



## COMMUNIQUÉ DE PRESSE

# Gen dévoile PharmaFraud : un empire mondial de pharmacies frauduleuses au cœur de l'essor des cybermenaces alimentées par l'IA

*Gen bloque un million d'attaques liées à de fausses pharmacies en ligne, propose un outil de déchiffrement gratuit de ransomware, et observe une hausse des violations de données, des escroqueries financières, des cas de sextorsion et des arnaques au support technique.*

**Paris (France), le 30 juillet 2025** - Gen (NASDAQ : GEN), leader mondial de la liberté numérique regroupant plusieurs marques de confiance telles que **Norton, Avast, LifeLock, MoneyLion** et d'autres, publie aujourd'hui son rapport sur les menaces pour le deuxième trimestre 2025. Les chercheurs de Gen analysent l'impact croissant de l'intelligence artificielle sur la cybercriminalité. Leur enquête met en lumière plus de **5000** sites frauduleux de fausses pharmacies, particulièrement sophistiqués, conçus pour piéger les internautes à la recherche de traitements très prisés. Ils ont également contribué au démantèlement du tout premier **ransomware** partiellement conçu à l'aide de l'IA. Le rapport révèle également une hausse de **21 %** des violations de données, une augmentation spectaculaire de **340 %** des escroqueries financières, un doublement des cas de sextorsion, ainsi qu'une forte recrudescence des **arnaques au support technique**, qui se multiplient notamment sur Facebook.

*« Les cybermenaces deviennent de plus en plus intelligentes, rapides et ciblées », a déclaré **Siggi Stefnisson, directeur technique de la cybersécurité chez Gen.** « Des ransomwares générés par l'IA aux fausses pharmacies en ligne, les risques sont bien réels et de plus en plus difficiles à détecter pour les utilisateurs. Mais grâce à une coopération internationale, à des technologies de détection avancées et à notre engagement sans faille dans le développement de solutions capables de contrer ces nouvelles menaces, nous restons en position de force. Les menaces évoluent, mais notre capacité à les combattre aussi. »*

## **PharmaFraud : quand l'escroquerie se fait passer pour de la médecine**

Lorsqu'on recherche un traitement, qu'il s'agisse d'un antibiotique courant, d'un médicament contre l'obésité très demandé ou d'un traitement plus intime, internet peut sembler la solution la plus rapide et la plus discrète. Les cybercriminels l'ont bien compris. Les chercheurs de Gen ont nommé **PharmaFraud** cette menace croissante des pharmacies en ligne frauduleuses. Ils ont mis au jour un vaste réseau de plus de **5 000 sites web** vendant, en toute discrétion ou à prix réduits, des médicaments recherchés comme des traitements contre les troubles de l'érection,



des pilules contre l'obésité et des antibiotiques. En 2025, Gen a bloqué un million de tentatives d'attaque émanant de ces plateformes à l'encontre de consommateurs non avertis.

Ces opérations reposent sur un large éventail de techniques : **injection de code malveillant sur des sites médicaux, manipulation des résultats de recherche, création de blogs santé générés par IA et de faux avis clients**. Les sites en question imitent de vraies pharmacies en ligne, avec un design soigné, un faux service client et des fiches produits détaillées. Mais la prudence est de mise : derrière cette apparence légitime se cachent bien souvent des arnaques visant à voler des **données personnelles ou bancaires**. Certains signes doivent alerter : prix anormalement bas pour des médicaments sur ordonnance, absence de coordonnées de contact, demandes de paiement en cryptomonnaie, processus de paiement non sécurisé, ou encore demande abusive d'informations sensibles, qu'elles soient personnelles, médicales ou financières.

### **Neutraliser les bots : Gen déjoue un ransomware alimenté par l'IA**

Dans le cadre de son engagement envers les victimes de ransomware, Gen a identifié une faille cryptographique majeure dans **FunkSec**, la première souche connue de ransomware partiellement conçue à l'aide de l'IA générative. Bien que le malware ait réussi à chiffrer les données et exiger une rançon, les chercheurs de Gen ont collaboré avec les autorités pour aider les victimes à récupérer leurs fichiers sans avoir à payer, grâce à un [outil de déchiffrement gratuit proposé par Avast](#). Depuis, FunkSec est resté silencieux.

### **Escroqueries financières et faux supports techniques sur Facebook**

Le risque d'être victime d'une escroquerie financière a été **multiplié par plus de trois (+340 %)** entre avril et juin 2025, avec de nombreuses attaques provenant de publicités trompeuses et de faux profils diffusés sur **Facebook**. Les cybercriminels ont eu recours à des vidéos deepfake et à des formulaires automatisés pour collecter des données personnelles et bancaires, en se faisant passer pour des services juridiques ou des opportunités d'investissement.

En parallèle, **14 %** des menaces bloquées sur Facebook étaient liées à des **arnaques au support technique**, une forte hausse alimentée par de **faux pop-ups** imitant l'interface de Messenger. Ces pages bloquent le navigateur des utilisateurs et les incitent à appeler de fausses lignes d'assistance. La portée de Facebook et son infrastructure publicitaire en font toujours un outil redoutablement efficace pour mener des fraudes à grande échelle.

Parmi les autres enseignements marquants du rapport :



- **+21 % d'augmentation des violations de données**, avec une hausse de près de 16 % du nombre d'adresses e-mail compromises.
- **Lumma Stealer est resté actif** malgré son démantèlement, s'appuyant sur une nouvelle infrastructure pour poursuivre le transfert de données volées.
- **+317 % de notifications push malveillantes**, souvent déguisées en lecteurs vidéo ou en alertes système.
- **+62 % d'attaques par accès à distance**, portées par le retour du cheval de Troie Wincir RAT et l'exploitation de services cloud comme OneDrive.
- **Le retour du DealPly adware**, dont l'activité était en recul, avec une recrudescence aux États-Unis, au Brésil, en France et en Inde.
- **Les petites entreprises** en ligne de mire, visées par des infostealers, des exploits et des outils d'accès à distance. Les escroqueries restent la principale menace pour les petites entreprises.

Les marques du groupe Gen réaffirment leur engagement à protéger les utilisateurs contre les arnaques mises en lumière dans ce rapport, grâce à des solutions comme [Norton Genie](#), une protection contre les escroqueries disponible en application autonome ou intégrée à l'offre Norton 360, ainsi que Scam Guardian, désormais inclus dans [Avast Free Antivirus](#) et [Avast Premium Security](#). En cas de vol ou de fuite de données personnelles, [LifeLock](#) propose un accompagnement complet pour aider les utilisateurs à faire face à l'usurpation d'identité.

Pour lire l'intégralité du rapport Gen Threat Report du deuxième trimestre 2025, rendez-vous sur <https://www.gendigital.com/blog/insights/reports/threat-report-q2-2025>

## À propos de Gen

Gen(TM) (NASDAQ : GEN) est une entreprise mondiale dédiée à la liberté numérique à travers ses marques de référence en termes de cybersécurité, Norton, Avast, LifeLock, MoneyLion et d'autres. Gen, une famille de marques grand public, est née de la volonté d'assurer la sécurité des premières générations numériques. Gen offre la possibilité au grand public de vivre leur vie numérique en toute sécurité, en toute confidentialité et en toute confiance, aujourd'hui et pour les générations à venir. Gen propose des produits et des services primés en matière de cybersécurité, de confidentialité en ligne et de préservation de l'identité avec près de 500 millions d'utilisateurs dans plus de 150 pays. Pour en savoir plus, consultez le site [www.GenDigital.com](http://www.GenDigital.com).

[Contacts presse](#)



[genfr@edelman.com](mailto:genfr@edelman.com)

Louna BALANCHE : +33(0) 6 11 48 51 11

Albane POTTIER : +33(0) 6 89 11 54 45