IAtlas

Comment Vous Aidez Les Escrocs!

Parfois les gens facilite la tâche des cybercriminels!

Préface

Il y a un certain nombre de choses que les gens font en-ligne qui a énormément augmenté leur risque de rencontrer des cybercriminels - l´utilisation imprudente du navigateur, pas de mise à jour de leurs logiciels et système d´exploitation, des mots de passe faciles à deviner, et ainsi de suite. Cet article traite d´une pratique très commune des courriels qui est beaucoup plus dangereuse qu´elle semble l´être, et qui n´a aucun but réel - le même résultat peut être atteint d´une manière différente, mais sans risque.

La victime

Un jour, sans aucun avertissement, Jeanne Dupond a perdu son identité personnelle - ses comptes bancaires ont été vidés, ses cartes de crédit ont été délibérément exploités, et pire, quelqu´un d´autre se faisait passer pour elle, crée des obligations financières à son nom. Puis, après un long processus coûteux et émotionnellement déchirant, sa vie revient lentement à la normale. Dans une analyse ultérieure par les autorités d´application de la loi avec l´expertise de l´Internet, le processus de vol d´identité a été révélée en détails. Dans l´ordre chronologique inverse, c´est arrivé comme ceci:

■ Dans la dernière étape, le compte bancaire en ligne de Jeanne a été raflé. La banque en ligne requiert son adresse courriel comme nom d´ouverture de session, mais les voleurs connaissaient l´adresse, et ils ont deviné son mot de passe en lisant ses courriels et ceux de ses amis.

■ Dans l´avant-dernière étape, les voleurs ont envoyés des courriels à Jeanne et tous ses amis, et dans chaque courriel, les noms de ses amis dans la liste ont été utilisés pour tromper le destinataire en faisant croire que le message venait d´eux. Chaque courriel contient un lien dangereux vers des logiciels malveillants et un message du genre: "Salut Jeanne, ce site est vraiment utile - essayes-le. Signé ton ami Paul"

■ Comment les criminels ont-ils eu le nom de Jeanne et son adresse courriel, et les noms et adresses courriel de tous ses amis? C´est facile - ils ont intercepté un type particulièrement dangereux de courriel qui contient plus d´une adresse de destination - un "multi-destinataire du courriel" ou **MRE**.

■ D´où venait ce courriel dangereux? Ça aussi c´est facile - Jeanne l´a composé, elle a joint une liste des noms et adresses courriel de tous ses amis, et cliqué sur "envoyer".

Voilà comment Jeanne a perdu son identité - tout simplement en composant un courriel avec plus d´une adresse de destination, un MRE. Est- ce vraiment si facile de perdre son identité, et un MRE est-il vraiment dangereux? Eh bien, oui et oui. Voici pourquoi:

■ Dans le système courriel, le nom d´une personne et l´adresse courriel sont jumelés comme ceci: "Jeanne Dupond <jdoe@monsite.fr>" Ce formulaire permet au destinataire de stocker le nom d´une personne et l´adresse courriel de manière pratique.

■ Si un cybercriminel peut s´emparer du courriel, il a le nom d´une personne, ainsi que le nom d´ouverture de session qui est utilisé par de nombreuses banques et les entreprises en ligne - l´adresse courriel d´une personne.

■ En obtenant ce type d´adresse courriel, le criminel est à mi-chemin dans la vie en ligne de la victime - l´autre moitié est un mot de passe.

■ Si un criminel peut capturer l´ensemble du courriel, il peut trouver des indices sur le mot de passe de la victime.

■ Mais il y a pire - bien pire. Si le courriel a plusieurs adresses de destinataires, le criminel peut commencer à attaquer tous les destinataires à la fois, et il peut exploiter le fait que les bénéficiaires sont tous des amis.

Voici un exemple - disons que Jeanne Dupond, Pierre Haddock et Paul Leblond sont tous amis, et ils envoient régulièrement des MRE à l´autre. Leurs adresses sont les suivantes:

Jeanne Dupond <jdupond@monsite.fr>

Pierre Haddock <phaddock@monsite.fr>

Paul Leblond <pleblond@monsite.fr>

Si Jeanne, Pierre et Paul s´envoient des courriels avec une adresse de destinataire, les messages interceptés seraient relativement inoffensifs. Mais un MRE intercepté est *un cadeau pour les escrocs*. Il fonctionne comme ceci:

L´escroc qui intercepte le message prend la liste d´adresses et envoie des courriels de phishing (hameçonnage ou filoutage) qui exploitent le fait que les bénéficiaires sont tous des amis, comme ceci:

Courriel de phishing à Jeanne:
Chère Jeanne,
Je viens de découvrir ce site cool de Paul - jettes-y un coup d´œil:
http://centrale_malveillante.fr
Ton ami, Pierre

Courriel de phishing à Paul:
Cher Paul,
Je viens de découvrir ce site cool de Pierre - jettes-y un coup d´œil:
http://centrale_malveillante.fr
Ton ami, Jeanne

Courriel de phishing à Pierre:

Cher Pierre,
Je viens de découvrir ce site cool de Jeanne - jettes-y un coup d´œil:
http://centrale_malveillante.fr
Ton ami, Paul

Ce qui est diabolique à ce sujet est qu´une fois qu´un cybercriminel a une liste d´adresses courriel, que le criminel sait que ce sont des amis, il peut exploiter ce fait pour endormir les destinataires avec ses courriels en les faisant cliquer sur un lien dangereux - après tout, le destinataire pense que c´est d´un ami. Et plus la liste d´adresses est longue, plus cette escroquerie est efficace. Et enfin, les escrocs sont notoirement paresseux, mais les courriels de phishing ci-dessus peuvent être composés automatiquement par ordinateur - l'escroc ne sue pas une seule goutte. Il existe des logiciels qui permettent d´automatiser complètement le processus de prise en charge de votre identité, mais ils ont tous une chose en commun - ils ont besoin de gens qui envoient des courriels à plusieurs destinataires.

Passons au prochain problème MRE - quel est le risque qu´un courriel sera intercepté par des criminels? Eh bien, cela dépend - si le message n´a qu´un seul destinataire, les chances ne sont pas très bonnes, mais si c´est un MRE, les chances sont nettement meilleures. Pourquoi en est-il ainsi?

■ Certains ordinateurs sont contaminés, infectés par des criminels de sorte que les activités de l´ordinateur peuvent être retracées à distance, et les documents peuvent être capturés.

■ Quel est le taux d´infection de l´ordinateur personnel en gros? Personne ne sait pour sûr, mais pour cet exemple, nous allons utiliser 10%, c´est une estimation raisonnable.

■ Étant donné que le taux d´infection, si un courriel avec une adresse de destinataire est envoyé, sa chance d´être intercepté par des criminels est faible, environ 6%.

■ Mais si le courriel est un MRE, parce que chaque copie est identique et que chaque copie est envoyée à un autre ordinateur, sa chance d´être intercepté dépend du nombre d´adresses attachés:

Adresses de Bénéficiaires	Risque d'Interceptions
5	5.76
10	58.32
15	96.01
20	99.92
25	100.00

■ Essentiellement, cela signifie que pour un message avec dix adresses attachés (et dix exemplaires envoyés), la chance qu´il sera capturé par des criminels est de près de 60%. Pour une liste d´adresses avec 25 ou plusieurs adresses, les chances de capture sont presque de 100%.

■ Comme expliqué ci-dessus, une fois que les criminels acquièrent le message, ils peuvent utiliser les noms des amis les uns contre les autres, exploiter le fait que les bénéficiaires se connaissent pour réduire leur prudence. Ils peuvent envoyer une foule de messages, tous apparemment de provenance d´amis, pour essayer de tromper les destinataires à révéler des informations personnelles ou en cliquant sur un lien hypertexte dangereux.

Expérience personnelle

J´ai une histoire personnelle à ce sujet. Lors de mes voyages, je rencontre beaucoup de gens et je donne parfois mon adresse de contact - avec prudence, mais pas trop. Il y a quelques années, j´ai donné mon adresse courriel à d´autres plaisanciers, et nous avons convenu de prendre contact à l´avenir.

Quelques semaines plus tard, les gens m´ont envoyé un courriel. Mais c´était le pire MRE que je n´avais jamais vu - il avait une liste jointe de plus de 300 adresses, de toutes les personnes qu´ils ont jamais rencontrés! Et pire encore, le message inclut était, "Chers amis - les problèmes que vous avez ne sont pas de notre faute, nous sommes victimes aussi!" En d´autres termes, les expéditeurs ont créé une catastrophe pour eux-mêmes et leur cercle d´amis, mais ils ne se rendaient pas compte que leur MRE était la source de tous les problèmes de leurs amis, y compris une tempête de neige de courriels de spam et de phishing astucieusement formulés apparemment en provenance de connaissances.

De toute évidence, en joignant une liste de 300 adresses, et en utilisant mon estimation antérieure de 10% des ordinateurs infectés, il y a de fortes chances que le message soit tombé dans les mains de plusieurs criminels, pas seulement un seul.

Comme je m´y attendais, après quelques heures de la réception du MRE, ma boîte de réception débordait de courriels de spam et de tentative de phishing. Après une courte lutte, j´ai abandonné et retiré cette adresse courriel. Normalement, je ne reçois pas de spam parce que je suis assez prudent en donnant mon adresse courriel, mais cet épisode m´a appris qu´il suffisait d´être négligent juste une fois.

Vu que je gère mon propre site, je peux changer d´adresse courriel en un clin d´œil, aucun problème. Mais les autres bénéficiaires qui ont leurs collection d´adresses courriel, ils n´ont que peu de recours significatifs. Ils seront placés sur pratiquement chaque liste de diffusion de spam, et seront inondés de messages de phishing interminables qui semblent venir d´amis.

Rien que d´y penser - il suffisait que les originaires du MRE résistent à l´impulsion d´envoyer leurs courriels de masse à la masse étant dans leurs liste d´adresses. Mais il y a une solution simple - les gens peuvent envoyer un message à tous leurs amis, mais sans y attacher une liste de toutes les adresses de destinataires.

Le Remède

C´est la première fois que j´ai essayé d´écrire sur ce problème et sa solution. Jusqu´à présent, j´ai juste dit aux gens en face-à-face comment l´éviter, mais le temps passe, je pense que je vais avoir cette conversation trop souvent, alors j´ai décidé de l´expliquer une seule fois et le mettre en ligne.

La solution au problème MRE est très simple:

■ Tout d´abord, jamais, jamais envoyer un courriel avec plus d´une adresse de destinataire visible. Peu importe à quel point cette pratique est commune, c´est dangereux et ça représente un des risques les moins appréciés associés au protocole de courriel.

■ Qu´est-ce que je veux dire quand je disais ci-dessus l´adresse courriel "visible"? Peut-on envoyer un message à plusieurs destinataires, mais sans y attacher la liste au message? Oui!

■ La solution au problème MRE est très simple - mettre la liste des destinataires dans le champ **BCC:** (ou CCI) (**B**lind **C**arbon **C**opy) de votre programme courriel, pas le champ **CC:** (**C**arbon **C**opy). Cela résout le problème!

■ Le champ **CC:** envoie une copie à chaque personne sur la liste, mais il inclut aussi la liste complète dans le message. Très mauvais!

■ Le champ **BCC:** envoie une copie à chaque personne sur la liste, mais n´inclut pas la liste dans le message. Très bien!

N´est-ce pas tout simple? Et presque tous les programmes de courriel existants ont cette fonction de **BCC:** (et si le vôtre ne l´a pas débarrassez-vous de lui).

La fonction **CC:** équivalent au papier carbone a été conçue pour un petit intranet local au bureau, où une personne envoie un message à un comité ou un cercle d´amis, et les bénéficiaires pouvaient faire un commentaire, cliquer sur "répondre au groupe" de sorte que tous les membres puissent lire leurs commentaires. Mais cette pratique intranet relativement inoffensif s´est transformé en une pratique très dangereuse de l´Internet, juste parce que l´Internet n´est pas un petit lieu avec des amis bénins - pas à distance.

En résumé, ne **jamais** utiliser CC: pour les communications par courriel dans l´internet - utilisez uniquement BCC: pour envoyer un message à un groupe de personnes. Ce qui nous amène à cette règle:

Le nombre d´adresses de destinataires visibles sur un courriel doit être "UN". ***Pas deux, pas une douzaine, "UN"***.

Petite anecdote cocasse

Une histoire révèle comment les talibans, ne connaissant pas mon site, ont publié leur liste entière de diffusion en créant accidentellement un MRE - tout simplement en cliquant sur "CC" au lieu de "BCC", distribuant ainsi leur liste de membres dans tout le texte brut. Quelle honte! Nous avons besoin de meilleurs terroristes.