AMAN Jean-Jacques William
L3 MIASHS Sciences Cognitives
S6 : Initiation à la recherche

Introduction

Face à une utilisation de plus en plus soutenue des outils technologiques, les attaques informatiques se sont renforcées au cours des dernières années. Les pratiques du piratage ont en effet évolué depuis l'invention du téléphone par Graham Bell en 1876 à nos jours. Dans la vie quotidienne, les individus ont désormais la possibilité d'effectuer des achats de biens ou de services via les appareils mobiles, de procéder aux démarches administratives en flashant un QR Code ou encore de communiquer par le biais de messageries instantanées**.** L'utilisation fréquente du réseau internet nécessite de s'intéresser aux cyberattaques dont peuvent souvent être victimes le**s** utilisateurs (particuliers, entreprises ou Etats).

Selon le ministère de l'Intérieur de France, chaque année près de 978 millions de personnes[1] dans le monde sont concernées par une cyberattaque. En plus de menacer la survie d'organisations publiques ou privées, les actes de cyber malveillance (ensemble d'infractions, de gravités diverses liées aux usages numériques) touchent tout aussi fréquemment les particuliers. Les motivations des attaquants peuvent être diverses : la fraude, le vol de données numériques, l'espionnage, l'usurpation d'identité…etc.

La pratique du télétravail, ayant fortement augmentée depuis la pandémie de Covid-19 (passant ainsi chez les salariés de 3% avant la crise sanitaire à 25% pendant la crise[2]), a eu un profond effet sur la quantité d'activité sur internet mais également sur l'accroissement du nombre d'attaques informatiques qui n'a cessé de s'étendre. Parmi ces dernières, le *phishing*. Cette méthode consiste à manipuler un individu dans le but de l'inciter à communiquer des informations ou des données sensibles. L'attaquant, afin de dissimuler la supercherie de son acte, peut alors usurper l'identité d'une personne présupposée digne de confiance dans le but

[1] Ministère de l'intérieur et des outre-mer, Cybersécurité : l'action du ministère en chiffres, Le ministère présent au FIC 2019, 18 janvier 2019, disponible à l'adresse : https://www.interieur.gouv.fr/Archives/Archives-des-actualites/2019-Actualites/Le-ministere-present-au-FIC-2019/Cybersecurite-l-action-du-ministere-en-chiffres.

[2] Hallepee S. Mauroux A., Enquête SUMER : quels sont les salariés concernés par le télétravail ?, Références en santé au travail , 03/2022, n°161.

d'obtenir des renseignements. A titre d'exemple, Monsieur X reçoit un courriel d'une personne se faisant passer pour un intervenant technique appartenant au service informatique de l'entreprise de la victime potentielle. Dans ce courrier, il est demandé à Monsieur X de mettre à jour, en cliquant sur un lien, les logiciels présents sur son ordinateur de travail à des fins de conformité des règles de sécurité de l'entreprise. Ce lien, qui pourrait permettre l'installation d'un logiciel malveillant (tel qu'un virus informatique), redirige cependant Monsieur X vers une page internet, ayant les mêmes caractéristiques visuelles (logo, police d'écriture, couleurs…etc.) que celles de l'organisation. Des champs de texte s'y trouvant, sollicitent alors les identifiants et mots de passe de la victime dans l'objectif de récupérer ses données sensibles et d'accéder au réseau de l'entreprise.

Le phishing est un acte malveillant faisant partie des cyberattaques les plus courantes. Ainsi, selon une enquête provenant de la Commission européenne et d'Eurobaromètre spécial, 35% des internautes européens interrogés[3] déclarent y avoir déjà été exposés. A titre d'exemple, la plateforme Cybermalveillance.gouv.fr (créée conjointement par l'Agence nationale de la sécurité des systèmes informatiques et le ministère de l'Intérieur) dont l'objectif est la prévention et l'assistance aux victimes de sécurité informatique, a été consultée par près de 2,5 millions d'utilisateurs[4] au cours de l'année 2021. Parmi les recherches et les demandes d'assistance recensée sur la plateforme, 1,3 millions de personnes y ont eu recourt à la suite d'un phishing.

Notons qu'il existe plusieurs formes de phishing dont l'une des plus employées et l'hameçonnage « *Spray and Pray* » qui consiste à envoyer un message à un grand nombre de victimes potentielles dans l'espoir que certaines d'entre elles communiquent des informations sensibles. Ce type de phishing est basé sur l'augmentation des chances de réussite par le nombre conséquent des messages envoyés, presque aléatoirement. A l'inverse, une méthode tout aussi

[3] INSEE, Sécurité et société, Édition 2021, 09/12/2021, *Commission européenne, Eurobaromètre spécial 480 (octobre 2018) et Eurobaromètre spécial 499 (octobre 2019).*
[4] Cybermalveillance.gouv, Rapport d'activité 2021, 2022, Clémentine Lemal et Maïlys Derville, disponible à l'adresse : https://www.cybermalveillance.gouv.fr/medias/2022/03/cybermalveillance-rapport-activite-2021.pdf.

utilisé et aux conséquences qui peuvent être davantage ravageuses, le *spear phishing*[5] : il s'agit d'une attaque de phishing de forme plus sophistiquée qui implique des courriels semblant provenir de sources plus fiables. Plus étudié que le *Spray and Pray*, dans ce cas de figure l'attaquant cible particulièrement une personne ou un groupe spécifique, en utilisant des informations non publiques qui seraient familières aux cibles[6]. Cela nécessite donc de recueillir au préalable des informations sur la victime. Pour ce faire, les attaquants procèdent au social engineering.

Considéré par Kevin D. Mitnick[7] comme étant l'Art de la supercherie, le *social engineering* (ingénierie sociale) est une technique exploitant les défauts de la logique humaine (biais cognitifs) dans le but d'accéder à l'information désirée[8]. Il peut être effectué grâce à un ordinateur, par téléphone, en face à face mais aussi en utilisant un courrier électronique. Ce procédé implique de persuader une personne de se conformer à une demande inappropriée, de fabriquer la demande en utilisant des indices trompeurs et enfin de recueillir des données (Tetri et Vuorinen, 2013). Ainsi, son but est la capture des informations d'un utilisateur et le phishing en est généralement l'aboutissement.

Face à une dépendance croissante des systèmes d'information, ce type d'attaque informatique est de plus en plus sophistiqué. Il devient alors complexe pour l'utilisateur de repérer les actes de cyber malveillance. Or, le niveau de suspicion porté sur un courrier

[5] KWAK Youngsun, LEE Seyoung, DAMIANO Amanda, VISHANATH Arun, *Why do users not report spear phishing emails ?, Telematics and Informatics*, 05/2020, volume 48, SciencesDirect, [Consulté le 03/11/2022], disponible à l'adresse : https://www.sciencedirect.com/science/article/abs/pii/S0736585320300022

[6] GRIMES Roger A., *Hacking et contre-Hacking, la sécurité informatique*, Deboeck supérieur, chapitre 4, 2019, [Consulté le 21/12/2022]

[7] MITNICK Kevin D., SIMON William L., *The art of deception* : *Controlling the human element of security*, 2003, [Consulté le 03/11/2022], disponible à l'adresse : https://ivanlef0u.fr/repo/madchat/esprit/textes/The_Art_of_Deception.pdf

[8] LUO Xin, BRODY Richard, SEAZZU Alessandro, BURD Stephen, *Social Engineering : The Neglected Human Factor for Information Security Management,* Information Ressources Management Journal, 24(3), [Consulté le 22/12/2022], disponible à l'adresse : https://www.igi-global.com/article/social-engineering-neglected-human-factor/55064

électronique est déterminant dans l'engagement que l'on a avec ce dernier (Vishwanath et al, 2018) et donc sur le risque d'être victime de phishing.

Selon de précédents travaux scientifiques, les éléments contextuels exercent une forte influence dans la vulnérabilité des individus à l'hameçonnage (Hassandoust et al, 2019). En effet, les individus sembleraient traiter les informations selon le modèle Heuristique-Systématique (Chen et Chaiken, 1999) : basé sur la persuasion en psychologie sociale, cette théorie soutient que les utilisateurs valident un message reçu par un mécanisme cognitif mêlant plusieurs facteurs dont la combinaison entre un traitement heuristique et un traitement systématique. Le traitement heuristique fait appel à un ensemble d'éléments (sujet, longueur, format…etc.) intégrés au message qui permettent sa validité. Le traitement systématique est l'étude attentive du message pour évaluer sa validité[9]. On parle ainsi de modèle à double processus dans lequel l'utilisateur utilise plus de ressources cognitives dans le traitement systématique et a une tendance à être inciter à interagir avec le message si les éléments contextuels qui l'entourent sont suffisant pour donner de la crédibilité à l'information.

Dans le cadre de ce mémoire, nous porterons donc notre intérêt sur cet élément que nous jugeons important, bien souvent négligé et peu étudié en matière de sécurité de l'information : le facteur humain. Rappelons le célèbre adage commun au sein de la communauté informatique qui stipule que généralement *le problème se situe entre la chaise et le clavier*.

[9] Luo Xin, Zhang Wei, *Investigating phishing victimization with the Heuristic-Systematic Model : A theoretical framework and an exploration*, Computers & Security, 10/2013, [Consulté le 23/12/2022], disponible à l'adresse : https://www.sciencedirect.com/science/article/pii/S0167404812001927?via%3Dihub