

CYBERCRIMINALITÉ – LA RA&D COMME INGRÉDIENT ESSENTIEL AU DÉVELOPPEMENT DES FORMATIONS POLICIÈRES

Février 2024

Renaud Zbinden
Sébastien Jaquier

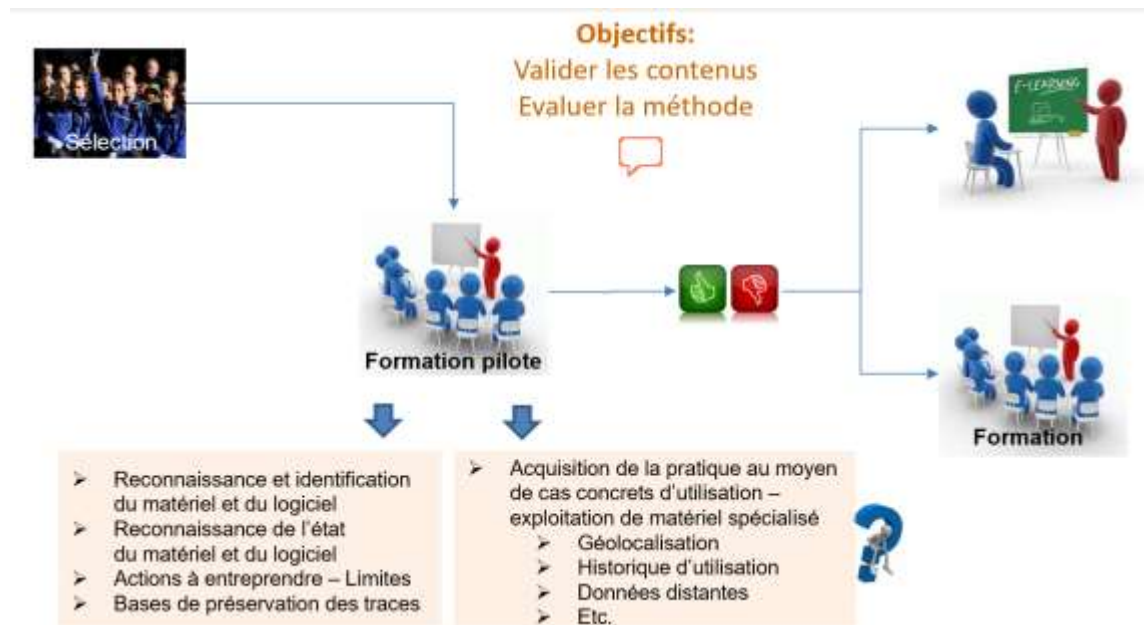
Cyber: L'émergence d'un besoin pour la police

Développement d'une formation nationale en ligne



Cyber: L'émergence d'un besoin pour la police

- Emergence du cyber dans le quotidien du policier
- 2014 – Idée de formation de base en préservation des traces numériques



Concept de formation policière en matière Cyber

Spécialistes

Formations spécialisées

Enquête
investigation numérique
Analyse

Enquêteurs

Cours cyber II pour enquêteurs

Tous les policiers

e-learning Cybercrime, e-CC

Evolution des besoins

L'enquête devient Cyber.

Constats:

- Le Cyber fait désormais partie de l'enquête
- Tous les enquêteurs ne sont pas informaticiens
- Les ressources spécialisées en informatiques sont limitées
- Emergence de l'enquête IT en tant que discipline



Gestion

**CAS Cybercriminalité,
option cyberenquête**

Exemple de projet de recherche

Darknet Monitoring (DarkMon)

Question de recherche :

Comment les fraudeurs présents sur le Darknet interagissent-ils dans les salles de discussions privées ?

Terrain d'observation :

Forums destinés à la vente de logiciels malveillants (malware)

Projet : Darknet Monitoring

- ✓ Projet effectué de mai 2020 à novembre 2021
- ✓ Partenariat avec une entreprise canadienne spécialisée dans la surveillance du Darkweb
- ✓ Quasi-totalité des recherches précédentes portées sur les salles de discussions publiques uniquement

Projet : Darknet Monitoring

Objectif :

Décrire et comprendre les impacts que peut avoir la nature privée des forums de discussion sur les activités de leurs participants

Comprendre si les réseaux de fraudeurs actifs dans les salles privées sont les mêmes qui opèrent dans les salles publiques et si les informations qu'ils échangent sont de nature différente de celles qui le sont dans les salles publiques.

Projet : Darknet Monitoring

Langel, S., Décary-Hétu, D., Beaudet-Labrecque, O., Brunoni, L., & Zbinden, R. (2022). Private clubs For hackers: how private forums shape the malware market. *The Journal on Cybercrime & Digital Investigations*.

Private Clubs For Hackers: How Private Forums Shape The Malware Market

Sandra Langel¹, David Décary-Hétu², Olivier Beaudet-Labrecque¹,
Luca Brunoni¹, Renaud Zbinden¹

¹Institut de lutte contre la criminalité économique, HEG Arc // HES-SO, ²Université de Montréal

This paper was presented at Botconf 2022, Nantes, 26-29 April 2022, www.botconf.eu
This paper is published in the Journal on Cybercrime & Digital Investigations by CECyF, <https://journal.cecyf.fr>
It is shared under the CC BY license <http://creativecommons.org/licenses/by/4.0/>.

Abstract

Offenders seek online private discussion forums where participants are screened before gaining access to connect with sophisticated peers and evade detection. Past research finds that most public discussion forum participants have a low level of technical skill and rely on more established participants for the tools and techniques they need to commit their offences. To date, research has mostly focused on public discussion forums of online offenders as gaining access to private forums comes with many challenges. The aim of this research is to describe and understand the impacts of the private nature of discussion forums on their participants' activities. Our driving hypothesis is that private discussion forums are host to more sophisticated participants that will, in turn, offer and have access to more sophisticated tools. To understand the impacts of the private nature of discussion forums, we selected two discussion forums available on the internet whose focus is the sale of malware; one of them is private, while the other is public. Our analysis suggests that while there are differences between private and public discussion forums, there are few significant differences between both inters of the products they advertise.

Keywords: malware, discussion forum, hacking.

1 Introduction

Discussion forums are the descendants of bulletin board systems (BBS) which were used in the

pre-internet days. BBS were used to post public messages, exchange private messages as well as files [26]. Their main limit came from their access method which limited the speed at which participants could communicate, as well as their geographical reach. Using phone lines to connect to BBS meant that participants had to pay international fees when connecting to a distant BBS, unless they could somehow bypass the phone companies' billing systems. BBS were often associated with illicit activities as they facilitated the pirating of software and enabled the sharing of hacking tactics and methods [3].

Discussion forums did not inherit the bad reputation of BBS but provide many of the services that BBS did in the 1970s, 1980s and early 1990s. Discussion forums quickly replaced BBS as they could be reached by any internet users at no additional costs to their basic internet connection. At their core, discussion forums are asynchronous communication channels hosted on internet websites [20]. Discussion forums are divided into subforums, which contain multiple discussion threads. Each thread usually discusses a very specific topic (ex. how to hack a Windows password) within a more general subforum (ex. hacking techniques).

Discussion forum participants are divided into multiple groups [21, 28]. The first, the administrators, manage the forum and enforce the social rules [21]. They publish the rules under which everyone else must abide by, and hand out the punishments to those that abuse the rules. Administrators can be elected in some cases but are most often those that create a discussion forum or receive or purchase the

Projet : Darknet Monitoring

Intérêt pour la formation :

- ✓ Observation des comportements criminels
= «Traque des cybercriminels»
- ✓ Potentiel de perturbation
- ✓ Enquête / Poursuite

Formation des spécialistes: Cyberpie

Objectifs visés:

- *Responsables de formation et commandement* : base d'orientation et de décision claire
- *Personnel à former* : Vue synthétique pertinente de l'offre de formations
- *Personnel formé* : Qualification de la formation suivie
- *Instituts et écoles* : Plateforme permettant de mettre en valeur leur offre

Formation des spécialistes: Cyberpie

S'appuie sur la matrice de compétence des profils police dans le domaine cyber

Méthodologie:

Détermination de 5 profils concernés par le cyber:

- Policier de terrain
- Enquêteur
- IT-Enquête
- IT-Forensique
- Analyse Cybercrime

Elaboration d'une matrice de compétence listant 13 domaines

Avec pour chaque domaine différents niveau de connaissance - compétence

Cyberpie

Illustrations

CYBERPIE
Formations pour les polices

Connexion Inscription FR

Rechercher 10 Profils Trier par Graph participent-e-s FILTER

- Blockchain et Cybercriminalité**
 20 heures de cours / 4 jours de pratique / 4

Blockchain: introduction, distribution, consensus, paradigmes de partage, hashing, anonymat. Il présente également, les vulnérabilités connues et le fonctionnement des attaques qui les cybercriminels ont étudiées sur la blockchain.
- CAS: Cyber Threat Intelligence**
 24 heures de cours / 4 jours de pratique / 4

Con l'effetto di questo nuovo Certificate of Advanced Studies (CAS), la SUPSI vorrà rispondere alle nuove sfide poste dagli sviluppi tecnologici in termini di sicurezza e della tendenza in atto nell'approcciare la sicurezza nell'era cybernetica in modo strategico.
- CAS: Introduzione alla Cybersecurity**
 24 ore di corso / 4 giorni di pratica / 4

Con l'effetto di questo nuovo Certificate of Advanced Studies (CAS), la SUPSI risponde alle nuove sfide poste dagli sviluppi tecnologici in termini di sicurezza e della tendenza in atto nell'approcciare la sicurezza nell'era cybernetica in modo strategico.
- CAS Computer System Forensic Analysis**
 20 ore di corso / 4 giorni di pratica / 4

Four modules, taught in English by experts from around the world, covers forensic analysis of storage and filesystems, analysis of operating system artifacts from Windows, Mac, and Linux, application and media file

HE HEMA
SD SUPSI DTI
SD SUPSI DTI
BD BRH DFC

Cyberpie – Aspects fonctionnels

Illustrations

CYBERPIE
Formations pour les polices

Formations | Compétences | Profils | Participant-e-s et notes | Écoles / Instituts | FR | AD

Rechercher [10] IT-Forensique Trier par per

CAS IN, CAS en investigation numérique

Jours de cours : 20
Jours de pratique : 5

Le CAS en investigation numérique a pour objectif de former des praticiennes et praticiens à réaliser toute la chaîne des opérations dans le cadre de l'analyse forensique d'un ordinateur (saisie du matériel, extraction, analyse et rédaction d'un rapport).

CAS CY-E, CAS Cybercriminalité option Cyberenquête

Jours de cours : 20
Jours de pratique : 5

Le CAS Cybercriminalité option cyberenquête (CAS CY-E) vise à former les spécialistes des autorités de poursuite pénale (enquêteurs, analystes, procureurs) en matière de lutte contre la criminalité informatique en leur fournissant les outils pertinents pour des enquêtes ayant une composante cyber.

CAS CY-E, CAS Cybercriminalité option Cyberenquête

Jours de cours : 20
Jours de pratique : 5

Jours de cours : 20 **Jours de pratique : 5**

ILCE
Institut de lutte contre la Criminalité Économique
Pôle de l'Ilote

Description | Compétences | Commentaires (0)

Titre obtenu
Les personnes suivant cette formation avec succès se verront délivrer le titre de Certificate of Advanced Studies HES-50 Cybercriminalité - Spécialisation Cyberenquête. Cette formation correspond à 16 crédits ECTS.

Public cible
Le CAS CY-E s'adresse exclusivement aux membres des autorités de poursuite pénale au bénéfice de bonnes connaissances de l'informatique et qui souhaitent développer leurs compétences dans le domaine de la cybercriminalité afin de les appliquer dans le cadre de l'enquête.

Durée et organisation des études
La formation comprend 180 leçons dispensées de la manière suivante :

- Tronc commun : en principe sur deux jours par semaine, les vendredis et samedis, durant huit semaines.
- Spécialisation Cyberenquête : deux sessions de cinq jours réparties sur une durée d'environ deux mois.

Conditions d'admission
Sont admises à suivre le CAS CY Cyberenquête les personnes au bénéfice d'un titre délivré par une haute école ou d'un titre jugé équivalent, qui disposent de bonnes connaissances informatiques et qui n'ont pas fait l'objet d'une poursuite pénale en lien avec la cybercriminalité ou la criminalité économique. Les personnes doivent en outre travailler au sein des autorités de poursuite pénale suisses ou étrangères.

Contenu

- Tronc commun (partagé avec le CAS Cybercriminalité - Cyber sécurité)
- Informatique Informatique générale, réseau et Internet
- Évaluation et sensibilisation Contexte cybercriminal, méthodes et outils de prévention et détection, mesures comportementales
- Cryptologie appliquée Cryptologie, signature, message, fichiers, conteneurs, volumes chiffrés, messagerie chiffrée, message, blockchain
- Typologie des menaces Malwares, attaques, facteur humain, bases de l'OSINT
- Droit informatique Infractions informatiques, responsabilité civile et pénale en matière de cybersécurité, limites géographiques
- Spécialisation Cyberenquête

Cyberpie – Aspects fonctionnels

Illustrations

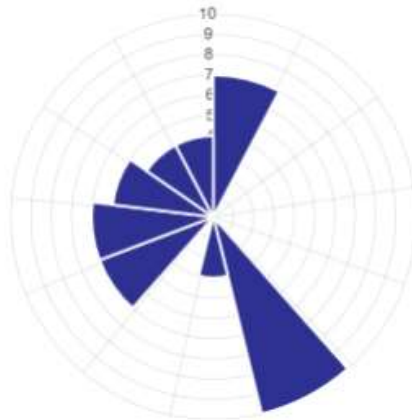
CYBERP
Formations pour les po

Q Rechercher

**CAS IN, CAS en inv
numérique**
Jours de cours : 20
Jours de pratique : 5

**CAS CY-E, CAS Cyt
option Cyberenquêt**
Jours de cours : 20
Jours de pratique : 5

Compétences



- Introduction au domaine spécialisé **7 POINTS**
- Introduction au domaine spécialisé et supports de données **3 POINTS**
- État et évolution aujourd'hui et dans un futur proche (caractéristiques et possibilités techniques fondamentales)
- Explications des termes / définitions (utilise l'internet comme moyen de communication, en se servant notamment de la messagerie électronique à des fins illicites)
- Cybercrime stricto sensu / types de délits (infractions commises à l'aide de TIC ou profitant des vulnérabilités de ces technologies)
- Explications des termes / définitions (utilisation de données publiques (« recherches open source »)) **10 POINTS**
- Infrastructure propre (processus de travail dans le corps/l'organisation)
- Domaines spécialisés **0 POINTS**
- Analyse **0 POINTS**
- Sécurité informatique (interne) **6 POINTS**
- Droit applicable **6 POINTS**
- Bénéficiaire des prestations / partenaires **5 POINTS**
- Sécurité informatique / protection des données/ prévention (externe) **4 POINTS**
- Engagement lié à un incident cybernétique **4 POINTS**

A votre disposition

Sébastien Jaquier
Doyen de l'ILCE
E-mail : sebastien.jaquier@he-arc.ch



Renaud Zbinden
Collaborateur scientifique
Tél. direct : +41 32 930 23 56
Email : renaud.zbinden@he-arc.ch



Questions / Informations complémentaires

ILCE / ERMP / CINC

HEG Haute école de gestion Arc

21, Espace de l'Europe

CH - 2000 Neuchâtel

Tél +41 32 930 20 15

www.ilce.ch

Merci !

