УДК 004[056.53+413.4]

**Антонішин М.В.,**
orcid.org/0000-0002-2665-0066,
**Дорогий Я.Ю.,** к.т.н.,
orcid.org/0000-0003-3848-9852,
**Міснік О.І.,**
orcid.org/0000-0002-4654-9125,
**Цуркан В.В.,** к.т.н.,
orcid.org/0000-0003-1352-042X

# ПОШУК РЕАЛЬНИХ МЕРЕЖЕВИХ АДРЕС ВЕБ ЗАСТОСУНКІВ ВИКОРИСТАННЯМ СЕРВІСУ CDN

**Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України**

antonishin.mihail@gmail.com
argusyk@gmail.com
oleksii.misnik@gmail.com
v.v.tsurkan@gmail.com

## *Вступ*

Пошук реальних мережевих адрес веб застосунків необхідний для виявлення уразливостей їх конфігурування. Дане завдання виконується при використанні різноманітних сервісів. Серед них виокремлюється сервіс на основі мереж доставляння контенту (англ. Content Delivery Network, CDN).

Аналіз публікацій, у яких розкривається використання сервісу CDN для забезпечення безпеки та пришвидшення функціонування веб застосунків, показав зосередженість переважно на описанні його технічних можливостей. Цим ускладнюється виявлення уразливостей програмного забезпечення, умов надання надійних функцій забезпечення безпеки сервісом CDN, а також його використання при конфігуруванні веб застосунків.

Наприклад, в [1] описано технічні характеристики одного з найбільш відомих різновидів сервісу CDN – Cloudflare. Він використовується для забезпечення безпеки від хакерських атак, DDoS-атак та реалізувань інших загроз [2]. Крім того ним автоматизується доставляння даних веб застосунків. При цьому поза увагою залишено розглядання наслідків, до настання яких може призвести експлуатування загрозами уразливостей конфігурування веб застосунків на основі сервісу Cloudflare.

У [3] проаналізовано інформаційні технології проведення веб застосунками банківських транзакцій. Встановлено, що тільки третиною з них використовується сервіс Cloudflare задля забезпечення безпеки. Однак, при цьому також не приділено уваги вірогідним проблемам конфігурування веб застосунків, що можуть призвести до зменшення рівня забезпечення їх безпеки.

У [4-5] розглянуто приклад застосування методів проектування та оптимізування сервісу CDN. Запропоновано виділення ресурсів для побудови мережевої інфраструктури з урахуванням вартості віртуальних машин, мереж та сховищ даних.

З огляду на [1-5] актуальним є унеможливлення уразливого конфігурування веб застосунків до реалізування загроз їх безпеці. Насамперед встановлення реальності IP адреси та, як наслідок, обходження функцій сервісу CDN. Це обумовлено тим, що її маскуванням визначається забезпеченість безпеки веб застосунків.

Отже, пошук реальних мережевих адрес веб застосунків використанням сервісу CDN є актуальним завданням.

### *Мета*

Метою є підвищення результативності пошуку реальних мережевих адрес веб застосунків за допомогою сервісу CDN. Для досягнення поставленої мети необхідно проаналізувати типові методи на прикладі їх програмних реалізацій, зокрема, показати застосовність при виявленні уразливостей конфігурування веб застосунків.

### *Основна частина*

Нині наявність уразливостей веб застосунків призводять до порушення властивостей інформації. Для запобігання цьому використовується сервіс CDN. Він характеризується можливостями як пришвидшення трафіку, так і наявністю функціоналу підвищення безпеки веб застосунків.

CDN – це географічно розподілена мережева інфраструктура [5-6], що дозволяє швидко передавати дані, наприклад: скрипти, зображення, відео. Доцільність її використання пов'язана з обробленням великих обсягів HTTPS трафіку через сервера CDN сервісу, зокрема, таких веб застосунків як Amazon.

Доступність інформації має пріоритетне значення, тому цим теж обумовлюється досить поширене використання CDN сервісу. CDN-мережами пропонується багато переваг для різних типів організацій. Серед таких переваг розглядаються [5]:

- зменшення швидкості роботи і часу відгуку на запити кінцевих користувачів;
- зменшення витрат на забезпечення необхідної пропускної здатності серверного обладнання;
- підвищення забезпеченості безпеки веб застосунків;
- масштабованість при надходженні великих обсягів трафіку від кінцевих користувачів;
- надійність доставки даних кінцевих користувачів.

При використанні сервісу CDN всі користувачі, що намагаються отримати доступ до контенту веб застосунку, використовують його кеш-версію з найближчого CDN-сервера. Це дозволяє пришвидшити завантаження і покращити доступність контенту у глобальній мережі Інтернет.

Використання сервісу CDN дозволяє направляти та аналізувати всі запити до веб застосунку через його сервери. У цьому випадку пропонується забезпечення безпеки використанням запитів DNS, перенаправленням HTTPS трафіку через CDN сервери та приховуванням реальної IP адреси серверу/веб застосунку (див. рис. 1). При спробі визначення реальної IP адреси отримується одна з пулу адрес сервісу CDN та можливість доступу до веб застосунку лише за допомогою доменного імені.

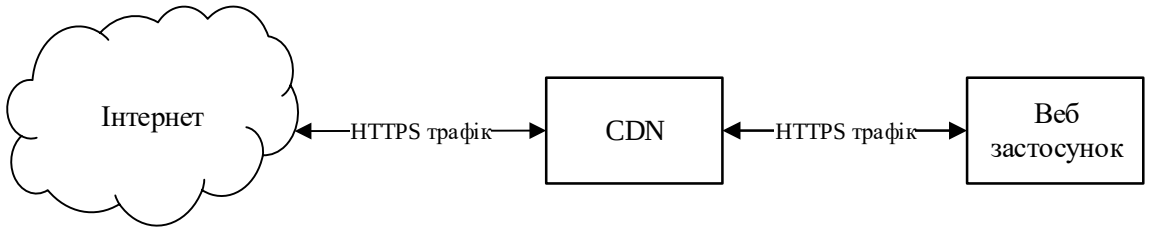


Рис. 1. Приклад використання сервісу CDN веб застосунками

Сервіс CDN характеризується наявністю додаткового функціоналу для покращення забезпеченості безпеки веб застосунків. Його використання дозволяє блокувати діяльність ботів, унеможливлювати експлуатування уразливостей за допомогою брандмауеру. Брандмауер веб застосунків допомагає захистити їх завдяки фільтруванню і відстеженню HTTPS трафіку між веб застосунком і глобальною мережею Інтернет через CDN сервер. До того ж протидіяти як міжсайтовому скриптингу (XSS), PHP-ін'єкціям, SQL-ін'єкціям.

При використанні сервісу CDN та його функціоналу приховується реальна

IP-адреса веб застосунку для запобігання DDoS-атакам зловмисників та доступу користувачів до нього через мережу CDN.

Однак, на практиці виконання цих завдань ускладнюється використанням хмарних технологій, проксі або служб на основі DNS. Зважаючи на це, оберемо найбільш популярні реалізації сервісу CDN та зіставимо за наявністю функціоналу брандмауера веб застосунків (див., наприклад [2, 6-9], табл. 1). Для цього за основу візьмемо інформацію від постачальників відповідних послуг.

Перевага використання брандмауерів на основі сервісу CDN полягає у налаштуванні DNS записів. Реалізування даної можливості є простою. Однак, з нею пов'язане існування проблем забезпечення безпеки веб застосунків. Так як знаходження реальної IP адреси їх серверу призводить до обходження функціоналу брандмауера.

Використаємо поширені реалізації сервісу CDN за табл. 1 для пошуку реальних IP адрес веб застосунків. Як припущення за основу взято її прихованість шляхом використання даного сервісу, зокрема, функціональних можливостей брандмауера.

Таблиця 1

| Назва сервісу CDN | Наявність брандмауера веб застосунків | Посилання на джерело |
|---|---|---|
| Cloudflare | + | https://www.cloudflare.com |
| Incapsula | + | https://www.imperva.com |
| F5 | + | https://www.f5.com/ |
| SUCURI | + | https://sucuri.net |
| Qrator | + | https://qrator.net |

Перед тестуванням веб застосунків виокремимо найбільш типові методи пошуку реальних мережевих адрес за сервісом CDN [10]:

1. Використання сервісів, які дозволяють переглядати поточні та архівні дані для будь-яких Інтернет-ресурсів, наприклад: історія IP і DNS, домену, SSL, відкриті порти. За отриманим результатом вивчаються всі DNS записи (A, AAA, CNAME або MX) як джерела реальної IP адреси.

2. Використання MX-записів як найбільш популярного джерела отримання реальних IP адрес. Наприклад, якщо поштовий сервер розміщено за аналогічною IP адресою з веб застосунком, то зловмисник може спробувати знайти його у вхідному повідомленні електронної пошти.

3. Надсилання листа електронною поштою за неправильною адресою. Завдяки цьому отримується відповідь поштового сервера. Це дозволяє перевірити заголовки листа на наявність інформації про домен, IP адресу. Її отримання може дозволити знайти реальну IP адресу веб застосунку.

4. Знаходження піддоменів для встановлення відсутності на них налаштувань сервісу CDN. Якщо вдалося їх знайти, то це дозволяє їх перевірити і, як наслідок, виявити реальні IP адреси серед прихованих. Після цього можна спробувати скористатися ними за допомогою командного рядка.

5. Отримання SSL сертифікату та інформації про інші піддомени, як наслідок, на їх основі знайти реальну IP адресу. Далі потрібно застосувати їх для веб застосунку, що аналізується.

6. Використання інформації за допомогою сервісу CrimeFlare. Ним накопичено базу IP адрес веб застосунків, безпека яких забезпечується використанням сервісу CDN.

7. Використання інструментів дослідження DNS імен. Ними виявляються IP адреси, що пов'язані з доменом, реальна мережева адреса якого шукається. Наприклад, завдяки сервісу DNSdumpster.com.

8. Проведення перебору субдоменів веб застосунку. Оскільки вони можуть функціонувати поза використанням сервісу CDN, з одного боку. Тоді як з іншого, мати одну й ту ж саму адресу з веб застосунком, що аналізується. При цьому можна знайти реальну IP адресу завдяки піддомену.

9. Використання IP адреси у HTML тегах та JavaScript коді. Це обумовлено залишанням такої інформації розробниками програмного забезпечення. Тому аналіз вихідних кодів на наявність вказаних IP адрес може бути корисним.

10. Використання сервісів пошуку IP адрес доменів, що можуть залишитися в кеші.

11. Використання спеціалізованих пошукових систем, наприклад, за допомогою Censys, Shodan.

12. Використання сервісів скорочених URL-адрес зі розширеною аналітикою трафіку за посиланнями. Це актуально за наявності функціоналу веб застосунків зі завантаженням, наприклад, фото за URL адресою. За допомогою даного сервісу можливо знайти IP адресу сервера.

Використання даних методів обумовлюється наявністю відповідної кваліфікації фахівця. Насамперед розуміння як використовується сервіс CDN для пошуку реальних мережевих адрес веб застосунків. Тому розглянемо відповідне програмне забезпечення.

Обиранню програмного забезпечення для тестування передує визначення його актуальності. Це означає, якщо спеціалізоване програмне забезпечення протягом останнього року не оновлювалося, то такий інструментальний засіб не можемо вважати актуальним. Оскільки існує можливість використання сторонніх сервісів, які вже припинили своє існування або змінилося їх застосування. Виокремимо основні параметри обирання спеціалізованого програмного забезпечення для тестування веб застосунків:

- дата оновлення програмного забезпечення;
- програмне забезпечення повинно бути з відкритим вихідним кодом, тобто не потребувати платної ліцензії для використання.

Таблиця 2

| Назва програмного забезпечення | Рік останнього оновлення | Можливість проведення тестування |
|---|---|---|
| Cloudflare-detect | 2017 | – |
| CloudFlair | 2018 | – |
| cloudflareBypasser | 2018 | – |
| Cloudfail | 2020 | + |
| HatCloud | 2018 | – |
| Bypass firewalls by DNS history | 2020 | + |

Програмне забезпечення за табл. 2 функціонує без втручання людини окрім введення доменного імені (посилання) веб застосунку для сканування. Перед початком його використання встановлюється придатність для ефективного вирішення поставлених перед ними завдань. Для цього визначається інформація про їх технічні специфікації. Тому в табл. 3 зведено перелік функціональних можливостей даного програмного забезпечення.

За табл. 3 встановлюються вірогідні шляхи пошуку прихованих реальних мережевих адрес веб застосунків. Зокрема, за своїми технічними характеристиками ні

CloudFail [11], ні Bypass firewalls by DNS history [12] не використовується всі можливі варіанти. У першому випадку унеможливлюється отримання доступу до історії IP адрес. Тоді як у другому – використання MX записів. Водночас аналіз даного програмного забезпечення не проводився.

Таблиця 3

| Назва програмного забезпечення | Функціонал програмного забезпечення | | | | |
|---|---|---|---|---|---|
| | Історія IP адреси | Підбір піддоменів | База даних Crimeflare | Використання DNS | Використання MX записів |
| Bypass firewalls by DNS history | + | + | + | + | – |
| CloudFlail | – | + | + | + | + |

Для проведення тестування обрано веб застосунок, яким використовується сервіс CDN, зокрема, Cloudflare. Наведемо перелік доменів веб застосунку, які знаходяться на різних фізичних серверах та мають різні IP-адреси:

- trustech.care;
- admin.trustech.care.

Програмне забезпечення CloudFail та Bypass firewalls by DNS history мають однакові алгоритми функціонування:

- завантажити вихідний код програмного забезпечення з відкритого репозиторію;
- встановити потрібні залежності для запуску обраного програмного забезпечення;
- запустити програмне забезпечення та вказати домені ім’я веб застосунку;
- проаналізувати звіт.

Почнемо з аналізу звіту Bypass firewalls by DNS history та бачимо, що за його допомогою знайдено реальну мережеву адресу веб застосунку trustech.care (див. рис. 2). Це стало можливим завдяки перевірці історії його IP адрес. При такому ж тестуванні admin.trustech.care реальну мережеву адресу не знайдено (див. рис. 3). Такий результат пояснюється зміненням розташування серверу веб застосунку після конфігурування сервісу CDN. У даному випадку є можливість обходу брандмауера для trustech.care.

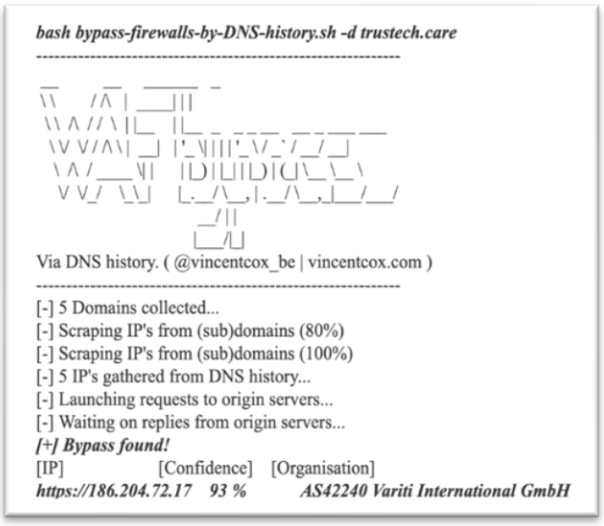


Рис. 2. Приклад пошуку реальної IP адреси веб застосунку trustech.care за допомогою Bypass firewalls by DNS history

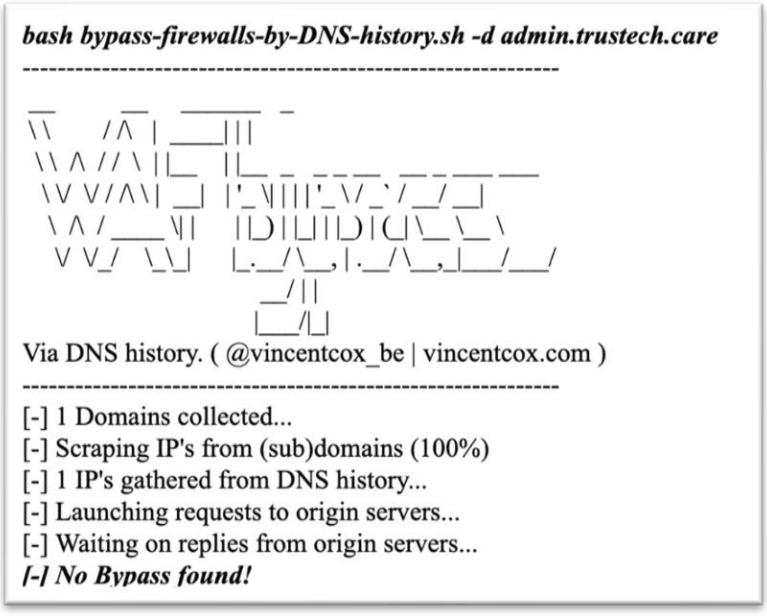


Рис. 3. Приклад пошуку реальної IP адреси веб застосунку admin.trustech.care за допомогою Bypass firewalls by DNS history

На наступному кроці розглянемо звіт за результатами використання Cloudfail. Ним демонструється зовсім інший результат. При скануванні веб застосунку trustech.care знайдено його піддомен admin.trustech.care. У даному випадку за табл. 3 бачимо, що у Cloudfail не має функціональної можливості перевіряти історію IP адрес веб застосунку, наявність якої виявилася вирішальною.


Рис. 3. Приклад пошуку реальної IP адреси веб застосунку trustech.care за допомогою Cloudfail

### *Висновки*

Проаналізувавши результати тестувань веб застосунків, встановлено, що Bypass firewalls by DNS history показав кращий результат, ніж Cloudfail. Як наслідок, встановлено недоліки його використання при знаходженні реальних мережевих адрес. Серед них найбільш суттєвою є

кількість перевірок, які використовуються даним програмним забезпеченням. Крім того його результативність обмежується, зокрема, відсутністю можливості переглядати історію IP адрес.

Тож за результатами даного дослідження встановлено, по-перше, різноманітність методів пошуку реальних мережевих адрес. По-друге, доцільність автоматизування даного процесу зі залученням фахівця тільки при введенні доменного імені або посилання на веб застосунок. Як наслідок, по-третє, потрібно передбачити можливості як використання, так і комбінування різних методів пошуку реальних мережевих адрес.

***Література***

1. *Estri D., Umar R., Riadi I.* Implementation of Cloudflare Hosting for Speeds and Protection on The Website. Fundamental and Applied Science for Advanced Technology: proceedings of conference. Yogyakarta. 21-22 January 2019. – Yogyakarta, 2019. [Electronic resource]. – Access mode: http://eprints.uad.ac.id/id/eprint/15073.

2. Understanding Cloudflares CDN [Electronic resource]. – Access mode: https://www.cloudflare.com/en-gb/.

3. *Солозобов О.* Анализ веб-технологий на сайтах легальных российских букмекеров. Наука, техника и образование. – 2019. – № 1 (54). – С. 50-55.

4. *Фабра С., Коновас С., Диаз Б., Бофриско Ф., Черных А.* Конструирование и оптимизация сетей распространения контента. Труды Института системного программирования РАН. – 2019. – Том 31, № 2. – С. 15-20.

5. *Majd N.E., Satyajayant Misra S., Tourani R.* Secure content delivery in information-centric networks: design, implementation, and analyses. ACM SIGCOMM workshop on information-centric networking: proceedings of workshop. Hong Kong. 12 August 2013. – Hong Kong, 2013. – P.73–78.

6. Incapsula: Protect your web applications and data [Electronic resource]. – Access mode: https://docs. imperva.com.

7. F5: Secure and deliver extraordinary digital experiences [Electronic resource]. – Access mode: https://F5.com.

8. SUCURI: we clean and protect websites [Electronic resource]. – Access mode: https://sucuri.net.

9. Qrator: DDoS Attacks Mitigation [Electronic resource]. – Access mode: https://qrator.net.

10. Ways to bypass CDN to find real IP [Electronic resource]. – Access mode: https://topic.alibabacloud.com/a/ 11-ways-to-bypass-cdn-to-find-real-ip_8_8_ 31062138.html.

11. CloudFail [Electronic resource]. – Access mode: https://github.com/ m0rtem/CloudFail.

12. Bypass firewalls by DNS history [Electronic resource]. – Access mode: https://github.com/vincentcox/bypass-firewalls-by-DNS-history.

**Антонішин М.В., Дорогий Я.Ю., Міснік О.І., Цуркан В.В.**

**ПОШУК РЕАЛЬНИХ МЕРЕЖЕВИХ АДРЕС ВЕБ ЗАСТОСУНКІВ ВИКОРИСТАННЯМ СЕРВІСУ CDN**

*Розглянуто завдання пошуку реальних мережевих адрес веб застосунків. Для цього використано сервіс на основі мереж доставляння контенту. З огляду на це проаналізовано відомі рішення і встановлено їх особливості використання. Серед них виокремлено орієнтованість даного сервісу на пришвидшення функціонування і забезпечення безпеки веб застосунків. Врахування цих особливостей ускладнюється зосередженістю уваги на описанні технічних можливостей відомих рішень. Цим обмежується виявлення уразливостей конфігурування веб застосунків. Для запобігання цьому використано можливості мереж доставляння контенту. За основу такого використання взято перенаправлення HTTPS трафіку через їх сервери та, як наслідок, приховування реальної IP адреси*

*веб застосунку. Виокремлено найбільш поширені реалізації сервісу на основі мереж доставляння контенту. Показано орієнтованість на застосування брандмауеру веб застосунків. Встановлено його застосовність при налаштуванні DNS запитів і знаходженні реальних мережевих адрес. Крім того виокремлено найбільш типові методи їх пошуку. Серед них акцентовано увагу на використанні сервісів переглядання поточних та архівних даних Інтернет-ресурсів; використанні MX записів як джерела IP адрес; надсиланні листів електронною адресою за вказаними (правильними, неправильними) електронним адресами; знаходженні піддоменів без налаштованого сервісу мереж доставляння контенту; отриманні SSL сертифікату; використанні інструментів дослідження DNS імен. Реалізування даних методів продемонстровано обраним програмним забезпеченням. Для цього введено критерії та зіставлено їх можливості. За результатами використання обраного програмного забезпечення показано обмеженість його функціональних можливостей. Для запобігання цьому рекомендовано комбінування методів пошуку реальних мережевих адрес веб застосунків використанням сервісу мереж доставляння контенту.*

***Ключові слова:*** *веб застосунок, мережева адреса, реальна мережева адреса, пошук реальної мережевої адреси, мережа доставляння контенту*

**Antonishyn M.V., Dorohyi Ya.Yu., Misnik O.I., Tsurkan V.V.**

**SEARCH OF REAL NETWORK ADDRESSES OF WEB APPLICATIONS USING THE CDN SERVICE**

*In the following research, we have considered the problem of finding real network addresses of web applications. For this purpose, we have used a service, which based on providing content delivery to networks. Thus, the known solutions are analyzed, and their features of use are established. Among them, the focus of this service on speeding up the operation and security of web applications is highlighted. Taking into account these features, this issue is complicated by the focus on describing the technical capabilities of the already known solutions. This limits the detection of web application of configuration vulnerabilities. To prevent this, the capabilities of content delivery networks have been used. This use is based on redirecting HTTPS traffic through their servers and, as a result, hiding the real IP address of the web application. The most common implementations of the service based on content delivery networks are highlighted. The focus on the web application firewall is shown. Its applicability at the configuration of DNS requests and finding of real network addresses is established. Also, the most typical methods of their search are identified. Among them, the emphasis is placed on the use of services for viewing current and archival data of Internet resources; using MX records as sources of IP addresses; sending letters by e-mail to the specified (correct or incorrect) e-mail addresses; finding subdomains without a configured service of content delivery networks; obtaining an SSL certificate; using DNS name research tools. The implementation of these methods is demonstrated by the selected software. To do this, the criteria are introduced and their capabilities are compared. The results of using the selected software show the limitations of its functionality. To prevent this, it is recommended to combine methods of searching for real network addresses of web applications using the service of content delivery networks.*

***Keywords:*** *web application, network address, real network address, search for real network address, content delivery network.*