"Ça peut vous arriver..."

Numéro 7

Les cas présentés décrivent des évènements réellement survenus au cours de ces dernières semaines.

Ils constituent une illustration de la diversité des comportements offensifs susceptibles, au profit d'opérateurs étrangers, de viser les entreprises françaises.

A vocation pédagogique, ce document est mis à disposition de tous les entrepreneurs et responsables de la « sécurité économique des entreprises ».

Par soucis de discrétion, les récits sont volontairement démarqués de tous éléments d'identification.

Les entreprises françaises seront donc appelées « *FFF* », tandis que leurs concurrentes étrangères répondront au nom de « *EEE* ».

:

UNE SOCIÉTÉ DE HAUTE TECHNOLOGIE VICTIME DE RÉTRO-INGÉNIERIE DE LA PART D'UNE ENTREPRISE D'ÉTAT ÉTRANGÈRE.

La société FFF a acquis une expertise reconnue dans la conception, la fabrication, et la commercialisation d'accélérateurs de particules. Elle est un acteur important sur ce marché de niche particulièrement concurrentiel à l'international.

Dans le cadre d'une « joint-venture », l'entreprise a installé il y a quelques années un accélérateur de particules à l'étranger, au bénéfice d'une entreprise d'Etat EEE, sans qu'il soit question d'un transfert de savoir-faire. Suite à la faillite de EEE, l'accélérateur a été revendu aux enchères à une entreprise française qui a procédé au rapatriement de la machine. Confrontée à des dysfonctionnements, la société a fait appel à FFF qui avait fabriqué l'accélérateur de particules.

Lors de l'examen de cet équipement de haute technologie, FFF a constaté que son accélérateur avait été démonté, et remonté de façon non conforme. Il présentait toutes les caractéristiques d'un équipement ayant fait l'objet de rétro-ingénierie.

Surprise par la démarche de l'entreprise d'Etat étrangère en dehors de tout transfert de technologie contractualisé, l'entreprise FFF craint désormais d'avoir à faire face à des manœuvres concurrentielles déloyales de la part d'entreprises mettant en circulation des copies de ses équipements de pointe.

La déconvenue subie par cette société française rappelle la nécessité pour toutes les entreprises qui exportent des matériels à l'étranger de protéger efficacement leur savoir-faire et de contractualiser avec rigueur tout transfert avec des clauses d'exclusivité et de confidentialité.

En l'absence de telles protections, les entreprises s'exposent à la perte du bénéfice de l'exploitation d'un savoir-faire dont elles auront assumé les coûts de développement et de commercialisation.

ATTAQUE INFORMATIQUE D'ENVERGURE CONTRE UNE GRANDE ENTREPRISE

Une grande entreprise a été victime durant un week-end d'une attaque de son PABX, c'est à dire l'autocommutateur téléphonique qui dessert ses locaux.

A en juger par l'automaticité des attaques, on peut en déduire qu'elles ne sont pas le fait d'un individu, mais plutôt de botnets, réseaux d'ordinateurs de particuliers et professionnels compromis par un cheval de Troie et qui permettent aux hackers de mener diverses attaques : dénis de service, mise en commun de la puissance de calcul pour casser des chiffrements, etc.

En l'espèce, ces botnets sont parvenus à utiliser des failles de programmation du matériel téléphonique de la marque utilisée par cette entreprise pour passer des appels surtaxés. Le programme malveillant a utilisé des codes normalement connus des seuls constructeurs, qui les utilisent pour des interventions de maintenance à distance. L'entreprise a déposé plainte auprès de la Brigade d'Enquête sur les Fraudes aux Technologies de l'Information (BEFTI).

Le préjudice, pour cette entreprise, est de plusieurs milliers d'euros. La politique de gestion des menus des téléphones a été revue.

A l'heure où l'informatique s'insère de plus en plus dans les appareils du quotidien (GPS, smartphones, tablettes…), il semble capital de sensibiliser tant les particuliers que les professionnels à la sécurité informatique, et surtout aux conséquences que peuvent engendrer des carences : la compromission de PC enrôlés dans un réseau de botnets mis à profit pour casser des codes ou saturer des serveurs.

Avec des milliers de PC compromis, les hackers disposent de la puissance de calcul nécessaire pour tenter de très nombreuses combinaisons (attaque par « force brute ») et procéder tant à des attaques de mots de passe qu'à des attaques de PABX.

DES COURS DE LANGUE ÉTRANGÈRE POUR FAIRE PARLER DES CADRES…

La société FFF évolue dans le secteur de l'énergie éolienne et dispose d'une cellule de R&D.

Une intervenante anime dans les locaux de l'entreprise une fois par semaine des cours de mise à niveau de langue vivante pour les cadres de la société.

Le directeur de l'entreprise ne dispose de presque aucun élément à son propos en dehors du fait qu'elle intervient dans d'autres entreprises du département.

Sous prétexte d'entrainement, les exercices oraux tournent souvent autour des performances de l'entreprise, et constituent une source utile de recueil d'information pour l'intervenante.

UN INGENIEUR D'UNE FILIALE D'UN GROUPE FRANÇAIS D'ARMEMENT VICTIME DE CHANTAGE SUITE AU VOL D'UN DISQUE DUR

Un ingénieur d'une filiale spécialisée dans l'armement d'un grand groupe industriel français était victime du vol, à son domicile lors d'une soirée privée, d'un disque dur personnel contenant des données professionnelles.

A la suite de ce vol, il a fait l'objet d'un chantage de la part d'individus qui tentaient de monnayer la restitution du disque dur pour un montant supérieur à la valeur vénale de l'objet, évoquant clairement ses fonctions chez l'industriel de l'armement.

Un dispositif policier a permis l'interpellation des auteurs de ce chantage en établissant que le mobile était purement crapuleux.

Cette mésaventure nous rappelle cependant que les personnels des entreprises françaises doivent être particulièrement vigilants à ce qu'ils enregistrent sur leurs outils nomades personnels.

L'accent doit encore être mis sur l'importance d'établir une frontière hermétique entre la sphère numérique professionnelle et privée.

UNE SOCIÉTÉ FRANÇAISE VICTIME D'UNE TENTATIVE D'ESCROQUERIE PORTANT SUR UNE COMMANDE.

FFF est une société spécialisée dans la confection de matériel médical qu'elle exporte dans le monde entier. Elle a récemment reçu une commande d'une société étrangère qui désirait acheter l'un de ses produits pour un montant de 32 000 euros.

La banque de la société FFF a cependant reçu de la part de son client un chèque de 165 100 euros. Les dirigeants ont alors fait part de l'erreur au client qui a demandé à la société FFF d'encaisser le chèque reçu et de lui rembourser la différence.

Face à la démarche pour le moins inhabituelle de leur client, les dirigeants de FFF n'ont ni encaissé le chèque reçu, ni honoré la commande.

La société FFF a vraisemblablement été victime d'une tentative d'escroquerie consistant à transmettre un chèque d'un montant supérieur à la commande, puis à demander un remboursement du trop perçu, alors que le chèque émis n'était pas provisionné.

Ces escroqueries ont souvent pour points communs :

a- l'usurpation d'identité de responsables du groupe (fondateur, P-DG, fils du P-DG, directeur financier, directeur marketing, etc.), de manière à intimider l'employé à qui il est demandé de faire le virement ;

b- un caractère d'urgence est avancé sous un prétexte quelconque (afin de ne pas laisser le temps de vérifier le bien-fondé de la demande de virement) ;

c- une totale discrétion est requise sous un prétexte quelconque (afin de ne pas alerter un responsable hiérarchique qui pourrait détecter l'escroquerie) ;

d- la demande de virement se fait au profit d'une banque généralement située hors de l'Union européenne, de manière à compliquer l'entraide judiciaire ;

e- les victimes sont majoritairement -mais pas exclusivement- des employés de filiales étrangères de groupes français ;

f- ces escroqueries sont en particulier, mais pas exclusivement- commises lorsqu'un weekend est suivi -ou précédé- d'un jour férié ou d'un pont engendré par un jour férié (ce délai permet de retarder la découverte du virement indu) ;

e- enfin, l'auteur de la supercherie prétextera le plus souvent être en déplacement pour ne pas laisser de coordonnées vérifiables.

UNE SOCIÉTÉ VICTIME D'UNE ESCROQUERIE À LA PROPRIÉTÉ INTELLECTUELLE

Acteur majeur d'un pôle de compétitivité spécialisé dans l'agroalimentaire, la société FFF a récemment reçu une facture portant sur le paiement d'une annuité pour le renouvellement d'un brevet déposé il y a plusieurs années à l'Institut National de la Propriété Intellectuelle (INPI) et à l'European Patent Office.

D'apparence authentique, le document portait les références d'un office des brevets d'un pays membre de l'Union Européenne. Ayant confié la gestion de son brevet à un cabinet d'affaires, la société française a aisément décelé la tentative d'escroquerie. Contacté par l'entreprise, l'office du pays en question n'a jamais été impliqué dans une telle démarche. La société n'entend évidemment pas honorer la facture indûment réclamée.

Bien que la tentative d'escroquerie porte sur un montant relativement faible, elle illustre une nouvelle forme d'atteinte aux entreprises portant sur la propriété intellectuelle. La fraude est facilitée par la publicité des brevets déposés au sein des organismes de gestion de la propriété intellectuelle.