Les dirigeants, cible préférée des hackers

● Il suffit d'un « like » d'un ami sur une photo ou d'un centre d'intérêt rendu public pour les exposer.
● Souvent inconscients du danger de leur activité en ligne, les dirigeants et cadres supérieurs sont douze fois plus ciblés par les cybercriminels.

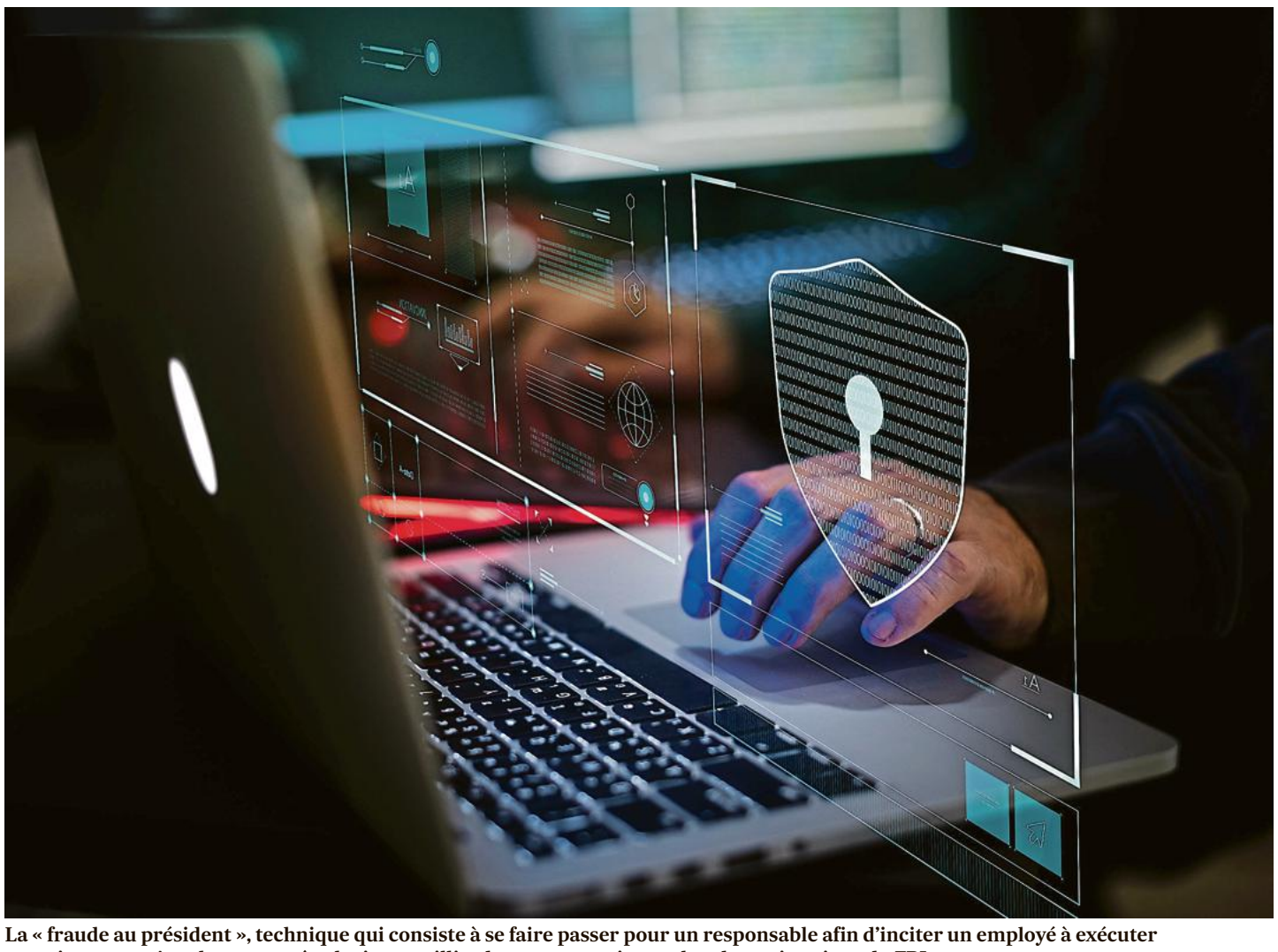
CYBERSÉCURITÉ

Leïla Marchand

Il est un secret encore bien gardé des entreprises : celui du nombre de fois où elles ont été ciblées par des cyberattaques. Mais il est un secret encore mieux gardé que celui-là : celui du nombre de fois où leurs dirigeants étaient directement dans le viseur des pirates. Et pourtant, le phénomène est aussi important que silencieux, rapporte la société Anozr Way.

« Les dirigeants et les membres de comex ou de codir sont douze fois plus ciblés que les autres par les attaques de toutes sortes », alerte Philippe Luc, cofondateur et CEO de cette start-up installée à Rennes, haut lieu de la cybersécurité en France, où se tenait justement cette semaine l'European Cyber Week (ECW 2023), un des grands événements du secteur.

Alors que le nombre de cyberattaques contre les organisations publiques et privées explose – au point de leur avoir coûté environ 2 milliards d'euros en 2022 en France, selon une évaluation récente du cabinet Asterès –, ces dommages viennent plus souvent qu'on ne le croit de fuites au plus haut niveau hiérarchique.



La « fraude au président », technique qui consiste à se faire passer pour un responsable afin d'inciter un employé à exécuter un paiement, coûte chaque année plusieurs milliards aux entreprises, selon des estimations du FBI. *Photo Shutterstock*

Des dirigeants pas assez méfiants

D'après une étude menée par Anozr Way, sept dirigeants sur dix présentent une exposition cyber à haut risque. *« Généralement, ils ne sont pas assez méfiants. Ils pensent qu'ils sont protégés car pas très actifs sur les réseaux sociaux ou, au contraire, ils considèrent qu'en tant que personnalités publiques, leur exposition est normale »*, pointe Philippe Luc, dont l'entreprise travaille surtout pour des grands comptes, dans la finance, l'industrie, l'énergie ou l'assurance. *« Les dirigeants – surtout les plus anciens – peuvent être peu sensibilisés aux bonnes pratiques. Et les patrons de PME pensent représenter une entreprise lambda parmi d'autres et ne pas être des cibles intéressantes »*, confirme Jonathan Gosselin, responsable Europe du Sud de SailPoint, entreprise américaine de solutions de gestion des identités.

Mais un simple commentaire sur une photo ou un centre d'intérêt rendu public les rend vulnérables, les pirates ayant vite fait d'exploiter ces informations personnelles, généralement accessibles facilement : d'après Anozr Way (qui s'appuie sur des cas réels anonymisés de 100 membres de comex ou codir d'entreprises de tous secteurs), environ 66 % des dirigeants affichent des réseaux sociaux personnels ouverts publiquement.

« On a eu par exemple le cas d'un haut cadre qui postait des publications en lien avec sa passion du tennis. En retour, il a été visé par des mails de phishing sur le thème du tennis », raconte l'entrepreneur Philippe Luc. Il n'est pas rare que les pirates usurpent l'identité d'un proche pour faire passer ces messages piégés : 70 % des décideurs font face à ce risque de phishing ciblé. *« Le nerf de la guerre aujourd'hui est de trouver des techniques pour crédibiliser l'attaque le plus possible, et affiner les scénarios d'hameçonnage »*, explique Jonathan Gosselin. Le mail ou le SMS reçus seront ainsi très difficiles à différencier d'un message authentique.

Un pseudonyme ne suffit pas

Autre cas d'école : celui d'un directeur financier avec une seule photo publiée sur Facebook et « likée » par sa conjointe. Il n'en fallait pas plus pour identifier les noms de tout son cercle proche, dont ses enfants, leurs photos et leur adresse personnelle. *« Ce sont des informations hautement sensibles, qui peuvent permettre de faire pression sur le dirigeant ou l'entreprise »*, relève Adèle Hayel, responsable marketing d'Anozr Way.

Très poreuse avec la sphère professionnelle et moins bien protégée, la sphère personnelle représente l'angle mort idéal. *« Certaines personnes pensent être bien cachées, par exemple en menant une vie privée sous pseudonyme. Mais ce n'est pas le cas ! »* prévient Adèle Hayel. Les pirates parviennent quand même à remonter la piste, notamment grâce aux données qui fuitent régulièrement sur le dark web : environ un dirigeant sur deux a un numéro de téléphone, ou au moins un mot de passe exposé en ligne.

Problématique, lorsque l'on sait que 80 % d'entre eux utilisent un seul et même mot de passe pour au moins 4 à 5 comptes différents, professionnels ou personnels. *« Aujourd'hui, acheter des bases de données, pour savoir si une entreprise a déjà payé pour un ransomware ou obtenir des mots de passe de dirigeants, est possible pour quelques centaines d'euros sur le dark web »*, a constaté Thomas Kerjean, CEO de l'entreprise française de cybersécurité Mailinblack.

Droits d'accès

Une fois ces données entre leurs mains, une des pratiques favorites des cybercriminels est celle de la « fraude au président ». La technique – qui coûte chaque année plusieurs milliards aux entreprises, selon des estimations du FBI – consiste à se faire passer pour le dirigeant et à profiter de son statut élevé pour convaincre des employés de lui transférer des fonds. *« En France, le ton d'autorité d'un message affiche un taux de succès deux fois supérieur que d'autres registres, quel que soit le profil de la personne visée »*, a pu vérifier Thomas Kerjean.

Changer régulièrement de mot de passe, bien vérifier l'expéditeur avant de cliquer… Outre ces pratiques élémentaires, les experts conseillent aux personnes haut placées de réduire le plus possible leur empreinte numérique – en limitant leurs infos publiques sur les réseaux sociaux – mais aussi en révisant leurs droits d'accès, comme le pointe Jonathan Gosselin : *« Ce n'est pas parce que vous êtes le PDG que vous avez besoin d'avoir accès à tout le système informatique de l'entreprise depuis votre session ! »* ■

« Les antivirus sont tous défaillants » : les chercheurs contre-attaquent face aux malwares

Grâce à leur collection de 35 millions de malwares, les chercheurs du Loria, à Nancy, ont mis au point un outil capable de détecter n'importe quel « variant » de programme malveillant. Prometteur, leur projet va se muscler grâce à un budget de cinq millions d'euros.

REPORTAGE

« Quand on a commencé, en 2010, l'université n'y croyait absolument pas. Alors on nous a mis au sous-sol… » raille malicieusement le chercheur Jean-Yves Marion en faisant visiter sa « cyberforteresse » dans les dédales de l'université de Lorraine. Ce lieu fermé par un sas sécurisé, dont les fenêtres *« ont été conçues pour résister à sept coups de hache »* et qui abrite *« des morceaux de code pouvant être considérés comme des armes de guerre »*, c'est le Laboratoire de haute sécurité (LHS) du Loria (Laboratoire lorrain de recherche en informatique et ses applications), situé à Nancy.

« Il s'agit d'un des plus importants lieux de recherche dédiés à la cybersécurité en France – avec Rennes et Paris – et le premier labo de haute sécurité ouvert sur le territoire », précise le professeur. Il y a près de quinze ans, aux prémices du LHS, *« on parlait encore de virus et de vers »* et *« d'ados boutonneux à capuche qui préparaient des cyberattaques gentillettes depuis leur garage »*, se souvient Jean-Yves Marion, presque nostalgique.

La technique du pot de miel

Ce temps est bien révolu ! Ce que l'on appelle désormais des programmes malveillants, malwares ou ransomwares, sont téléguidés par des organisations cybercriminelles qui sont parfois proches d'Etat, comme la Russie ou la Chine. *« Ce sont quasiment des entreprises, qui passent des annonces sur le web, revendent des données sur le marché noir, organisent des concours de recherche de vulnérabilités… »* décrit le chercheur.

Face à cette menace mouvante et grandissante – *« plus les appareils sont connectés, plus les possibilités d'attaques augmentent ! »* –, une foultitude de solutions de cybersécurité a été lancée sur le marché, que ce soit par les grands noms du secteur, comme Trellix, Microsoft ou Symantec, ou par des start-up mettant à profit les dernières avancées de l'intelligence artificielle.

Un écosystème très dynamique, mais où le monde académique a son rôle à jouer. *« Les entreprises ont un calendrier court terme, au mieux moyen terme quand elles en ont les moyens. Tandis que la recherche peut se consacrer à du long terme »*, rappelle Jean-Yves Marion, en donnant l'exemple du phénomène mondial ChatGPT, issu de plusieurs décennies de recherche en laboratoire.

Alors, quel serait le « ChatGPT » du Loria ? Dans sa « cyberforteresse », le laboratoire a confiné 35 millions de programmes malveillants, collectés sur Internet. *« On utilise la technique du pot de miel, qui consiste à se faire passer pour un ordinateur vulnérable, pour les attirer »*, glisse le chercheur. Cette base de virus est soigneusement disséquée par la petite équipe de chercheurs, pour améliorer leurs connaissances sur l'état de la cybermenace, mais pas seulement. Ils sont aussi parvenus à concevoir un système capable d'identifier n'importe lequel de ces virus, ainsi que n'importe quelle *« souche »* issue de ces virus, même sous forme de *« variants »*, légèrement modifiés.

Une start-up, Cyber-Detect, a été lancée en 2017 pour commercialiser l'outil. *« Tous les antivirus que l'on a aujourd'hui sur nos ordinateurs sont défaillants, car ils sont conçus pour identifier les virus déjà connus. Dès qu'un programme sort de ce périmètre, par exemple s'il a été construit spécifiquement pour vous attaquer, ils ne le repèrent plus »*, pointe Régis Lhoste, à la tête de la start-up, qui emploie une dizaine de personnes. *« De notre côté, on ne s'intéresse pas à la forme complète d'un virus mais uniquement aux petits morceaux de code, aux variants, qui correspondent à des morceaux malveillants »*, explique l'entrepreneur, dont l'outil a déjà été adopté par une quinzaine de clients, dont la moitié dans le secteur public.

Une discipline devenue « plus attirante »

Si la cyber souffrait encore d'un problème de popularité auprès des chercheurs il y a quelques années, car considérée *« trop technique »*, cette voie universitaire *« est devenue plus attirante »* et *« d'énormes moyens ont été mis sur la table au fur et à mesure »*, a pu constater Jean-Yves Marion.

A l'image du quantique qui a bénéficié d'un plan de financement de 1,8 milliard d'euros en 2021, la filière cybersécurité a été dotée l'an dernier d'une enveloppe de 65 millions d'euros dans le cadre du programme national PEPR Cybersécurité, piloté par le CNRS, Inria et le CEA. Sur cette somme, le projet Defmal de l'université de Lorraine – consacré aux programmes malveillants – a décroché un budget inédit de 5 millions d'euros, échelonné sur six ans.

De quoi mobiliser une douzaine de chercheurs, et surtout développer une approche pluridisciplinaire dans le domaine. *« Une plateforme d'échange doit être mise en place pour partager nos données avec les services de l'Etat et des partenaires industriels »*, précise l'expert. In fine, le but est de multiplier les ponts entre public et privé pour couvrir les multiples facettes de l'écosystème cybercriminel, par exemple, explique-t-il, en entretenant des relations avec les forces de l'ordre, des juristes ou des sociologues. — ***Le. M.***

Il a dit

DR

« Les entreprises ont un calendrier court terme, au mieux moyen terme quand elles en ont les moyens. Tandis que la recherche peut se consacrer à du long terme. »

JEAN-YVES MARION
Professeur à l'université de Lorraine