

ARTICLE DE VULGARISATION — SCIENCESWIKI

Comment les forces de l'ordre parviennent-elles à traquer les activités illicites sur le dark web et les cryptomarchés ?

Question : Comment les forces de l'ordre parviennent-elles à traquer les activités illicites sur le dark web et les cryptomarchés ?

Méthodes de traque

La traque des activités illicites sur le dark web et les cryptomarchés se fait par des méthodes techniques avancées. Les forces de l'ordre utilisent des logiciels de "ciblage" pour pénétrer directement dans les appareils des criminels, contournant l'anonymat [1](#). Pour analyser les vastes zones de données, elles déploient des programmes robots appelés "crawlers" pour récolter automatiquement du contenu et des informations sur les sites [26](#). Elles installent aussi des pièges numériques appelés "honeypots" pour piéger les délinquants et collecter des preuves [3](#). Enfin, pour les transactions financières, des outils d'analyse sont utilisés pour suivre l'utilisation des cryptomonnaies [5](#).

Analyse scientifique

Les forces de l'ordre utilisent des techniques de hacking pour accéder directement aux appareils des suspects [1](#). L'analyse de données et les méthodes de "crawling" permettent de collecter automatiquement du contenu depuis les serveurs [6](#). Les systèmes de "honeypots" servent à piéger les criminels [3](#). Le suivi des transactions sur les cryptomarchés nécessite des outils spécifiques comme MFScope [5](#). Ces méthodes s'appliquent au contexte du dark web et aux systèmes de cryptomonnaies.

[\[1\]](#) Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web — Ahmed Ghappour (2017). DOI:n/a

[\[2\]](#) Crawling and Mining the Dark Web: A Survey on Existing and New Approaches — Mohammed Khalafallah Alshammery, Abbas Fadhil Aljuboori (2022). DOI:10.24996/ijcs.2022.63.3.36

[\[3\]](#) Investigating The Darknet — Rachid Bou Zeid, Joanna Moubarak, Carole Bassil (2020). DOI:10.1109/iwcmc48107.2020.9148422

[\[4\]](#) Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers — Gemma Davies (2020). DOI:10.1177/0022018320952557

[\[5\]](#) Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web — Seunghyeon Lee, Changhoon Yoon, Heedo Kang, Yeonkeun Kim, Yongdae Kim, Dongsu Han, Sooel Son, Seungwon Shin (2019). DOI:10.14722/ndss.2019.23055

[\[6\]](#) Exploring Dark Web Crawlers: A Systematic Literature Review of Dark Web Crawlers and Their Implementation — Jesper Bergman, Oliver Popov (2023). DOI:10.1109/access.2023.3255165

[\[7\]](#) Crawling the Dark Web: A Conceptual Perspective, Challenges and Implementation — Bassel Alkhatib, Randa Basheer (2019). DOI:10.6025/jdim/2019/17/2/51-60

[\[8\]](#) Perceptual Operating Systems for the Trade Associations of Cyber Criminals to Scrutinize Hazardous Content — Romil Rawat, Anand Rajavat (2024). DOI:10.4018/ijcwt.343314

[\[9\]](#) Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach — Saiba Nazah, Shamsul Huda, Jemal Abawajy, Mohammad Mehedi Hassan (2020).

DOI:10.1109/access.2020.3024198 [10] Mining the Dark Web: A Novel Approach for Placing a Dark Website under Investigation — Bassel Alkhatib, Randa Basheer (2019). DOI:10.5815/ijmecs.2019.10.01

Sources

- [1] **Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web** — Ahmed Ghappour (2017). eYLS (Yale Law School).
- [2] **Crawling and Mining the Dark Web: A Survey on Existing and New Approaches** — Mohammed Khalafallah Alshammery, Abbas Fadhil Aljuboori (2022). Iraqi Journal of Science. <https://doi.org/10.24996/ijcs.2022.63.3.36>
- [3] **Investigating The Darknet** — Rachid Bou Zeid, Joanna Moubarak, Carole Bassil (2020). <https://doi.org/10.1109/iwcmc48107.2020.9148422>
- [4] **Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers** — Gemma Davies (2020). The Journal of Criminal Law. <https://doi.org/10.1177/0022018320952557>
- [5] **Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web** — Seunghyeon Lee, Changhoon Yoon, Heedo Kang, Yeonkeun Kim, Yongdae Kim, Dongsu Han et al. (2019). <https://doi.org/10.14722/ndss.2019.23055>
- [6] **Exploring Dark Web Crawlers: A Systematic Literature Review of Dark Web Crawlers and Their Implementation** — Jesper Bergman, Oliver Popov (2023). IEEE Access. <https://doi.org/10.1109/access.2023.3255165>
- [7] **Crawling the Dark Web: A Conceptual Perspective, Challenges and Implementation** — Bassel Alkhatib, Randa Basheer (2019). Journal of Digital Information Management. <https://doi.org/10.6025/jdim/2019/17/2/51-60>
- [8] **Perceptual Operating Systems for the Trade Associations of Cyber Criminals to Scrutinize Hazardous Content** — Romil Rawat, Anand Rajavat (2024). International Journal of Cyber Warfare and Terrorism. <https://doi.org/10.4018/ijcwt.343314>
- [9] **Evolution of Dark Web Threat Analysis and Detection: A Systematic Approach** — Saiba Nazah, Shamsul Huda, Jemal Abawajy, Mohammad Mehedi Hassan (2020). IEEE Access. <https://doi.org/10.1109/access.2020.3024198>
- [10] **Mining the Dark Web: A Novel Approach for Placing a Dark Website under Investigation** — Bassel Alkhatib, Randa Basheer (2019). International Journal of Modern Education and Computer Science. <https://doi.org/10.5815/ijmecs.2019.10.01>

Article généré automatiquement par IA à partir des seules sources citées, à des fins de vulgarisation. Modèle : glm-4.7-flash:latest · 116 s. À vérifier auprès des sources primaires ; ne constitue pas un avis d'expert.
SciencesWiki — <https://scienceswiki.eu>