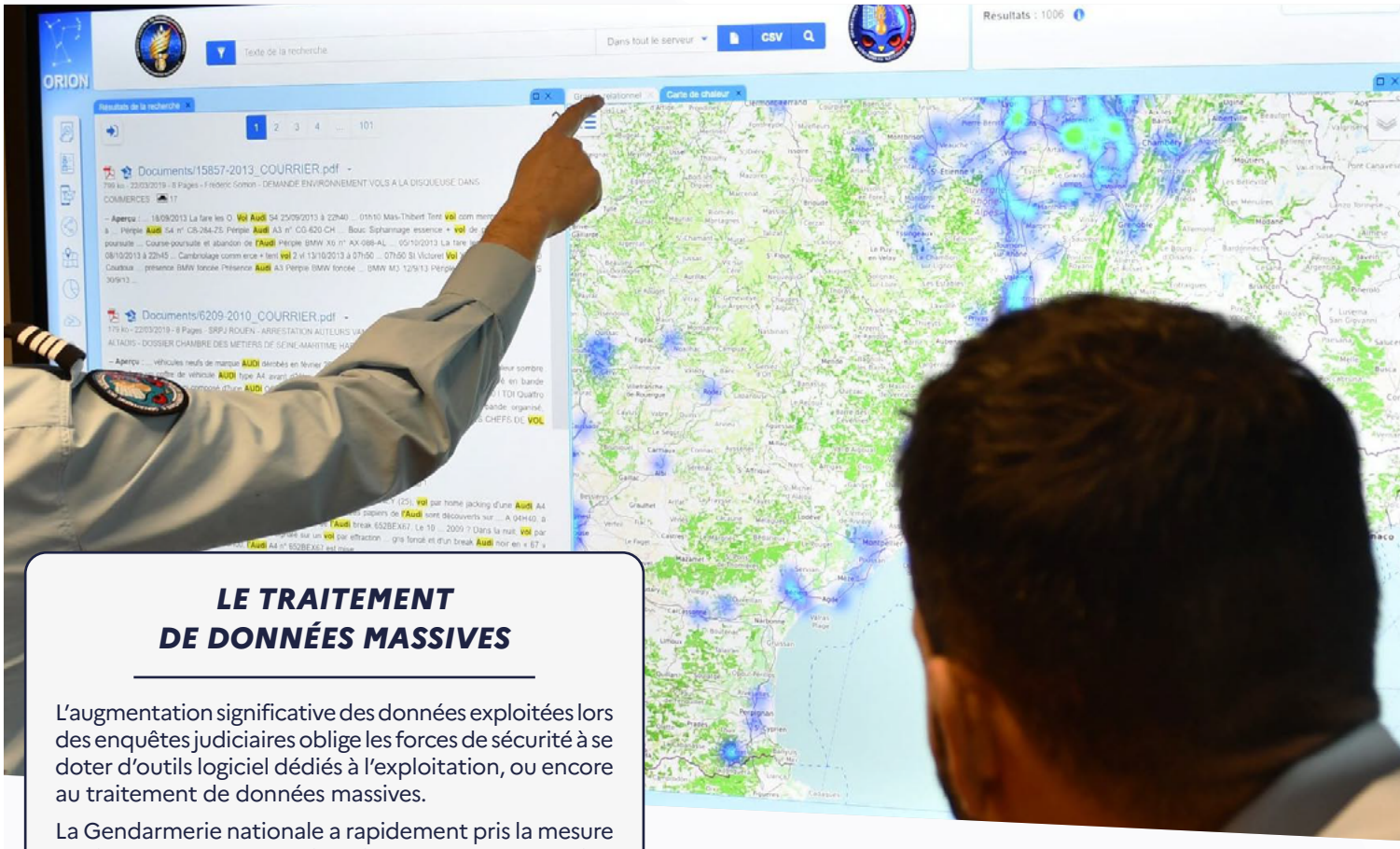
MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

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

La MInute Cyber 5



LE TRAITEMENT DE DONNÉES MASSIVES

L'augmentation significative des données exploitées lors des enquêtes judiciaires oblige les forces de sécurité à se doter d'outils logiciel dédiés à l'exploitation, ou encore au traitement de données massives.

La Gendarmerie nationale a rapidement pris la mesure de l'importance de cet enjeu, *via* notamment la création d'unités dédiées et l'allocation de moyens humains et techniques, pour utiliser les avantages du traitement de données à des fins judiciaires. Le but est de poursuivre l'amélioration du service rendu à la population tout en respectant les différents cadres juridiques en vigueur.

Ainsi, dès sa création, le COMCYBER-MI s'est doté d'un centre des sciences de la donnée (CSD), département hérité du Service Central de Renseignement Criminel de la Gendarmerie nationale (SCRCGN), ayant pour mission de développer des solutions technologiques afin d'offrir aux unités opérationnelles de la Gendarmerie nationale ou de la Police nationale la possibilité de traiter des masses importantes de données à des fins judiciaires.

Il développe ainsi, entièrement en interne et sans appel à des prestataires extérieurs, des logiciels *ad hoc*.

Pour réaliser ces missions, le COMCYBER-MI s'est enrichi de personnels qualifiés dans ce domaine : des ingénieurs, des développeurs et des datascientists afin d'exploiter de la manière la plus efficiente possible l'ensemble des données collectées.

Les logiciels développés proposent des fonctionnalités permettant l'affichage de statistiques, de cartes de chaleur ou cartes de punaises permettant de mettre en avant des phénomènes criminels, voire l'affichage de graphes relationnels d'entités communes (individus, téléphones, immatriculations, etc.) provenant de différents documents.

Les deux cadres juridiques les plus employés dans le traitement des données sont :

- les « logiciels de rapprochements judiciaires[1] », qui permettent l'exploitation et le rapprochement d'informations sur les modes opératoires réunis au cours d'une même enquête judiciaire ;
- les « bases d'analyse sérielle[2] » qui permettent de rassembler les preuves et d'identifier les auteurs des crimes et délits présentant un caractère sériel, grâce à l'établissement de liens entre les individus, les évènements ou les infractions.

1. *Décret du 7/05/2012 n°2012-687 relatif à la mise en œuvre de logiciels de rapprochements judiciaires.*
2. *Décret du 22/11/2013 n°2013-1054 autorisant les bases d'analyse sérielle.*

WORKSHOP CRYPTO 2024

Du 20 au 24 mai 2024, le Centre National de Formation Cyber (CNF-Cyber) a accueilli la 3ème édition du *workshop crypto* 2024, stage international dédié à l'investigation sur les crypto-actifs.

Co-financé et co-animé par Europol, l'Unité Nationale Cyber de la Gendarmerie nationale et le COMCYBER-MI, l'événement a réuni 32 experts de 25 nationalités, parmi lesquels figurent des représentants des états membres d'Europol, mais également d'états tiers (Canada, USA, etc.) qui coopérent régulièrement avec la France d'un point de vue opérationnel.

Combinant cours magistraux, exercices de manipulation et de traçage des crypto-actifs et cas pratiques, le *workshop crypto* assume un haut niveau de technicité en la matière, dans un domaine extrêmement spécifique et en constante évolution, et pour lequel le besoin en compétences ne cesse de croître. Les échanges directs entre les participants ont également permis de renforcer les liens entre les nombreuses forces de police présentes.

En visite au sein du CNF-Cyber, le Général de division Christophe HUSSON, chef du COMCYBER-MI, s'est adressé aux apprenants et a ainsi pu apprécier les apports techniques et humains de cet événement.

Priorité gouvernementale, l'expertise nationale judiciaire en crypto-actifs est l'un des domaines portés par le COMCYBER-MI au profit des forces de sécurité intérieure.

Pour aller + loin...

Division de la proximité numérique (UNCyber)

L'escroquerie, stratagème frauduleux élaboré par une personne au préjudice d'une autre, est probablement aussi vieille que l'humanité elle-même. Une faille humaine est toujours exploitée, pour tromper et délester une victime (le plus souvent de son argent ou d'un bien). L'ère numérique a permis d'agrandir le « terrain de chasse » des escrocs qui, désormais, ont le monde entier à portée de « clics ». Les escroqueries sur Internet constituent d'ailleurs près de 80% du contentieux judiciaire cyber de notre pays. Leur conception est simple (souvent un simple texte), leur diffusion rapide (mails, *SMS*, réseaux sociaux) et leur coût quasi nul, rendant cette activité peu risquée physiquement et extrêmement lucrative.

COMPRENDRE ET AGIR :

La mécanique mise en place reposant sur l'humain, elle nécessite de mettre en œuvre des émotions pour faciliter la manœuvre frauduleuse. Quatre grandes familles d'émotions sont utilisées :

- **L'amitié, l'amour et la proximité ;**
- **Les injonctions ou promesses d'une figure d'autorité *(police, gendarmerie, impôts, banquier, tribunal judiciaire, etc.)* ;**
- **Les menaces, le risque imminent, la peur, l'urgence à agir ;**
- **L'appât du gain, la bonne affaire ou la bonne fortune.**

La finalité est dès lors d'amener la victime à remettre volontairement les fonds, pensant ainsi solder un sujet d'une apparente urgence.

Si un portrait robot des escroqueries les plus vivaces sur internet devait être brossé, nous pourrions alors retenir :

- L'exploitation d'un état émotionnel ;
- L'instillation d'un temps d'exécution court voire d'une urgence ;
- La propagation via des vecteurs de distribution de masse : mails, *SMS*, réseaux sociaux, etc. ;
- L'injonction d'utiliser des moyens de paiement présumés difficilement traçables : crypto-monnaies, coupons PCS, transcash, Neo surf, etc.

NOS CONSEILS :

- Mettre en place un protocole immuable sur lequel l'état émotionnel n'a aucun impact ;
- Se départir du sentiment d'urgence qui n'est pas la réalité ;
- Ne jamais payer quoi que ce soit hors les canaux sécurisés connus.

Division des opérations DO / C3N (UNCyber)

Quatre personnes ont été arrêtées et plus de 100 serveurs mis hors ligne lors de « la plus grande opération jamais réalisée » contre des logiciels malveillants jouant un rôle majeur dans le déploiement de rançongiciels, a annoncé Europol.

Cette opération judiciaire, baptisée « Endgame » et coordonnée côté français par l'Office anti-cybercriminalité de la police judiciaire (Ofac), a donné lieu entre les 27 et 29 mai derniers à près d'une vingtaine de perquisitions en Arménie, Ukraine, ainsi qu'au Portugal et aux Pays-Bas.

Plus de 100 serveurs ont été saisis dans différents pays européens, aux États-Unis et au Canada.

Ce sont principalement des entreprises, autorités et institutions nationales qui ont été victimes des « systèmes malveillants » démantelés, selon l'agence judiciaire européenne Eurojust. « Des millions de particuliers ont également été victimes parce que leurs systèmes ont été infectés, ce qui les a intégrés » à ces logiciels malveillants, a précisé quant à elle la police néerlandaise dans un communiqué.

Dans un premier temps, les autorités ont visé les groupements à l'origine des six familles de logiciels malveillants : IcedID, SystemBC, Bumblebee, Smokeloader, Pikabot et Trickbot. Ces « droppers » sont associés à au moins 15 groupements de rançongiciels, ont précisé dans un communiqué conjoint l'Office fédéral de police criminelle allemand et le parquet de Francfort.

Côté français, les enquêteurs ont identifié l'administrateur de « SystemBC », cartographié les infrastructures liées au « dropper », et coordonné le démantèlement de dizaines de serveurs de contrôle, a indiqué la procureure de la République de Paris, Laure Beccuau. Les enquêteurs du C3N ont, pour leur part, identifié l'un des acteurs principaux du dropper « Bumblebee ». Deux gendarmes sont ainsi partis en Arménie appuyer la police locale lors de son audition et de la perquisition, qui a permis la saisie de matériel informatique.

Cette opération se poursuit et d'autres arrestations sont attendues, a précisé Europol.

Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 005 - Mai 2024

Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : LCL F. RUBENS - LCL J-E. LECOMTE - CEN J. TABARIES - CEN D. BOGE
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***