FUTURA

Scam contre scam : les arnaqueurs… arnaqués !

Podcast écrit et lu par Adèle Ndjaki

[*Générique d'intro, une musique énergique et vitaminée.*]

Les scammers piégés par leurs propres pièges ! C'est le décryptage de la semaine dans Vitamine Tech.

[*Fin du générique.*]

Vous connaissez l'expression « à malin, malin et demi » ? Et si les rois de l'arnaque se faisaient, à leur tour, piéger ? C'est ce qui est arrivé à LockBit, l'un des groupes de hackers les plus redoutés au monde. Leur site vitrine a été piraté et leurs données exposées. Un retour de bâton spectaculaire. Mais qui sont ces justiciers de l'ombre ? Et surtout, est-ce que ces attaques permettent aux victimes d' être dédommagées ? Bonjour à toutes et à tous, je suis Adèle Ndjaki et aujourd'hui dans Vitamine Tech on parle de ce moment où les cybercriminels deviennent les cibles.

[*Une musique électronique calme.*]

Les cybercriminels deviennent de plus en plus ingénieux. Ils envoient des e-mails ou des messages frauduleux qui semblent provenir de sources fiables, offrent des services inexistants, infectent des systèmes avec des malwares, réalisent des transactions frauduleuses et saturent des serveurs pour les rendre inutilisables. En somme, c'est un véritable jeu du chat et de la souris, avec des arnaqueurs qui se réinventent constamment au gré des avancées technologiques. Cette situation devient de plus en plus complexe. À l'échelle mondiale, les chiffres sont vertigineux. Ces dernières années, les tentatives d'extorsion en ligne ont explosé. En 2024, la mission d'Interpol dédiée à cette problématique a permis plus de 5 500 arrestations et la saisie de 400 millions de dollars (371 millions d'euros), des chiffres jamais atteints auparavant. Cette activité serait devenue d'après les professionnels « l'un des secteurs d'activité clandestins les plus lucratifs au monde ». Et oui, avec des millions de victimes partout sur la planète, qu'il s'agisse de particuliers, d'entreprises ou d'infrastructures hospitalières ou étatiques…Mais attention, personne n'est à l'abri … pas même ces malfrats 2.0 qui tombent dans les pièges qu'ils ont eux-mêmes tendus. Dernièrement, le groupe de cybercriminels LockBit, connu pour ses ransomwares, a été victime d'une attaque spectaculaire. Les ransomwares sont des logiciels malveillants qui ont pour but de bloquer l'accès à votre ordinateur ou à vos données personnelles en échange d'une rançon. Leur site a été piraté et modifié pour publier un message ironique : « Ne commettez pas de crime, c'est mal, bisous de Prague ». En plus de ce message, une

base de données contenant des informations cruciales sur leurs ransomwares, leurs victimes, les montants exigés et même des identifiants d'administrateurs a été exposée. Ce n'est pas la première fois que LockBit se fait attaquer. En 2024, des services de sécurité internationaux ont repris le contrôle de leur site, un revers majeur pour l'organisation criminelle. Et puis…LockBit n'est pas le seul à avoir été pris à son propre jeu. En 2022, le groupe Conti, l'un des plus grands réseaux de ransomwares, a vu ses opérations exposées après la fuite de milliers de messages internes, ce qui a conduit à sa dissolution. En 2021, REvil, un autre groupe notoire, a été démantelé après des pressions internationales et une attaque ciblée contre ses serveurs. Alors, qui sont ces héros numériques qui piègent les arnaqueurs sur Internet ? On les appelle des scambaiters, ou pour les intimes, des croque-escrocs. Ce sont des personnes, souvent anonymes. Mais parfois ils peuvent être des figures publiques assez célèbres. comme Jim Browning qui compte 4,41 millions d'abonnés sur YouTube, Kitboga avec 3,72 millions d'abonnés, ou encore Scammer Payback avec 8,22 millions d'abonnés. À travers leurs vidéos, ces stars internationales du hacking affirment vouloir rendre justice et sensibiliser le public. Pour ce faire, ils comptent sur l'anonymat et la traçabilité. Ils utilisent des outils sophistiqués pour cacher leur identité et leur localisation, comme des masques d'IP et des machines virtuelles. Cela leur permet de tester les arnaques sans risque. Mais ce n'est pas tout. Les scambaiters vont encore plus loin en utilisant des honeypots, des pièges virtuels pour attirer les cybercriminels. Une fois qu'ils tombent dedans, les scambaiters sortent l'artillerie lourde. Ils utilisent des scripts ultra-réalistes et même de l'intelligence artificielle pour imiter des voix humaines, ce qui rend les arnaques encore plus crédibles. Ils se glissent souvent dans la peau de victimes vulnérables pour tromper les escrocs. Et puis, une fois rentrés dans leur système, certains scambaiters vont même jusqu'à prendre le contrôle à distance de l'ordinateur de l'arnaqueur. Ils accèdent parfois à ses caméras de surveillance pour récupérer des preuves incriminantes. Mais ce n'est pas la seule technique ! Ces cybercriminels tombent souvent dans un autre piège. Beaucoup d'entre eux cherchent à acheter des services pour mener des attaques, comme des logiciels de hacking ou des outils pour pénétrer des systèmes. Mais ces « services » sont en réalité des arnaques destinées à les piéger. Résultat : ces outils inutilisables leur font finalement perdre à leur propre jeu.

[*Virgule sonore, une cassette que l'on accélère puis rembobine*.]
[*Une musique de hip-hop expérimental calme*.]

Bien que les scambaiters jouent un rôle non négligeable contre les cybercriminels, leur action ne peut pas remplacer les démarches légales nécessaires pour récupérer les fonds volés. Si ces justiciers 2.0 parviennent à démanteler des arnaques, la route vers la réparation des victimes reste semée d'embûches. Pour cela, les autorités compétentes restent indispensables, et les victimes doivent s'appuyer sur les canaux traditionnels, malgré les obstacles. Bien que l'impact exact du scambaiting sur la réduction des arnaques soit difficile à évaluer, de nombreux rapports suggèrent qu'il a un effet dissuasif notable. Et oui occuper les arnaqueurs et exposer leurs techniques, ça paye. Le scambaiting est un outil précieux dans la lutte contre la cybercriminalité, mais il doit s'inscrire dans un cadre légal et éthique rigoureux pour être véritablement efficace.

[*Virgule sonore, un grésillement électronique*.]

C'est tout pour cet épisode de *Vitamine Tech.* Pour ne pas manquer nos futurs épisodes, abonnez-vous dès à présent à ce podcast, et si vous le pouvez, laissez-nous une note et un commentaire. Cette semaine, je vous recommande le dernier épisode de Futura Santé, dans lequel Melissa Lepoureau vous parle du papillomavirus, et des dernières recommandations en vigueur ! Pour le reste, je vous remercie pour votre fidélité à Vitamine Tech, je vous souhaite tout le meilleur, et, comme d'habitude, une excellente journée ou une très bonne soirée et rester branché !

[*Un glitch électronique ferme l'épisode*.]