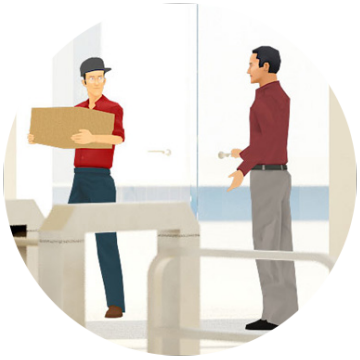
# ESPIONNAGE INDUSTRIEL
## L'envers du décor

Cette attaque est menée par deux pirates « professionnels », passés par un intermédiaire, pour le compte de… de qui en fait ? Des concurrents ? Des revendeurs d'information ? On ne sait jamais trop, et on peut soupçonner beaucoup de monde.

Pour cette opération, les pirates se font connaître sous les noms de Mark et Irina. Pourquoi pas ? Ça sonne bien. Voyons ensemble comment ils ont mené leur offensive…



Mark se gare devant les locaux d'Alsium, en camion et tenue de livreur, encombré d'un paquet volumineux. Le voyant en difficulté, un collaborateur l'aide à entrer en lui tenant la porte, puis en lui faisant passer le portique de sécurité avec son badge. Mark ne s'attarde pas trop lors de ce premier repérage, mais ralentit tout de même devant un bureau, en entendant un homme évoquer la prochaine soirée d'entreprise, qui aura lieu à deux pas d'ici. Un supporter de l'équipe de basketball locale, les « Slashers », à en croire la décoration de son bureau.

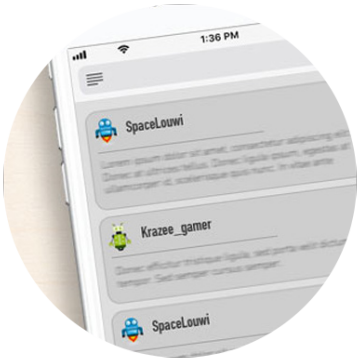
Un peu plus loin dans le couloir, Mark repère l'imprimante, et quelques feuilles dans le bac de sortie. Une banale convention de stage, qu'il prend en photo : Louis Keller, élève ingénieur, accueilli pour trois mois au sein du

service technique. Peut-être ce garçon qui portait un tee-shirt à l'effigie du dernier jeu vidéo à la mode, à l'entrée de l'open space ?

Mark confie sans tarder ces éléments à Irina, qui lance une recherche sur Internet. Un nom, une entreprise, un stage… une amorce suffisante pour commencer à tirer le fil. Surtout que Louis possède des profils un peu partout, dont un sur le réseau social professionnel « JobIsLove ». Il publie vite, et beaucoup… beaucoup trop d'ailleurs, même des détails sur sa mission. Elle apprend qu'il participe au déploiement dans toute l'entreprise d'un nouvel antivirus, nommé « Goldchain ».

Mark développe donc un malware spécifiquement étudié pour contourner cette protection. C'est plus facile quand on connaît l'adversaire. Il conçoit un Remote Access Tool (RAT), une charmante petite bête, qui une fois installée sur un poste utilisateur permet d'en prendre le contrôle, en obtenant le niveau de droits attribué à l'utilisateur officiel du poste. L'hameçon est prêt, il reste à fournir l'appât.

Irina trouve une nouvelle trace de Louis sur un forum de jeux vidéo. Peut-être une faille à exploiter ? Elle crée un compte, et sympathise avec lui sous pseudonyme. Facile entre « gamers ». Elle propose de lui transmettre un petit logiciel pour jouer gratuitement à des jeux vidéo. Louis ne résiste pas. Impatient de pouvoir jouer au bureau, pendant sa prochaine pause de midi, il lui indique son adresse e-mail professionnelle.




Dès le lendemain, Louis ouvre l' e-mail de son « nouvel ami du forum », et clique sur le lien. Le malware installé, Irina s'engouffre dans la brèche. Que peut-on trouver sur le poste d'un stagiaire ? Pas grand-chose, à priori… Ah, tiens ? L'organigramme de l'entreprise. De quoi cibler un plus gros poisson. Pourquoi pas Nolan Ellenberg ? Administrateur systèmes et réseaux, il dispose forcément des droits administrateur : le Graal pour des pirates !

Deux jours plus tard, Irina, dont le visage est inconnu des collaborateurs d'Alsium, se rend à la soirée d'entreprise. Elle s'installe seule, écoute les conversations… Au bout de quelques minutes, elle entend le prénom « Nolan », et tourne la tête discrètement… Voilà, c'est lui. Après, ce n'est pas très compliqué, il suffit d'aller commander au comptoir en même temps que lui, et de créer le contact. Avant la fin de la soirée, elle en sait un peu plus sur sa vie professionnelle, et privée. Sa compagne, son fils, et lui, sont supporters de la première heure des Slashers, l'équipe de basket de la ville. Tiens, Mark en avait en déjà parlé.

De nouveau, Irina enchaîne les recherches en ligne, mais pas de trace de Nolan. Il ne joue pas au Petit Poucet comme le faisait Louis. Il va falloir trouver autre chose. Il a dit qu'il était fan de basket… alors elle lui envoie sur sa messagerie professionnelle une fausse offre alléchante : 3 places gratuites pour le prochain match de l'équipe nationale. Offre limitée dans le temps, bien sûr, pour rajouter un peu de pression. Son adresse e-mail ? Elle l'a devinée en repartant de celle de Louis, et en appliquant le même schéma d'écriture nom + prénom @ alsium.com. Et ça marche ! Dès le lendemain, Nolan s'authentifie machinalement avec son compte administrateur, fait défiler ses e-mails, et tombe dans le piège en cliquant sur la belle image de basket pour télécharger les places. Il suffit de baisser la garde un instant, juste le temps d'un clic.

Surprise ! Nolan vient d'installer sans le savoir un ensemble d'outils pour pirater le système d'information, bien cachés dans un répertoire invisible. Et aussi d'offrir sur un plateau les droits administrateurs aux pirates ! Plus que quelques heures à attendre. Mieux vaut opérer la nuit, pour éviter que quelqu'un puisse voir les souris bouger toutes seules sur les ordinateurs piratés ! Le moment venu, Irina et Mark aspirent toutes les données contenues dans les serveurs de l'entreprise. Mission accomplie. Alsium ne se rendra peut-être même pas compte du piratage.

Attendez un instant… Irina repère qu'un ordinateur est resté allumé. Celui du directeur ! Et hop, un petit malware de plus sur son poste, pour détecter la frappe au clavier. Merci les droits administrateur ! Dès le lendemain, le directeur consulte un document confidentiel, stocké sur son ordinateur, dans un container chiffré. Il tape le mot de passe pour y accéder, qui tombe aussitôt entre les mains des pirates. Irina et Mark disposent désormais d'un accès aux dossiers les plus confidentiels de l'entreprise, directement à la source, sur l'ordinateur du directeur. Merci pour tout Alsium, au revoir !

Voilà, cette histoire est terminée. Enfin, « histoire », ce n'est pas un scénario de film, c'est la réalité de la cybersécurité aujourd'hui. En combinant intrusion physique et offensive à distance, les pirates ont mené avec succès une stratégie nommée « escalade des privilèges ». Ils ont d'abord attaqué un poste faiblement protégé, avant de monter progressivement dans les strates de l'organisme, pour obtenir les droits administrateur, et enfin prendre le contrôle de l'entreprise. Et tout ça, en exploitant des erreurs et oublis qui peuvent sembler insignifiants. C'est ça, ce qu'il faut retenir : la meilleure prévention, c'est l'addition de petits gestes de sécurité au quotidien. Tous ensemble.