L'équipe d'experts en cybersécurité de KnowBe4 dévoile ses prédictions pour 2022

KnowBe4, fournisseur de la plus grande plateforme mondiale de formation, sensibilisation à la sécurité, et simulation d'hameçonnage, a annoncé aujourd'hui les prédictions en matière de cybersécurité pour 2022, de son équipe d'experts du secteur.

Les tendances prévues dans le domaine de la cybersécurité pour 2022 incluent :

- **Rançongiciel nucléaire 3.0**

  Parmi les tendances qui façonnent actuellement l'avenir du côté des acteurs malveillants figure le fait que les gangs de rançongiciels se transforment en « gangs multitâches ». Loin de se consacrer uniquement aux rançongiciels et à l'exfiltration des données, ces gangs effectuent également du cryptominage, créent des botnets, réalisent des attaques DDoS, etc. Les gangs d'attaque du futur considéreront toutes les nouvelles victimes comme une source de profits, et tenteront de déterminer les actions à mener et dans quel ordre pour maximiser l'extraction financière.
- **Nouvelle gamme de logiciels malveillants : pas le genre d'hôte que vous accueilleriez volontiers chez vous**

  Une nouvelle gamme de logiciels malveillants métamorphiques, aussi dangereuse que persistante, et baptisée « Tardigrade » est une nouvelle souche de logiciels malveillants Windows. Ils s'adaptent constamment pour éviter leur détection, et ont été pour la première fois découverts alors qu'ils ciblaient l'industrie biotechnologique, notamment les infrastructures à l'origine de la fabrication de vaccins, d'après plusieurs chercheurs en sécurité. Cette capacité « métamorphique » empêche le logiciel malveillant de laisser derrière lui une signature cohérente, ce qui rend sa détection très difficile pour les programmes d'antivirus. Il possède la capacité sournoise de se propager à la fois via des e-mails d'hameçonnage et via des appareils USB.
- **Virtually Pwned**

  Meta, marque connue antérieurement sous le nom de Facebook, incitera le plus grand nombre à rejoindre le Metaverse. Ceci engendrera une ruée vers l'établissement d'une domination dans le monde virtuel. Par conséquent, les hackers seront également entraînés dans cet univers, et nous assisterons à des attaques virtuelles affectant à la fois des particuliers et des organisations. Nous assisterons à l'explosion de méfaits à l'encontre des individus et des ressources dans le monde virtuel… pillage virtuel, vol virtuel, prises de contrôle de comptes, et autres exploits criminels créatifs.
- **La désinformation alimentée par les hypertrucages engendrera un désordre politique/financier**

  Nous assisterons à une campagne de désinformation coordonnée qui s'appuiera massivement sur les hypertrucages et les montages manipulés pour engendrer un

désordre politique/financier. Un hypertrucage pourra être utilisé pour manipuler l'opinion de certains partis politiques, en déclarant de fausses opinions, promesses ou croyances concernant un candidat particulier. Ceci pourrait entraîner la réaction en chaîne de certaines organisations qui retireraient leurs fonds d'une campagne politique sur la base des déclarations fabriquées par l'hypertrucage.

- **Une attaque contre les cryptomonnaies affectera les économies du monde réel**

  Une cryptomonnaie majeure sera attaquée, causant la perte de plusieurs milliards de dollars, soit via un vol direct, soit via une perte de valeur. De nombreux particuliers et organisations seront gravement touchés, et cette attaque sera baptisée le Black Crypto Day (Journée noire pour les cryptomonnaies).
- **Une centrale électrique ou un fournisseur de services publics, majeur en Europe sera paralysé par une nouvelle forme d'attaque, autre qu'un rançongiciel**

  Il est très probable que des acteurs malveillants, quelque part en Europe de l'Est, coupent votre électricité, votre gaz et votre eau. Puis, lorsque vous constaterez avec effroi la décharge de votre téléphone, de votre tablette et de votre ordinateur portable, ils vous tendront un brin d'olivier qu'un grand nombre sera prêt à accepter, mais à quel prix ?
- **Une opération de contre-piratage sera lancée contre un acteur malveillant pris par erreur pour l'auteur des attaques, déclenchant ainsi un incident diplomatique**

  Un chercheur en sécurité trop impatient pensera en effet avoir identifié le coupable d'une attaque majeure. En guise de représailles, il procédera à un contre-piratage, avant de découvrir qu'il n'a pas attribué l'attaque correctement. Ceci engendrera un incident diplomatique majeur, et l'organisation responsable sera placée sous haute surveillance.
- **Essor des fusions-acquisitions sur le marché noir**

  De nombreux gangs criminels sont devenus extrêmement riches. En effet, certaines organisations douteuses sont suffisamment importantes pour être cotées en bourse. Nous assisterons ainsi à l'émergence d'un marché noir plus officiel, où se joueront diverses activités de fusions-acquisitions, dans un contexte où certains gangs tenteront d'encaisser de l'argent en vendant leur organisation, tandis que d'autres s'attacheront à développer leurs capacités et leur portée.
- **Lorsque l'IA tournera mal en 2022**

  Nous assisterons à la première vague de robots d'attaque intelligents. Le futur opposera la chasse aux menaces livrée par les bons robots, à celle des robots malveillants, et le meilleur algorithme sortira vainqueur.

« À de nombreux égards, il semble que les choses tournent mal pour les professionnels de la cybersécurité qui s'efforcent de protéger leur organisation », a déclaré Stu Sjouwerman, PDG de KnowBe4. « Je pense toutefois que nous commençons à nous focaliser davantage sur le facteur humain, notamment le comportement humain, en ce qui concerne les mesures de cybersécurité axées sur la protection. Il s'agit d'un changement de direction positif, dans la mesure où même si les individus appliquent tous les outils et contrôles techniques au monde, s'ils ne focalisent pas

leurs efforts sur la couche de sécurité humaine, ils seront confrontés à des défis. En fin de compte, le plus important réside dans l'adoption d'une solide culture de sécurité, et c'est ce sur quoi nous verrons les organisations concentrer leurs efforts à l'approche de 2022. »

Les tendances prévues ont été recueillies auprès de l'équipe mondiale des défenseurs de la sensibilisation à la sécurité, de KnowBe4, laquelle est composée d'experts possédant plusieurs dizaines d'années d'expérience dans le domaine de la cybersécurité. Pour en savoir plus sur l'équipe d'experts de KnowBe4, rendez-vous sur https://www.knowbe4.com/security-awareness-training-advocates.

À propos de KnowBe4

KnowBe4, le fournisseur de la plus grande plateforme mondiale de formation à la sensibilisation à la sécurité et de simulation d'hameçonnage, prête ses services à plus de 44 000 organisations à travers le monde. Fondée par le spécialiste de la sécurité informatique et de la sécurité des données, Stu Sjouwerman, KnowBe4 aide les organisations à prendre en compte l'élément humain de la sécurité, en sensibilisant aux ransomwares, aux impostures des fraudeurs se faisant passer pour des cadres dirigeants (« CEO fraud »), et autres tactiques d'ingénierie sociale, grâce à une approche nouvelle de la formation axée sur la sensibilisation à la sécurité. Kevin Mitnick, un spécialiste de la cybersécurité de renommée internationale, et responsable du Hacking, chez KnowBe4, a contribué à la conception de la trousse de formation de KnowBe4, sur la base de ses tactiques d'ingénierie sociale soigneusement documentées. Des dizaines de milliers d'organisations s'appuient sur KnowBe4 pour faire en sorte que leurs utilisateurs finaux soient leur dernière ligne de défense.

Le texte du communiqué issu d'une traduction ne doit d'aucune manière être considéré comme officiel. La seule version du communiqué qui fasse foi est celle du communiqué dans sa langue d'origine. La traduction devra toujours être confrontée au texte source, qui fera jurisprudence.

Consultez la version source sur businesswire.com : https://www.businesswire.com/news/home/20211202005374/fr/