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

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

La MInute Cyber 3

FOCUS SUR OVERCLOCK

Le projet OVERCLOCK, co-financé à hauteur de 4 millions d'euros par le Fond pour la sécurité intérieure de la Commission Européenne, est piloté par le Commandement du ministère de l'Intérieur dans le cyberespace (COMCYBER-MI). Il rassemble les forces de l'ordre allemandes (BKA et ZITiS), néerlandaises (NFI) et norvégiennes (NCIS) ainsi qu'une entreprise française privée partenaire SYNACKTIV. Financé pour une durée de 3 ans (2021-2024), OVERCLOCK a pour objectif de capitaliser sur les efforts des laboratoires forensiques des forces de l'ordre européennes, afin de maintenir leur capacité à répondre aux réquisitions judiciaires.

Afin de réaliser cet objectif, OVERCLOCK recense et centralise les fiches générées par le projet sur l'innovation Lab d'Europol, ouvert à toute les forces de l'ordre européennes. Cette action dite de « dissémination » favorise les échanges d'outils et d'analyses permettant de monter des collaborations internationales et des opérations judiciaires. La plateforme comprend aujourd'hui plus de 50 fiches sur des téléphones ou applications et rassemble 70 membres de 18 pays.

QU'EST-CE QUE LA RETRO-CONCEPTION ?

La rétro-conception ou « reverse engineering » en anglais, émerge comme une compétence essentielle pour les enquêteurs forensiques. Comme son nom l'indique, il s'agit d'une étape inverse de la conception : la rétro-conception a pour principal but de « déconstruire » des logiciels et des systèmes afin d'en comprendre le fonctionnement pour retrouver des preuves cruciales sur différents supports numériques.

Dans le cadre de procédures judiciaires encadrées, la rétro-conception est utilisée pour atteindre la donnée provenant de dispositifs saisis impliqués dans des crimes. Aujourd'hui, la protection des communications est devenue une priorité avec une généralisation de l'emploi du chiffrement. Cependant, dans un contexte où les réseaux criminels se professionnalisent, les systèmes de sécurité additionnels qu'ils déploient ajoutent une couche de complexité supplémentaire.

Réussir à déchiffrer la donnée nécessite souvent des mois de travaux de recherche approfondie. Ce métier requiert une compétence rare, car il n'existe pas de formation structurée ou de diplôme à ce sujet. Ce sont des experts qui acquièrent leur expertise avec l'expérience, en s'auto-formant et en explorant de manière autodidacte les intrications complexes de la rétro-conception dans le contexte forensique.

Le COMCYBER-MI, au sein du Centre national d'expertise numérique (Cnenum) de la Division des enquêtes spécialisées, de la donnée et des investigations techniques (DEDT), dispose d'un Laboratoire de la rétro-conception. Il est composé de personnels civils et militaires basés à Pontoise (95), dont les profils vont du technicien au docteur en informatique en passant par l'enquêteur spécialisé en technologie numérique (NTECH).

FOCUS SUR LE « DDOS »

Le déni de service distribué ou *DDoS* (*Distributed Denial of Service*) est un type d'attaque informatique visant à saturer le réseau d'un service ou d'une machine. Pour cela, l'attaquant utilise un groupe d'ordinateurs corrompus (*botnet*) ou un serveur dédié (*stresser*) pour envoyer une multitude de requêtes sur le site internet ou le service en ligne ciblé. De la même façon qu'une foule envahirait un magasin, empêchant les clients légitimes d'entrer, le service ou la machine cible ne peut plus répondre à ce trafic fictif massif. Cela peut provoquer des temps d'attente interminables voire des indisponibilités totales (*crash*).

Une des plus grosses attaques *DDoS* a eu lieu en 2020, lorsque une grande entreprise logistique de e-commerce a vu son volume de trafic de pointe monter à 2,3 Tbps, soit l'équivalent de 100 films de 1h30 par seconde.

Avec le « *DDoS as a service* », cette attaque se démocratise et devient accessible à des cyberdélinquants sans compétences techniques avancées. En effet, des individus malveillants proposent désormais des services en ligne permettant de louer ce type d'attaque et cibler un site *web* ou une adresse *IP* spécifique.

Le *DDoS* se retrouve également de plus en plus couplé à une demande de rançon, dont la somme varie en fonction des victimes ciblées. On parle alors de « *Ransom DDoS* ».

Les individus malveillants utilisant l'attaque *DDoS* sont animés par différentes motivations : causer des dommages, obtenir un avantage concurrentiel, extorquer de l'argent, détourner l'attention des équipes informatiques pour réaliser d'autres activités illégales ou encore par idéologie (hacktivisme). Cela fait aujourd'hui de l'attaque *DDoS* un incontournable du cybercrime.

Pour aller + loin...

Division de la proximité numérique (UNCyber)

C'était un automne comme il en avait déjà passé des dizaines. Les journées restaient douces, mais lorsque le soleil déclinait il se sentait enlacé par une bise tourbillonnante qui accompagnait ses balades vespérales.

Romain avait une routine dont il ne dérogeait jamais. Lorsqu'il rentrait du travail, il nourrissait son chien, puis allait faire sa balade contemplative avant de « *checker* » ses mails et ses éventuels SMS avant d'aller au lit.

La lecture mécanique de ses SMS s'arrêta net et d'un seul coup il eut l'impression que son sang quittait son visage :

Un monsieur, « *Death angel* », lui indiquait qu'il était tueur à gage et qu'un contrat lui avait été donné pour le tuer.

Il proposait à ce dernier de racheter, en quelque sorte, ce contrat pour éviter qu'il ne soit honoré. Le tueur l'avisait qu'il le surveillait et qu'aucune échappatoire n'était possible.

Romain réfléchit rapidement : ça pouvait être à cause de son divorce ou peut être ce voisin avec lequel il avait des rapports houleux.

La terreur l'avait saisi tout autant que la lucidité l'avait abandonné. La seule solution était de payer le tueur pour échapper à la mort.

ALERTE : PAS DE PANIQUE ROMAIN !

Ce mail est totalement impersonnel et ne s'adresse donc pas spécifiquement à vous. Il s'agit d'un sms d'arnaque pour vous soutirer de l'argent.

NOS CONSEILS :

- Ne paniquez pas, ne payez pas,
- Signalez le message sur **signal Spam** et sur la plateforme de signalement :

www.internet-signalement.gouv.fr

Coopération Gendarmerie nationale / COJOP

A l'approche des Jeux Olympiques et Paralympiques 2024, *Le Figaro* a consacré un article à la coopération entre le Comité d'Organisation (COJOP) et l'Unité Nationale Cyber (UNCyber) de la Gendarmerie nationale dans le cadre de la lutte contre la vente de faux billets.

Le colonel Hervé Pétry, chef de l'unité, et le capitaine Étienne Lestrelin, responsable fraude dans le cadre du programme européen EMPACT, ont notamment évoqué une collaboration remontant à 2022, la détection de 257 sites illicites, dont 57 ont été neutralisés, ou encore la mobilisation à temps plein de 200 cybergendarmes dédiés.

Aussi, l'UNCyber a souhaité, en lien avec le COJOP et avec le concours du SIRPA-G et de l'INSEP, intensifier son message de prévention. Ainsi, deux vidéos mettant en scène la judokate Clarisse Agbégnénou et le joueur de para badminton Thomas Jakobs, membres de « l'armée des champions », ont été réalisées. Diffusées sur les réseaux sociaux en langue française le 28 mars dernier, elles ont d'ores et déjà suscité l'intérêt du Comité International Olympique (CIO), qui envisage à court terme de les rendre accessibles à l'ensemble des spectateurs des cinq continents.

Création de cyberpatrouilles

M. Gérald Darmanin a adressé une note à tous les préfets jeudi 21 mars dernier, lançant l'offensive contre les narcotrafiquants qui se développent *via* Internet. Le ministre de l'Intérieur et des Outre-mer a indiqué compter à la fois sur le renseignement, l'infiltration et la création de cyberpatrouilles.

Pour entraver les nouveaux modes de distribution, et notamment « *l'ubershit* » à domicile, M. Darmanin considère que les forces de l'ordre « doivent adapter leurs méthodes et leurs moyens », et qu'il « faudra développer très largement la présence et la veille numérique par des cyberpatrouilles et généraliser le recours aux enquêtes sous pseudonyme et aux coups d'achat sur les réseaux sociaux, sous l'autorité des magistrats » *(Le Parisien)*.

Commandement du ministère de l'Intérieur dans le cyberespace
#LaMInuteCyber n° 003 - Mars 2024

Directeur de la publication : GDI C. HUSSON
Responsable éditorial : CEN D. MALET
Rédacteurs : CEN D. BOGE - CEN D. MALET - Mme S. VIARD DE GALBERT - Mme L. HACHIN
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***