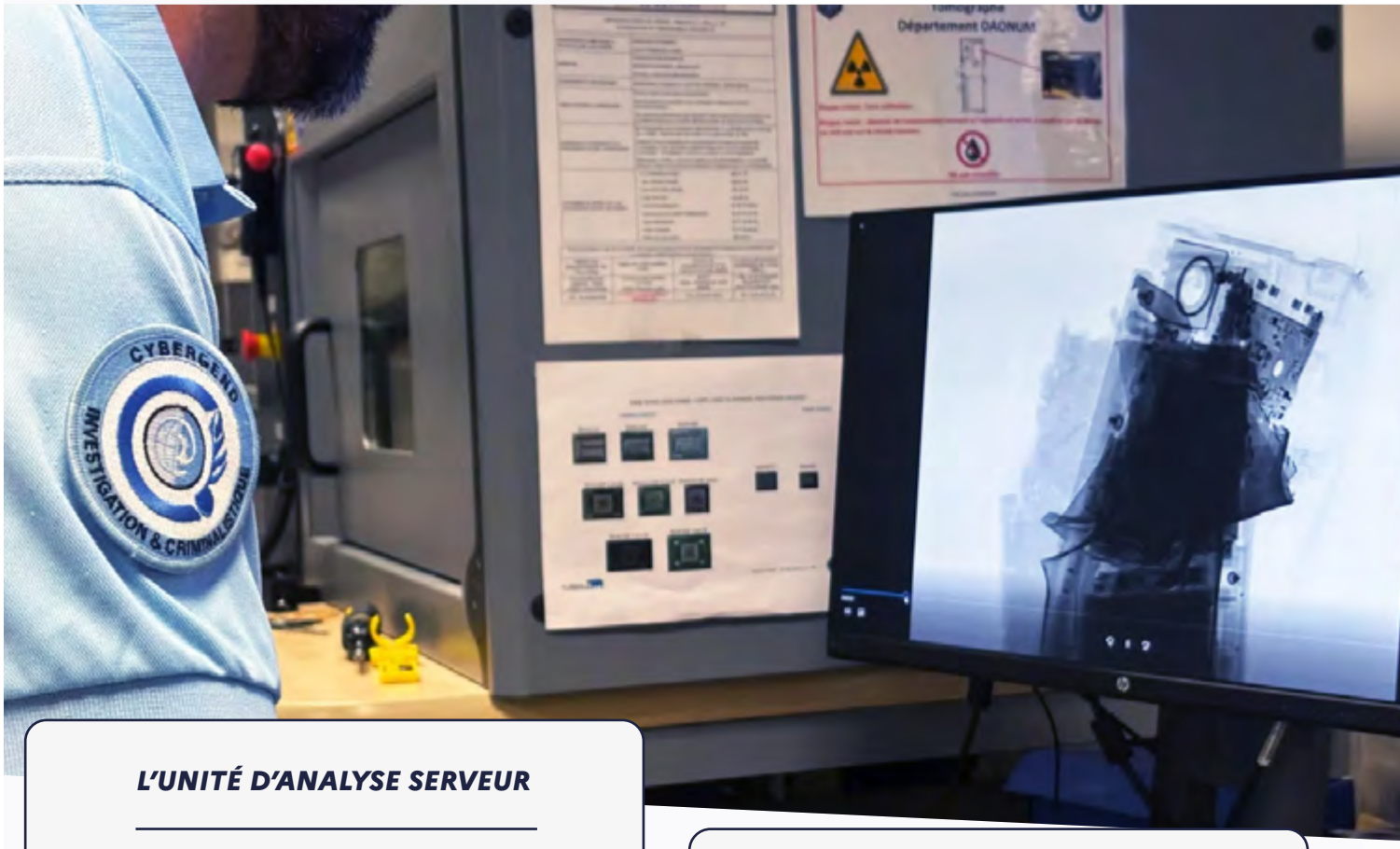
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

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

La MInute Cyber 6



L'UNITÉ D'ANALYSE SERVEUR

Au cœur des enquêtes judiciaires en cybersécurité, le Centre National d'Expertise Numérique (CNENUM) est composé d'experts en analyse de serveurs, qui jouent un rôle clé dans la lutte contre les cyberattaques. Face à des attaques de plus en plus sophistiquées, à l'image des attaques par rançongiciels, l'unité intervient pour préserver les preuves numériques, analyser les systèmes compromis et participer à l'identification des attaquants.

Outre cette typologie d'attaque, leurs missions incluent de plus l'identification et l'analyse des serveurs de commande et de contrôle (C2), utilisés par les cybercriminels pour coordonner les attaques. En examinant les communications réseau et les traces numériques, l'unité reconstitue les chronologies des incidents de sécurité tout en caractérisant la méthodologie employée par les attaquants. Contribuant à la manifestation de la vérité dans un cadre judiciaire, cette approche analytique permet également de prévenir de futures attaques et d'aider les victimes à traiter les incidents de cybersécurité.

En parallèle, l'unité effectue des récupérations de données perdues ou supprimées, reconstituant des bases de données endommagées et fournissant des éléments cruciaux pour les enquêtes. Elle cartographie également les réseaux compromis pour visualiser les mouvements des attaquants et analyser les malwares en profondeur, anticipant ainsi les menaces futures.

L'unité est également engagée dans des processus de formation et collabore avec d'autres unités de la Gendarmerie nationale ou des organismes externes, académiques comme professionnels, pour renforcer la réponse globale aux incidents de cybersécurité. D'autre part, leur travail de veille technologique et leur participation à des exercices de simulation garantissent une haute capacité opérationnelle.

En résumé, cette unité composée d'experts en analyse de serveurs se distingue par son expertise technique et sa capacité à traiter et prévenir les incidents de cybersécurité, contribuant de manière significative à la résilience des systèmes d'information tout en assurant la mise à disposition d'éléments de preuve numérique aux autorités judiciaires.

NOMINATION DE MONSIEUR JÉRÔME MARILLY

Depuis le 1er Juin 2024, Monsieur Jérôme Marilly est nommé adjoint du GDI Husson, chef du COMCYBER-MI.

Titulaire d'un Diplôme d'études approfondies en droit privé délivré par l'université de Lille, M. Marilly a été admis au premier concours d'entrée à l'École Nationale de la Magistrature en décembre 1994. Après une année de service militaire, il a intégré l'ENM en février 1996, puis a été nommé en premier poste en qualité de substitut placé auprès du procureur général près la cour d'appel de Douai en septembre 1998.

M. Marilly a par la suite exercé les fonctions de substitut du procureur de la République à Douai (2000), vice-procureur à Valenciennes (2006), procureur de la République à Cambrai (2011), ou encore chef de la section des affaires économiques, financières et commerciales dite F2 (2017) et chef de la section JUNALCO/JIRS en charge de la lutte contre la délinquance économique et financière dite J2 au tribunal judiciaire de Paris. En septembre 2020, il a été nommé avocat général près la cour d'appel de Paris, notamment en charge à compter de mars 2022 du département de la lutte contre la criminalité organisée (affaires JUNALCO/JIRS) et la cybercriminalité.

LA CYBERVICTIMISATION

Le Service Statistique Ministériel de la Sécurité Intérieure (SSMSI) conduit chaque année, auprès de la population française, une enquête statistique nationale dénommée « Vécu et Ressenti en matière de Sécurité » (VRS). Elle a pour objectif principal de mesurer l'insécurité ressentie et les préoccupations des citoyens en matière de sécurité, ainsi que d'obtenir leurs opinions au regard de l'action des forces de sécurité intérieure.

Le 5 avril 2024, sur proposition du Commandement du ministère de l'Intérieur dans le cyberespace (ComCyberMi) et en collaboration avec le SSMSI, le thème de la cybervictimisation a été, pour la première fois, retenu pour permettre l'étude de la victimologie relative aux faits de cybercriminalité. Cette enquête, qui sera rendue publique en début d'année 2027, aura pour effet de mieux informer les Français, ainsi que d'apprécier les adaptations à prendre en compte dans la stratégie de prévention des forces de l'ordre pour mieux sensibiliser face aux cybermenaces.

Pour aller + loin...

Médiatisation de l'UNCyber

Durant le mois écoulé, plusieurs médias ont mis en lumière la forte activité de l'Unité Nationale Cyber de la Gendarmerie nationale (UNCyber), dans le cadre d'affaires ou d'actions d'ampleur.

TF1 ou encore le Parisien sont tout d'abord revenus sur les missions des 200 «cyberpatrouilleurs» de l'UNCyber, chargés de surveiller les réseaux sociaux, les moteurs de recherche et les créations de noms de domaine, et pleinement mobilisés pour accompagner et protéger les futurs spectateurs des JOP Paris 2024. Face à la «montée des alertes» à l'approche des épreuves, les médias ont mis en avant la «vigilance accrue» de ces cybergendarmes, affectés dans une cellule spécialisée collaborant avec Europol et le Comité d'organisation des Jeux Olympiques et Paralympiques Paris 2024 (COJOP 2024) depuis mars 2023. Commandée par le capitaine Etienne Lestrelin, ladite cellule est à l'origine du recensement de 338 sites frauduleux de vente illicite de billets, «entièrement virtuels», de 51 fermetures et 140 mises en demeure.

De très nombreux médias, dont TF1, ont également relayé la fermeture du site coco, le 25 juin dernier, dans le cadre d'une enquête judiciaire menée sous la direction de la JUNALCO du parquet de Paris, par l'UNCyber et l'Office National Anti-Fraude (ONAF), avec l'appui du commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI), en France, en Bulgarie, en Allemagne, en Lituanie, aux Pays-Bas et en Hongrie.

Les opérations ont été coordonnées avec Eurojust.
Le site coco.gg est connu depuis de nombreuses années comme étant un facilitateur de commission de diverses infractions, notamment des actes de pédocriminalité, de proxénétisme, de prostitution, de viols, de vente de stupéfiants, de guet-apens, voire d'homicides. Entre le 1er janvier 2021 et le 7 mai 2024, il ressort de l'exploitation des fichiers de police que pas moins de 23 051 procédures judiciaires en lien avec la plateforme coco ont été ouvertes.

Coopération nationale et internationale

Le 7 Juin 2024, l'Unité Nationale Cyber (UNCyber) a reçu à Pontoise une délégation technique du Security Operations Center (SOC) de la société Orange, dont les analystes, experts et consultants sont chargés de l'anticipation et du traitement des menaces en cybersécurité.

Durant cette journée, la Division des Opérations (DO/C3N) et la Division Technique (DT) ont présenté leur activité et les grandes opérations judiciaires ayant marqué l'UNCyber et le C3N.

Aussi, la capacité de développement d'outils d'investigation agiles et opérationnels a été mise en avant ; le Département d'Appui Technique à l'Enquête (DATE) a notamment présenté plusieurs outils d'investigation sur Internet, de criminalistique numérique et d'analyse des archives numériques.

Ces échanges se poursuivront après la période des Jeux Olympiques Paris 2024, et aboutira sur un parrainage dans le cadre de la montée en puissance des activités de l'UNCyber.

Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 06 - JUIN 2024

Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : M. J. MARILLY - LCL E. MERCIER - LCL F. RUBENS - CEN D. MALET
Conception graphique et maquettage : Mme M. BARREAU

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

*sur **www.gendarmerie.interieur.gouv.fr***

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