





# Private club for hackers

## Comment les forums privés façonnent le marché des malwares ?

Olivier Beaudet-Labrecque  
Doyen & Prof @ ILCE

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

**Sandra Langel<sup>1</sup>, David Décary-Hétu<sup>2</sup>, Olivier Beaudet-Labrecque<sup>1</sup>,  
Luca Brunoni<sup>1</sup>, Renaud Zbinden<sup>1</sup>**

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

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





## Forums cybercriminels



📌

Looking for c/c++ developer for new botnet project - 100k budget

Подписаться 1

Автор:

3 октября в [Работа] - поиск, выполнение работ

Создать тему

Ответить в тему

байт

Опубликовано: 3 октября

Жалоба

I am new to this forum, but I am not new to the game.  
I have a large budget, 100k USD+  
I am looking for a developer for a new http botnet project.  
Please PM me if you would like to discuss this job with me. Include your jabber inside your message and a time when you will be online. (Moscow timezone)

Платная регистрация

3 публикации

Регистрация

26.09.2022 (ID: 136941)

Деятельность

вирусология / malware

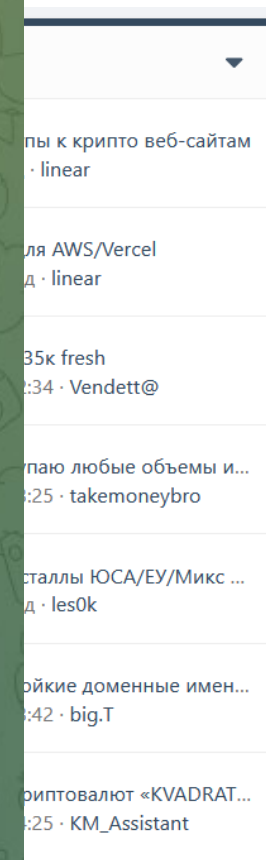
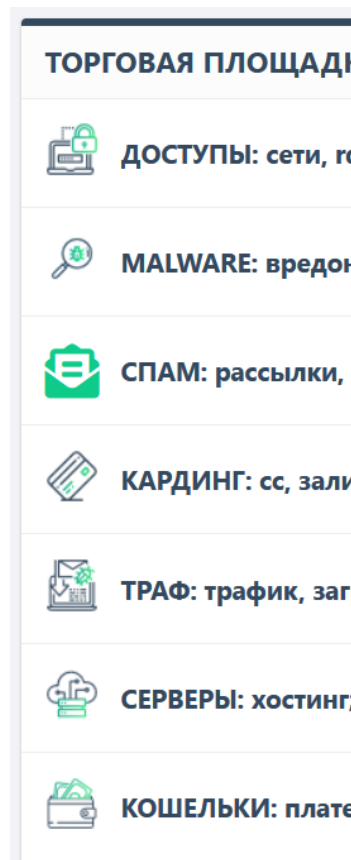
Депозит

0.000586 ₿

+ Цитата



## Forums cybercriminels



## Données étudiées



Projet de recherche exploratoire



**Un forum privé** (env. 60k membres; + de 1 mio de posts)



**Un forum public** (env. 185k membres; + de 340k posts)

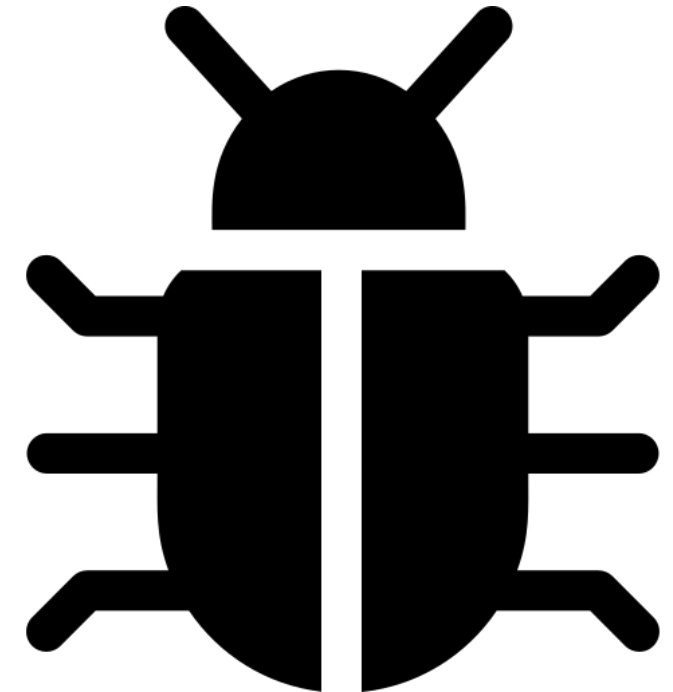


Collecte de données entre le 1<sup>er</sup> juin 2020 et le 10 février 2021

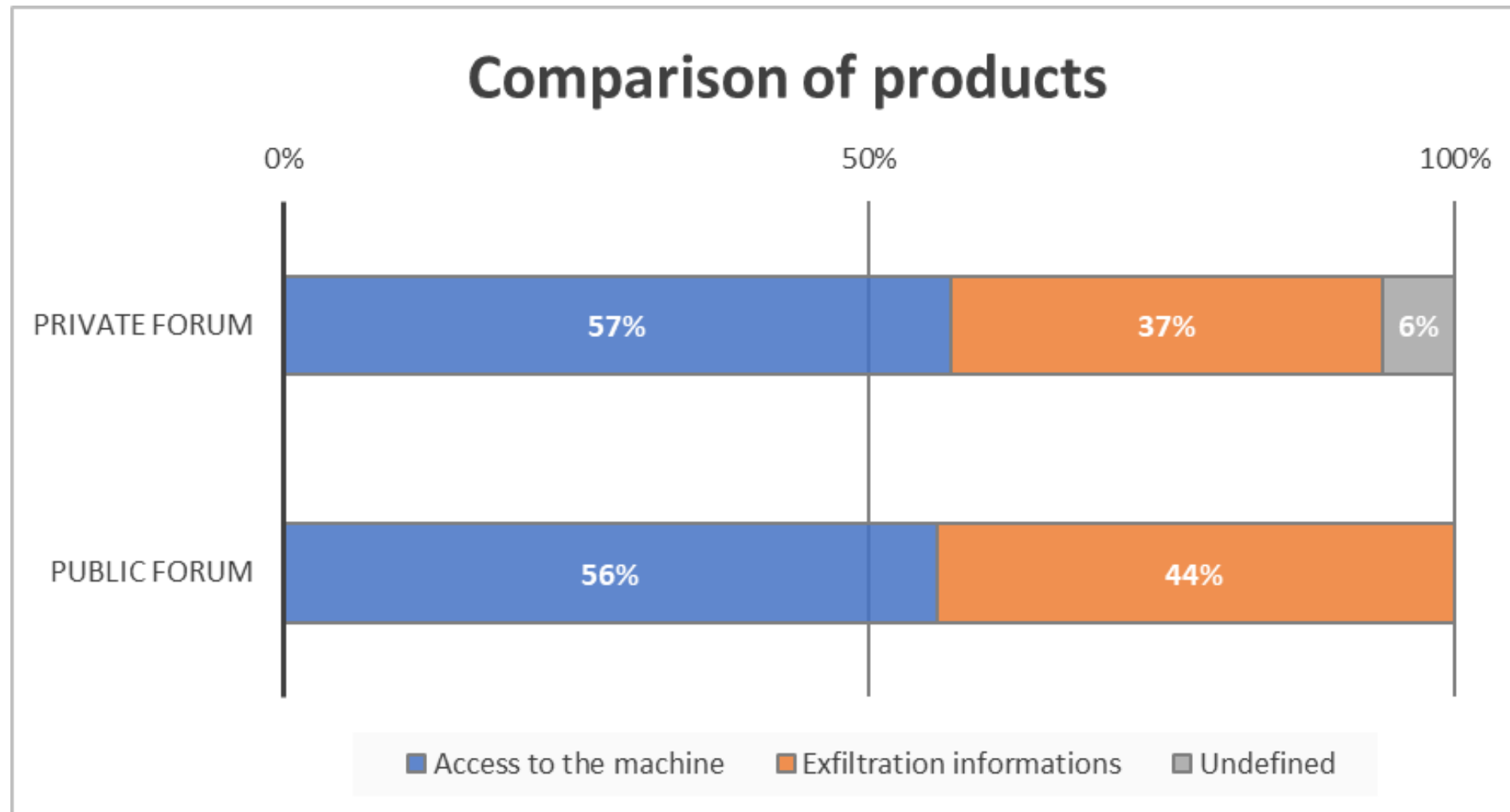


Analyse et comparaison des  
offres de **malware**

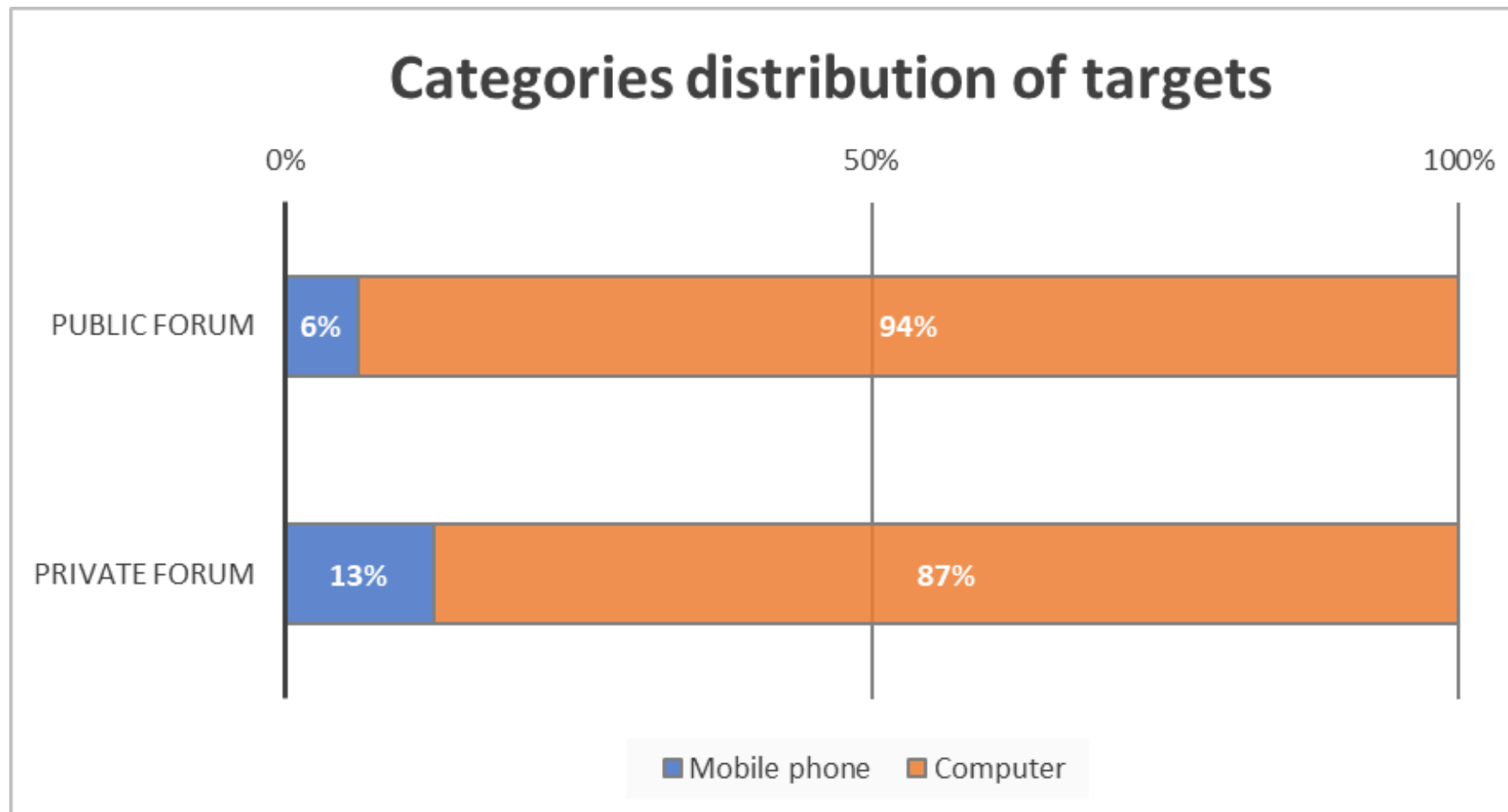
**136 sur le forum privé**  
**86 sur le forum public**



## Types de malware



## Appareils ciblés

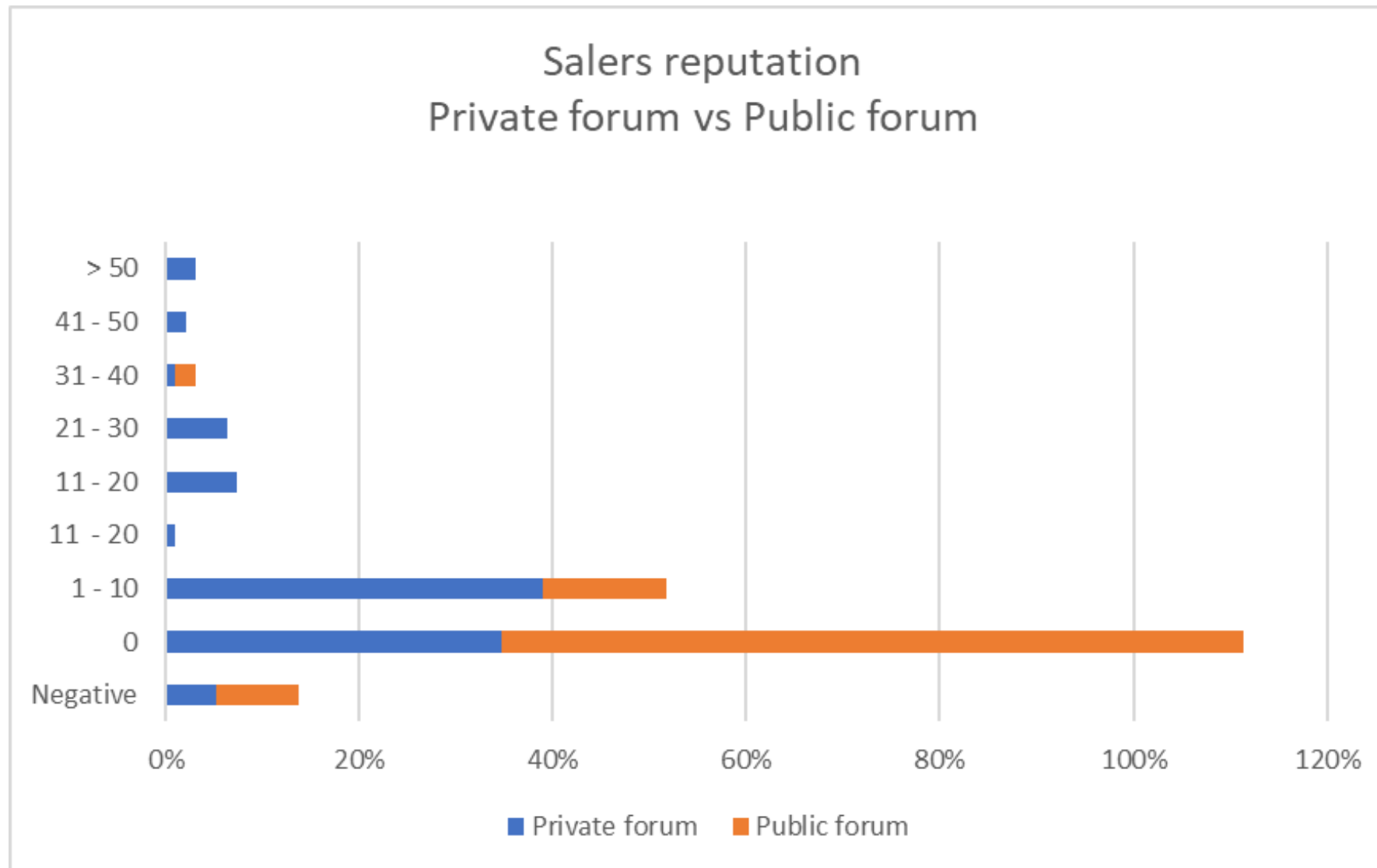




## « Fraîcheur » des malwares



## La réputation des vendeurs



## Observations

- Relativement peu de différence sur les malwares vendus
- Les forums privés semblent permettre la création de profils de vendeurs établis
- Certains vendeurs sur le forum privé demandaient de ne pas déployer les malwares sur les territoires russophones
- Certains acteurs sont présents sur les deux forums
- Des informations quant aux ve

## Conclusions

- Faible impunité
- Formes d'engagement dans les forums privés
- D'autres études doivent être menées sur le sujet

## Parallèle avec la fraude en ligne





## Parallèle avec la fraude en ligne



**Buraliste**

«Privés» et «Publics»



**2MIL NATIONAL**

**Réception De virement**

|              |                  |
|--------------|------------------|
| France 🇫🇷    | Côte D'Ivoire 🇨🇮 |
| Espagne 🇪🇸   | Mali 🇲🇱          |
| Italie 🇮🇹    | Burkina 🇸🇳       |
| Allemagne 🇩🇪 | Sénégal 🇸🇳       |

**Whatsapp 0585051078**

**Mandat**

|                  |
|------------------|
| Côte d'Ivoire 🇨🇮 |
| France 🇫🇷        |
| Burkina 🇸🇳       |
| Mali 🇲🇱          |

**Retraite des Cartes**

BBVA PCS MoneyGram Money Transfer Neosurf Virement Bancaire bitnovo

PayPal CE MasterCard VISA

ENVOI D'ARGENT SUR WESTERN UNION

100% de fonds de garantie

De nombreux réseaux

MAJ

Un homme en une veste orange et blanche tient un billet de banque.

## Questions ?

