AEGE

Club Cyber

BULLETIN DE VEILLE CYBER

4 février 2025

EDITION N°10

LE CLUB CYBER S'UNIT POUR CÉLÉBRER LA JOURNÉE MONDIALE CONTRE LE CANCER CE 4 FÉVRIER !

IA : CRÉATION DE L'INESIA EN FRANCE ET PREMIÈRES MESURES DE L'IA ACT

[3 février 2025] - La France a lancé l'Institut national pour l'évaluation et la sécurité de l'intelligence artificielle (INESIA), afin structurer l'évaluation et la régulation de l'IA. Cette initiative fait suite à la Déclaration de Séoul, qui met en avant la nécessité de renforcer la sécurité et la régulation des modèles d'IA.

L'INESIA a pour missions d'analyser les risques liés à l'IA, d'évaluer la performance des modèles et de soutenir leur régulation. Il collaborera également avec des acteurs internationaux comme l'AI Safety Institute du Royaume-Uni et contribuera à l'élaboration de normes de sécurité.

Parallèlement, les premières mesures du règlement européen IA Act sont entrées en vigueur le dimanche 2 février. Pour l'instant, ce premier volet ne concerne que certaines pratiques jugées inacceptables, comme les logiciels de « notation sociale » et les systèmes de « police prédictive individuelle ». La mise en œuvre complète de l'IA Act se fera progressivement.

Le Sommet pour l'action sur l'IA qui débutera le 10 février à Paris, devrait apporter son lot de nouveautés en la matière. Affaire à suivre...

Source :

- https://www.theregister.com/2025/01/08/mitel_0_day_oracle_rce_under_exploit/
- https://www.lemonde.fr/economie/article/2025/02/02/intelligence-artificielle-les-premieres-mesures-du-reglement-europeen-ai-act-entrent-en-vigueur_6527570_3234.html

STMICROELECTRONICS : PRÈS DE 3 000 EMPLOIS SUPPRIMÉS EN FRANCE ET EN ITALIE

[3 février 2025] - Le fabricant de semi-conducteurs STMicroelectronics s'apprêterait à supprimer entre 2 000 et 3 000 emplois en France et en Italie, soit environ 6% de ses effectifs. Les sites de Crolles et de Grenoble en Isère seraient les plus touchés.

Ces suppressions d'emplois seraient motivées par une baisse de la demande de composants, notamment dans le secteur automobile, et une diminution des revenus. En effet, le chiffre d'affaires annuel de 2024 a diminué de 23,2 % par rapport à l'année précédente, et le bénéfice a chuté de 63 %. L'entreprise prévoit un plan d'économies de 300 millions de dollars à partir de 2027.

Le groupe privilégie les départs volontaires et les retraites anticipées, tout en assurant vouloir investir dans les compétences d'avenir. D'autres acteurs du secteur, tels qu'AMD, Intel et Infineon, ont également procédé à des licenciements.

Un projet de relance du site de Crolles, en partenariat avec GlobalFoundries, est actuellement au point mort.

Source : https://www.lemondeinformatique.fr/actualites/lire-stmicroelectronics-supprimerait-des-milliers-d-emplois-en-isere-95946.html

Sébastien P.

MESSAGERIES CHIFFRÉES ET BACKDOORS : UN VOTE CONTROVERSÉ DU SÉNAT

[31 janvier 2025] - Le Sénat français a voté un amendement imposant aux messageries chiffrées comme Signal et WhatsApp d'intégrer des portes dérobées pour faciliter l'accès aux communications dans le cadre de la lutte contre le narcotrafic. Soutenue par le ministre de l'Intérieur, cette mesure pourrait entraîner des sanctions financières en cas de non-respect.

Toutefois, elle suscite des inquiétudes : absence d'étude d'impact, perte de confiance des utilisateurs et risques accrus de cybersécurité. Le rapporteur du texte s'y oppose, estimant qu'elle pourrait pousser ces services à quitter la France.

De son côté, Guillaume Poupard, ancien DG de l'ANSSI, a rappelé sur LinkedIn une analyse de 2016 qui reste dans l'air du temps :

« Imposer un affaiblissement généralisé des moyens cryptographiques serait attentatoire à la sécurité numérique et aux libertés de l'immense majorité des utilisateurs respectueux des règles tout en étant rapidement inefficace vis-à-vis de la minorité ciblée. »

Source :

- https://www.zdnet.fr/actualites/signal-whatsapp-les-senateurs-demandent-une-explosive-backdoor-dans-les-messageries-chiffrees-405423.htm
- https://www.linkedin.com/posts/guillaume-poupard-3604531b5_contr%C3%B4ler-le-chiffrement-un-calcul-difficile-activity-7292070577576554496-U-X-/?utm_source=share&utm_medium=member_desktop

PARAGON : WHATSAPP MET FIN À UNE CAMPAGNE DE CYBER-ESPIONNAGE

[31 janvier 2025] - WhatsApp a récemment interrompu une campagne de cyber-espionnage visant environ 90 journalistes et militants de 20 pays, menée par la société israélienne Paragon.

Cette campagne exploitait des fichiers PDF malveillants pour infiltrer les appareils des cibles, permettant ensuite l'accès aux messages chiffrés des victimes sans interaction de leur part.

WhatsApp a informé les victimes et a adressé une injonction à Paragon, envisageant des actions légales. L'entreprise, spécialisée dans les logiciels espions, a été acquise par AE Industrial Partners et a des contrats avec des agences gouvernementales américaines.

Cette situation fait écho à l'affaire Pegasus, où un autre logiciel espion israélien a été utilisé pour surveiller illégalement des journalistes, des activistes et des politiques, dont le président Emmanuel Macron.

Source : https://techcrunch.com/2025/01/31/whatsapp-says-it-disrupted-a-hacking-campaign-targeting-journalists-with-spyware/

Sébastien P.

GEMINI : GOOGLE PUBLIE UN RAPPORT SUR L'UTILISATION DE SON IA PAR LES ACTEURS DE LA MENACE

[29 janvier 2025] - Google a publié un rapport sur les acteurs de la menace qui utilisent son IA générative Google Gemini pour amplifier leurs attaques.

Cette analyse révèle que l'IA n'est pas encore une technologie révolutionnaire pour ces acteurs, mais qu'ils utilisent l'IA principalement pour des tâches courantes, et de deux manières principales : pour accélérer leurs campagnes (via du code malveillant ou du phishing), et pour instruire les modèles à effectuer des actions malveillantes.

Parmi les acteurs affiliés à un État (APT), ceux liés à l'Iran sont les plus actifs, suivis par la Chine et la Corée du Nord, tandis que l'utilisation des acteurs russes est plus limitée. Sans surprise, les opérations d'influence exploitent également l'IA pour créer et manipuler du contenu.

Bien que l'IA leur permette d'agir plus rapidement, les LLM actuels ne leur offrent pas de nouvelles capacités majeures. Les mesures de sécurité de Gemini ont limité les risques et les tentatives de les contourner ont échoué (il aurait été surprenant de lire le contraire sur le site de Google).

Source :

- https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai?hl=en
- https://www.csoonline.com/article/3812699/threat-actors-using-google-gemini-to-amplify-attacks-report.html

SANCTIONS DE L'UE CONTRE DES AGENTS DU GRU POUR CYBERATTAQUES EN ESTONIE

[29 janvier 2025] - L'Union européenne a sanctionné trois agents du renseignement russe impliqués dans des cyberattaques contre les ministères estoniens. Ils sont soupçonnés d'avoir dérobé « des milliers de documents confidentiels ».

Ces attaques font partie d'une série d'opérations de piratage informatique liées à la Russie et considérées comme des actes de déstabilisation. En effet, ces agents sont membres du groupe cybercriminel russe « Unit-29155 », notamment responsable d'un certain nombre de cyberattaques contre l'Ukraine et ses alliés, mais aussi des membres de l'OTAN.

En septembre dernier, il a été démontré que le groupe « Unit-29155 » était affilié au GRU, le service de renseignement russe. Certains de ses membres s'étaient fait connaître dans les médias français il y a quelques années pour avoir résidé (et mené des opérations) en Haute-Savoie.

L'UE a gelé les avoirs des responsables et leur a interdit l'entrée sur le territoire européen.

Source : https://www.usine-digitale.fr/article/l-ue-sanctionne-trois-agents-du-renseignement-russe-pour-avoir-pirate-des-ministeres-estoniens.N2226477

Sébastien P.