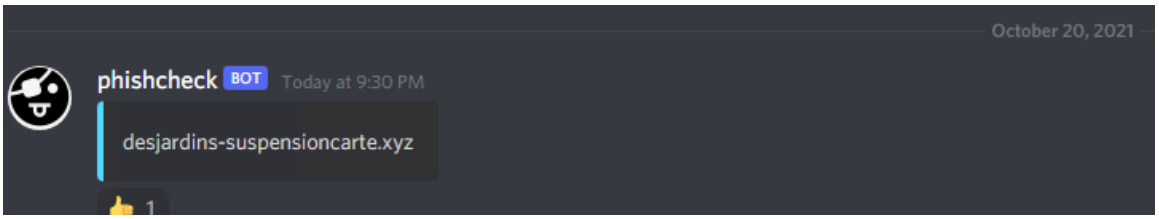
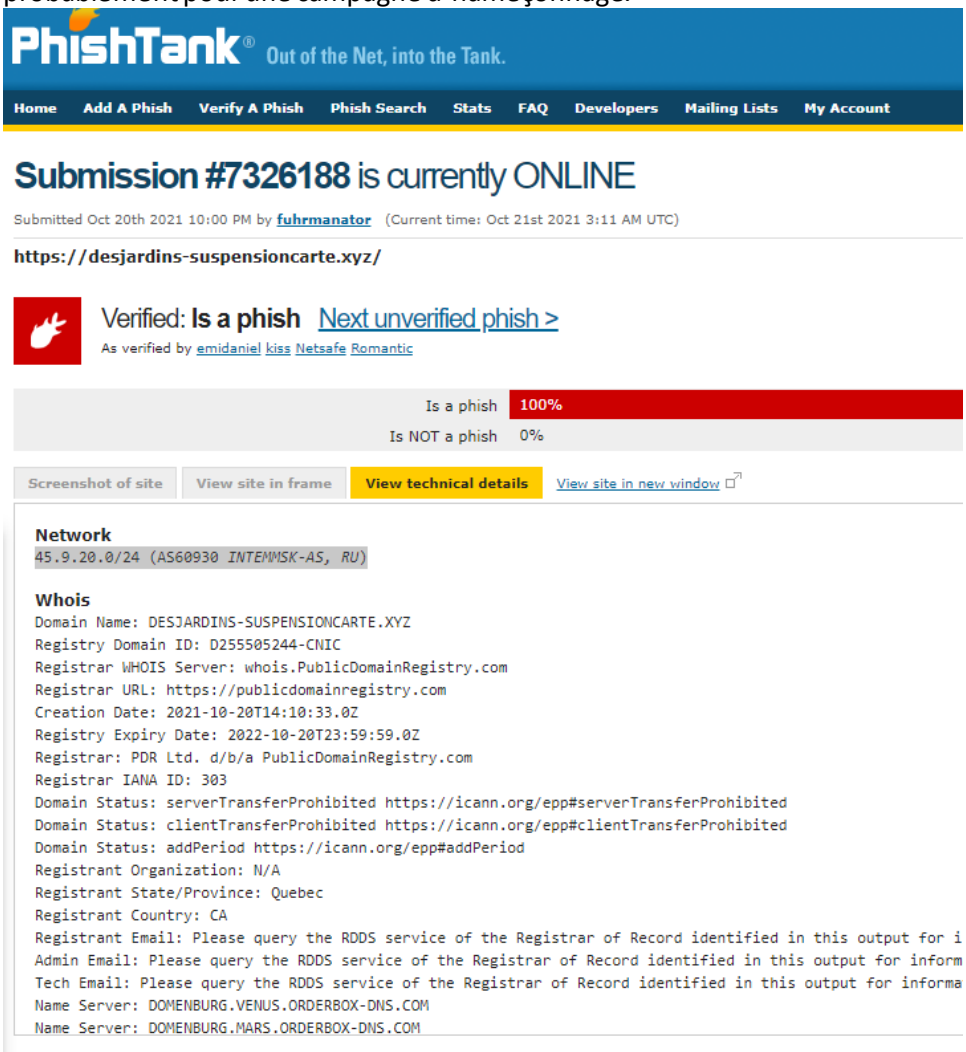
**** Avertissement, ce texte contient un peu de sarcasme qui pourrait offenser certains êtres humains dotés d'une âme sensible ****

Un script qui surveille certains mots clés dans des listes/ioc d'hameçonnage retourne une notification à 21:30 PM le 20 octobre (heure de Québec) sur un obscur serveur discord :




Une vérification sur le site phishtank.com semble confirmer qu'il s'agit d'un site/domaine qui est ou sera utilisé très probablement pour une campagne d'hameçonnage.




Le domaine a été enregistré le 20 octobre.

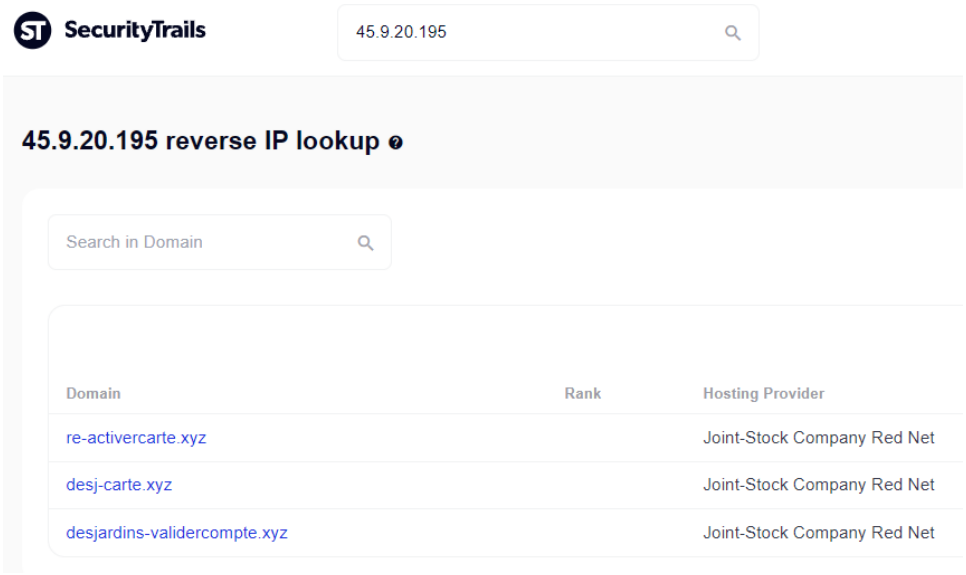
Let's encrypt a délivré un certificat pour ce domaine le 20 octobre :
https://transparencyreport.google.com/https/certificates?cert_search_auth=&cert_search_cert=&cert_search=include_subdomains:false;domain:desjardins-suspensioncarte.xyz&lu=cert_search

État actuel :

| Autorité de certification | Nombre de certificats émis | |
|---|---|---|
| C=US, O=Let's Encrypt, CN=R3 | 2 | Filtrer |

| Objet | Autorité de certification | Nombre de noms DNS | Valide à partir du | Valide jusqu'au | Nombre de journaux du projet de transparence des certific |
|---|---|---|---|---|---|
| desjardins-suspensioncarte.xyz | R3 | 1 | 20 oct. 2021 | 18 janv. 2022 | |
| desjardins-suspensioncarte.xyz | R3 | 1 | 20 oct. 2021 | 18 janv. 2022 | |

Le domaine pointe sur un IP en Russie 45.9.20.195
Selon securitytrails.com, cet IP héberge 3 autres sites/domaines qui semble cibler exclusivement Desjardins :




Le domaine re-activercarte.xyz est enregistré depuis le 7 octobre 2021 (14 jours) et n'est pas identifié comme hameçonnage/malveillant/nameIT sur les listes
Exemple virustotal :
https://www.virustotal.com/gui/url/5f98dbbb15ea7f7b3f563aa5d3c38dc7f3825043fe630846104c115ecda4cd7a/detection
let's encrypt a délivré un certificat pour ce domaine le 7 octobre :
https://crt.sh/?q=re-activercarte.xyz

crt.sh Identity Search Group by Issuer

| Criteria | Type: Identity Match: ILIKE Search: 're-activercarte.xyz' |
|---|---|

Certificates

| crt.sh ID | Logged At ⇧ | Not Before | Not After | Common Name | Matching Identities | Issuer Name |
|---|---|---|---|---|---|---|
| 5370727654 | 2021-10-07 | 2021-10-07 | 2022-01-05 | re-activercarte.xyz | re-activercarte.xyz | C=US, O=Let's Encrypt, CN=R3 |
| 5370728105 | 2021-10-07 | 2021-10-07 | 2022-01-05 | re-activercarte.xyz | re-activercarte.xyz | C=US, O=Let's Encrypt, CN=R3 |

Le domaine desj-carte.xyz est enregistré depuis le 11 octobre 2021 (10 jours) et semble identifié comme hameçonnage seulement par phishlabs (depuis 13 heures).
Let's encrypt a délivré un certificat pour ce domaine le 11 octobre 2021 :

https://crt.sh/?q=desj-carte.xyz


| Criteria | Type: Identity Match: ILIKE Search: 'desj-carte.xyz' |
|---|---|

Certificates

| crt.sh ID | Logged At ⇧ | Not Before | Not After | Common Name | Matching Identities | Issuer Name |
|---|---|---|---|---|---|---|
| 5395232879 | 2021-10-11 | 2021-10-11 | 2022-01-09 | desj-carte.xyz | desj-carte.xyz | C=US, O=Let's Encrypt, CN=R3 |
| 5395231908 | 2021-10-11 | 2021-10-11 | 2022-01-09 | desj-carte.xyz | desj-carte.xyz | C=US, O=Let's Encrypt, CN=R3 |

Le domaine desjardins-validercompte.xyz est enregistré depuis le 16 octobre 2021 (5 jours) . Ce domaine n'est pas identifié comme hameçonnage/malveillant/etc sur les listes. Ce domaine était même inconnu de la part de virustotal avant il y a quelques minutes lorsque je l'ai soumis.
Let's encrypt a délivré un certificat pour ce domaine le 16 octobre. J'aurais pensé que minimalement Desjardins fait minimalement une recherche sur le mot "desjardins" dans les journaux "certificate transparency" https://transparencyreport.google.com/https/certificates.


| Criteria | Type: Identity Match: ILIKE Search: 'desjardins-validercompte.xyz' |
|---|---|

Certificates

| crt.sh ID | Logged At ⇧ | Not Before | Not After | Common Name | Matching Identities | Issuer Name |
|---|---|---|---|---|---|---|
| 5426038204 | 2021-10-16 | 2021-10-16 | 2022-01-14 | desjardins-validercompte.xyz | desjardins-validercompte.xyz | C=US, O=Let's Encrypt, CN=R3 |
| 5426039643 | 2021-10-16 | 2021-10-16 | 2022-01-14 | desjardins-validercompte.xyz | desjardins-validercompte.xyz | C=US, O=Let's Encrypt, CN=R3 |

Recommandation pour Desjardins :

1.
Entamer les démarches pour que ces sites et cet IP soient blacklistés par la majorité des solutions de sécurité.

2.
Les journaux "Certificate Transparency" sont comme nos informations personnelles, elles sont disponible s gratuitement sur internet.
Il existe des solutions gratuites ( voir sur github ) pour récupérer presque en temps réels les journaux d'émissions de certificats. Ensuite, en fonction d'une liste de mots/pattern vous pouvez faire des recherches pour identifier des domaines qui pourraient potentiellement être utilisés pour usurper votre identité corporative pour inciter vos clients à soumettre des informations sensibles à une personne malveillante, sans que cette dernière n'ai eu à débourser en carte cadeau St-Hubert.
Il existe aussi des solutions payantes qui pour moins de 2 000$ par années ( pour contextualiser 2 000$, ça équivaut à 40 cartes cadeaux St-Hubert de 50 dollars chacune ou encore ça équivaut aux données personnelles d'environ 2 000 de vos clients selon l'indice François Baillargeon-Bouchard (payé cash pas de facture, pas de taxe)),

3.
Abonnement à des feed/ioc/liste en lien avec le phishing pour identifier des domaines comme "desjardins-validercomte.xyz" (suggestion de recherche : * Desjardins*, *accesd* , *accessd*, *ilyatudupouleticitte-si-ilyapasdepouleticitte-moijecrissmoncampdicitte.com*

4.
Pour les prochains jours, surveiller étroitement l'IP 45.9.20.195,

5.

Si ce n'est pas Desjardins qui est responsable de l'acquisition des noms de domaine ci-dessous, il serait préférable de les surveiller étroitement :
desjardins.top le 13 octobre 2021 (8 jours)
desjardins.xyz en septembre 2021

Après avoir procédé à la collecte massive toutes ces données (big data) dans mon logiciel d'intelligence artificielle et superficielle sec/dev/lol/impro*ops , il a été possible d'identifier certain point commun qui sont normalement impossible à identifier sans un cluster d'ordinateur quantique ( military grade multi-cloud-trust security with zero trust ).

- Les 4 domaines sont achetés à quelques jours d'interval
- Ils pointent tous vers le même IP
- Ils obtiennent un certificat émis par let's encrypt le même jour que la création du nom de domaine
- Enregistrés chez le même registraire
- Les 4 domaines utilisent la même entrée SOA Email "s007.yopmail.com". Cette entrée SOA est associée à au moins 3 autres noms de domaine qui semble être toujours dans le même thème :

validationcar.xyz
valider.xyz
validatecar.fun
desjardins-validecompte.xyz

- Les nouveaux domaines identifiéss pointent vers l'IP 45.9.20.146
    - Le 24 septembre 2021 l'ip 45.9.20.146 exposait un certificat let's encrypt au nom de desjardins-valders.xyz
    - Le 2 octobre 2021 l'ip 45.9.20.146 exposait un certificat let's encrypt au nom de val-infos.xyz
    - Le 3 octobre 2021 l'ip 45.9.20.146 exposait un certificat let's encrypt au nom de infos-val.xyz
    - Le 10 octobre 2021 l'ip 45.9.20.146 exposait un certificat let's encrypt au nom de validatecar.fun
    - Le 13 au 15 octobre 2021 l'ip 45.9.20.146 exposait un certificat let's encrypt au nom de valider.xyz

Résumé : Plusieurs domaines en "stand-by" prêt à être utilisé pour des campagnes d'hameçonnage visant Desjardins.

1. desjardins-suspensioncarte.xyz, re-activercarte.xyz ,desj-carte.xyz, desjardins-validercompte.xyz, 45.9.20.195
2. desjardins-validecompte.xyz, validationcar.xyz, valider.xyz, validatecar.fun, 45.9.20.146

Il est possible relativement facilement d'automatiser la surveillance de « mots/patterns » et de recevoir des notifications lorsqu'un des mots est identifié dans une des listes qui sont analysées.

Bien que le code de mon script soit très probablement gênant à exposer, je suis prêt à fournir une partie de mon script à Desjardins à condition que j'aie des garanties écrites que le nom du fichier de script sur le serveur se nommera « que-celui-qui-na-jamais-vendu-son-ame-comme-sebastienboulangerdorval-pour-des-cartes-st-hubert-lui-lance-la-premiere-cuisse.sh ».