وزارة المالية
MINISTERE DES FINANCES

CTRF CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER خلية معالجة الإستعلام المالي خ م إ

LETTRE D'INFORMATION : BON A SAVOIR (N°22)

Les nouvelles formes de scam : Les mules et le blanchiment

Méthode de nouveaux trafiquants: les scammeurs

Les nouvelles victimes de scam ne sont plus des individus naïfs qui se font soustraire leur argent. Maintenant, ce sont des personnes crédules mêlées à des trafics d'argent. Bientôt fini le temps du scams 419 où des correspondants soi-disant nigérians arnaquent des personnes naïves et leur soutirent jusqu'à plusieurs dizaines de milliers d'euros ? Il semble que la nouvelle forme de scam soit plus imaginative dans la mesure où le scammeur ne cherche plus à soutirer directement de l'argent à la victime. Il acquiert l'argent par d'autres moyens illégaux (vol de carte bleue, piratage de comptes bancaires ou de comptes paypal, etc…), mais se sert de la victime comme d'une mule.

En matière de trafic de drogue, une mule est une personne qui fait passer la drogue au travers des postes de contrôles. Le trafiquant a donc intérêt à choisir la mule qui semble la plus innocente possible, de manière à ne pas alerter les contrôleurs. De même, il doit cloisonner totalement la mule, qui ne devra pas savoir qui est son commanditaire.

En matière de fraudes sur l'Internet, le plus dur n'est pas la fraude elle-même, mais de pouvoir profiter des fruits de la fraude tout en restant intraçable. Or, pour recevoir l'argent ou les colis achetés grâce à une CB volée, il faut une identité et une adresse, tous les deux aisément traçables. C'est ici qu'interviennent les mules, que les scammeurs convainquent d'accepter de recevoir et garder un paquet ou une somme chez eux jusqu'à ce qu'on vienne les récupérer à une date future.

Le principe est le même que pour un scam traditionnel. Le scammeur entre en contact avec une mule potentielle.

Il faut noter ici l'apport immense des réseaux sociaux du type Facebook ou Second Life, qui facilitent la tâche des scammeurs, puisque non seulement on peut y trouver les centres d'intérêts de la mule, mais on peut également la contacter plus facilement que par l'envoi d'un mail classique dont les gens se méfient de plus en plus.

Imaginons un exemple typique : un scammeur va déterminer suivant le profil d'une personne qu'elle s'intéresse aux œuvres humanitaires destinées aux écoles du Tiers Monde. Il va alors imaginer un scam personnalisé en se faisant passer pour un directeur d'une école d'Afrique qui a besoin d'ordinateurs portables pour son école. Là où le scammeur classique va demander que la victime lui envoie de l'argent, le nouveau scammeur aura déjà obtenu l'argent autrement, et dira à sa victime que de généreux bienfaiteurs ont déjà acquis les matériels informatiques en question, mais que pour des problèmes d'acheminement (par ex, parce qu'un regroupement de marchandises dans un conteneur coûte moins cher), les matériels doivent être stockés temporairement en France. Malheureusement, le directeur d'école ne connaît personne en France et déposer le matériel dans un entrepôt spécialisé coûterait trop cher. Il cherche donc quelqu'un qui puisse les recevoir et les stocker le temps que toutes les marchandises soient prêtes à l'expédition, et à ce moment là un transitaire va les récupérer chez la victime. La victime a tout lieu de croire à la sincérité de son

correspondant puisqu'en apparence, c'est celui-ci qui supporte les risques en entreposant du matériel coûteux chez un parfait inconnu, accepte que la marchandise soit envoyée à son nom à son domicile et consent à la garder jusqu'à ce qu'on vienne la récupérer. En réalité, il devient complice et receleur, et risque de sérieux ennuis judiciaires s'il ne parvient pas à faire la preuve du scam.
Le scammeur, lui, récupère tranquillement les marchandises en se faisant passer pour un agent du transitaire, et disparaît avec dans la nature.
Parce que les mules ne se sentent pas escroquées (aucune tentative de soustraction d'argent, et il arrive même que les scammeurs leur versent de l'argent en compensation), et sont de plus sollicitées dans des domaines qui leur sont chers (grâce aux réseaux sociaux entre autres), cette forme de scam se répandra de plus en plus dans l'avenir, et permettra aux fraudeurs en tous genre sur l'Internet de blanchir l'argent ou les produits résultant de leurs sinistres actions.
Lien : http://www.altospam.com/actualite/2009/02/les-nouvelles-formes-de-scam-les- mules-et-le-blanchiment/

Mule financière

Pour les criminels, Internet est devenu un maillon essentiel de leur chaîne de blanchiment d'argent. Ainsi, ils peuvent construire des réseaux d'agents aux quatre coins du globe prêts à opérer contre rétributions dans ce processus.

L'argent blanchi grâce à des mules financières

Comme pour le trafic de drogue, les cybercriminels ont également leur mules. Dans ce cas, il ne s'agit pas de transporter de la drogue, mais de l'argent afin de complexifier la traçabilité des flux de blanchiment. La mule se voit confier une somme d'argent qu'elle doit remettre à un certain endroit, une autre banque ou un service de transfert international d'argent en échange d'une rétribution financière. A noter que ce type d'activité n'est pas anodine car elle est bien entendu pénalement répréhensible.

Des mules financières recrutées grâce aux spams

Internet est aujourd'hui un canal incontournable lorsque l'on recherche un nouvel emploi. Ce n'est donc pas étonnant que les cybercriminels utilisent également ce même principe pour recruter des mules via des pseudo-emplois habillés de revenus alléchants. Ainsi, pour la recherche de mules financières, ils utilisent aujourd'hui très souvent de larges campagnes d'envois de spams.
Inutile de chercher à obtenir une information quelconque sur l'expéditeur originel par ce biais. Dans un email, le format de l'expéditeur peut être modifié très facilement et permettre d'utiliser des adresses totalement valables comme celle du londonstockexchange.com par exemple. C'est néanmoins pas important dans le cas de ces emails car les différentes adresses de réponse sont sans lien avec ces expéditeurs et utilisent des messageries publiques distinctes comme gmail ou aol.com par exemple.

Difficile de croire à un vrai emploi

Au vu des nombreux éléments incohérents tant sur la forme que le contenu de tels emails, la véracité de telles propositions d'emploi est donc facilement contestable. Il s'avère néanmoins que, comme pour la combinaison *spam* + *phishing*, de telles campagnes obtiennent la postulation naà¯ve ou volontaire de personnes dans le besoins … avec le risque qu'elles se retrouvent bien seules devant le juge.
https://www.ledecodeur.ch/2012/11/18/comment-devenir-une-mule-financiere/

Les mules :
A l'intérieur des opérations de cyber-criminalité

Les experts en sécurité offrent un aperçu de la façon dont les mules sont recrutées, payées et gérées par des cyber-gangs qui cherchent à voler vos données et votre argent.

Les passeurs d'argent recrutés ne sont peut être pas le plus sexy dans le cadre d'une opération de cyber-criminalité, mais ils sont pourtant parmi les points vitaux du trafic. Cela a d'ailleurs été souligné l'année dernière quand le FBI a arrêté des mules liées à un gang accusé du pillage de millions de banques à travers le monde.

Selon ***Fortine***t, les recruteurs de mules font de plus de plus en plus d'efforts en ciblant des pays spécifiques. Par exemple, l'entreprise a trouvé certaines de ces campagnes "localisées"qui ont utilisé des noms de domaine à consonance tels que asia-sitezen.com et australia-resume.com , qui tous deux ont été enregistrés avec le même contact en Russie.

"Les services se déplacent furtivement sur la Toile en changeant de pays et de monnaie en se basant sur la géolocalisation IP des visiteurs. Maintenant, cette méthode est aussi appliquée pour le recrutement des mules", a déclaré ***Derek Mank***y, chef de projet de cyber-sécurité et chercheur sur les menaces chez ***Fortinet***. "Ce faisant, il est plus ciblé. L'un des exemples que nous avons vu avait établi une relation avec des banques locales comme une condition préalable. C'est parce que mules doivent généralement ouvrir plusieurs comptes et il est beaucoup plus facile de le faire si vous êtes un client de longue date."

En ouvrant plusieurs comptes dans plusieurs régions, les cyber-criminels créent une couche de redondance dans leurs opérations, a t-il ajouté.

Dans la plupart des cas, le recrutement est local et cible des pays spécifiques, a déclaré Uri Rivner, chef des nouvelles technologies pour les consommateurs Identity Protection de la division d'EMC de sécurité RSA. Une exception à cela, cependant, est l'Europe, où le SEPA (Single European Payment Area) rend cette initiative moins nécessaire.

"Par exemple, si un fraudeur cible des victimes en Allemagne, ils n'ont pas à recruter des mules de l'Allemagne en raison du SEPA," déclare Rivner. "Ils ne peuvent virer de l'argent d'une banque allemande à une banque en Lettonie. Selon la loi, il est considéré comme une transaction interne. Aux États-Unis, ce serait comme les banques le traitement des transactions entre les Etats. Les banques américaines devraient être très heureuses de ne pas fonctionner de cette façon en Europe parce qu'en Europe, le problème est beaucoup plus difficile en raison du SEPA. Il est donc plus facile de recruter des mules de n'importe où en Europe.

"Dans de nombreux cas que nous avons étudiés, les opérateurs des mule sont physiquement situés aux États-Unis où ils ont les coordonnateurs locaux des mule dans certains pays, a t-il poursuivi. "Ils gèrent les appels téléphoniques des mules, les questions de soutien, etc. Une chose qui semble être une nouvelle tendance est que de nombreuses mules sont des étudiants qui viennent tout en sachant qu'ils font partie d'une organisation criminelle ou alors qu'ils sont tout simplement stupides. Mais les opérateurs des mules leur promettent du travail aux États-Unis, et ils obtiennent un visa d'étudiant, ils volent aux États-Unis pour étudier et travailler à temps partiel comme une mule. "

Les experts de la sécurité conviennent que les organisations cyber-criminelles se présentent maintenant comme des entreprises de l'underground, une sorte de cyber-monde souterrain. Selon RSA, le nombre de sites Web spécialisés dans le recrutement de mules est passé de 34 en décembre 2007 à 591 en décembre 2009.

Les salaires des mules peuvent varier, avec des offres parfois exagérées par rapport à ce que les mules vont réellement obtenir, explique Manky.

La plupart des paiements, a t-il dit, se présentent sous la forme d'une commission, généralement environ 10 pour cent de chaque transaction. En raison de lois sur le blanchiment d'argent, la plupart des transactions restent sous la barre des $ 10,000 (USD), la moyenne se situant dans les milliers, a t-il ajouté.
"Comme toute relation d'affaire, une mule établie et ayant fait ses preuves aura plus de confiance vis à vis des opérateurs, et recevra donc des transactions plus importantes le plus souvent sur une base plus fréquente; donc ils vont gagner plus que d'autres," a déclaré Manky.
Une autre façon utilisée par les fraudeurs est le vol en espèces suivit d'une opération de réexpédition, qui est l'endroit où un criminel utilise une carte de crédit volée pour acheter un article en ligne, puis expédié au domicile d'une mule.
"Les opérations avec des mules sont les grandes entreprises. Les cybercriminels recrutent des mules, et ces dernières expédient des marchandises hors du pays, vendent des marchandises sur les sites d'enchères, etc", a déclaré Rivner. C'est beaucoup de travail de contrôler les mules, les recruter et répondre à leurs questions. C'est une main-d'œuvre tout à fait unique. Les opérateurs de mules doivent être plus des managers que des pirates, il est donc logique de séparer les opérations. "
https://www.undernews.fr/hacking-hacktivisme/les-mules-a-linterieur-des-operations-de-cyber-criminalite.html

Les nouvelles formes de scam : les mules et le blanchiment
Méthode de nouveaux trafiquants: les scammeurs

Les nouvelles victimes de scam ne sont plus des individus naïfs qui se font soustraire leur argent. Maintenant, ce sont des personnes crédules mêlées à des traffics d'argent.
Bientôt fini le temps du scams 419 où des correspondants soi-disant nigérians arnaquent des personnes naïves et leur soutirent jusqu'à plusieurs dizaines de milliers d'euros ? Il semble que la nouvelle forme de scam soit plus imaginative dans la mesure où le scammeur ne cherche plus à soutirer directement de l'argent à la victime. Il acquiert l'argent par d'autres moyens illégaux (vol de carte bleue, piratage de comptes bancaires ou de comptes paypal, etc…), mais se sert de la victime comme d'une mule.
En matière de trafic de drogue, une mule est une personne qui fait passer la drogue au travers des postes de contrôles. Le trafiquant a donc intérêt à choisir la mule qui semble la plus innocente possible, de manière à ne pas alerter les contrôleurs. De même, il doit cloisonner totalement la mule, qui ne devra pas savoir qui est son commanditaire. En matière de fraudes sur l'Internet, le plus dur n'est pas la fraude elle-même, mais de pouvoir profiter des fruits de la fraude tout en restant intraçable. Or, pour recevoir l'argent ou les colis achetés grâce à une CB volée, il faut une identité et une adresse, tous les deux aisément traçables. C'est ici qu'interviennent les mules, que les scammeurs convainquent d'accepter de recevoir et garder un paquet ou une somme chez eux jusqu'à ce qu'on vienne les récupérer à une date future.
Le principe est le même que pour un scam traditionnel. Le scammeur entre en contact avec une mule potentielle. Il faut noter ici l'apport immense des réseaux sociaux du type Facebook ou Second Life, qui facilitent la tâche des scammeurs, puisque non seulement on peut y trouver les centres d'intérêts de la mule, mais on peut également la contacter plus facilement que par l'envoi d'un mail classique dont les gens se méfient de plus en plus. Imaginons un exemple typique : un scammeur va déterminer suivant le profil d'une personne qu'elle s'intéresse aux œuvres humanitaires destinées aux écoles du Tiers Monde. Il va alors imaginer un scam personnalisé en se faisant passer pour un directeur d'une école d'Afrique qui a besoin

d’ordinateurs portables pour son école. Là où le scammeur classique va demander que la victime lui envoie de l’argent, le nouveau scammeur aura déjà obtenu l’argent autrement, et dira à sa victime que de généreux bienfaiteurs ont déjà acquis les matériels informatiques en question, mais que pour des problèmes d’acheminement (par ex, parce qu’un regroupement de marchandises dans un conteneur coûte moins cher), les matériels doivent être stockés temporairement en France. Malheureusement, le directeur d’école ne connaît personne en France et déposer le matériel dans un entrepôt spécialisé coûterait trop cher. Il cherche donc quelqu’un qui puisse les recevoir et les stocker le temps que toutes les marchandises soient prêtes à l’expédition, et à ce moment là un transitaire va les récupérer chez la victime. La victime a tout lieu de croire à la sincérité de son correspondant puisqu’en apparence, c’est celui-ci qui supporte les risques en entreposant du matériel coûteux chez un parfait inconnu, accepte que la marchandise soit envoyée à son nom à son domicile et consent à la garder jusqu’à ce qu’on vienne la récupérer. En réalité, il devient complice et receleur, et risque de sérieux ennuis judiciaires s’il ne parvient pas à faire la preuve du scam. Le scammeur, lui, récupère tranquillement les marchandises en se faisant passer pour un agent du transitaire, et disparaît avec dans la nature.
Parce que les mules ne se sentent pas escroquées (aucune tentative de soustraction d’argent, et il arrive même que les scammeurs leur versent de l’argent en compensation), et sont de plus sollicitées dans des domaines qui leur sont chers (grâce aux réseaux sociaux entre autres), cette forme de scam se répandra de plus en plus dans l’avenir, et permettra aux fraudeurs en tous genre sur l’Internet de blanchir l’argent ou les produits résultant de leurs sinistres actions.
http://www.altospam.com/actualite/2009/02/les-nouvelles-formes-de-scam-les-mules-et-le-blanchiment/

Arnaque et recrutement de Mules

Depuis plusieurs années, il est devenu courant de recevoir dans sa boite mail des messages proposant un travail à temps partiel, depuis son domicile, qui consiste simplement à transférer des fonds pour le compte d'une société étrangère. Ces messages sont des spams classiques, c’est à dire qui proposent une escroquerie qui a de faibles chances de marcher, mais ils sont envoyés à un si grand nombre de cibles (pour un coût marginal) que plusieurs victimes finiront bien par se présenter. Dans le cas qui nous préoccupe les victimes ne vont pas acheter des fausses Rolex ou du Viagra, ni pianoter leur mot de passe bancaire, mais se présenter pour un « travail » d’appoint.
Ce travail d'intermédiaire est bien sûr une escroquerie et la personne ainsi recrutée est couramment appelé "une mule" (par analogie aux passeurs recrutés pour transporter – parfois à leur insu – de la drogue ou tout autre matériel illicite). Le travail qui est proposé à la mule consiste le plus souvent à :

- recevoir de l'argent sur un compte que son recruteur lui demande de créer (par exemple un compte PayPal),
- convertir cet argent en cash et transférer cet argent liquide vers l'étranger en utilisant des services de mandat international tel que Western Union,
- garder au passage, en rétribution du service rendu, un petit pourcentage du montant d'argent acheminé.

Ce phénomène de mule est connu depuis plusieurs années. Le CLUSIF lui consacrait par exemple en début 2007 un exposé détaillé à l'occasion de son Panorama 2006 sur la cybercriminalité (voir la rubrique "pour plus d'information"). A cette époque les emails

proposant ce type d'arnaque étaient encore peu fréquents et rédigés très majoritairement en anglais.

Exemple d'e-mail

Depuis les choses ont bien évolué. Voici par exemple ci-dessous un e-mail que nous avons reçu à la mi octobre. Si l'on écarte l'objet de l'e-mail (qui est un peu maladroit), il est étonnant de voir le soin qui a été apporté à sa rédaction :

- il ressemble vraiment à une offre d'emploi,
- le français utilisé est tout à fait correct,
- les termes employés (CDD, CDI, etc..) sont crédibles.

Cet e-mail, comme tous les spams, a été envoyé en masse en utilisant des moteurs d'émission anonymes ou compromis, sans possibilité de remonter à la source. Le seul lien que l'on a avec l'émetteur est l'adresse d'un compte Gmail. Dans d'autres échantillons que nous avons examinés pour ce spam l'adresse de l'émetteur et l'adresse Gmail étaient différentes, mais le corps était lui inchangé.

Le seul élément suspect à la lecture est la mention "effectuer des versements par WU/ MG" qui fait en fait référence à "Western Union" et "MoneyGram" : deux services permettant d'envoyer de l'argent liquide à l'étranger …

http://junon.univ-cezanne.fr/u3iredic/?p=13074

Arnaque et recrutement de Mules

Depuis plusieurs années, il est devenu courant de recevoir dans sa boite mail des messages proposant un travail à temps partiel, depuis son domicile, qui consiste simplement à transférer des fonds pour le compte d'une société étrangère. Ces messages sont des spams classiques, c'est à dire qui proposent une escroquerie qui a de faibles chances de marcher, mais ils sont envoyés à un si grand nombre de cibles (pour un coût marginal) que plusieurs victimes finiront bien par se présenter. Dans le cas qui nous préoccupe les victimes ne vont pas acheter des fausses Rolex ou du Viagra, ni pianoter leur mot de passe bancaire, mais se présenter pour un « travail » d'appoint.

Ce travail d'intermédiaire est bien sûr une escroquerie et la personne ainsi recrutée est couramment appelé "une mule" (par analogie aux passeurs recrutés pour transporter – parfois à leur insu – de la drogue ou tout autre matériel illicite). Le travail qui est proposé à la mule consiste le plus souvent à :

- recevoir de l'argent sur un compte que son recruteur lui demande de créer (par exemple un compte PayPal),
- convertir cet argent en cash et transférer cet argent liquide vers l'étranger en utilisant des services de mandat international tel que Western Union,
- garder au passage, en rétribution du service rendu, un petit pourcentage du montant d'argent acheminé.

Ce phénomène de mule est connu depuis plusieurs années. Le CLUSIF lui consacrait par exemple en début 2007 un exposé détaillé à l'occasion de son Panorama 2006 sur la cybercriminalité (voir la rubrique "pour plus d'information"). A cette époque les emails proposant ce type d'arnaque étaient encore peu fréquents et rédigés très majoritairement en anglais.

Exemple d'e-mail

Depuis les choses ont bien évolué. Voici par exemple ci-dessous un e-mail que nous avons reçu à la mi octobre. Si l'on écarte l'objet de l'e-mail (qui est un peu maladroit), il est étonnant de voir le soin qui a été apporté à sa rédaction :

- il ressemble vraiment à une offre d'emploi,
- le français utilisé est tout à fait correct,
- les termes employés (CDD, CDI, etc..) sont crédibles.

Cet e-mail, comme tous les spams, a été envoyé en masse en utilisant des moteurs d'émission anonymes ou compromis, sans possibilité de remonter à la source. Le seul lien que l'on a avec l'émetteur est l'adresse d'un compte Gmail. Dans d'autres échantillons que nous avons examinés pour ce spam l'adresse de l'émetteur et l'adresse Gmail étaient différentes, mais le corps était lui inchangé.

Le seul élément suspect à la lecture est la mention "effectuer des versements par WU/ MG" qui fait en fait référence à "Western Union" et "MoneyGram" : deux services permettant d'envoyer de l'argent liquide à l'étranger …

Que se passe-t-il ensuite pour la mule ?

Une fois la mule recrutée, de nombreux scénarios sont possibles, en fonction du type d'escroquerie. Voici les plus classiques :

- Le blanchiment d'argent : La mule reçoit sur son compte de l'argent. Elle doit alors retirer cet argent en liquide et l'envoyer par mandat international vers son commanditaire.
- L'extraction d'argent volé dans une banque : Le commanditaire demande à la mule d'ouvrir un compte dans une banque précise. Ce compte est ensuite alimenté à partir d'autres comptes de cette même banque qui ont été piratés (les transferts entre comptes d'une même banque sont généralement moins surveillés). La mule est chargée alors de retirer l'argent et de le transférer par mandat international vers son commanditaire.
- Les fausse ventes sur Internet : Le commanditaire demande à la mule de créer un compte PayPal, puis vend un objet sur internet en indiquant à l'acheteur qu'il doit envoyer l'argent sur le compte PayPal de la mule. En fait l'acheteur ne recevra jamais l'objet qu'il a acheté et la mule aura déjà transféré l'argent au commanditaire lorsque la supercherie sera découverte.

D'après les témoignages, la mule n'est pas utilisée très longtemps : soit parce qu'elle va être repérée par la banque du fait des transferts et retraits qu'elle fait, soit parce que les victimes des escroqueries vont se plaindre et que la mule sera alors immédiatement repérée.

A titre d'anecdote, il a été identifié récemment que le malware URLZone (un cheval de Troie bancaire), lorsqu'il détecte qu'il est analysé, change de comportement et transfère l'argent qu'il détourne vers des victimes innocentes qui passent ainsi auprès des enquêteurs pour des mules…

La réaction des entreprises impliquées

Les sociétés impliquées par ces escroqueries (les banques, Western Union, les sites de ventes entre particuliers, etc…) sont bien conscientes de ce phénomène et prennent des mesures pour les contrer. Il s'agit en tout premier lieu de communications vers leurs clients pour les informer et les mettre en garde. Western Union a également annoncé en octobre 2008 la création d'une "Alliance" (avec Microsoft, Yahoo et African Development Bank) pour lutter contre les arnaques sur Internet. Il existe aussi sans doute des mesures techniques plus discrètes (non publiques). On peut par exemple imaginer qu'une banque puisse surveiller les opérations de ses clients et déclencher des alarmes lors d'événements jugés comme significatifs. Une banque avait indiqué lors de l'intervention du CLUSIF avoir identifié en 2006 12 mules parmi ses clients.

Conclusion

L'activité de mule est bien sûr illégale (la mule est considérée comme complice des escrocs qui l'embauchent), dangereuse (la première conséquence est en général l'exclusion immédiate de la mule par la banque) et de courte durée.

Il est par contre préoccupant de voir se multiplier ce type d'offre dans des emails de plus en plus crédibles. On le voit sur l'exemple que nous avons pris ici, il est tout à fait possible de se faire appâter par ce type d'e-mail.
Agir avec prudence et bon sens devrait permettre de se rendre compte qu'il s'agit d'une escroquerie, mais une fois appâté, on peut aussi être tenté de croire que l'on a déniché une bonne affaire…
http://www.cert-ist.com/public/fr/SO_detail?code=fraudes_mules