Виявлення і аналіз обмежень існуючих практик DNS-тунелювання шляхом моделювання заходів обходу мережевої фільтрації

УДК 004.7.056

Кирило Оніщенко[1], Юрій Дорофєєв[2], Ірина Назарова[3]

Національний університет «Одеська політехніка»,
[1]kirill93549@stud.op.edu.ua, [2]dym@op.edu.ua, [3]nazarova.i.v@op.edu.ua

У сучасних мережах протокол DNS залишається критичним і часто найбільш вразливим вектором атак. Через архітектурну необхідність підтримки Captive-порталів (сторінок авторизації або поповнення рахунку за нульового балансу) та політик безкоштовного трафіку, провайдери змушені залишати 53-й порт (UDP/TCP) відкритим для проходження базових запитів. Як свідчить аналіз ландшафту сучасних загроз [1], зловмисники та APT-угруповання (наприклад, автори інструментарію Decoy Dog [2] або ChamelDoH [3]) масово відмовляються від класичних утиліт на кшталт iodine чи dnscat2. Замість цього вони розробляють спеціалізовані протоколи інкапсуляції, які легко обходять системи глибокого аналізу трафіку шляхом динамічної зміни структури пакетів та експлуатації станів “Fail-Open” під час високих навантажень на мережеве обладнання. Таким чином, статичні сигнатурні правила більше не є ефективними проти нестандартного зашифрованого DNS-трафіку. Стає необхідним перехід від сигнатурного виявлення до проактивного тестування стійкості мережевих периметрів.

У цих умовах стають актуальними розробка методів виявлення вразливостей мережевого обладнання від атак, описаних вище, проведення аудиту безпеки та виявлення недоліків у DPI-системах національних операторів зв'язку та інтернет-провайдерів [4, 5].

Метою роботи є виявлення і аналіз обмежень існуючих підходів DNS-тунелювання шляхом моделювання методів обходу мережевої фільтрації.

Для реалізації такого моделювання пропонується виконання комплексу дій:

- використання методу динамічної обфускації, в якому застосування XOR-маски з випадковим початковим байтом усуває будь-які статичні сигнатури в пакетах;
- інтеграція логічного рівня надійної доставки (модель ковзного вікна Sliding Window) із селективними підтвердженнями SACK поверх UDP;
- суворе дотримання структури (Base32-кодування субдоменів з обмеженням upstream-навантаження), яке забезпечує стійкість протоколу до втрати пакетів та невидимість для фільтрів форматування.

Виходячи із запропонованого комплексу дій, основним завданням є розробка PoC-версії спеціалізованого протоколу DNS-тунелювання для проведення безпечного аудиту. У подальшому практичну апробацію цього протоколу планується провести у контрольованому середовищі, яке імітує мережі операторів мобільного зв’язку.

Результати попередніх тестувань, проведених в ізольованих тестових мережах, продемонстрували, що актуальні DPI-системи є вразливими до

базових технік інкапсуляції та безперешкодно пропускають трафік тестових DNS-тунелів. Цей факт підтверджує наявність вразливостей і обґрунтовує необхідність глибокого моделювання методів обходу фільтрації, для чого проєктований протокол виступатиме основним інструментом тестування.

Попередній аналіз підтверджує, що традиційні DPI-рішення провайдерів, орієнтовані на сигнатурний пошук, є критично вразливими до методів динамічної обфускації та нестандартного шифрування на рівні DNS. Для надійного захисту інфраструктури та закриття цих "сліпих зон" необхідно змістити фокус із прямої інспекції корисного навантаження на евристичні моделі. Ефективна протидія сучасним прихованим каналам зв'язку потребує впровадження систем поведінкового аналізу на базі машинного навчання [6], здатних своєчасно виявляти аномалії та нетипові патерни DNS-комунікації.

1. Duan R., Liu D. Understanding DNS Tunneling Traffic in the Wild. Unit 42, Palo Alto Networks. 2023. URL: https://unit42.paloaltonetworks.com/dns-tunneling-in-the-wild/
2. Decoy Dog Is No Ordinary Pupy – Infoblox Reveals Shift in Malware Tactics After Initial Discovery. Infoblox. 2023. URL: https://www.infoblox.com/news/news-events/press-releases/decoy-dog-is-no-ordinary-pupy-infoblox-reveals-shift-in-malware-tactics-after-initial-discovery/
3. Mayer D. ChamelGang and ChamelDoH: A DNS-over-HTTPS implant. Stairwell Threat Research. 2023. URL: https://blog.netmanageit.com/content/files/2023/06/Report-ChamelGang-and-ChamelDoH-A-DNS-over-HTTPS-implant.pdf
4. Amirov N., Isik B., Tuncer B. I., Bahtiyar S. DNS Tunneling: Threat Landscape and Improved Detection Solutions. arXiv preprint arXiv:2507.10267. 2025. URL: https://arxiv.org/abs/2507.10267
5. Salat L., Davis M., Khan N. DNS Tunnelling, Exfiltration and Detection over Cloud Environments. Sensors. 2023. Vol. 23, №5. P. 2760. DOI: 10.3390/s23052760
6. Ali F., Afaq M., Niazi M., Behzad M. From Graphs to Gates: DNS-HyXNet, A Lightweight and Deployable Sequential Model for Real-Time DNS Tunnel Detection. arXiv preprint arXiv:2512.09565. 2025. URL: https://arxiv.org/abs/2512.09565

GPU-Adapted Compact Hashing with Bitonic Sort for Neighborhood Search in SPH

UDC 004.94 (043.2)

Ostap Hrytsyshyn[1], Valeriy Trushevskyy[2]

Ivan Franko National University of Lviv, [1]ostap.hrytsyshyn@lnu.edu.ua, [2]valeriy.trushevsky@lnu.edu.ua

Smoothed Particle Hydrodynamics (SPH) is a Lagrangian particle-based method widely used for simulating fluid dynamics. Each particle interacts only with neighbors