Le point d'entrée du fraudeur:
Mettant fin au « transfert de SIM » au Canada

Exposé pour le Comité Permanent de L'industrie, des Sciences et de la Technologie

Randall Baran-Chong
Cofondateur de « Canadian SIM-swap Victims United »
Le 12 mars 2020
Traduction: Chelsea Lee

« La TNSF (Transférabilité des Numéros Sans Fil) est une initiative au service des consommateurs qui leur offrira plus de choix et qui rendra possible un marché des services plus concurrentiel. Cette initiative s'inscrit dans l'objectif du gouvernement de restructurer le secteur des télécommunications en vue d'en faire bénéficier les consommateurs...»

- Maxime Bernier, Ministre de l'industrie, le 14 mars 2007[1]

Malgré ces bonnes intentions, cette commodité a ouvert la porte aux fraudeurs au portage non autorisé/SIM swap scamming.

SIM*-swap Scam

Connu sous le nom « transfert de *SIM » ou « *Le portage non autorisé»*

Le transfert d'un numéro de téléphone d'une carte SIM par quelqu'un sans l'autorisation du titulaire de compte.

De l'anglais * – « *Subscriber Identity Module* »

La structure du « *SIM swap* »*

1 Collection des informations

L'objectif

Tout renseignement personnel:

- Numéro de téléphone et l'un des suivants :
- Numéro de compte
- L'ID- d'appareil, par exemple, IMEI

La Méthode

- Ingénierie sociale (l'opérateur de téléphonie mobile)
- Hameçonnage
- Informations ouvertes, par exemple les réseaux sociaux
- Les fuites des données, par exemple la violation de Koodo[3]
- Les employés internaux

2 L'exécution du portage

Créer un nouveau compte

Le fraudeur achète un téléphone prépayé sans présentant l'identification personnelle

Le fraudeur demande le portage

Avec l'information correcte, le nouveau opérateur de téléphonie mobile exécute l'ordre de l'opérateur initiale dans quelques heures

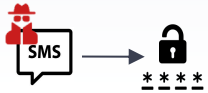
Indisponible

La carte SIM est débranchée du réseau

3 Prise de possession

Le portage est complet

Tous les appels et les SMS sont envoyés au fraudeur



Oublier? Réinitialiser!

Le fraudeur identifie des comptes communs en utilisant l'authentification à double facteur[5], et il réinitialise les mots de passe pour bloquer l'accès au client

Le client remarque...

Le client rapport la fraude

4 Le pillage

Le chaos systématique

Le fraudeur travaille vitement et prend les comptes, incluant :

- Le courriel
- Les comptes cryptomonnaies
- Les services bancaires en lignes
- Les applications avec une carte de crédit associée
- Le stockage en nuage
- Les réseaux sociaux

Récupération de compte

Le client contacte leur opérateur de téléphonie mobile (des heures ou jours pour récupérer)

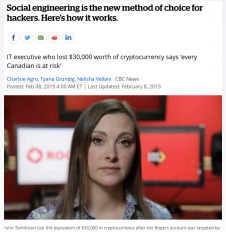
* – reflète un scénario commun de recherche primaire et sécondaire

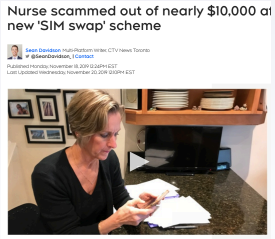
Le mal est fait…

Les vols :

Accès aux comptes bancaires ou cryptomonnaies

Faire des achats en ligne





Les vols de données :

L'extorsion ou le chantage

La monétisation des données ou de l'identité sur le « *dark web* »

« Prix du marché »[6]:

Informations d'intentifications : 20 – 120 $

ID complète : 3 000 $ ou plus

Le piratage de comptes ou l'usurpation d'identité :

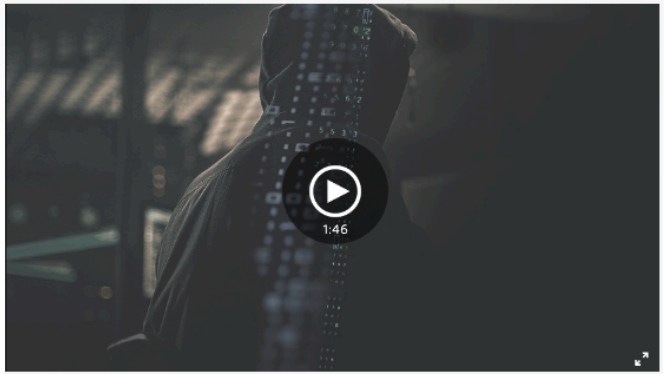
Le « *trolling*» de comptes des vedettes

Des comptes originaux « *OG* »

Note: Les images sont un lien aux sources des médias.

…et les canadiens en profitent…

Un présumé pirate montréalais aurait volé des millions en cryptomonnaie



Un jeune crack en informatique de 18 ans, dont la résidence des parents a fait l'objet d'une perquisition à Montréal par la police de Toronto et la Sûreté du Québec en novembre dernier, est soupçonné de faire partie d'un cercle de pirates informatiques qui a dérobé des dizaines de millions de dollars en accédant aux téléphones cellulaires de détenteurs de cryptomonnaies.

En novembre 2019, un Montréalais de 18 ans a été arrêté pour sa participation au vol de **300 000 $ au Canada et 50 M$ de cryptomonnaies des Américains**.[7]

Les «transferts de SIM » ne sont pas de la haute technologie. En fait, la plupart des gens arrêtés aux États-Unis et au Canada ont moins de 25 ans.[8]

La réalité est…

Nos numéros de téléphones sont notre **nouvelle forme d'identité**.

La sécurité est aussi **forte que le maillon le plus faible**, qu'elle soit technique ou facteur humain.

Le portage non autorisé a un impact **dévastateur toute un vie**, même s'il n'est pas répandu.

Il n'existe pas de solution parfaite, mais l' éducation, la coopération, et un changement de paradigme vers **« *non-SMS 2FA* »** peuvent nous aider.

De toute façon, tous les clients de services sans fil canadiens sont en danger.

Et ailleurs?

Aux États-Unis : les « transferts de SIM » sont une ménace sérieuse

Lettre du Sénateur Ron Wyden au Président Pai du FCC, janvier 2020[9]

Menacer les consommateurs: via les fraudes financières (estimé à 70 M$ et plus de 3 000 cas) et la violation de la vie privée.

Menacer la sécurité nationale: un « ...cybercriminel ou gouvernement étranger peut utiliser une carte SIM a pirater... »; il peut l'utiliser contre « un fonctionnaire de sécurité publique locale pour émettre des alertes d'urgence »

Actions: un examen de la réglementation et l'identification des réformes

Mondial: l'identification du risque de fraude

La réforme de partage des données en Afrique[10]

Le Mozambique a initié le partage des données en temps reel en 2018: un système API de « oui/non » identifie si le consommateur a exécuté un portage pendant un temps donné comme approche d' évaluation du risque pour identifier les transferts d'argent suspicieux.

Actions: les approches similaires déjà adoptées en Zambie, au Kenya, et au Nigéria

En Australie: une réforme des réglementations à réduire le portage non autorisé

L'ACMA codifie des nouvelles mesures[11,12]

L'introduction d'un nouveau processus avant le portage: le nouveau opérateur communique par appel ou SMS avec le consommateur avant le portage (ou en personne avec l'identification du gouvernement)

Les amendes jusqu' à 250 000 $ A pour les processus de vérifications faibles.

L' éducation publique par les entreprises de télécom pour apprendre ces mesures.

Actions: annoncé le 28 février 2020; mis en place le 30 avril 2020

Le portage non autorisé au Canada

La communication sur le portage non autorisé

- En octobre 2019 : le conseil WNP* élabore un « accorde de principe »; les opérateurs peuvent réviser leur calendrier du projet[13]
- Le 15 janvier 2020 : CRTC envoye une lettre[14] à CWTA à propos du portage non autorisé : l' état, la prévalence, les actions, etc.
- Le 14 février 2020: CWTA, les réponses des opérateurs[15,16] – **aucune communication au public des chiffres ni des actions**

Les actions jusqu'à présent par les opérateurs[18]

- **Les pratiques varient** par opérateur
- Les incohérences dans les pratiques de protection offertes **par les représentants du service à la clientèle**
- **Les fraudes continuent** avec une notification du portage par SMS et la solution de « appel si ce n'est pas vous »:
  - Le scepticisme du SMS[19]
  - Trop rapidement exécuté pour réagir[20]
  - Ne peut pas atteindre le service hotline[21]

L'engagement du public et la réduction du portage non autorisé

- Le 21 janvier 2020 : le PIAC envoye une lettre à demander pour un avis de consultation[21]
- Le 30 janvier 2020 : le CWTA a répondu que – **« la consultation publique n'apporterait pas de valeur… »** [22]
- **Les expériences des victimes sont les meilleurs promoteurs de la sensibilisation** du portage non autorisé
- Le manque de sensibilisation des **alternatives** plus sécurisées que l'authentification à double facteur par SMS

Les préoccupations

L'erreur « sécurité par l'obscurité »[17]

Aucune indication comment le CRTC l'évalue, le mesure ni l'enforce

Incohérent, des pratiques inefficaces entre les opérateurs

L'ignorance des problèmes et des solutions du public

* – Le conseil *Wireless Network Portability* (WNP) consiste de Bell, Eastlink, Freedom Mobile, Rogers, SaskTel, Tbaytel, TELUS et Vidéotron

L'appel à l'action au Canada

La demande: une solution cohérente de friction minimale

Le CRTC codifiera une pratique d'authorisation avant le portage d'une carte SIM aux règlements du WNP

(comme la politique australienne)

Le CRTC étudier avec l'aide de industrie la possibilité d'adopter des protections supplémentaires

(mot de passe obligatoire)

La demande: plus de transparence et de la résponsibilité

Le CRTC annoncera le plan du conseil WNP

(incluant la formation des employés et la gestion des intervenants)

Le progrès, le prévalence du portage non autorisé et l'application mise en place seront transparents au public

La demande: l'investissement dans l' éducation du public

Étudier et faciliter l'adoption d'une alternative plus sécurisée que l'authentification à double facteur par SMS dans des principaux organismes et industries

Campagne publique sur les risques de l'authentification facteur et les alternatives plus sécurisées

Merci de votre attention.

Laissez-nous changer le monde du portage non autorisé…

Canadian SIM-swap Victims United | March 12, 2020

Références

1. "Wireless Portability Now Available in Canada" https://www.canada.ca/en/news/archive/2007/03/wireless-number-portability-now-available-canada.html
2. "Canadian Wireless Telecommunications Association (CWTA) response to CRTC file: 8665-C12-202000280": https://crtc.gc.ca/public/otf/2020/c12_202000280/3806745.pdf
3. "Telus Says Koodo Suffered Data Breach Leaking Account and Phone Numbers": https://www.iphoneincanada.ca/carriers/telus/telus-koodo-data-breach/
4. "Telecom Decision CRTC 2005-72": https://crtc.gc.ca/eng/archive/2005/dt2005-72.htm
5. "Two Factor Auth List": https://twofactorauth.org/#social
6. "IMF: The Truth About the Dark Web", Sept. 2019: https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm#targetText=A%20recent%20report%20by%20a,than%20%241%20billion%20in%202019.
7. "Un présumé pirate montréalais aurait volé des millions en cryptomonnaie": https://www.lapresse.ca/actualites/justice-et-faits-divers/202001/12/01-5256560-un-presume-pirate-montrealais-aurait-vole-des-millions-en-cryptomonnaie.php
8. "The Rise of SIM Swapping": https://www.nasdaq.com/articles/the-rise-of-sim-swapping%3A-how-and-why-bitcoiners-need-to-protect-themselves-2020-02-04
9. "010920 SIM Swap Scam Letter to FTC", January 9, 2020: https://www.wyden.senate.gov/imo/media/doc/010920%20SIM%20Swap%20Scam%20Letter%20to%20FTC.pdf
10. "The SIM Swap Fix That the US Isn't Using ": https://www.wired.com/story/sim-swap-fix-carriers-banks/
11. "Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020": https://www.legislation.gov.au/Details/F2020L00179
12. "ACMA Announces New Measures to Fight Mobile Number Fraud": https://www.acma.gov.au/articles/2020-02/acma-announces-new-measures-fight-mobile-number-fraud
13. "CWTA response to CRTC file: 8665-C12-202000280": https://crtc.gc.ca/public/otf/2020/c12_202000280/3806745.pdf
14. "Telecom Commission Letter addressed to Mr. Eric Smith (Canadian Wireless Telecommunications Association)": https://crtc.gc.ca/eng/archive/2020/lt200115.htm
15. "CWTA response to CRTC file: 8665-C12-202000280": https://crtc.gc.ca/public/otf/2020/c12_202000280/3806745.pdf
16. "Fraudulent Wireless Customer Transfers – 2020 – 01 – 15": https://crtc.gc.ca/otf/eng/2020/8665/c12_202000280.htm
17. "What is Security Through Obscurity?": https://securitytrails.com/blog/security-through-obscurity
18. "CRTC Should Open Public Consultations to Update Port Protection, Industry Experts": https://ca.finance.yahoo.com/news/crtc-should-open-public-consultations-to-update-existing-number-port-protection-industry-experts-143838064.html
19. "New scam uses your phone number to steal your online identity": https://winnipeg.ctvnews.ca/new-scam-uses-your-phone-number-to-steal-your-online-identity-1.4815791
20. "Vancouver man says scammers stole his phone number to access his online accounts": https://vancouversun.com/news/local-news/vancouver-man-says-scammers-stole-his-phone-number-to-access-his-online-accounts
21. "London woman recounts cellphone scam that led to theft of passwords, number": https://lfpress.com/news/local-news/london-woman-victim-of-cellphone-porting-scam
22. Public Interest Advocacy Centre (PIAC) Letter to CRTC Requesting Commission to Issue a Notice of Consultation: https://crtc.gc.ca/public/otf/2020/c12_202000280/3791193.pdf
23. CWTA response to PIAC January 21, 2020 Letter: https://crtc.gc.ca/public/otf/2020/c12_202000280/3797644.pdf