Résumé

# L'être humain, nouvelle cible des pirates

**Raj Samani, Directeur des technologies pour la région EMEA**

**Charles McFarland, Responsable de recherche du MTIS**

intel Security

De nombreuses cyberattaques incluent une part d'ingénierie sociale, laquelle vise à convaincre l'individu ciblé d'effectuer une action spécifique dans le but de provoquer une infection ou de permettre la fuite d'informations précieuses.

Bien que la réponse à ce type d'attaque passe par une solution technique, l'angle humain de ces attaques entraîne souvent une culpabilisation de la cible et le besoin de renforcer la sensibilisation à la sécurité. En vérité, la plupart des entreprises cherchent rarement à comprendre les raisons qui ont conduit à l'exploitation d'une cible et, plus grave encore, à déterminer ce qui doit être fait, au-delà du renforcement de la sensibilisation, pour réduire le risque d'attaques ultérieures.

L'ingénierie sociale peut être définie de la manière suivante :

> *Utilisation délibérée de techniques trompeuses ayant pour objet de manipuler un individu afin de le forcer à divulguer des informations ou à exécuter certaines actions pouvant entraîner une telle divulgation.*

Lors d'une attaque d'ingénierie sociale, la victime n'a pas conscience des conséquences dramatiques de ses actes. L'auteur de l'attaque exploite l'innocence de la cible, et non ses instincts criminels. Il existe deux catégories d'attaques :

- Les attaques de type « chasse » visent à extraire des informations par une interaction limitée avec la cible. Cette approche implique généralement une prise de contact unique, avec arrêt total de la communication dès que le cybercriminel obtient les informations recherchées.
- Les attaques de type « récolte » ont pour but d'établir une relation continue avec la cible et de lui soutirer des informations sur une période prolongée.

Les attaques d'ingénierie sociale qui s'appuient sur des communications par e-mail utilisent généralement la chasse comme méthode principale. Il existe des exceptions à cette règle, comme la fraude nigériane (ou fraude 4-1-9), qui visent à prolonger l'attaque sur une longue période afin de soutirer le plus d'argent possible. Les attaques d'ingénierie sociale de type « chasse » et « récolte » se déroulent généralement en quatre étapes :

1. Recherche — Cette phase facultative vise à recueillir des informations sur la cible. Le but pour le pirate est de tendre un piège efficace en identifiant par exemple les passe-temps, le lieu de travail ou le fournisseur de services financiers de la cible.
2. Hameçonnage — Cette étape vise à établir un scénario qui permettra d'entrer en contact avec la cible et servira de prétexte pour une interaction. Pour le psychologue Robert Cialdini, six leviers d'influence permettent de manipuler le subconscient d'une cible :
   - Réciprocité — Une personne qui reçoit quelque chose se sent par la suite moralement obligée de rendre la pareille.
   - Rareté — Les gens ont tendance à vouloir acquérir une chose lorsqu'ils pensent que sa disponibilité est limitée.
   - Cohérence — Une cible qui a fait une promesse aura tendance à la respecter quoi qu'il arrive pour ne pas paraître indigne de confiance.
   - Appréciation — Les cibles sont plus enclines à obtempérer si l'auteur de l'attaque est une personne qu'elles tiennent en estime.
   - Autorité — Les gens ont tendance à se conformer plus facilement aux demandes émanant de personnes faisant figure d'autorité.
   - Preuve par la masse — Les gens ont tendance à se conformer aux actions du plus grand nombre.

3. Exécution — Cette étape constitue la phase principale de l'attaque. Il peut s'agir d'une fuite d'informations, d'un clic sur un lien, d'un transfert de fonds, etc.
4. Désengagement — Le cybercriminel met fin à toute interaction. Bien qu'il puisse être préférable de finaliser une attaque de type « récolte » sans éveiller les soupçons, ce n'est pas obligatoire. Par exemple, lorsque les cybercriminels manipulent des cibles dans le but d'obtenir des informations de carte de crédit, ils préfèrent généralement ne pas éveiller les soupçons pour éviter que les victimes ne fassent opposition à leurs cartes. En revanche, si les cybercriminels parviennent à subtiliser du code source ou d'autres informations personnelles, même si les cibles en prennent conscience, elles ne pourront rien faire pour récupérer les données volées.

Les attaques d'ingénierie sociale ne sont pas nécessairement linéaires : une attaque en apparence isolée peut s'inscrire dans une campagne de bien plus grande envergure visant à recueillir différents fragments d'informations liées. Les cybercriminels peuvent par exemple lancer une attaque, récupérer les informations souhaitées, puis disparaître ou, au contraire, mener différentes attaques de type « chasse » et utiliser les informations ainsi recueillies pour mettre en place une attaque de type « récolte ».

## Canaux d'attaque

Les cybercriminels ont à leur disposition plusieurs vecteurs d'attaque :

- Sites web — Les attaques d'ingénierie sociale tirent souvent parti de sites web malveillants. Selon le rapport d'enquête 2014 de Verizon sur les compromissions de données (*2014 Verizon Data Breach Investigations Report*), « 20 % des attaques réalisées à des fins d'espionnage utilisent des sites web compromis pour distribuer des logiciels malveillants ».
- E-mail — Les formes d'ingénierie sociale par e-mail les plus courantes sont le phishing et sa version plus ciblée appelée spearphishing (harponnage). Les e-mails constituent un outil particulièrement efficace pour les cybercriminels. En effet, d'après le rapport Verizon, « 18 % des utilisateurs cliquent sur des liens contenus dans des e-mails de phishing ».
- Téléphone — Ce canal est particulièrement apprécié par les revendeurs d'informations.
- Face-à-face — un employé peut être abordé physiquement, puis piégé ou contraint à divulguer des informations.
- Service postal — Bien que ce canal semble moins utilisé que les autres, certaines attaques d'ingénierie sociale exploitent encore à ce jour le courrier postal.
- Fax — On trouve notamment des exemples de messages prétendument envoyés par des services de paiement en ligne.

## Protection contre l'ingénierie sociale

Les mesures suivantes peuvent être utilisées pour limiter les risques d'ingénierie sociale. Elles sont divisées en trois catégories : personnes, procédures et technologies. Cette liste n'est pas exhaustive et les mesures répertoriées peuvent ne pas s'appliquer à toutes les entreprises.

**Personnes**

- Définition de limites claires — Tous les membres du personnel doivent être parfaitement conscients des stratégies mises en place en matière de divulgation d'informations et des chemins d'escalade à respecter en cas de requête se situant en dehors des limites définies.
- Formation continue — Développez un programme de sensibilisation à la sécurité pour assurer la formation de vos employés au fil du temps. Utilisez des outils tels que le quiz McAfee sur le phishing pour mettre en évidence des stratégies spécifiques souvent utilisées dans les attaques.

- Encouragement des vérifications — Encouragez votre personnel à remettre en question les requêtes, même si elles sont a priori inoffensives. Un employé doit ainsi pouvoir interpeller une personne qui tenterait de profiter de son passage pour s'introduire sur le site de l'entreprise.
- Sensibilisation à l'importance des informations — Même des informations a priori peu significatives, comme des numéros de téléphone (informations à potentiel d'action), peuvent être utilisées pour organiser une attaque.
- Environnement bienveillant — Les cibles des attaques d'ingénierie sociale sont bel et bien des victimes. Punir un employé qui a été abusé ne fera que décourager les autres de signaler toute fuite d'informations dont ils seraient à l'origine. Une fois dupés, ils pourraient en effet très bien se retrouver sous la coupe de l'auteur de l'attaque et subir le chantage de ce dernier.

**Procédures**

- Signalisation des arnaques téléphoniques — Dès qu'un événement suspect se produit, le personnel devrait soumettre un rapport décrivant l'incident. Cette procédure est essentielle pour la suite de l'enquête.
- Pages de blocage informatives — Lorsqu'un employé tente d'accéder à une page web malveillante, utilisez une page de blocage pour l'informer des raisons pour lesquelles l'accès à cette page n'est pas autorisé. Il pourra ainsi réfléchir aux actions qui l'ont amené à cette page et contribuer à l'identification des sources des attaques.
- Notification aux clients — Lorsque des appelants se voient refuser l'accès à certaines informations, l'entreprise doit les en informer et vérifier s'ils étaient ou non autorisés à les obtenir. Les entreprises doivent également réfléchir à la manière dont elles communiquent avec les clients. PayPal propose par exemple des recommandations pour permettre aux utilisateurs de déterminer si les e-mails qu'ils reçoivent sont authentiques : « PayPal ne vous demandera jamais votre numéro de compte bancaire ou de carte de paiement/crédit, etc. par e-mail. De même, nous ne vous demanderons jamais votre nom complet, votre mot de passe ou les réponses à vos questions de sécurité par e-mail. ».
- Chemin d'escalade — Mettez en place une procédure claire pour les employés en première ligne afin qu'ils puissent signaler tout message potentiellement frauduleux au moindre doute.
- Tests éclairs — Testez régulièrement votre personnel afin de vérifier sa sensibilité aux attaques d'ingénierie sociale par le biais de différents canaux de communication. Ces tests permettent de mesurer l'efficacité des programmes de formation.

**Technologies**

- Enregistrement des appels — Enregistrez systématiquement les appels entrants afin de simplifier les opérations d'investigation.
- Lignes factices — Redirigez les appels suspects vers un numéro surveillé.
- Filtrage des e-mails — Supprimez automatiquement les e-mails frauduleux contenant des logiciels malveillants connus ou inédits.
- Filtrage de contenu web — Bloquez l'accès aux sites web malveillants et détectez les logiciels malveillants en ligne avec accès à Internet.
- Authentification forte — Bien que la mise en place d'une authentification multifacteur ne permette pas de contrer totalement les attaques d'ingénierie sociale visant à obtenir des informations d'identification, une telle approche complique néanmoins considérablement la tâche des cybercriminels.

Suivre McAfee Labs

## Synthèse

La menace représentée par l'ingénierie sociale est bien réelle. Les cybercriminels utilisent cette technique pour obtenir des informations de manière frauduleuse à diverses fins malveillantes. Pour pouvoir lutter efficacement, il est essentiel de comprendre la nature réelle de ces attaques d'ingénierie sociale. Cela passe par une identification des acteurs probables, de leurs méthodes d'attaque et de leurs ressources, puis par l'application des mesures adaptées pour réduire le risque de voir aboutir l'attaque.

Un exemplaire du rapport complet est disponible à l'adresse suivante : **www.mcafee.com/hacking-human-os**.

**Twitter@Raj_Samani**

**Twitter@CGMcFarland**

1. **http://www.verizonenterprise.com/DBIR/2014/**
2. **https://www.paypal.com/gb/webapps/helpcenter/helphub/article/?solutionId=FAQ2061&m=HTQ**

**McAfee. Part of Intel Security.**
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.intelsecurity.com