Вертиполох О.О., Ільєнко А.В.

Національний авіаційний університет, м.Київ

СУЧАСНИЙ СТАН ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ТРАФІКУ ВІД ВТРУЧАННЯ DPI СИСТЕМ

Резюме.

Аналіз мережевого трафіку є все більш поширеним засобом виявлення загроз безпеки, на жаль, такі методи аналізу часто призводять до порушення конфіденційності. Хоча DPI системи і можуть використовуватися у благих цілях, як частина IPS/IDS – систем попередження та виявлення вторгнень або для запобігання атакам типу DDoS за допомогою аналізу трафіку у реальному часі, системи DPI все частіше використовуються для фільтрації трафіку, блокування мережевих протоколів та цензурування загалом, що призвело до створення чисельних інструментів обходу таких блокувань.

Ключові слова:

Протокол, аналіз трафіку, DPI, TLS, HTTPS, VPN, проксі, обфускація, фронтінг домену, маршрутизація приманки.

Abstract.

Network traffic analysis is an increasingly common means of detecting security threats, unfortunately such analysis methods often lead to privacy violations. Although DPI systems can be used for good purposes, as part of IPS (Intrusion Prevention System) / IDS (Intrusion Detection System) or to prevent DDoS attacks through real-time traffic analysis, DPI systems are increasingly used for traffic filtering, network protocol blocking and censorship in general, which led to the creation of numerous circumvention tools.

Keywords:

Protocol, traffic analysis, DPI, TLS, HTTPS, VPN, proxy, obfuscation, domain fronting, decoy routing.

Традиційний аналіз пакетів зазвичай перевіряє інформацію в заголовках

пакетів мережевого та транспортного рівнів. DPI виконує, так званий, глибокий аналіз мережевих пакетів, серед яких є: поведінковий аналіз трафіку у режимі реального часу, наприклад, співвідношення вхідного та вихідного трафіку, періодичність запитів та відповідей, що дозволяє розпізнавати стандартні протоколи, а також інші, що можуть маскуватися під них з метою приховування, та сигнатурний аналіз, що дозволяє зіставляти заголовки та структуру пакетів зі зразками, таким чином визначаючи його призначення, наприклад, VPN-тунель, SOCKS/HTTP-проксі або користувацький додаток. Таким чином приналежність трафіку, категоризація якого може бути корисною в рамках DPI, можна розбити на декілька груп:

- широко використовувані та загальновідомі протоколи (HTTPS, TLS);
- протоколи додатків (прикладне ПЗ, месенджери, ігрові клієнти);
- VPN тунелі та проксі (OpenVPN, Wireguard, IPSec, SOCKS);
- протоколи, що можуть використовуватися як транспорт подвійного призначення (SSH);
- інші з’єднання, тип яких не вдалося встановити.

Як було вказано в резюме, DPI системи можуть виступати частиною систем захисту мережі, водночас час інші ситуації використання таких систем виглядають менш оптимістично: оператори зв’язку та провайдери можуть будувати поведінкову модель абонента, що дозволяє створити деякий цифровий відбиток користувача і використовувати його для оптимізації в свої цілях або як товар та продавати його третім особам – рекламодавцям та компаніям, що спеціалізуються на цьому, останні у свою чергу також продадуть або передадуть дані у розвідувальні агентства [1]. Але найголовнішим способом використання DPI стало його використання для блокування сервісів, додатків та протоколів, що успішно використовується у Китаї, Ірані, Єгипті, Саудівській Аравії, ОАЕ, Сирії, Малайзії, Венесуелі, Ефіопії, Азербайджані, Туркменістані, Туреччині, Казахстані, Білорусії та РФ, а також менш активно для вибіркового

блокування чи спостереження у США, Великобританії, Австралії та інших державах по всьому світу [2].

TLS – протокол безпеки транспортного рівня, швидко став найпопулярнішим протоколом в Інтернеті і завдяки своїй поширеності він є популярним протоколом для інструментів обходу блокування, але оскільки рукостискання TLS не зашифровані, DPI системи можуть використовувати дані, які відправляються у відкритому вигляді в першому повідомленні Client Hello, а широкий спектр функцій, підтримуваних в TLS, уможливлює здатність розрізняти реалізації одну від одної за набором шифрів, еліптичних кривих, алгоритмів підпису та інших розширень [3].

Варто згадати, що TLS працює поверх транспортного протоколу TCP, оскільки перший є окремим протоколом і спочатку передбачався для окремого використання, таким чином зашифрованим є лише корисне навантаження (payload) TLS-over-TCP пакету, а заголовки та поля є відкритими, що допомагає в аналізі. Своєю чергою, після 5 років розробки підходить до завершення реалізація протоколу QUIC, який базується на простому протоколі UDP, що відповідає лише за порти, а вся логіка від TCP, наприклад, процес рукостискання. підтвердження отримання пакетів та повторної передачі, буде знаходитися безпосередньо в цьому протоколі, але найголовніше нововведення те, що TLS тепер інтегровано у протокол, таким чином зашифрованими будуть, як і більшість заголовків пакету, так і метадані, а в самому протоколі передбачено легке створення розширень, що дасть поштовх для швидкого розгортання і його використання в якості інструменту протидії DPI, бо поверх нього вже працює HTTP/3.

HTTPS – безпечний протокол передачі гіпертекстових документів, що базується на TLS зайняв величезну нішу у створенні інструментів обходу тому, що складно піддається аналізу зі зіставленням зі зразками, а його блокування чи зниження швидкості позначатиме паралізацію роботи вебу. Широке

використання протоколу дозволило створити цілий механізм обходу блокування – фронтінг доменного імені (domain fronting), який використовує протокол HTTPS для спілкування із забороненим хостом, одночасно створюючи видимість спілкування з іншим хостом, що не є заблокованим, таким чином один домен з'являється ззовні запиту HTTPS – у запиті DNS та SNI – індикації імені сервера, тоді як інший домен з'являється всередині – у заголовку хосту HTTP запиту, який вже є зашифрованим та невидимим для систем аналізу [4].

VPN – віртуальні приватні мережі створені для побудови захищених тунелів між користувачем та іншим вузлом, зазвичай, сервером, можуть бути використані та для обходу блокувань, але найпоширеніші реалізації (OpenVPN, Wireguard, IPSec, L2TP) піддаються блокуванню через блокування портів, за допомогою аналізу пакетів або блокування IP-адрес сервісів, що надають послуги. В ряді країн доступ до VPN сервісів або повністю заблоковано і є навіть нелегальним, або дуже ускладнено через блокування [5].

У більшості країн, де VPN є заблокованим, під блокування підпадає і найбільш розповсюджений спосіб обходу – використання мережі Tor, яка використовує так звану цибулеву маршрутизацію (onion routing) з багатошаровим шифруванням та відправкою трафіку через декілька вузлів, які тримають волонтери та компанії, з забезпеченням прямої секретності. Підключення до мережі передбачає з’єднання з одним зі вхідних вузлів, список яких знаходиться у відкритому вигляді, тому підключення до них може бути легко заблоковане. Для протидії цьому існують мости (bridges) – вхідні вузли, адреси яких не публікуються в каталозі, але вони успішно блокуються у таких країнах як Китай чи Іран за допомогою активного зондування (active probing), спочатку виконуючи пошук потенційних зв’язків Tor на основі списку шифрів клієнтів TLS, і, якщо така сигнатура виявлена, виконується підключається до підозрюваного мосту зі спілкуванням з ним за протоколом Tor, з подальшим внесенням адреси цього мосту у чорний список. Для обходу використовуються

розширення підключення транспорту (pluggable transport). На цей час серед таких активно використовуваних транспортів можна виділити [6, 7]:

1. obfs4 – заснований на ідеях попередника ScrambleSuit, який захищає від атак активного зондування, здатний змінювати відбиток трафіку (розподіл довжин пакетів, час між обміном даними тощо). Новостворений транспорт використовує обфускацію публічних ключів без їх розкриття за допомогою математичного алгоритму, бо вони призначені для передачі у відкритому вигляді, то DPI системи можуть знаходити їх серед трафіку, та використовує протокол односторонньої аутентифікації, таким чином трафік виглядає абсолютно випадковим.

2. meek – використовує фронтінг домену з використанням Google App Engine, таким чином для DPI систем трафік від користувача здається звичайним HTTPS трафіком з відвідуванням незаблокованих серверів, існує реалізація meek-azure з використанням серверів Microsoft. На жаль через вже описані проблеми TLS, цей транспорт інколи може бути заблокований за допомогою створення цифрового відбитка (fingerprinting) TLS підключення, що було випробувано у Турції.

3. Snowflake – використовує фронтінг домену для підключення до проксі, які включені у волонтерів, а сам транспорт використовує WebRTC – протокол підключення клієнт-клієнт для комунікації у режимі реального часу.

Такі транспорти використовуються не тільки для мережі Tor, meek, наприклад, також використовується в Psiphon – мережі із тисяч проксі серверів по всьому світу. Додатково він використовує інший транспорт – обфускований SSH, мета якого протистояти DPI системам для фінгерпрінтингу підключення, а список серверів розташовано і завантажується зі хмарного сховища AWS S3, що ускладнює його блокування [8].

Популярним проксі протоколом є Shadowsocks, який використовує SOCKS5 та дозволяє передавати і TCP, і UDP трафік, може протидіяти атакам

повторного відтворення (replay attack) і успішно дозволяє обходити Великий Китайський Фаєрвол, хоча останній і намагається блокувати його за допомогою атак активного зондування [9]. Протокол підтримує плагіни, наприклад, для включення фронтінгу домену (GoQuiet, Cloak) або пересилки shadowsocks поверх Websockets чи QUIC (V2ray).

Іншим підходом є розташування проксі серверів не на кінцях мережевого підключення, а посередині (end-to-middle – E2M), така реалізація має назву маршрутизація приманки (decoy routing), яка передбачає розгортання маршрутизаторів в мережах доброзичливих провайдерів, які знаходяться між цензурованими користувачами та незаблокованими адресами (приманками) [10]. Клієнт підключається до місця приманки, після надсилає прихований сигнал з інформацією, що сигнал потрібно підмінити (hijack), після чого приманка функціонує як стандартний проксі SOCKSv5, а трафік тегується і може бути виявлено лише спеціальними маршрутизаторами. Серед реалізацій можна виділити Telex, Cirripede. TapDance, Rebound та Slitheen, останні два намагаються зменшити можливість виявлення DPI системами на базі аналізу розмірів пакетів, затримок у мережі тощо.

Висновки.

Питання захисту мережевого трафіку є і завжди буде актуальним, провідні IT компанії розробляють та активно впроваджують нові мережеві стандарти та протоколи, що роблять Інтернет більш безпечним, швидким та ефективним, а одночасно з ними інші компанії, провайдери та держави намагаються протидіяти цьому, витискаючи максимум корисної інформації навіть зі зашифрованих комунікацій. На жаль, DPI системи стали компаньйонами мережевих екранів з метою фільтрації трафіку, блокування протоколів та цензурування загалом, що перетворилося в перегони озброєнь між звичайними користувачами, які намагаються захистити трафік вже не тільки від зловмисників, а і від розробників та користувачів таких систем.

Література:

1. How Data Brokers Sell Access to the Backbone of the Internet [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru

2. Use of deep packet inspection to censor the Internet [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://blog.torproject.org/category/tags/deep-packet-inspection

3. Sergey Frolov, Eric Wustrow. The use of TLS in Censorship Circumvention. 2019 – 15 с.

4. David Fifield, Chang Lan, Rod Hynes, Percy Wegmann, Vern Paxson. Blocking-resistant communication through domain fronting. 2015. – 19 с.

5. Countries that have banned VPNs [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://protonvpn.com/blog/are-vpns-illegal/

6. Tor: Pluggable Transports [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://2019.www.torproject.org/docs/pluggable-transports

7. Snowflake Technical Overview [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://keroserene.net/snowflake/technical/

8. Psiphon Guide [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://psiphon.ca/en/psiphon-guide.html

9. Shadowsocks Protocol [Електронний ресурс] – Режим доступу: World Wide Web. – URL: https://shadowsocks.org/en/wiki/Protocol.html

10. Josh Karlin, Daniel Ellard, Alden W. Jackson, Christine E. Jones, Greg Lauer, David P. Mankins, W. Timothy Strayer. Decoy Routing: Toward Unblockable Internet Communication. 2011. – 6 с.