



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

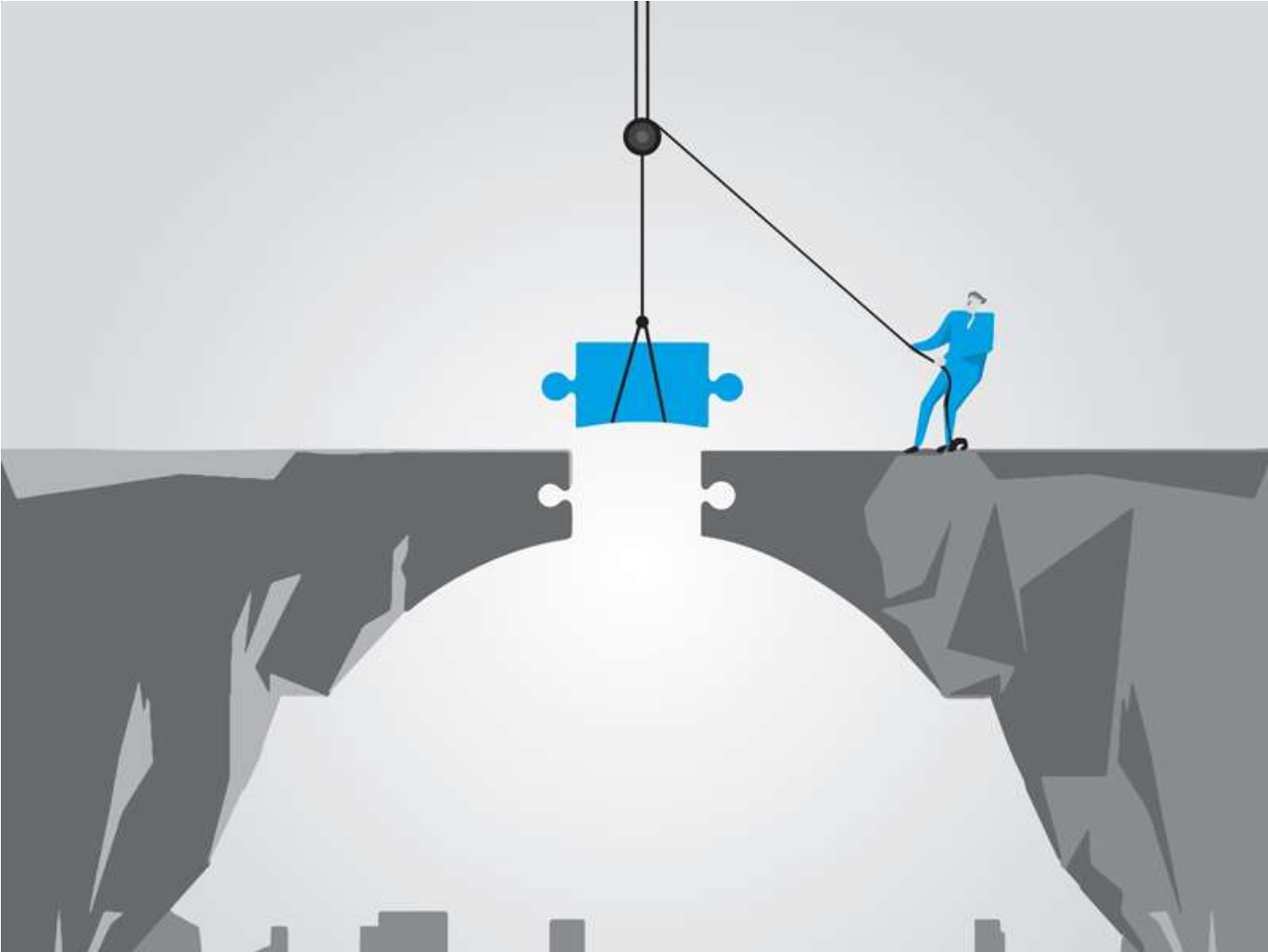
David Décary-Héту, Luca Brunoni,
Sandra Langel and Olivier
Beaudet-Labrecque



**ilce - institut de lutte contre
la criminalité économique**

heg - haute école de gestion

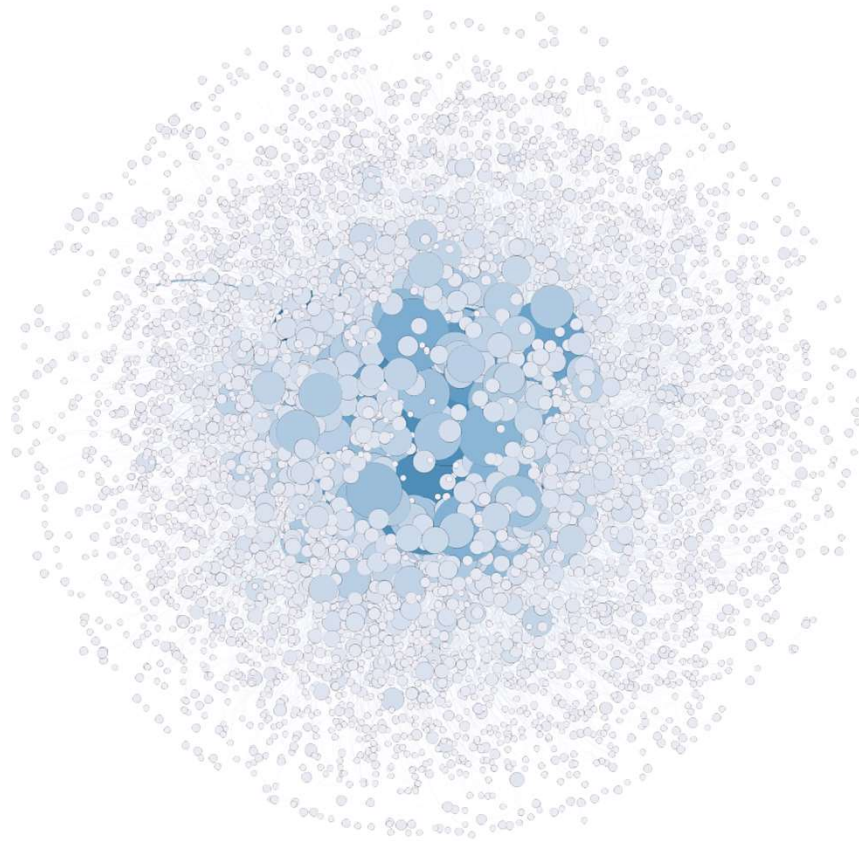
The logo for ARC (Association for Research in Crime and Justice) is rendered in a bold, blue, sans-serif font. The letters 'a', 'r', and 'c' are lowercase and connected, with the 'a' and 'c' having a rounded, bowl-like shape. The 'r' is a simple vertical stem with a curved top. The 'c' is a simple, rounded shape.













Forums as information sharing platforms



Forums as transactional platforms

ТОРГОВАЯ ПЛОЩАДКА			
 ДОСТУПЫ: сети, rdp, шеллы, ftp, sql-inj, DB's	Темы 2.3K	Сообщения 10.2K	 Куплю доступы к крипто веб-сайтам 6 мин. назад ·
 MALWARE: вредоносы, крипт, инжекты, 0/1day экспы	Темы 2.2K	Сообщения 17.4K	 Куплю RCE для AWS/Vercel 14 мин. назад ·
 СПАМ: рассылки, отклики, базы, mail-дампы	Темы 1.6K	Сообщения 6.7K	 FullInfo USA 35к fresh Сегодня в 02:34 ·
 КАРДИНГ: сс, заливы, вещьвуха, банки, стафф	Темы 1.8K	Сообщения 10.6K	 Дорого покупаю любые объемы и... Сегодня в 03:25 ·
 ТРАФ: трафик, загрузки, инсталлы	Темы 1.3K	Сообщения 5.7K	 [Сервис] Инсталлы ЮСА/ЕУ/Микс ... 21 мин. назад ·
 СЕРВЕРЫ: хостинг; VPN, проху, socks	Темы 561	Сообщения 4.7K	 [СЕРВИС] Стойкие доменные имен... Сегодня в 03:42 ·
 КОШЕЛЬКИ: платежные системы, разлок, обмен валют	Темы 513	Сообщения 3.5K	 Обменник криптовалют «KVADRAT... Сегодня в 04:25 ·

Countless forums in the criminal underground



Restricted access



The “myth” of the elite, private forum



Darkode: Recruitment Patterns and Transactional Features of “the Most Dangerous Cybercrime Forum in the World”

American Behavioral Scientist
2017, Vol. 61(11) 1219–1243
© 2017 SAGE Publications
Reprints and permissions:
sagepub.com/journalsPermissions.nav
DOI: 10.1177/0002764217734263
journals.sagepub.com/home/abs



**Benoît Dupont¹, Anne-Marie Côté¹, Jean-Ian Boutin²,
and José Fernandez³**

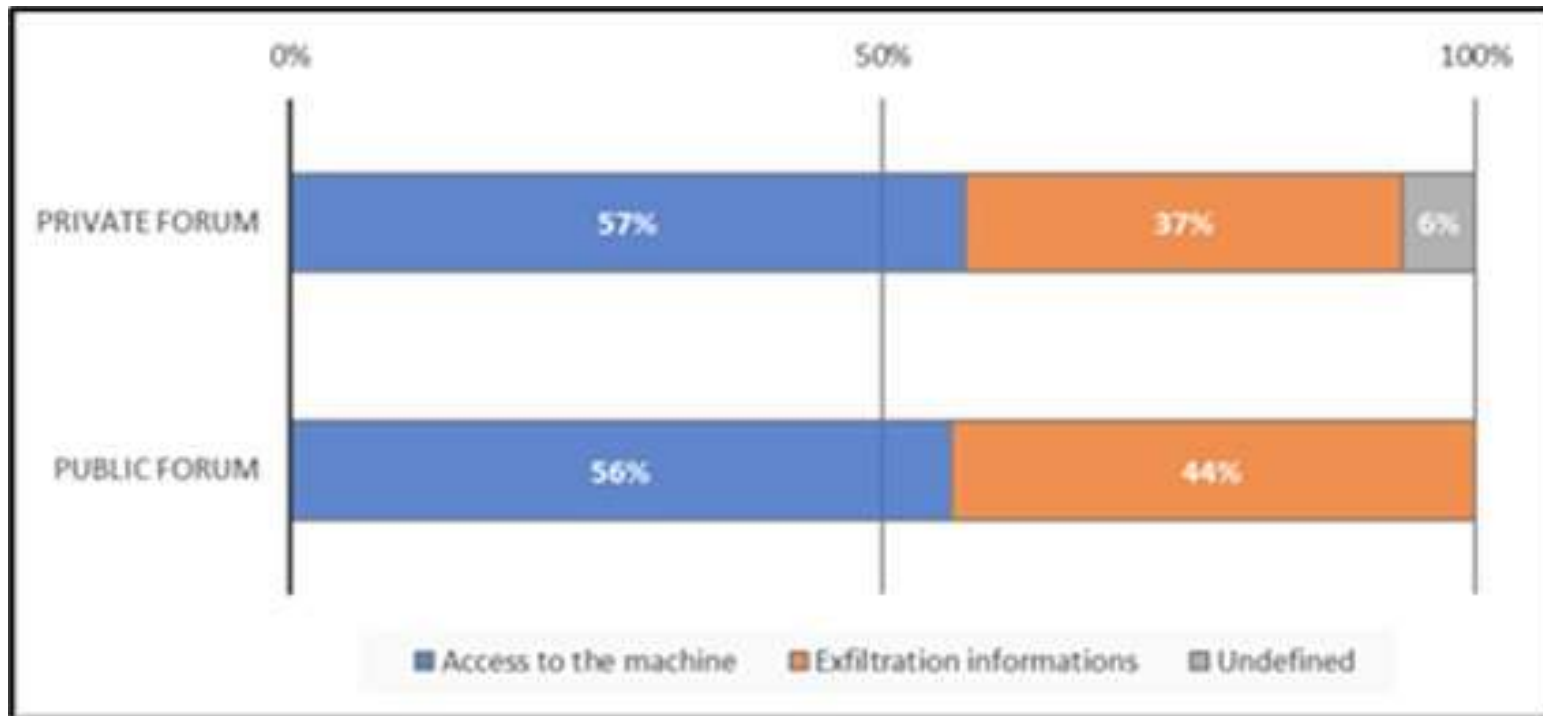
Abstract

This article explores the social and market dynamics of Darkode, an invitation-only cybercrime forum that was dismantled by the FBI in July 2015 and was described by a U.S. Attorney as “the most sophisticated English-speaking forum for criminal computer hackers in the world.” Based on a leaked database of 4,788 discussion threads, we examine the selection process through which 344 potential new members introduced themselves to the community in order to be accepted into this exclusive group. Using a qualitative approach, we attempt to assess whether this rigorous procedure significantly enhanced the trust between traders, and therefore, contributed to the efficiency of this online illicit marketplace. We find that trust remained elusive and interactions were often fraught with suspicion and accusations. Even hackers who were considered successful faced significant challenges in trying to profit from the sale of malicious software and stolen data.

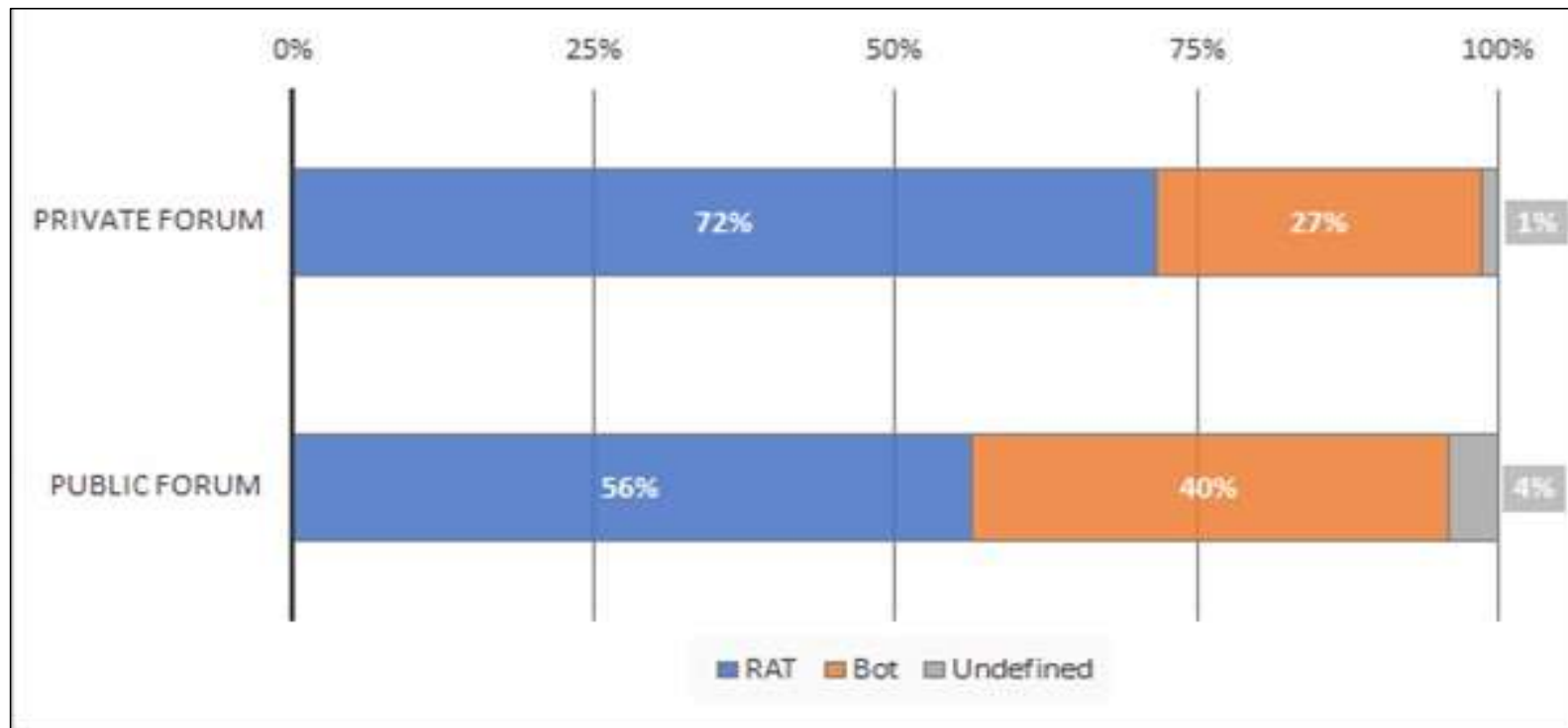
Dataset

- Exploratory research project
- 1 private forum with >60,000 members and >1,000,000 posts
- 1 public forum with >185,000 members and >345,000 posts
- Threads between June 1st 2020 and February 10th 2021
- Analysis of malware offers
 - 86 from the public forum
 - 136 from the private forum

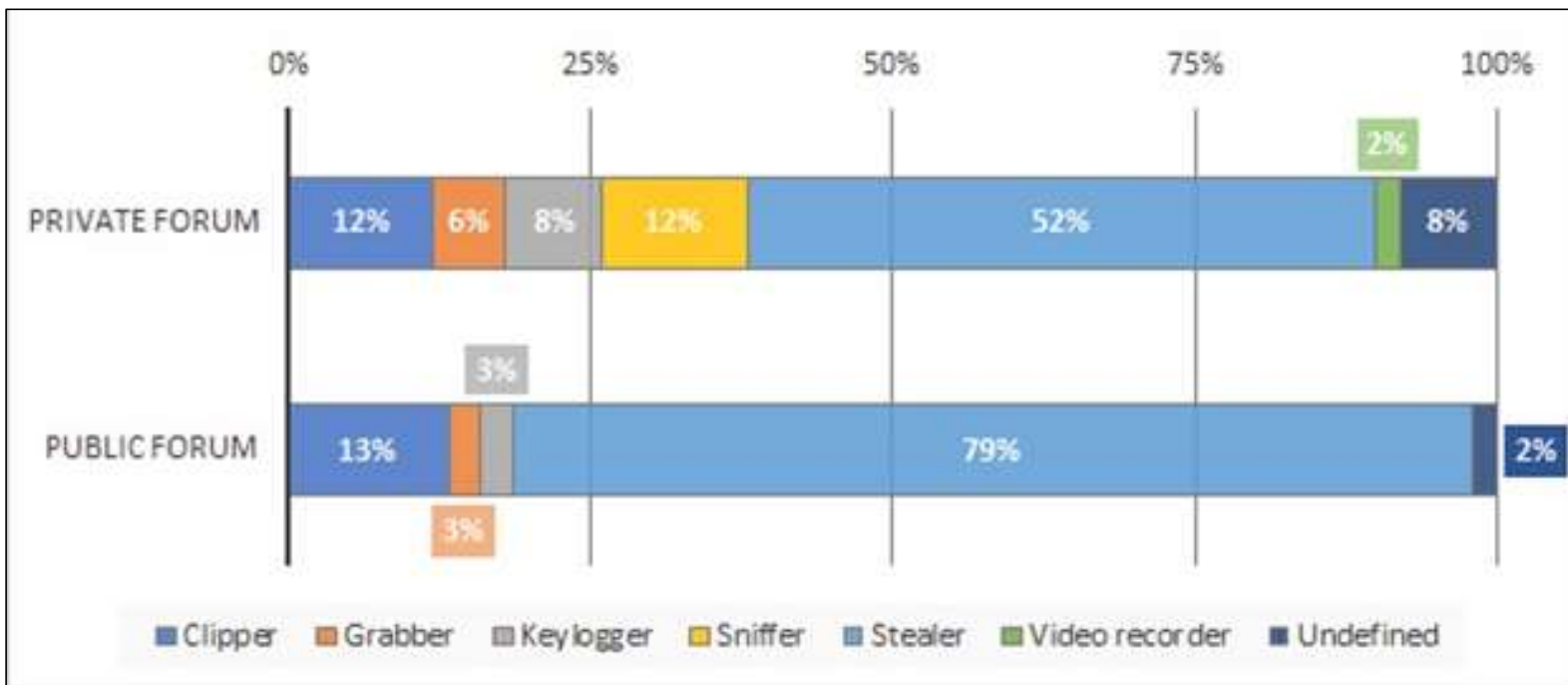
Distribution of the type of malware



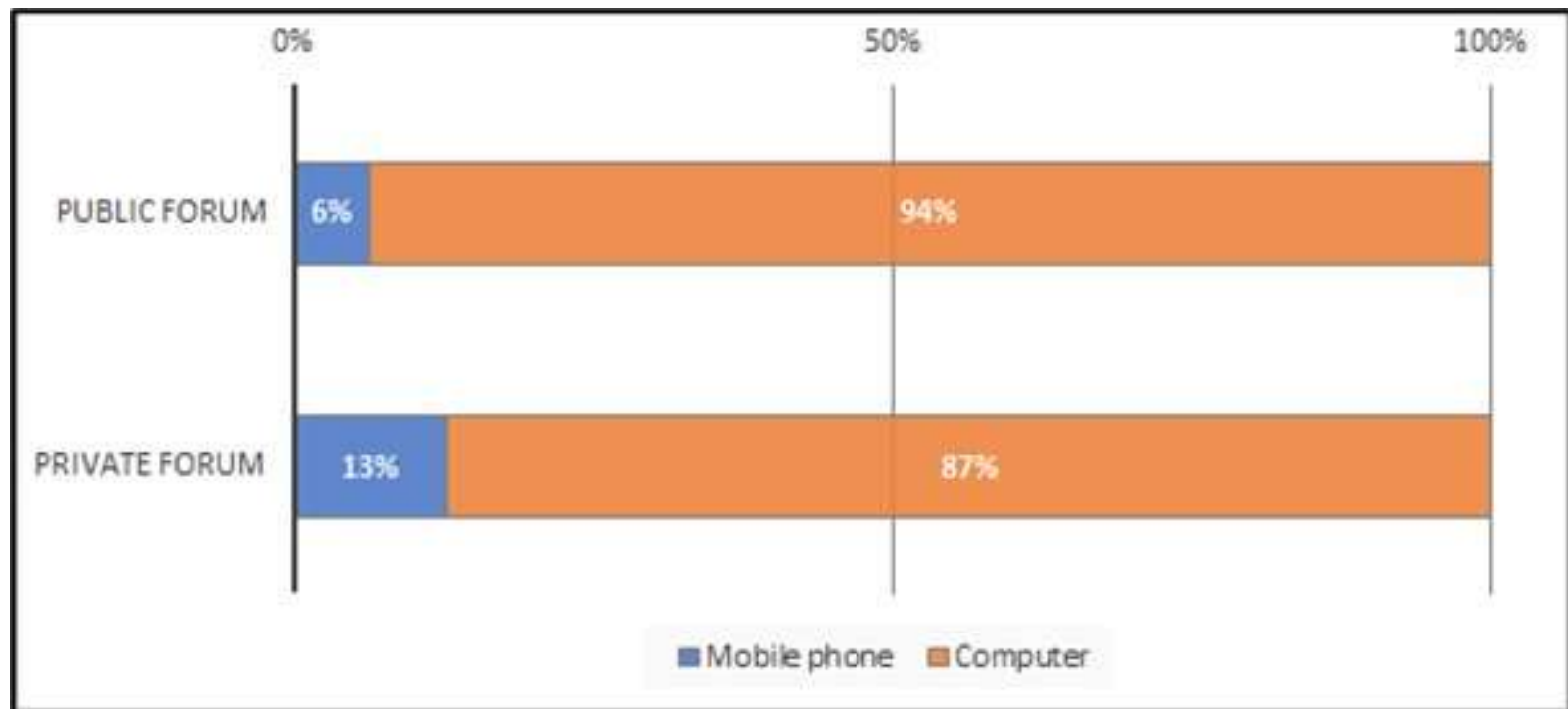
Access to the machine



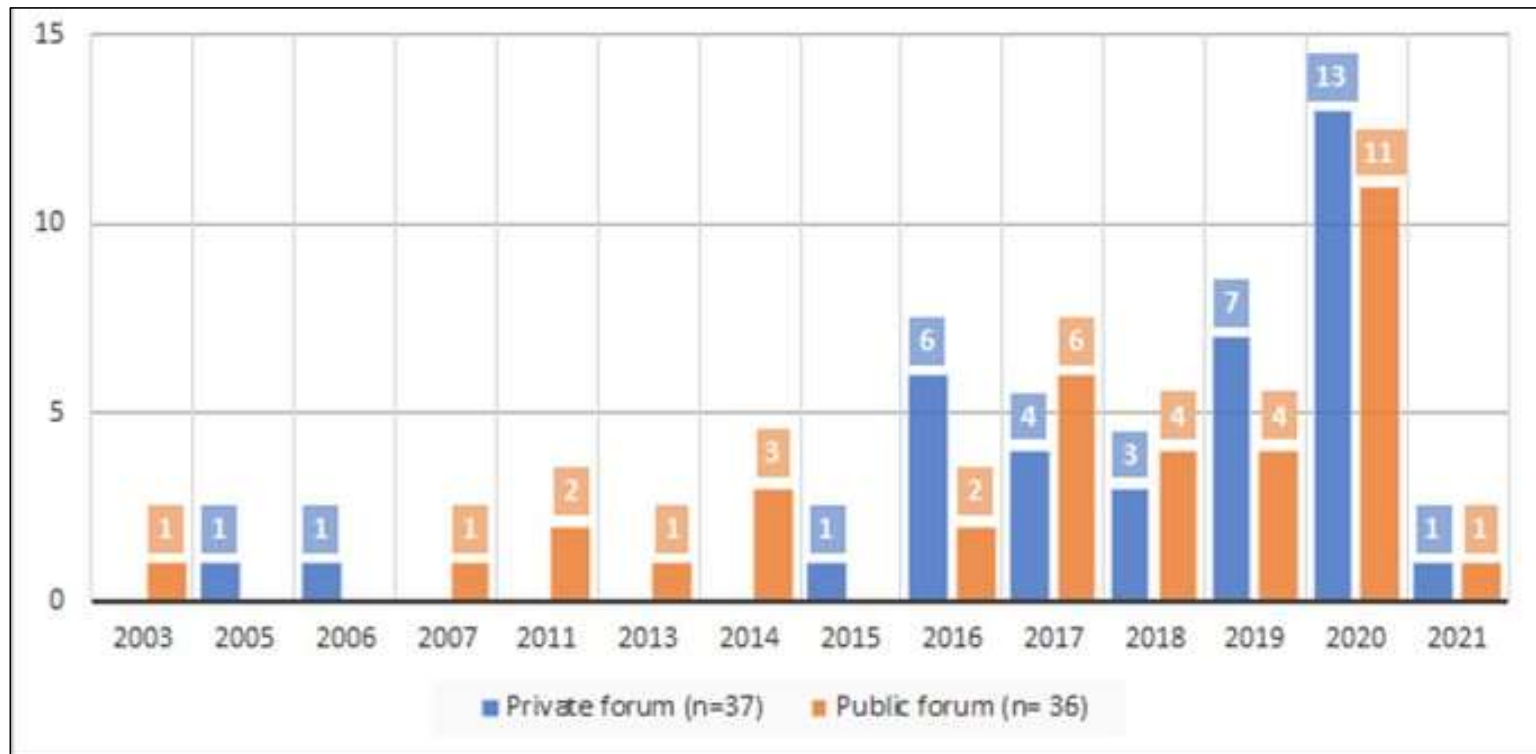
Data exfiltration



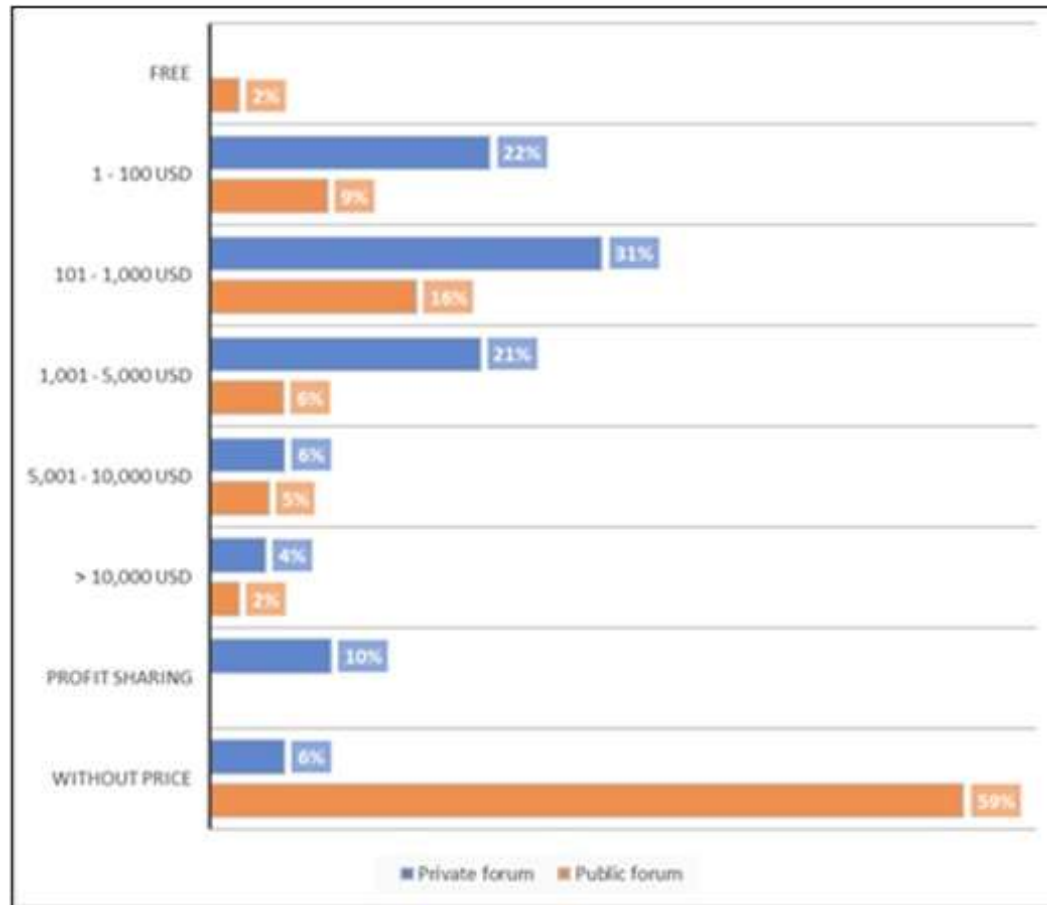
Targeted infrastructure



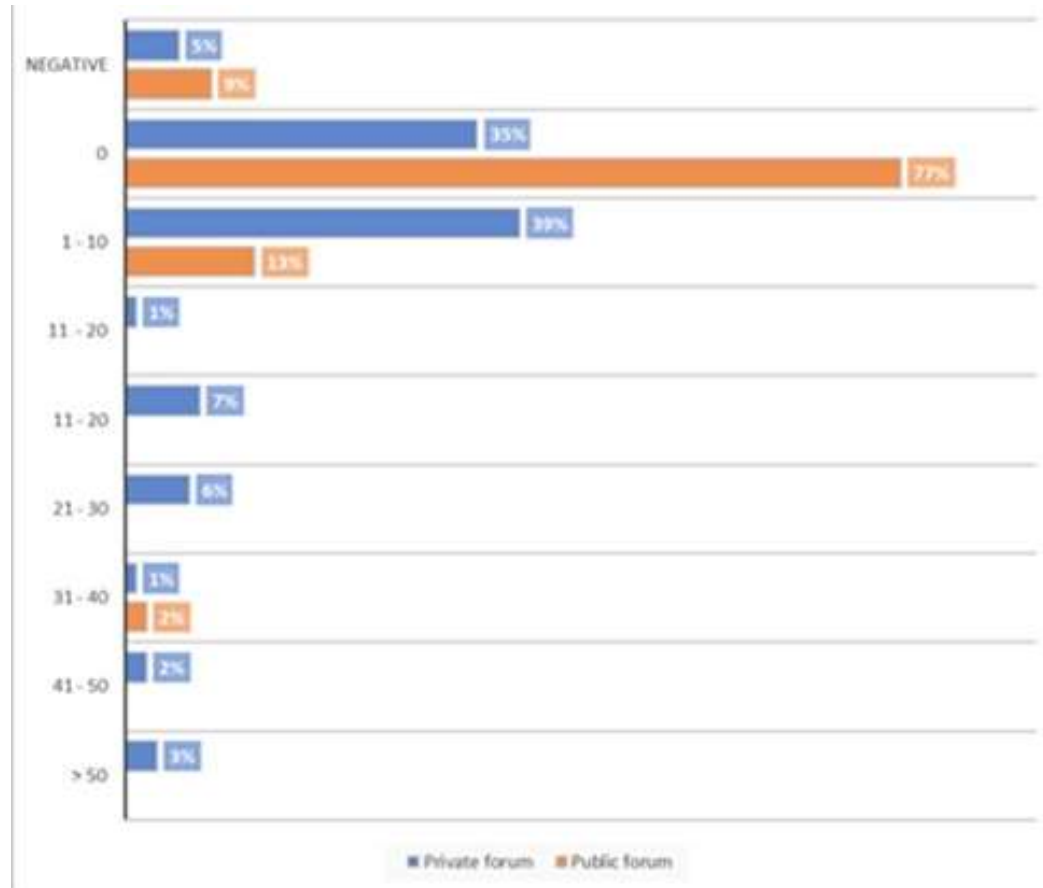
Publication date of malware



Price comparison of malware



Reputation of vendors



Main differentiators between public and private forums

- Few differences in regards to the quality, creation date of malware for sale
- Private forums enable the creation of established profiles on private forums
- Messages asking not to attack Russia in private forum
- High sense of impunity

Main differentiators between public and private forums

- Few differences in regards to the quality, creation date of malware for sale
- Private forums enable the creation of established profiles on private forums
- Messages asking not to attack Russia in private forum
- High sense of impunity

Main differentiators between public and private forums

- Few differences in regards to the quality, creation date of malware for sale
- Private forums enable the creation of established profiles on private forums
- Messages asking not to attack Russia in private forum
- High sense of impunity

Main differentiators between public and private forums

- Few differences in regards to the quality, creation date of malware for sale
- Private forums enable the creation of established profiles on private forums
- Messages asking not to attack Russia in private forum
- High sense of impunity

Conclusion

- Need more validation of the differences in public vs private forums
 - Ethical considerations make it harder to study private forums
- Private forums may be too exclusive
 - Too few partners to conduct business with
- Private forums may not be private enough
 - Sale of 0day exploits through personal networks

Conclusion

- Need more validation of the differences in public vs private forums
 - Ethical considerations make it harder to study private forums
- Private forums may be too exclusive
 - Too few partners to conduct business with
- Private forums may not be private enough
 - Sale of 0day exploits through personal networks

Conclusion

- Need more validation of the differences in public vs private forums
 - Ethical considerations make it harder to study private forums
- Private forums may be too exclusive
 - Too few partners to conduct business with
- Private forums may not be private enough
 - Sale of 0day exploits through personal networks