MINISTÈRE
DE L'INTÉRIEUR
*Liberté
Égalité
Fraternité*

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

La MInute Cyber 02

LES CRYPTOACTIFS AU SERVICE DE LA CRIMINALITÉ

Les cryptoactifs, comme le Bitcoin et l'Ethereum, séduisent de plus en plus d'utilisateurs en France : en 2024, 6,5 millions de Français en possédaient (soit 12% de la population), plaçant la France au troisième rang en Europe et au douzième rang mondial en matière de flux de cryptoactifs. Bien qu'ils soient majoritairement utilisés de manière légale, ces actifs attirent également des criminels. Environ 40 milliards de dollars de transactions en cryptoactifs chaque année seraient liés à des activités illégales, comme le blanchiment d'argent, le financement de cyberattaques ou divers trafics.

Les cryptoactifs sont devenus un levier majeur pour les cybercriminels, leur offrant des moyens de financement anonymes et rapides.

Certains groupes criminels utilisent, en effet, les cryptoactifs pour financer des cyberattaques, payer des infrastructures illégales ou financer des attaques par déni de service *(DDoS)*.

Ils peuvent aussi user de rançongiciels *(ransomware)*, les victimes de cyberattaque devant souvent payer une rançon en cryptoactifs pour récupérer leurs données.

Par ailleurs, effectuer des transactions sur les forums clandestins peut être un moyen retenu des criminels, puisque l'achat et la vente de données volées, logiciels malveillants, armes ou faux documents s'effectuent souvent via des paiements en cryptoactifs.

Ces transactions bénéficient d'un certain anonymat, bien que des progrès aient été réalisés dans le traçage de flux financiers sur la *blockchain*.

L'usage des cryptoactifs dépasse le cadre du « cybercrime » et touche également la criminalité organisée dite « classique », notamment dans les domaines du narcotrafic et de l'extorsion.

En matière de narcotrafic, sur le *dark web*, la vente de drogues s'est largement développée grâce aux cryptoactifs, qui permettent d'éviter les circuits bancaires classiques et de blanchir l'argent plus facilement. S'agissant d'extorsions et kidnappings, certains criminels ciblent les détenteurs de cryptoactifs, les localisent et les forcent à transférer leurs fonds sous la menace. Un dirigeant d'une société spécialisée en sécurité des cryptoactifs en a récemment été victime.

Toutefois, les forces de l'ordre s'adaptent : plusieurs plateformes clandestines ont été démantelées et de nouveaux outils permettent d'identifier certaines transactions suspectes.

Si les cryptoactifs offrent des opportunités aux criminels, ils comportent aussi des risques pour eux.

S'agissant des avantages, citons la rapidité et l'absence d'intermédiaire. En effet, les transactions sont quasi instantanées et échappent aux banques. Relevons aussi la difficulté de traçabilité : bien que la *blockchain* soit transparente, l'identification des auteurs reste un défi.

Concernant les risques encourus, notons la surveillance accrue des forces de l'ordre, qui utilisent désormais des outils avancés pour retracer certaines transactions, de même que la volatilité des actifs. En effet, contrairement aux monnaies classiques, les cryptoactifs peuvent perdre rapidement de la valeur, rendant leur détention risquée.

Face aux dérives, les régulateurs mettent en place de nouvelles règles. En Europe, le règlement MiCA *(Markets in Crypto-Assets)* vise à renforcer la surveillance des flux financiers et à lutter contre le blanchiment d'argent.

Les forces de l'ordre, notamment en France, collaborent avec des experts en analyse *blockchain* pour identifier les transactions criminelles et démanteler les réseaux utilisant ces technologies.

En conséquence, les cryptoactifs sont légaux, mais leur rapidité, leur accessibilité et leur anonymat en font un outil attractif pour pratiquer certaines activités illégales. Cyberattaques, trafics et extorsions exploitant ces monnaies numériques, posent un défi majeur en matière de lutte contre la criminalité organisée.

Face à ces risques, les détenteurs de cryptoactifs doivent sécuriser leurs fonds et éviter d'exposer leurs investissements en ligne. De leur côté, les régulateurs doivent renforcer la surveillance pour limiter leur détournement à des fins criminelles.

LE CNF-CYBER EN FORMATION

L'engouement pour les cryptoactifs a, pour corollaire, une augmentation du nombre d'enquêtes judiciaires avec une composante « cryptoactifs ». Le COMCYBER-MI s'engage résolument dans le transfert des compétences en la matière, au travers de son centre national de formation, le CNF-Cyber.

Afin de pouvoir accompagner les enquêteurs dans l'acquisition des compétences techniques et procédurales afférentes à ce type d'affaires, plusieurs nouvelles formations sont proposées depuis la création du COMCYBER-MI le 1er décembre 2023 : le Fintech 1 et le Fintech 2. La vocation du stage Fintech 1 est de mettre les enquêteurs en capacité de détecter l'usage de cryptoactifs et d'en réaliser la saisie le cas échéant. Le stage Fintech 2 est quant à lui d'un niveau plus avancé et consiste à mettre en exergue des mécanismes complexes de blanchiment à partir de l'analyse des « *blockchains* ».

Afin d'accélérer la diffusion des compétences associées au Fintech 1, une formation de formateurs relais territoriaux est lancée par le CNF-Cyber à partir de mars 2025. Cette formation s'adresse à des praticiens éprouvés, permet de former aux bonnes pratiques pédagogiques et de s'approprier la mallette pédagogique (cours et environnements d'exercice). La première session nationale de cette formation connaît un fort succès et verra ainsi la création de 12 premiers formateurs relais. Une seconde session de formation sera à nouveau mise en place au mois de mai (S21).

Reconnu pour la qualité de son approche des enjeux judiciaires relatifs aux cryptoactifs, le CNF-Cyber œuvre également à la déclinaison de cette formation au niveau européen afin d'harmoniser les pratiques policières en la matière.

ENGAGEMENT DU COMCYBER-MI DANS LE PROJET CYBER4TOMORROW

Le 18 décembre dernier, à travers la signature de la charte C4T, le COMCYBER-MI s'est engagé dans une dynamique collective visant à construire un numérique plus sûr, plus attractif et plus durable. L'initiative C4T repose sur un catalogue d'actions concrètes, conçues par et pour les professionnels de la cybersécurité, favorisant le passage à l'action grâce à des ressources accessibles.

Trois piliers sont identifiés :

- CyberCitizenship : sensibiliser les organisations et les individus aux bonnes pratiques d'hygiène numérique afin de rendre le numérique sûr et accessible à tous.
- CyberSpecialists : encourager la diversité des profils et des compétences dans le secteur de la cybersécurité, en renforçant l'attractivité des métiers et l'accès à la formation.
- CyberSustainability : promouvoir des pratiques durables pour réduire l'impact environnemental de la cybersécurité, notamment en élaborant une méthodologie pour mesurer et limiter les émissions de gaz à effet de serre (GES) dans ce domaine.

Le COMCYBER-MI contribue à cette initiative en mettant à disposition ses ressources telles que le rapport annuel sur la cybercriminalité (RACY) et le MOOC Sensy-crise. De plus, il participe à l'élaboration de fiches actions, dont certaines sont déjà disponibles sur la plateforme cyber4tomorrow.

www.cyber4tomorrow.fr

Pour aller + loin...

Vulnérabilités du cloud

Face à la démocratisation des solutions *cloud*, qui s'accompagne de nouvelles problématiques en matière de sécurité, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a publié le 19 février dernier son état de la menace sur le *cloud computing*.

Les environnements *cloud* sont de plus en plus la cible d'attaquants. Cela s'explique notamment par l'intérêt pour les données traitées par les fournisseurs de service *cloud*, mais également parce qu'ils offrent, potentiellement, un moyen d'accès aux organisations qui utilisent ces services. Les attaquants, qui ont développé des compétences bien spécifiques, poursuivent des finalités lucratives, d'espionnage, et ou de déstabilisation. Les vulnérabilités dans des équipements de bordure (tels que des VPN), les mauvaises configurations et les défauts de sécurisation sont particulièrement ciblés. Les acteurs malveillants utilisent également des services *cloud* à des fins malveillantes, dans le but de stocker des codes malveillants ou des données volées sur des plateformes grand public. Il devient alors très complexe de détecter les activités malveillantes en les dissimulant au sein du trafic légitime des utilisateurs de ces plateformes.

Pour l'ANSSI, l'utilisation du *cloud* pose donc de nouveaux défis en matière de sécurité informatique, et interroge sur les responsabilités incombant tant aux fournisseurs de services qu'aux utilisateurs de ces plateformes. Pour accompagner ce public, l'ANSSI met à disposition une série de recommandations qui précisent les types d'offres *cloud* à privilégier. En parallèle, l'Agence recommande de privilégier des offres cloisonnées entre clients de type *SecNumCloud* pour des activités sensibles. Enfin, le recours au *cloud* impose la prise en compte de l'évolution des capacités de supervision afin de se prémunir contre les menaces abordées dans le document.

Publication mensuelle éditée par :
Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 02 - FÉVRIER 2025
Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : LCL S. LAMBERT - LCL G. DECKMYN - CEN D. MALET - CNE F. SAVARY
Conception graphique et maquettage : Mme M. BARREAU

En attendant le prochain numéro de La MInute cyber, suivez notre actualité :

sur LinkedIn et sur X (ex-Twitter) : ***@ComCyberMI***