, permettant de vérifier la présence de lignes en dur plutôt qu'en dynamique.

On retrouve effectivement une fuite du service "Boomerang" dans le code source Tesla :

A screenshot of a web browser displaying a GitHub repository page for 'tesla/autodiscover.tesla.com'. The browser's address bar shows the URL. The GitHub interface includes tabs for 'Code' and 'Blame', and a toolbar with icons for file operations. The main content area displays a code snippet with a highlighted 'BOOMR_API_key' value.

(Il s'agit d'un repo "public-bugbounty-data", donc techniquement pour qu'on repère ce genre de fuite, ça ne compte pas "vraiment". Par contre j'ai trouvé un guignol non lié à Tesla qui a vraiment fait fuiter la sienne.)

Un script Python `hibp_bulk_checker.py` (généré par IA) itérant sur chaque adresse d'un fichier "addresses.txt" permet d'exporter dans un fichier CSV

5. Documents publics

Les documents accessibles publiquement sur le site sont des notices techniques de véhicules de plusieurs pays différents en plusieurs alphabets différents. Les métadonnées indiquent juste les informations de création des documents, les auteurs et les formats de sortie. Rien ne semble, en surface, exploitable comme tel.

(Je n'ai rien trouvé de concret.)

6. Recommandations finales

Pour pallier à toutes ces fuites, plusieurs axes d'améliorations, du plus simple (simples rappels de sécurité, modules de formation, etc) au plus complexe (changement de paradigme, matériel de sécurité supplémentaire, rotation complète de la base courriel, etc) :

1. Pas d'inscription "personnelle" depuis un compte courriel professionnel
2. Pas d'usage multiplié d'un unique mot de passe
3. Activation de l'Authentification à Facteur Multiple dès que possible
4. Pas de génération de clef API sauf nécessité absolue (privilégier accès SSO)
5. Secrets techniques gérés en Coffre-Fort type VAULT
6. Chiffrement courriel géré par le client
7. Adjonction de caractères aléatoires à la structure des courriels (type jsmith038@tesla.com) pour éviter les recoupements
8. Activer le téléversement des documents publics avec suppression totale et définitive des métadonnées