UNIVERSITAS
GADJAH MADA
**IMPLEMENTASI MULTI-STAGE RISK DETECTION TOOL PADA BROWSER EXTENSION DENGAN ACTIVE TERMINATION**
Salma Nur Jihan, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
**Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/**

# DAFTAR PUSTAKA

[1] Kaspersky, "1.3 Million Users Encountered *Browser Extension Threat*s in the First Half of 2022," Aug. 16, 2022. Available: https://www.kaspersky.com/about/press-releases/13-million-users-encountered-*browser-extension-threat*s-in-the-first-half-of-2022

[2] Y. Wang, W. Cai, P. Lyu, and W. Shao, "A Combined Static and *Dynamic analysis* Approach to Detect *Malicious Browser Extension*s," *Security and Communication Networks*, vol. 2018, pp. 1–16, May 2018. doi: 10.1155/2018/7087239.

[3] A. Fass, R. P. Krawczyk, M. Backes, and B. Stock, "JaSt: Fully Syntactic Detection of *Malicious* (Obfuscated) Javascript," in *Proc. 15th Int. Conf. Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2018)*, Lecture Notes in Computer Science, vol. 10885, Springer, Cham, Jun. 2018, pp. 303–325. doi: 10.1007/978-3-319-93411-2_14.

[4] S. B. Seetharam, M. Nabeel, and W. Melicher, "*Malicious* GenAI Chrome *Extension*s: *Unpacking Data exfiltration* and *Malicious Behaviour*s," presented at *Virus Bulletin Conference (VB2025)*, Berlin, Sep. 2025, arXiv:2512.10029. [Online]. Available: https://arxiv.org/abs/2512.10029

[5] A. Cohen, "JavaSith: A Client-Side *Framework* for Analyzing Potentially *Malicious Extension*s in *Browser*s, VS *Code*, and NPM Packages," arXiv:2505.21263, May 2025. [Online]. Available: https://arxiv.org/abs/2505.21263

[6] J. M. Moreno, N. Vallina-Rodriguez, and J. Tapiador, "Fakeium: A *Dynamic* Execution Environment for Javascript Program *Analysis*," *SoftwareX*, vol. 32, Sep. 2025. doi: 10.1016/j.softx.2025.102301.

[7] S. Singh, G. Varshney, T. K. Singh, V. Mishra, and K. Verma, "A Study on *Malicious Browser Extension*s in 2025," arXiv:2503.04292, Mar. 2025. [Online]. Available: https://arxiv.org/abs/2503.04292

UNIVERSITAS
GADJAH MADA
**IMPLEMENTASI MULTI-STAGE RISK DETECTION TOOL PADA BROWSER EXTENSION DENGAN ACTIVE TERMINATION**
Salma Nur Jihan, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
**Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/**

[8] V. Mishra, "Securing the *Browser*: A *Hybrid Static analysis Framework* for Detecting *Malicious* Chrome *Extension*s *via* Local *Threat Intelligence*," *International Journal of Latest Technology in Engineering, Management & Applied Science*, vol. 15, no. 1, pp. 1259–1269, 2026. doi: 10.51583/IJLTEMAS.2026.1501000102.

[9] C. Curtsinger, B. Livshits, B. Zorn, and C. Seifert, "ZOZZLE: Fast and Precise In-*Browser* Javascript *Malware* Detection," in *Proc. 20th USENIX Security Symposium (USENIX Security 11)*, San Francisco, CA, Aug. 2011, pp. 33–48. [Online]. Available: https://www.usenix.org/conference/usenix-*security*-11/zozzle-fast-and-precise-*browser*-javascript-*malware*-detection

[10] M. AbdelKhalek and A. F. Shosha, "JSDES: An Automated De-*Obfuscation* System for *Malicious* Javascript," in *Proc. 12th Int. Conf. Availability, Reliability and Security (ARES 2017)*, Reggio Calabria, Italy, Aug.–Sep. 2017, Article 80, pp. 1–13. doi: 10.1145/3098954.3107009.

[11] O. Starov and N. Nikiforakis, "Extended Tracking Powers: Measuring the Privacy Diffusion Enabled by *Browser Extension*s," in *Proc. 26th Int. Conf. World Wide Web (WWW 2017)*, Perth, Australia, Apr. 2017, pp. 1481–1490. doi: 10.1145/3038912.3052596.

[12] R. Perrotta and F. Hao, "Botnet in the *Browser*: Understanding *Threat*s Caused by *Malicious Browser Extension*s," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 66–81, Jul./Aug. 2018. doi: 10.1109/MSP.2018.3151234.

[13] Google LLC, "Chrome *Extension*s — *Manifest File* Format," Google for *Developer*s, 2024. [Online]. Available: https://*developer*.chrome.com/docs/*extension*s/mv3/*manifest*/

[14] Google LLC, "Chrome *Extension*s — *Permission*s," Google for *Developer*s, 2024. [Online]. Tersedia: https://*developer*.chrome.com/docs/*extension*s/mv3/declare_*permission*s/

[15] J. M. Moreno, N. Vallina-Rodriguez, dan J. Tapiador, "Did I Vet You Before?

UNIVERSITAS
GADJAH MADA
**IMPLEMENTASI MULTI-STAGE RISK DETECTION TOOL PADA BROWSER EXTENSION DENGAN ACTIVE TERMINATION**
Salma Nur Jihan, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
**Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/**

Assessing the Chrome *Web store* Vetting Process through *Browser Extension* Similarity," arXiv:2406.00374, Jun. 2024. [Online]. Tersedia: https://arxiv.org/abs/2406.00374

[16] Sekoia *Threat Intelligence Team*, "Targeted *Supply chain* Attack Against Chrome *Browser Extension*s," *Sekoia.io Blog*, Jan. 10, 2025. [Online]. Tersedia: https://blog.sekoia.io/targeted-supply-chain-attack-against-chrome-*browser-extension*s/

[17] The Hacker News, "Trust Wallet Chrome *Extension* Hack Drains $8.5M *via* Shai-Hulud *Supply chain* Attack," Jan. 2, 2026. [Online]. Tersedia: https://thehackernews.com/2025/12/trust-wallet-chrome-*extension*-hack.html

[18] K. Pandya, "5 *Malicious* Chrome *Extension*s Enable Session Hijacking in Enterprise HR Platforms," *Socket Threat Research Team*, Jan. 15, 2026. [Online]. Tersedia: https://socket.dev/blog/5-*malicious*-chrome-*extension*s-enable-session-hijacking

[19] OWASP Foundation, "Vulnerability *Scanning Tool*s," OWASP, 2024. [Online]. Tersedia: https://owasp.org/www-community/Vulnerability_*Scanning*_*Tool*s

[20] CircleCI, "SAST vs DAST: What They Are and When to Use Them," *CircleCI Blog*, 2024. [Online]. Tersedia: https://circleci.com/blog/sast-vs-dast-when-to-use-them/

[21] Imperva, "What Is *Malware Sandbox*ing: *Analysis* and Key Features," *Imperva Learning Center*, 2024. [Online]. Tersedia: https://www.imperva.com/learN/*Application-security*/*malware-sandbox*ing/

[22] GeeksforGeeks, "*Dynamic Malware Analysis*," *GeeksforGeeks*, 2024. [Online]. Tersedia: https://www.geeksforgeeks.org/ethical-hacking/*dynamic-malware-analysis*/

[23] M. A. Sarker, H. Janicke, L. Maglaras, and B. Crispo, "Hiding in Plain Sight:

UNIVERSITAS
GADJAH MADA
**IMPLEMENTASI MULTI-STAGE RISK DETECTION TOOL PADA BROWSER EXTENSION DENGAN ACTIVE TERMINATION**
Salma Nur Jihan, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
**Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/**

Detecting Javascript *Obfuscation* through Concealment of Overlong *Identifier*s," in *Proc. ACM Internet Measurement Conf. (IMC 2020)*, Pittsburgh, PA, Oct. 2020, pp. 648–661. doi: 10.1145/3419394.3423624.

[24] I. Sanchez-Rola, I. Santos, and D. Balzarotti, "*Extension* Breakdown: *Security Analysis* of *Browser*s *Extension* Re*source*s Control Policies," in *Proc. 26th USENIX Security Symposium*, Vancouver, BC, Aug. 2017, pp. 679–694.

[25] P. Karthikeyan and M. Nandha Kumar, "*Obfuscation* Techniques in *Malware*: A Survey," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 3, 2017.

[26] Microsoft, "Playwright Documentation," Microsoft Open *Source*, 2024. [Online]. Available: https://playwright.dev/docs/intro

[27] A. Shlyapnikov, "mitmproxy: An Inter*active* TLS-Capable Intercepting HTTP Proxy," 2024. [Online]. Available: https://mitmproxy.org/

[28] Google LLC, "chrome.*management* ," *Chrome for Developers*, 2024. [Online]. Tersedia: https://*developer*.chrome.com/docs/*extension*s/reference/api/*management*

[29] Google LLC, "*Native messaging*," *Chrome for Developers*, 2024. [Online]. Tersedia: https://*developer*.chrome.com/docs/*extension*s/develop/concepts/native-messaging

[30] M. Haverbeke and *Open-source* contributors, "Acorn — A Small, Fast, Javascript-*based* Javascript Parser," GitHub, 2024. [Online]. Available: https://github.com/acornjs/acorn

[31] M. Bonnet and *Open-source* contributors, "A*string* — Javascript *Code* Generator from an ESTree-compliant AST," GitHub, 2024. [Online]. Available: https://github.com/davidbonnet/a*string*

[32] Docker, Inc., "Docker Documentation," 2024. [Online]. Available:

UNIVERSITAS
GADJAH MADA
**IMPLEMENTASI MULTI-STAGE RISK DETECTION TOOL PADA BROWSER EXTENSION DENGAN ACTIVE TERMINATION**
Salma Nur Jihan, Ir. Unan Yusmaniar Oktiawati, S.T., M.Sc., Ph.D., IPU.
**Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/**

https://docs.docker.com/

[33] BI.zone and *Open-source* contributors, "Box.js — A *Tool* for Studying Javascript *Malware*," GitHub, 2024. [Online]. Available: https://github.com/BI-ZONE/box-js

[34] Pallets, "Flask Documentation," Pallets Projects, 2024. [Online]. Available: https://flask.palletsprojects.com/