

TP4 - Florian POMPIDOU

NB : Encore une fois, tout passage entre parenthèses et **INTEGRALEMENT** en italique (comme ceci) constitue un commentaire hors-rapport, pour donner du contexte ou du détail.

Demande client

Votre chef de mission vous contacte une dernière fois en fin d'après-midi :

"Le RSSI de Tesla veut un document livrable propre d'ici 17h. Pas un dump de terminal — un rapport structuré qu'il peut présenter à son DG demain matin. Résumé exécutif, surface d'attaque, findings priorités, recommandations actionnables. Et nettoyez vos métadonnées avant d'envoyer."

Vous produisez le rapport final.

1. Résumé

A la demande du client (ici nommé **Tesla Motors**), la société **Synapse Security** a conduit un ensemble de recherches et de dévoilement de surfaces d'attaques techniques et sociales dans un contexte dit **Passif** (c'est à dire par la récupération de rapports, d'analyses et d'éléments tiers sans approche directe) pour simuler, au mieux, les capacités d'Intelligence en Sources Ouvertes (dites **OSINT**) venues d'individus isolés ou d'organisations désireuses d'agir sans trace.

Après une analyse topographique classique en partant du domaine principal et commercialement exploité **tesla.com**, et par un maillage d'outils spécialisés disponibles gratuitement dans leur version la plus simple pour la plupart des systèmes d'exploitation :

- **Synapse Security** peut attester que les informations autour des domaines et sous-domaines sont bien accessibles depuis l'extérieur, avec ou sans obfuscation
- Que la structure de l'environnement technique est trop facilement exploitable en l'état, avec l'ensemble des sous-domaines techniques, administratifs et de test accessibles

2. Périmètre

Synapse Security a procédé à plusieurs analyses de surface selon les besoins concrets de chaque périmètre :

- Le domaine racine et ses sous-domaines
- Les équipements affectés par chaque des précédents (sous-)domaines
- Les technologies utilisées derrière chaque équipement
- Les vulnérabilités derrière chaque technologie

3. Périmètres techniques

A. Outils primaires grand publics

Les informations relevées par des outils basiques "WHO IS", accessibles depuis de nombreux sites internet spécialisés, indiquent une structure nominale basique et sécurisée. Date de dépôt du nom de domaine, serveurs courriels, informations sur les services autorisés à user du domaine **tesla.com**, etc.

B. Moteur de recherche "Internet Of Things"

En deuxième instance, nous avons relevé les équipements liés à **tesla.com** depuis un moteur de recherche spécialisé dans l'Internet Des Objets (IoT), **Censys**, capable de relever tout équipement publiquement accessible, même si noyé dans la masse informative.

(Requête Censys utilisée, mais derrière plan payant :)

```
(tesla.com) and (web.cert.names = tesla.com) and (host.services.vulns.id: * or web.vulns.id: *)
```

Les premiers rapports relèvent les adresses, emplacements, prestataires et nature des équipements constituant l'infrastructure de **tesla.com**, à savoir nominativement des bases de données, des unités de calcul et éléments de publication web, situés majoritairement aux Etats-Unis, avec réplication locale en Allemagne, loué quasi intégralement chez AKAMAI.

Ce moteur indique également les ports ouverts sur chaque équipement, les services connectés derrière chacun d'eux, et recoupe ces informations avec les bases de données publiques sur les vulnérabilités techniques, dites CVEs.

C. Surface d'attaque par Ingénierie Sociale

En troisième instance, **Synapse Security** a procédé par le biais d'un outil de recherche relationnelle d'éléments, via l'outil **Maltego**, à trouver toute fuite potentielle d'éléments permettant d'établir un organigramme avec éléments personnels - comme les adresses courriel - et une base de contact non sanctionnée.

Par un recoupement depuis le domaine **tesla.com** et sur base d'une terminaison d'adresse en **@tesla.com** a été établie une liste de plus de 50 personnes, incluant des membres de la direction, dont les sources renvoyaient vers des blogs amateurs, des sites d'affichage de rapports techniques (sans gravité ni éléments confidentiels) ainsi que des espaces de recrutement.

Récupérant ces informations, nous avons pu identifier :

- la structure d'adressage interne
- un organigramme des personnes à responsabilité (Ressources Humaines, Direction Générale, etc) ainsi que leurs adresses professionnelles
- les profils sur les réseaux sociaux

D. Recherche d'éléments techniques fuités dans le code source ouvert

Des examens sur **GitHub**, dépôt centralisé de codes sources (ouverts ou fermés) dont celui de **Tesla Motors**, il a été retrouvé plusieurs morceaux incluant des informations de connexion tiers (nominativement une clef API [permettant la connexion à des services par ligne de commande] ainsi qu'un compte de test avec un mot de passe en clair prédéfini).

E. Surface d'attaque par exploitation des métadonnées

En dernière instance, les documents accessibles, intégralement des documents techniques à usage des particuliers et des concessionnaires, ont semblé comporter des métadonnées attendues pour de tels documents, et ne semble constituer aucun problème majeur.

4. Failles majeures

(Faute de rapport généré par moi, voici un relevé de CVEs passées autour de tesla.com. Relevé et détails donnés par Gemini Pro 3.5 en mode Raisonnement.)

A. Interface de gestion détournable sur serveur principal

- **Élément concerné** : Interface F5 BIG-IP
- **Description** : Un serveur exécutant l'interface de gestion TMUI a été concerné par la "CVE-2023-46747", permettant l'accès au compte administrateur total du serveur
- **Criticité** : 80/100 (Critique)
- **Points de faille** :
 - Version FR BIG-IP 17.x
- **Correction** : Mise à jour de version

B. Injection de script malveillant sur le portail employé Support

- **Élément concerné** : Zone support de tesla.com
- **Description** : Le portail de connexion des employés support.tesla.com et vitals.tesla.com permettent l'injection de script (vulnérabilité Cross-Site Scripting, dite XSS) envoyé depuis les formulaires accessibles au client, exécuté avec les privilèges des employés connectés.
- **Criticité** : 59,5/100 (Elevé)
- **Points de faille** :
 - Code source propriétaire mal revu
- **Correction** : Revue de code prioritaire

C. Injection de script malveillant sur la page d'achat

- **Élément concerné** : Page de paiement de tesla.com
- **Description** : La page gérant le tunnel d'achat et le configurateur des paiements permet également l'injection de script (XSS), le serveur principal pouvant recevoir des requêtes de paiement de domaines n'étant pas tesla.com.
- **Criticité** : 45/100 (Moyenne)
- **Points de faille** :
 - API HTML5 window.postMessage mal utilisé et mal implémenté
- **Correction** : Revue de code prioritaire

D. Certificats de sous-domaines expirés

- **Élément concerné** : Sous-domaines avec certificat de sécurité/authenticité expiré
- **Description** : Plusieurs sous-domaines (notamment engage.tesla.com) ont
- **Criticité** : 28/100 (Faible)
- **Points de faille** :
 - Erreur de gestion dans le renouvellement des certificats
- **Correction** : Renouvellement manuel, puis reprise des mécaniques de renouvellement automatique

5. Recommendations

Les recommandations pour éviter les attaques exploitant ces aspects évoqués :

1. Utiliser des domaines racines différents selon l'environnement
 - tesla.com pour la vitrine commerciale
 - tesla.net pour les APIs et autres serveurs "privés" devant communiquer aux éléments publics (comme les véhicules)
 - tesla.io pour la préproduction et les environnements de test, accessible UNIQUEMENT derrière un VPN d'entreprise
2. Utiliser un autre paradigme pour les courriels internes
 1. Utiliser un nom de domaine racine différent, type **people-tesla.com**
 2. Ajouter un identifiant numérique après la structure pnom@tesla.com pour randomiser les adresses
3. Mise à jour de la base de code et des versions logicielles en priorité
4. Mettre en place des tests unitaires avec des analyseurs de code statique (type **SonarQube**) pour vérifier l'absence d'identifiants en dur


6. Annexes

Annuaire d'adresses

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
+	@	awedell@tesla.com			37	1	0	0
+	@	ax-support@tesla.com			37	1	0	0
+	@	dwuertele@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

Sources des fuites d'adresses

- ☐ **Patrick Glaser** | Senior Staff Soft Saved ▾ ✉
pglaser@tesla.com  | **in** 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  | **in** 4 sources ^

Email

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

Email

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

Email

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

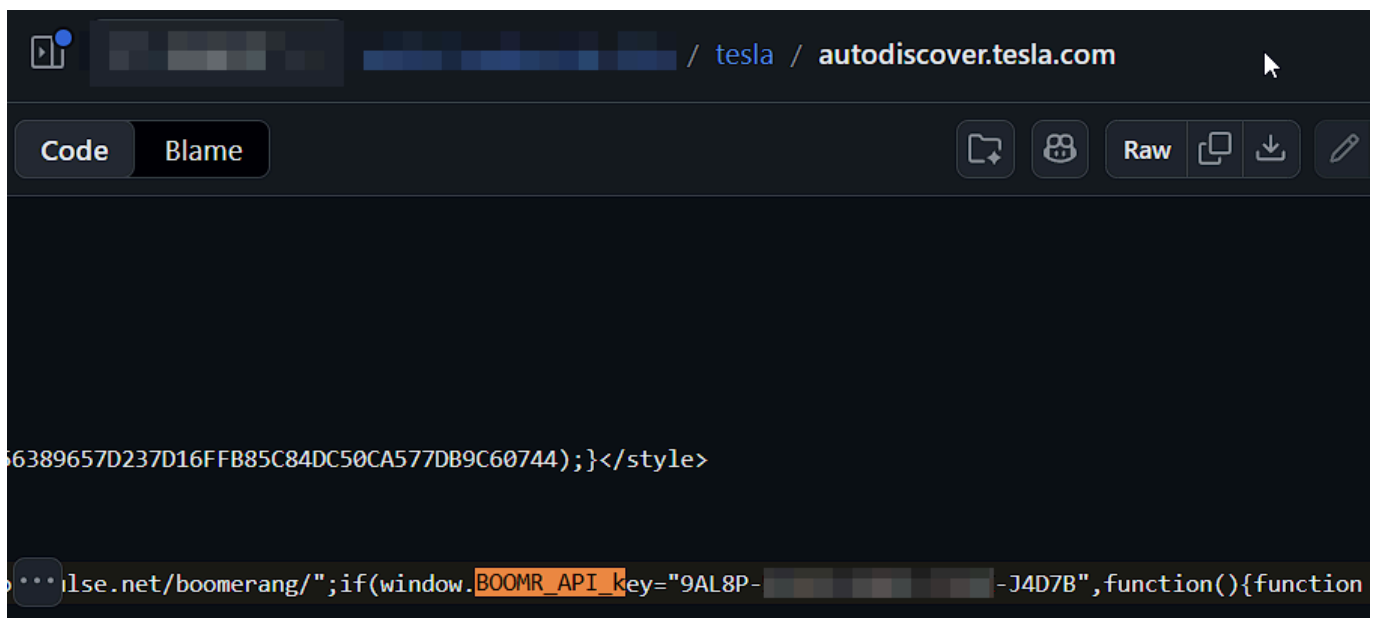
Removed

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

Individus avec profils sociaux



Identifiants en base de code



HORS RAPPORT : Les métadonnées

Partie Hors Rapport, donc c'est moi qui parle.

J'exporte le Markdown en PDF (je fais un premier export avant de rédiger pour exploiter les métadonnées) et voici le retour terminal :

```
> exiftool .\TP4_BOICHE_Gauvain.pdf
ExifTool Version Number      : 13.59
File Name                    : TP4_BOICHE_Gauvain.pdf
Directory                    : .
File Size                    : 794 kB
File Modification Date/Time   : 2026:06:09 17:14:56+02:00
File Access Date/Time        : 2026:06:09 17:16:09+02:00
File Creation Date/Time      : 2026:06:09 15:52:39+02:00
File Permissions              : -rw-rw-rw-
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.4
Linearized                   : No
Page Count                   : 7
Tagged PDF                   : Yes
Language                     : en-US
Title                        : TP4_BOICHE_Gauvain.md
Creator                      : Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/149.0.0.0 Safari/537.36
Edg/149.0.0.0
Producer                     : Skia/PDF m149
Create Date                  : 2026:06:09 15:14:55+00:00
Modify Date                  : 2026:06:09 15:14:55+00:00
```

```
> exiftool .\TP4_BOICHE_Gauvain.md
ExifTool Version Number      : 13.59
File Name                    : TP4_BOICHE_Gauvain.md
Directory                    : .
File Size                    : 8.9 kB
File Modification Date/Time   : 2026:06:09 17:14:52+02:00
File Access Date/Time        : 2026:06:09 17:14:52+02:00
File Creation Date/Time      : 2026:06:09 15:48:39+02:00
File Permissions              : -rw-rw-rw-
File Type                    : TXT
File Type Extension          : txt
MIME Type                    : text/plain
MIME Encoding                 : utf-8
Byte Order Mark               : No
Newlines                     : Windows CRLF
Line Count                   : 139
Word Count                   : 1218
```

Ce n'est pas grand chose. Je prends un de mes vieux CV pour voir si les métadonnées que j'y ai passées sont bien affichées :

```
> exiftool .\BOICHE_Gauvain_CV_Devops_01.pdf
ExifTool Version Number      : 13.59
File Name                    : BOICHE_Gauvain_CV_Devops_01.pdf
Directory                    : .
```



```

File Size : 285 kB
File Modification Date/Time : 2025:07:25 11:08:52+02:00
File Access Date/Time : 2025:07:31 09:52:20+02:00
File Creation Date/Time : 2025:07:25 11:08:52+02:00
File Permissions : -rw-rw-rw-
File Type : PDF
File Type Extension : pdf
MIME Type : application/pdf
PDF Version : 1.7
Linearized : Yes
Language : fr-FR
XMP Toolkit : Adobe XMP Core 9.1-c002 79.a6a6396, 2024/03/12-07:48:23
Format : application/pdf
Title : Curriculum Vitae - Gauvain BOICH  
Creator : Gauvain BOICH  
Rights : Les   l  ments pr  sents peuvent librement servir d'inspiration.
Create Date : 2025:07:25 11:08:51+02:00
Metadata Date : 2025:07:25 11:08:51+02:00
Modify Date : 2025:07:25 11:08:51+02:00
Creator Tool : Adobe InDesign 19.4 (Windows)
Instance ID : uuid:1abfa9bc-9932-4199-91e0-8d855f45b98d
Original Document ID : xmp.did:3d94839e-3e42-d742-8ba4-d2b929b49275
Document ID : xmp.id:94e5fbc4-11d0-f245-8fb0-2d135c6aa1cb
Rendition Class : proof:pdf
History Action : converted
History Parameters : from application/x-indesign to application/pdf
History Software Agent : Adobe InDesign 19.4 (Windows)
History Changed : /
History When : 2025:07:25 11:08:51+02:00
Derived From Instance ID : xmp.iid:7cd9b83f-2caa-f944-9109-f24033eabcec
Derived From Document ID : xmp.did:3d94839e-3e42-d742-8ba4-d2b929b49275
Derived From Original Document ID: xmp.did:3d94839e-3e42-d742-8ba4-d2b929b49275
Derived From Rendition Class : default
Authors Position : Administrateur Syst  mes & R  seaux
Country : France
City : [Ca je censure pour ici, faut pas d  conner]
Date Created : 2024:03:09 17:00
Marked : False
Producer : Adobe PDF Library 17.0
Trapped : False
Creator Work Telephone : [Ca je censure pour ici, faut pas d  conner]
Creator Work Email : [Ca je censure pour ici, faut pas d  conner]
Creator Work URL : https://gauvainboiche.bzh
Creator City : [Ca je censure pour ici, faut pas d  conner]
Creator Country : [Ca je censure pour ici, faut pas d  conner]
Creator Postal Code : [Ca je censure pour ici, faut pas d  conner]
Page Layout : OneColumn
Page Count : 1
Profile CMM Type : Linotronic
Profile Version : 2.1.0
Profile Class : Display Device Profile
Color Space Data : RGB

```

```

Profile Connection Space      : XYZ
Profile Date Time            : 1998:02:09 06:49:00
Profile File Signature       : acsp
Primary Platform             : Microsoft Corporation
CMM Flags                    : Not Embedded, Independent
Device Manufacturer         : Hewlett-Packard
Device Model                 : sRGB
Device Attributes            : Reflective, Glossy, Positive, Color
Rendering Intent              : Perceptual
Connection Space Illuminant  : 0.9642 1 0.82491
Profile Creator              : Hewlett-Packard
Profile ID                   : 0
Profile Copyright            : Copyright (c) 1998 Hewlett-Packard Company
Profile Description          : sRGB IEC61966-2.1
Media White Point            : 0.95045 1 1.08905
Media Black Point            : 0 0 0
Red Matrix Column            : 0.43607 0.22249 0.01392
Green Matrix Column          : 0.38515 0.71687 0.09708
Blue Matrix Column           : 0.14307 0.06061 0.7141
Device Mfg Desc              : IEC http://www.iec.ch
Device Model Desc            : IEC 61966-2.1 Default RGB colour space - sRGB
Viewing Cond Desc            : Reference Viewing Condition in IEC61966-2.1
Viewing Cond Illuminant     : 19.6445 20.3718 16.8089
Viewing Cond Surround        : 3.92889 4.07439 3.36179
Viewing Cond Illuminant Type : D50
Luminance                   : 76.03647 80 87.12462
Measurement Observer         : CIE 1931
Measurement Backing          : 0 0 0
Measurement Geometry         : Unknown
Measurement Flare            : 0.999%
Measurement Illuminant       : D65
Technology                   : Cathode Ray Tube Display
Red Tone Reproduction Curve  : (Binary data 2060 bytes, use -b option to
extract)
Green Tone Reproduction Curve : (Binary data 2060 bytes, use -b option to
extract)
Blue Tone Reproduction Curve  : (Binary data 2060 bytes, use -b option to
extract)
Author                       : Gauvain BOICHE

```

C'est déjà plus rigolo. Mais contrôlé.

Voici un effet de nettoyage du PDF :

```

> exiftool .\TP4_BOICHE_Gauvain.pdf
ExifTool Version Number      : 13.59
File Name                    : TP4_BOICHE_Gauvain.pdf
Directory                    : .
File Size                     : 794 kB
File Modification Date/Time   : 2026:06:09 17:14:56+02:00
File Access Date/Time        : 2026:06:09 17:16:22+02:00
File Creation Date/Time      : 2026:06:09 15:52:39+02:00

```

```
File Permissions      : -rw-rw-rw-
File Type             : PDF
File Type Extension   : pdf
MIME Type             : application/pdf
PDF Version           : 1.4
Linearized            : No
Page Count            : 7
Tagged PDF            : Yes
Language              : en-US
Title                 : TP4_BOICHE_Gauvain.md
Creator               : Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/149.0.0.0 Safari/537.36
Edg/149.0.0.0
Producer              : Skia/PDF m149
Create Date           : 2026:06:09 15:14:55+00:00
Modify Date           : 2026:06:09 15:14:55+00:00
```

```
> exiftool -all= .\TP4_BOICHE_Gauvain.pdf
```

```
Warning: [minor] ExifTool PDF edits are reversible. Deleted tags may be recovered!
```

```
- ./TP4_BOICHE_Gauvain.pdf
  1 image files updated
```

```
> exiftool .\TP4_BOICHE_Gauvain.pdf
```

```
ExifTool Version Number : 13.59
File Name                 : TP4_BOICHE_Gauvain.pdf
Directory                 : .
File Size                 : 794 kB
File Modification Date/Time : 2026:06:09 17:21:50+02:00
File Access Date/Time     : 2026:06:09 17:21:50+02:00
File Creation Date/Time   : 2026:06:09 15:52:39+02:00
File Permissions          : -rw-rw-rw-
File Type                 : PDF
File Type Extension       : pdf
MIME Type                 : application/pdf
PDF Version               : 1.4
Linearized                : No
Page Count                : 7
Tagged PDF                : Yes
Language                  : en-US
```