BULLETIN DE VEILLE CYBER

18 février 2025

EDITION N°12

PHOBOS AETOR : ARRESTATIONS DE RANÇONNEURS DE 8BASE/PHOBOS EN THAÏLANDE

[14 février 2025] - PHOBOS AETOR est une opération internationale conjointe menée par les forces de police thaïlandaises, suisses et américaines. Elle a pour objectif le démantèlement de réseaux cybercriminels spécialisé dans les rançongiciels. Leur récente opération aurait conduit à l'arrestation de quatre individus à Phuket, suspectés d'appartenir au réseau cybercriminel 8Base, spécialisé dans les attaqués. Cette intervention a permis de mettre un terme aux activités de ce groupe, qui aurait orchestré plus de 1 000 attaques à l'échelle mondiale, engendrant des pertes estimées à 16 millions de dollars.

L'enquête a révélé que le groupe utilisait le rançongiciel Phobos, qui leur permettait de s'infiltrer dans les systèmes informatiques de leurs victimes, de chiffrer leurs données et d'exiger une rançon en cryptomonnaies sous menace de divulgation des informations volées. Entre avril et octobre 2024, au moins 17 entreprises suisses ont été attaquées. Pour masquer leurs traces financières, les cybercriminels utilisaient des mixers de cryptomonnaies, compliquant ainsi le travail des enquêteurs.

Source : https://www.zataz.com/phobos-aetor-arrestations-de-ranconneurs-de-8base-en-thailande/

LES CAPTCHAS : OUTILS DE SÉCURITÉ OU INSTRUMENTS DE COLLECTE DE DONNÉES PERSONNELLES ?

[14 février 2025] - Les tests CAPTCHA conçus pour différencier les humains des robots en ligne, sont largement utilisés pour protéger les sites web contre les activités automatisées malveillantes.

Cependant, des préoccupations croissantes émergent quant à leur utilisation pour la collecte de données personnelles. Des services tels que reCAPTCHA de Google collectent des informations sur les utilisateurs, notamment l'adresse IP, les cookies, les données de l'appareil et de l'application, ainsi que l'historique de navigation souvent sans consentement explicite.

Ces données peuvent être utilisées à des fins autres que la sécurité, soulevant des questions sur la conformité au Règlement Général sur la Protection des Données (RGPD).

La Commission nationale de l'informatique et des libertés (CNIL) a notamment mis en demeure des organismes utilisant reCAPTCHA sans mesures adéquates de protection des données. Face à ces enjeux, des alternatives plus respectueuses de la vie privée comme hCaptcha, sont recommandées pour concilier sécurité et protection des données personnelles.

Source : https://www.lemondeinformatique.fr/actualites/lire-collecter-et-vendre-des-donnees-la-double-vie-des-captchas-96073.html

Cristina GURAU

LA CAISSE DES DÉPÔTS VICTIME D'UNE FUITE DE DONNÉES

[13 février 2025] - La Caisse des Dépôts a été victime d'une importante fuite de données, touchant environ 70 000 personnes, dont des agents contractuels de la fonction publique, des élus locaux et des praticiens hospitaliers. L'incident a été révélé le 17 février 2025 et concerne des informations sensibles telles que les numéros de sécurité sociale, les noms et prénoms, les dates, départements et villes de naissance, ainsi que les adresses postales lorsqu'elles étaient renseignées.

Les cybercriminels ont pu accéder à ces données en dérobant des identifiants de connexion à une plateforme utilisée par les employeurs publics pour gérer les cotisations de retraite des affiliés à l'Ircantec.

Source : https://www.usine-digitale.fr/article/une-cyberattaque-vise-la-caisse-des-depots-les-donnees-de-70-000-personnes-subtilisees.N2227416

SIRI AU CŒUR D'UN SCANDALE SUR LA VIE PRIVÉE

[13 février 2025] - La Ligue des droits de l'homme (LDH) a déposé plainte devant le parquet de Paris contre des personnes non identifiées, visant implicitement Apple pour des pratiques liées à son assistant vocal Siri. Cette plainte repose sur les révélations d'un ex-employé lanceur d'alerte et évoque plusieurs infractions présumées : violation de la vie privée, traitement illégal de données personnelles et pratiques commerciales déloyales.

L'affaire concerne la captation massive d'enregistrements vocaux sans consentement explicite des utilisateurs. Bien qu'Apple assure ne pas utiliser ces données à des fins marketing ni les vendre, la LDH estime que ces pratiques posent un problème de transparence et de respect du RGPD.

Source : https://siecledigital.fr/2025/02/17/siri-dans-le-viseur-apple-face-a-une-plainte-pour-atteinte-a-la-vie-privee-en-france/

UN COLLÈGE À BRIVE A ÉTÉ VICTIME D'UN RANSOMWARE

[12 février 2025] - Le collège La Salle à Brive en Corrèze, a été victime d'une cyberattaque en janvier 2025. Un rançongiciel a infecté son système après qu'un salarié ait ouvert un mail piégé, entraînant le chiffrement et la perte de toutes les données informatiques. Une rançon de 8 000 euros a été demandée, mais l'établissement a choisi de ne pas la payer, faute de garantie de récupération des fichiers.

Cette situation a posé des difficultés aux familles, notamment pour celles qui n'avaient pas encore téléchargé les bulletins scolaires et ne peuvent plus y accéder. Certains élèves, comme ceux préparant leur entrée au lycée, rencontrent des complications administratives. Seules les archives comptables ont été préservées grâce aux impressions annuelles réalisées par la comptable de l'établissement.

Pour éviter qu'un tel incident ne se reproduise, l'établissement a investi 25 000 euros dans l'amélioration de sa cybersécurité. Cette attaque souligne la vulnérabilité des établissements scolaires face aux cybermenaces.

Source : https://france3-regions.francetvinfo.fr/nouvelle-aquitaine/correze/brive/le-montant-de-la-rancon-qui-etait-de-8-000-euros-ce-college-perd-tous-les-bulletins-des-eleves-apres-une-cyberattaque-3107128.html

Cristina GURAU