УДК 004.056.53

Байлюк Є. М., асистент,
Непша І. О., студент
Державний університет «Житомирська політехніка»

АНАЛІЗ ПРОТОКОЛУ DNS OVER HTTPS

В сучасному світі інформаційних технологій однією з найактуальніших проблем є збереження конфіденційності даних, що передаються в мережі Інтернет. Незалежно від того, що користувач шукає в Інтернеті – вдома, на роботі чи в дорозі на особистому пристрої, є віртуальна стежка, доступна практично кожному, хто знає, як і де шукати. Навіть якщо користувач відвідує сайт за допомогою HTTPS, його DNS-запит надсилається через незашифроване з'єднання., інші пристрої можуть також збирати (або навіть блокувати або змінювати) ці дані. Друга проб-лема з незашифрованим DNS полягає в тому, що зловмисник, який діє за сценарієм атаки «Людина посередині», може змінити відповіді DNS на зловмисне програмне забезпечення або на сайт зловмисного спостереження, за допомогою яких він може зібрати конфіденційні дані користувача. Для боротьби з цією проблемою Cloudflare пропонує використовувати DNS через кінцеву точку HTTPS (DNS over HTTPS) замість надсилання DNS-запитів через відкритий текст для підвищення безпеки.

DNS over HTTPS (DoH) – це протокол для виконання віддаленого дозволу системи доменних імен (DNS) через протокол HTTPS. Метою цього протоколу є підвищення конфіденційності та безпеки користувачів, запобігаючи підслуховуванню та маніпулюванню даними DNS за допомогою атак виду «Людини посередині» за допомогою протоколу HTTPS для шифрування даних між клієнтом та сервером DNS. До бе-резня 2018 року Google та Mozilla Foundation розпочали тестування вер-сій DNS over HTTPS. У лютому 2020 року Mozilla випустила версію Firefox, яка шифрує доменні імена за замовчуванням для користувачів із США.

DNS через HTTPS є більш безпечним, ніж традиційний DNS, оскіль-ки він використовує захищене, зашифроване з'єднання. Використання DNS через HTTPS означає, що ваш Інтернет-провайдер та будь-яка інша сторона не зможуть побачити певні аспекти процесу пошуку DNS, ос-кільки вони будуть зашифровані [1].

По суті, нещодавнє повідомлення Firefox про перехід на DNS через HTTPS включатиме: шифрування всіх запитів DNS за допомогою DNS через HTTPS; безпечне вирішення DNS-запитів, використовуючи Cloudflare як довірений рекурсивний резолютор.

Таким чином, змушуючи DNS-запити користувачів США проходити через DNS-сервери Cloudflare, використовуючи HTTPS замість UDP, означає, що запити доменних імен будуть вирішені довіреною особою, а певні частини запитів DNS самі будуть зашифровані.

Переваги DNS over HTTPS. Оскільки DNS over HTTPS по суті шифрує запити на підключення до веб-сайтів для користувачів, які використовують браузер Firefox, він допомагає підвищити безпеку організації, не перешкоджаючи можливості команди IT-безпеки контролювати мережевий трафік веб-сайту.

Серед переваг DNS over HTTPS можна виділити наступні: DoH пропонує більшу загальну конфіденційність для користувачів щодо їх запитів; DoH пом'якшує можливість підслуховування та реалізації атак виду «Людина посередині»; DoH мінімізує можливість підробки DNS.

Недоліки DNS over HTTPS. Як і будь-яка технологія, протокол DoH не є ідеальним. Ось декілька можливих недоліків DNS щодо HTTPS, про які слід знати:

1. DoH за замовчуванням обходить локальний DNS-дозвіл.
2. Довірені рекурсивні резолютори, як Cloudflare, бачать запити користувачів.
3. Запити, здійснені через DoH, можуть призвести до більш повільного часу реагування[2].

Таким чином, зараз відбувається чимало змін, що стосуються конфіденційності даних та безпеки веб-сайту. Законодавство про безпеку даних впроваджується впродовж останніх кількох років – GDPR, CCPA, Закон про SHIELD Нью-Йорку та ін. Незважаючи на недоліки, які в майбутньому можуть бути усунуті, протокол DNS over HTTPS необхідно використовувати під час передачі конфіденційних даних в мережі Інтернет.

Список використаних джерел

1. DNS over HTTPS. URL: https://developers.cloudflare.com/1.1.1.1/ dns-over-https/ (дата звернення 24.03.2020).
2. DoH! Firefox Engages More Secure DNS Over HTTPS Protocol. URL: https://www.thesslstore.com/blog/doh-firefox-engages-more-secure-dns-over-https-protocol-heres-what-that-means-for-you/ (дата звернення 25.03.2020).