Criminalité organisée en ligne: **comment Europol enraye la mécanique de la cybercriminalité**

Europol, dont le siège est situé à La Haye, aux Pays-Bas, aide ses États membres à prévenir et à combattre toutes les formes graves de criminalité internationale organisée, de terrorisme et de cybercriminalité.

La lutte contre la cybercriminalité est l'une des priorités absolues de l'agence, comme le souligne la dernière évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA UE). Selon la SOCTA UE, les cybercrimes suivants sont considérés comme des menaces majeures dans l'Union européenne (UE): les cyberattaques, les mécanismes de fraude en ligne et l'exploitation sexuelle des enfants (en ligne).

| **Europol, Criminalité organisée en ligne: comment Europol enraye la mécanique de la cybercriminalité**

PDF Web | ISBN 978-92-9414-075-3 | DOI-10.2813/8241277 | QL-01-25-021-FR-N

© Agence de l'Union européenne pour la coopération des services répressifs, 2025

La présente synthèse a été traduite à des fins pratiques.
Veuillez noter que la version anglaise est la version officielle de référence.

Reproduction autorisée, moyennant mention de la source.

Toute utilisation ou reproduction de photos ou de tout autre matériel dont l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) ne possède pas les droits d'auteur requiert l'autorisation préalable des titulaires des droits en question.

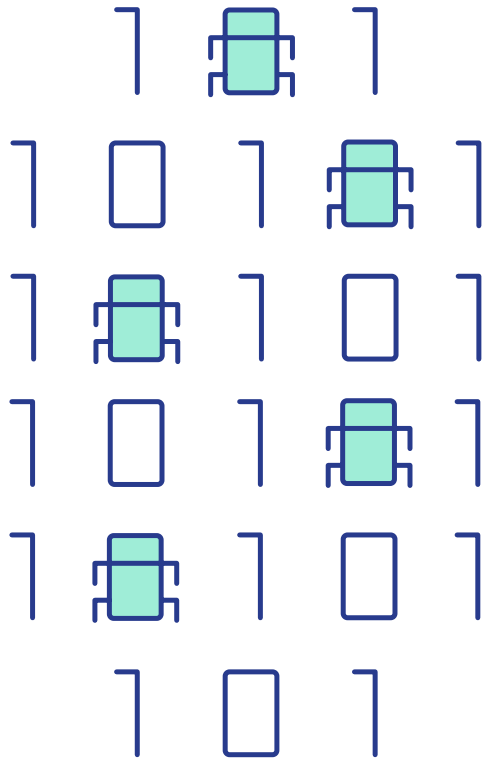
Merci de citer cette publication comme suit: Europol, Criminalité organisée en ligne: comment Europol enraye la mécanique de la cybercriminalité, Office des publications de l'Union européenne, Luxembourg, 2025.

L'intégralité du rapport est disponible sur le site web d'Europol à l'adresse suivante:
www.europol.europa.eu

Les cyberattaques sont le fait de cybercriminels qui ciblent, via l'internet, les infrastructures critiques, les gouvernements, les entreprises et les citoyens. Elles sont souvent exécutées pour le compte d'acteurs de la menace externes, de plus en plus de niveau étatique et motivés par des raisons idéologiques.

Principales tendances en matière de cyberattaques

- **Les données constituent une matière première incontournable dans la sphère de la menace par maliciels** et servent à la fois de cibles, de munitions pour perpétrer les attaques et de produits dérivés de celles-ci.
- **Ce type de criminalité repose sur l'économie du «crime en tant que service»,** notamment des forums à but lucratif du dark web qui vendent des données volées et proposent des services d'intrusion, ainsi que des fournisseurs illicites d'hébergement et de services de proxy.
- **Le paysage cybercriminel s'est peu à peu fragmenté** Det se compose aujourd'hui de marchés éclatés et de groupes formés en vue d'attaques par rançongiciels dont la durée de vie est plus courte, ce qui complexifie l'identification des acteurs de la menace.



Cibler les réseaux de cybercriminalité

L'opération Eastwood avait pour but le démantèlement du réseau cybercriminel NoName057(16). Cette opération interne menée conjointement avec Eurojust s'est déroulée du 14 au 17 juillet 2025.

Les individus agissant pour le compte de NoName057(16) sont principalement des sympathisants russophones qui se servent d'outils automatisés pour mener des attaques par déni de service distribué (DDoS). Opérant hors commandement officiel et sans compétences techniques sophistiquées, ils sont motivés par une idéologie et des récompenses.

Les autorités nationales ont contacté plusieurs centaines de personnes soupçonnées de soutenir ce réseau de cybercriminels. Les messages transmis au moyen d'une application de messagerie d'usage courant informent les destinataires des mesures officielles et soulignent la responsabilité pénale de ceux-ci en vertu de la législation nationale.

Jusqu'à présent, cette opération a permis de démanteler une infrastructure d'attaque composée de 100 systèmes informatiques à travers le monde, et de mettre hors ligne une bonne partie de l'infrastructure des serveurs centraux du groupe.

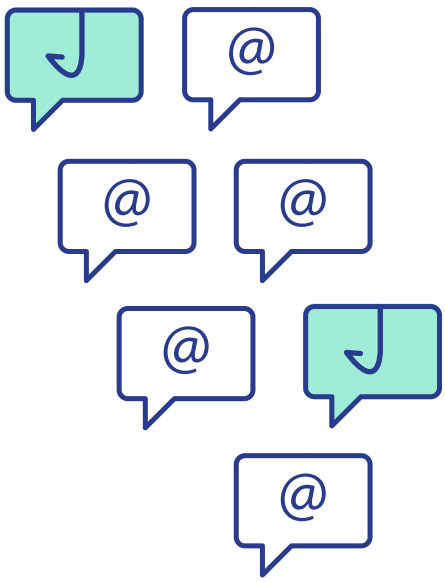
Nous vous invitons à consulter le rapport IOCTA complet ici

Les systèmes de fraude en ligne font partie des domaines de la criminalité organisée qui se développent le plus rapidement, ciblant un large éventail de victimes. L'ampleur de la fraude en ligne a atteint un niveau sans précédent et devrait continuer à croître, sous l'effet des avancées réalisées en matière d'automatisation et d'intelligence artificielle.

Principales tendances des systèmes de fraude en ligne:

- **Les systèmes de fraude en ligne** deviennent de plus en plus difficiles à détecter, car ils tendent à être tenaces, sur mesure et hautement sophistiqués.
- **Le vol de données à caractère personnel à partir des systèmes de paiement est particulièrement inquiétant.** Les données sont exploitées directement ou vendues à d'autres acteurs criminels, avec pour conséquence la victimisation répétée des sujets cibles.
- **Certains fraudeurs font montre d'un niveau élevé d'expertise.** et perfectionnent continuellement leurs techniques, les risques futurs s'aggravant à l'aune de la capacité d'adaptation des cybercriminels.

Le paysage de la menace que représente la fraude en ligne est caractérisé par des activités criminelles sophistiquées et méticuleusement organisées, qui ciblent non seulement les victimes, mais offrent également des services professionnels aux criminels. Les fraudeurs tirent parti des technologies avancées, des comportements humains et des vides juridiques.



Enquête sur les plateformes d'hameçonnage en tant que service

Europol a joué un rôle clé dans le démantèlement de LabHost, l'une des plus grandes plateformes mondiales d'hameçonnage en tant que service. Dans le cadre de cette opération de démantèlement, qui a duré un an, 70 perquisitions ont été effectuées à travers le monde entre le 14 et le 17 avril 2024, aboutissant à 37 arrestations.

Moyennant un abonnement mensuel, la plateforme LabHost proposait un service personnalisable allant des kits d'hameçonnage aux pages d'hébergement d'infrastructures. En fonction de leur abonnement, les criminels se voyaient proposer une gamme toujours plus fournie de cibles, dont des institutions financières, des services de livraison postale et des fournisseurs de services de télécommunications. L'abonnement comprenait également un outil de campagne appelé LabRat, qui permettait à des criminels inexpérimentés de surveiller et de contrôler les attaques en temps réel.

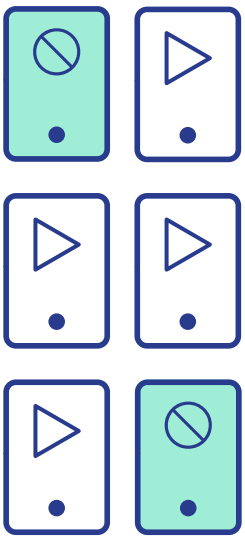
Jusqu'à présent, cette opération a permis de mettre au jour 40 000 domaines d'hameçonnage et plus de 10 000 utilisateurs dans le monde entier. Les données recueillies auprès de LabHost et de LabRat serviront aux opérations internationales en cours.

Écoutez notre épisode de podcast sur la manière dont la criminalité se développe en ligne

L'exploitation sexuelle des enfants en ligne renvoie à toute agression sexuelle commise sur une personne âgée de moins de 18 ans, ainsi qu'à la production et au partage en ligne d'images de telles agressions. Il s'agit d'un crime odieux et grave, car il consiste en des violences physiques et psychologiques perpétrées sur des enfants, qui ont un impact considérable sur leur santé et leur développement.

Principales tendances en matière d'exploitation sexuelle des enfants en ligne:

- **L'accélération numérique a déclenché une évolution rapide de l'exploitation sexuelle des enfants en ligne.** Elle a engendré l'apparition de plateformes cryptées de bout en bout, sans frontières, permettant aux auteurs d'infractions de créer, de stocker et d'échanger du matériel pédopornographique ainsi que de solliciter, de manipuler et de piéger des victimes.
- **L'accessibilité des outils d'intelligence artificielle a transformé l'exploitation sexuelle des enfants en ligne.** Ces outils peuvent être utilisés pour modifier le matériel existant ou créer de nouveaux contenus, par exemple en permettant aux adultes d'avoir l'air plus jeunes qu'ils ne sont sur des images explicites ou en transformant des images non explicites en images sur lesquelles les corps sont dénudés.
- **Divers groupes tirent parti des plateformes numériques.** Ces plateformes sont utilisées pour recruter à la fois des auteurs et des victimes d'infractions à l'échelle mondiale, pour normaliser des actes d'une extrême cruauté, pour extorquer de l'argent aux victimes, pour partager du matériel pédopornographique, voire radicaliser des individus et les pousser jusqu'à l'extrémisme violent.



Lutte contre l'exploitation sexuelle des enfants

L'opération Stream (également appelée «opération Kidflix») est l'une des plus importantes opérations de lutte contre l'exploitation sexuelle des enfants de l'histoire d'Europol. Lancée en 2022, l'enquête a abouti à deux semaines d'action, du 10 au 23 mars 2025.

Kidflix a été créée en 2021 et est rapidement devenue une plateforme populaire parmi les pédophiles. Selon les autorités, 91 000 vidéos uniques ont été téléchargées et partagées, soit une durée totale de 6 288 heures. Contrairement à d'autres plateformes de ce type, Kidflix permettait à ses utilisateurs de télécharger du matériel pédopornographique, mais également de diffuser des fichiers vidéo. Les paiements étaient réalisés en cryptomonnaies.

À ce jour, cette opération a permis d'identifier 1 393 suspects, d'arrêter 79 personnes, de saisir 3 000 appareils électroniques et de protéger 39 enfants.

Pour en savoir plus sur les cyberattaques, les systèmes de fraude en ligne et l'exploitation sexuelle des enfants en ligne, nous vous invitons à consulter le rapport SOCTA UE ici

Évolution de la cybercriminalité: exploitation des données

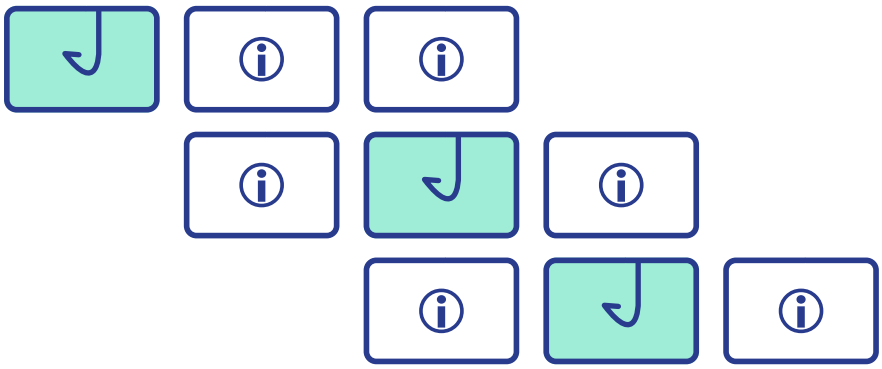
Au cours des 12 derniers mois, Europol a continué d'enquêter sur l'évolution des menaces et des tendances en matière de cybercriminalité. Il en ressort avant tout que la manipulation et l'usage impropre de données constituent le moteur de l'écosystème criminel, allant de la fraude en ligne aux attaques par rançongiciels, en passant par l'exploitation sexuelle des enfants. Ce constat était le thème principal de l'édition 2025 de l'évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA), **«Voler, vendre, recommencer: comment les cybercriminels commercialisent et exploitent vos données».**

« On ne peut pas défendre ce qu'on ne comprend pas. Le rapport IOCTA 2025 d'Europol met en lumière l'économie cachée des données volées qui alimente les cybermenaces actuelles les plus dangereuses et fournit les informations nécessaires aux forces de l'ordre, aux décideurs politiques et à l'industrie pour agir avec détermination.»

Edvardas Šileris, chef du Centre européen de lutte contre la cybercriminalité d'Europol.

Les conclusions de cette année mettent en évidence les principales tendances suivantes, qui illustrent la manière dont les cybercriminels adaptent leurs méthodes et étendent leurs activités:

- **Les données compromises sont très précieuses pour un vaste éventail d'acteurs criminels,** qui les exploitent comme une marchandise à part entière, mais également comme un bien à acquérir à d'autres fins, y compris d'autres activités criminelles.
- **Les cybercriminels utilisent diverses techniques pour accéder aux données à caractère personnel et les subtiliser,** en exploitant à la fois les vulnérabilités des systèmes et les négligences humaines. L'ingénierie sociale se distingue comme une technique particulièrement répandue.
- **Les grands modèles de langage (GML) et d'autres formes d'intelligence artificielle générative améliorent l'efficacité des techniques d'ingénierie sociale,** en adaptant la communication aux victimes et en automatisant les processus criminels.
- **Une partie florissante de l'écosystème criminel s'articule autour de la vente d'accès à des systèmes et comptes compromis.** Les courtiers en accès initial font de plus en plus de publicité pour ces services, ainsi que pour les matières premières qui y sont liées, sur des plateformes criminelles spécialisées utilisées par un ensemble très divers de cybercriminels.
- **Les courtiers en données font connaître leur activité sur plusieurs plateformes afin de diversifier leurs opérations et d'accroître leur résilience face aux opérations répressives.** Les applications de communication chiffrées de bout en bout (E2EE) sont de plus en plus utilisées pour négocier, faire la promotion, et effectuer des transactions commerciales concernant des données piratées, ainsi que pour partager les données à caractère personnel des victimes ciblées, notamment des enfants.



Focus sur les moyens utilisés pour récolter des données

Les cybercriminels utilisent diverses techniques qui exploitent soit les vulnérabilités des systèmes, soit les négligences humaines pour accéder à des données à caractère personnel et les voler. Le recours à des techniques d'ingénierie sociale est de plus en plus courant dans le cadre de l'acquisition de données. En voici quelques exemples:

Hameçonnage

Type d'attaque qui consiste à infecter les comptes et systèmes des victimes au moyen de maliciels ou à les persuader de saisir leurs identifiants sur des sites web frauduleux créés à l'aide de kits d'hameçonnage.

Logiciels malveillants voleurs d'informations

Catégorie de maliciels spécifiquement conçue pour extraire de manière illicite des informations sensibles de dispositifs compromis, en collectant des identifiants de connexion, des jetons d'application et des cookies de session. Les criminels utilisent des courriels, des SMS ou des messages publiés sur les réseaux sociaux, qui contiennent des pièces jointes ou des URL malveillantes pour introduire des maliciels dans le système de la victime.

Hameçonnage vocal

Des appels téléphoniques frauduleux incitent les victimes à fournir des informations sensibles, ce que rendent possible les services d'usurpation d'identité[1], qui permettent aux criminels de se faire passer pour des entreprises locales et de bonne réputation.

Freiner les réseaux zombies

Figurant parmi les plus vastes opérations de ce type jamais menées, Endgame fait partie d'un ensemble d'opérations dont le but est de perturber les activités des réseaux zombies. Lancée en mai 2024, elle est toujours en cours.

Les réseaux zombies sont des réseaux de dispositifs infectés par des maliciels, ce qui permet aux pirates informatiques de les contrôler à distance, à l'insu de leurs propriétaires. Ces infections par maliciels commencent généralement par l'utilisation de programmes seringues (droppers), un type de programme informatique intrusif conçu pour installer des maliciels supplémentaires sur un système ciblé.

Europol et la force d'action anticybercriminalité européenne (J-CAT) ont continué de soutenir les enquêtes en facilitant l'échange d'informations entre les autorités concernées et en apportant un renfort analytique et criminalistique aux enquêteurs.

La dernière opération Endgame en date a été menée entre le 19 et le 22 mai 2025. Au cours de cette période, les autorités ont fermé quelque 300 serveurs partout dans le monde, neutralisé 650 domaines et délivré des mandats d'arrêt internationaux contre 20 personnes, portant un coup direct à la chaîne d'attaques par rançongiciels.

1. Service permettant aux utilisateurs de passer des appels téléphoniques à partir de numéros de téléphone fictifs ou qui changent constamment, ou d'envoyer des courriels qui semblent provenir d'une source fiable.

www.europol.europa.eu