RSA sÃ©curitÃ© : Chercheurs dâ□□emplois â□□ gare aux offres frauduleuses !
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 15/1/2010 0:00:00

Quand les pirates informatiques crÃ©ent de fausses offres dâ□□emploi : vigilance ! Depuis lâ□□automne dernier, le laboratoire de recherche **RSA Fraud Action** enquÃªte sur diffÃ©rents mÃ©canismes de la Â« fraude Ã la logistique dâ□□expÃ©dition Â».

Cette fraude particuliÃ¨re consiste Ã Â« encaisser Â» des marchandises achetÃ©es frauduleusement en ligne avec des cartes de paiement volÃ©es, en faisant appel Ã des Â« Mules Â» par le biais de fausses offres dâ□□emploi.

Le laboratoire de recherche RSA FraudAction est parvenu Ã mettre Ã jour le fonctionnement dâ□□Air Parcel Express, un service de rÃ©expÃ©dition Ã grande Ã©chelle, centralisÃ© et opÃ©rÃ© par un rÃ©seau de criminels, dont nous allons vous rÃ©vÃ©ler les dÃ©tails pour la premiÃ¨re fois.

Mode de fonctionnement de ce type dâ□□arnaque

Un ensemble de fraudeurs travaille en rÃ©seau. Une partie dâ□□entre eux achÃ¨tent des produits en ligne et paient avec des cartes de crÃ©dit volÃ©es ; les autres revendent ces produits acquis frauduleusement. Ces cartes ont souvent Ã©tÃ© volÃ©es Ã la suite de malversations informatiques (phishing, chevaux de Troie, piratage de bases de donnÃ©es de commerÃ§ants, etc.) et sont utilisÃ©es, sans scrupule, par les fraudeurs. Lâ□□argent collectÃ© suite Ã la revente de ces produits est partagÃ© entre les membres de ce rÃ©seau.

ConcrÃ¨tement, pour pouvoir revendre ces produits, les fraudeurs ont recours Ã des Mules. Ces Mules, recrutÃ©es Ã leur insu, sont tout simplement des individus Ã la recherche dâ□□un emploi et qui scrutent rÃ©guliÃ¨rement les offres en ligne. Les fraudeurs publient de fausses offres dâ□□emplois sur des rÃ©seaux lÃ©gitimes, tels que des sites de recrutement ou des moteurs de recherche et, alors que ces offres sont particuliÃ¨rement attractives dans le climat Ã©conomique actuel (flexibilitÃ©, travail Ã domicile, salaire confortableâ□¦), les Mules rÃ©pondent

Ã lâ□□offre sÃ©lectionnÃ©e et sont recrutÃ©es. Dans la plupart des cas, ces mules ne savent pas pour qui elles travaillent et nâ□□ont aucune idÃ©e de lâ□□illÃ©galitÃ© des opÃ©rations qui sont menÃ©es sous couvert de cet emploi.

Leur travail est ensuite simple. Des marchandises achetÃ©es illÃ©galement leur sont livrÃ©es Ã leur domicile. Chaque mule nâ□□a plus quâ□□Ã rÃ©expÃ©dier les produits dans le pays dâ□□origine de son employeur, oÃ¹ rÃ©sident effectivement le fraudeur et ses complices. Les mules sont supposÃ©es recevoir une petite commission Ã chaque livraison, or, le plus souvent, celle-ci ne leur est jamais payÃ©e.

Le processus de rÃ©expÃ©dition rÃ©alisÃ© par la mule consiste Ã dÃ©conditionner les produits reÃ§us (sur lesquels figure la marque du vendeur), Ã les reconditionner dans un emballage neutre et Ã les livrer Ã lâ□□Â« employeur Â» dans un autre pays. Les marchandises rÃ©expÃ©diÃ©es sont gÃ©nÃ©ralement des ordinateurs portables, des smartphones ou dâ□□autres produits chers et high tech, peu encombrants et faciles Ã revendre en raison de la forte demande.

Lorsque le fraudeur (employeur) reÃ§oit la marchandise, il nâ□□a plus quâ□□Ã la revendre aux enchÃ¨res contre rÃ¨glement en espÃ¨ces. Le produit de la vente est ensuite partagÃ© entre les fraudeurs et leurs clients.

Exemple dâ□□Air Parcel Express

Le site Internet Air Parcel Express a Ã©tÃ© conÃ§u par des fraudeurs, spÃ©cialistes de la Â« fraude Ã la logistique dâ□□expÃ©dition Â». Le site avait pour objectif dâ□□asseoir la crÃ©dibilitÃ© dâ□□une sociÃ©tÃ© fictive de transport : Air Parcel Express, Inc (le site prÃ©sentÃ© ci-contre nâ□□est plus actif et nâ□□a jamais Ã©tÃ© celui dâ□□une firme lÃ©gitime).

Remarque importante : il existe bien une sociÃ©tÃ© de transport parfaitement lÃ©gitime et accrÃ©ditÃ©e, basÃ©e Ã Miami (Floride) et dÃ©nommÃ©e Air Parcel Express (ou APX). APX nâ□□est en aucune faÃ§on associÃ©e Ã cette fraude opÃ©rÃ©e sous le mÃªme nom pendant quelques mois.

Les offres dâ□□emploi visant Ã recruter des mules figuraient dans la section CarriÃ¨res du site, sous l'intitulÃ© Â« Correspondence Manager Â». La description de poste est parfaitement dÃ©taillÃ©e : responsabilitÃ©s majeures, qualitÃ©s personnelles et professionnelles requises, exigences du poste, conditions de travail, etc.

Comment Ã©viter ce type dâ□□arnaque

Les donnÃ©es collectÃ©es par RSA tendent Ã dÃ©montrer que plus de 1 900 personnes ont postulÃ© Ã une offre dâ□□emploi frauduleuse dâ□□Air Parcel Express Inc â□□ dont 30 ont Ã©tÃ© effectivement Â« engagÃ©es Â».

Le succÃ¨s de ces offres dâ□□emploi sâ□□explique par le manque dâ□□information du public sur ce type de fraude et par lâ□□attractivitÃ© de lâ□□offre dâ□□un point de vue financier.

Pourtant, pour un Â□il exercÃ©, les signes rÃ©vÃ©lateurs de la fraude sont patents dÃ¨s la page dâ□□accueil :

â□¢ Les textes anglais ne sont pas dâ□□excellente qualitÃ© et sont trop longs.

â□¢ Le site se rÃ©fÃ¨re Ã un nouvel entrepÃ´t basÃ© en Lettonie, or, on sait, par expÃ©rience, quâ□□il sâ□□agit dâ□□un pays particuliÃ¨rement prisÃ© par les fraudeurs.

â□¢ Des mots clÃ©s tels que Â« livraison rÃ©sidentielle Â», Â« intermÃ©diaire Â», Â« eBay Â» et Â«

crÃ©er une illusion Â» Ã©veillent la vigilance.

Il y a Ã©galement des dÃ©tails troubles sur le mode de paiement (ou non paiement) du salaire des mules pour les efforts fournis. Il est par exemple expliquÃ© aux mules quâ□□elles seront payÃ©es aprÃ¨s un mois complet dâ□□activitÃ© de rÃ©expÃ©dition. Dans ce cas elles effectuent les rÃ©expÃ©ditions puis au bout de ce laps de temps, lâ□□employeur peut cesser tout simplement de rÃ©pondre Ã leurs e-mails. Certaines mules semblent avoir reÃ§u des fonds de loin en loin, mais la plupart dâ□□entre eux nâ□□a jamais Ã©tÃ© payÃ©e. Selon les informations en possession de RSA, les personnes rÃ©alisent gÃ©nÃ©ralement quâ□□elles sont impliquÃ©es dans une fraude aprÃ¨s quelques rÃ©expÃ©ditions.

Parmi les biens rÃ©expÃ©diÃ©s lors de ces fraudes :

â□¢ PC Portables de marques reconnues :

â□¢ iPhones dâ□□Apple et smartphones Nokia

â□¢ Appareils photo Canon, Nikon et Kodak

â□¢ PlayStation 3 (Sony)

â□¢ SystÃ¨mes de mixage et Ã©quipements pour DJ Pioneer et Technics

â□¢ iPods dâ□□Apple

â□¢ Divers autres produits en dehors de lâ□□Ã©lectronique grand public

Identifier une offre dâ□□emploi frauduleuse â□□ Raisons de la vulnÃ©rabilitÃ© de certaines personnes

DiffÃ©rents organismes, tels que la Commission FÃ©dÃ©rale amÃ©ricaine sur le Commerce (FTC) ou Monster.com, ont fourni dâ□□importantes informations permettant d'Ã©viter ces offres dâ□□emploi frauduleuses.

Cependant, les fraudeurs tentent en permanence de dÃ©jouer les autoritÃ©s. Ils ne se limitent plus aux sites dâ□□offres dâ□□emploi et ont Ã©tendu leur champ dâ□□action en plaÃ§ant des annonces sur des sites majeurs dâ□□actualitÃ© tels que Google etc.

Il est possible quâ□□en raison des conditions Ã©conomiques instables, du fort taux de chÃ´mage et du besoin urgent de revenus pour les personnes sans emploi, les candidats dâ□□Air Parcel Express aient recherchÃ© des postes hors de leur domaine ou tout simplement aient Ã©tÃ© moins sÃ©lectifs quâ□□Ã lâ□□accoutumÃ©e. Reconnaissons que les offres sont attractives et promettent Â« de lâ□□argent facile Â» tout en travaillant Ã domicile. Elles sont pourtant parfaitement illÃ©gales.

Les candidats recrutÃ©s Ã leur insu pour participer Ã un montage frauduleux de ce type sont en outre menacÃ©s dâ□□usurpation dâ□□identitÃ© et de diffÃ©rentes autres fraudes, commises Ã leur insu par leur Â« employeur Â». Les fraudeurs opÃ©rant sous couvert dâ□□Air Parcel Express et dâ□□autres faÃ§ades similaires collectent en effet une multitude de donnÃ©es personnelles sur les candidats et les personnes effectivement recrutÃ©es.

Les mules sont donc aussi des victimes potentielles car :

â□¢ elles peuvent totalement ignorer leur implication dans une activitÃ© criminelle

â□¢ elles peuvent Ãªtre la cible dâ□□un vol dâ□□identitÃ© perpÃ©trÃ© par ceux Ã qui elles ont accordÃ© leur confiance pour leur fournir un emploi.

Les fraudes Ã la rÃ©expÃ©dition ne sont que lâ□□une des facettes dâ□□une vÃ©ritable chaÃ®ne de services frauduleux dâ□□approvisionnement en ligne. Dans le cas que nous venons de dÃ©voiler dans cette Ã©tude, une organisation criminelle propose Ã dâ□□autres fraudeurs des Â« prestations Ã la demande Â» (ou FaaS pour Â« Fraud-as-a-Service Â») pour simplifier les phases dâ□□Â« encaissement Â» postÃ©rieures Ã la fraude initiale au commerce en ligne. Cette malversation connaÃ®t de multiples variantes â□□ dâ□□autres consistant Ã recruter des mules passeurs dâ□□argent.

En fournissant les clÃ©s pour comprendre un mÃ©canisme tel que celui dâ□□Air Parcel Express, nous espÃ©rons aider plus dâ□□individus Ã Ã©viter de tomber dans les piÃ¨ges de la criminalitÃ© organisÃ©e.

Quâ□□est ce que le RSA Anti Fraud Command Center ?

Le RSA Â® Anti-Fraud Command Center (AFCC) analyse lâ□□activitÃ© de la fraude en ligne chaque mois pour RSA, la division sÃ©curitÃ© dâ□□EMC.

Le RSA Anti-Fraud Command Center est un centre de commandement antifraude. Actif 24h/24 et 7j/7, il aide les entreprises Ã dÃ©tecter, bloquer, surveiller, suivre et stopper le phishing, le pharming et les attaques de Trojan.

ProtÃ©geant plus de 300 entreprises contre les attaques en ligne, le RSA Anti-Fraud Command Center a contrecarrÃ© plus de 240 000 attaques de phishing Ã ce jour et est une source clÃ© pour le renseignement sur les nouvelles menaces en ligne.