CUA-14-01A
Рекомендації CERT-UA для усунення вразливостей, пов’язаних з некоректним налаштуванням DNS-серверів

Державна служба спеціального зв’язку та захисту інформації України
Державний центр захисту інформаційно-телекомунікаційних систем
04119, Україна, м. Київ, вул. Мельникова, 83б
тел.: +380 44 281 88 25
факс: +380 44 489 31 33
www: cert.gov.ua

ЗМІСТ

1. Загальна інформація

1.1 Вразливі системи

- DNS-сервери

1.2 Інформація про сервіс DNS

Доменна система імен (англ. *Domain Name System*, DNS) – комп'ютерна розподілена система для отримання інформації о доменах. Частіше за все, використовується для отримання IP-адреси за ім'ям хоста (комп'ютера чи пристрою), для отримання інформації про маршрутизацію пошти, обслуговуючі вузли для протоколів в домені [1].

Розподілена база DNS підтримується за допомогою DNS-серверів, взаємодіючих між собою по відповідному протоколу передачі даних.

Основою DNS є ієрархічна структура доменних імен і зони. Кожний сервер, відповідальний за ім'я, може передавати відповідальність за частину домена іншому серверу (наприклад, іншої організації або людини), що дозволяє перекласти відповідальність за актуальність інформації на сервери різних організацій, відповідальних тільки за свою частину доменного імені.

DNS-сервер, **name server** – програмний додаток, призначений для відповіді на DNS-запити по відповідному протоколу. Також DNS-сервером можна назвати хост, на якому запущено такий програмний додаток [2].

Докладна реалізація протоколу й системи в цілому описана в:

- RFC 1034 — Domain Names — Concepts and Facilities
- RFC 1035 — Domain Names — Implementation and Specification
- RFC 1912 — Common DNS Operational and Configuration Errors
- RFC 1591 — Domain Name System Structure and Delegation
- RFC 1713 — Tools for DNS Debugging
- RFC 2606 — Reserved Top Level DNS Names

1.3 Вразливість до атак типу DNS-amplification (підсилення).

Атаки з використанням технології DNS-amplification є популярною формою DDoS атак, в яких зловмисники використовують публічно доступні відкриті DNS-сервери (open resolvers) для завантаження системи жертви надмірним трафіком, який складається з DNS-відповідей (DNS-response) (Рис. 1).

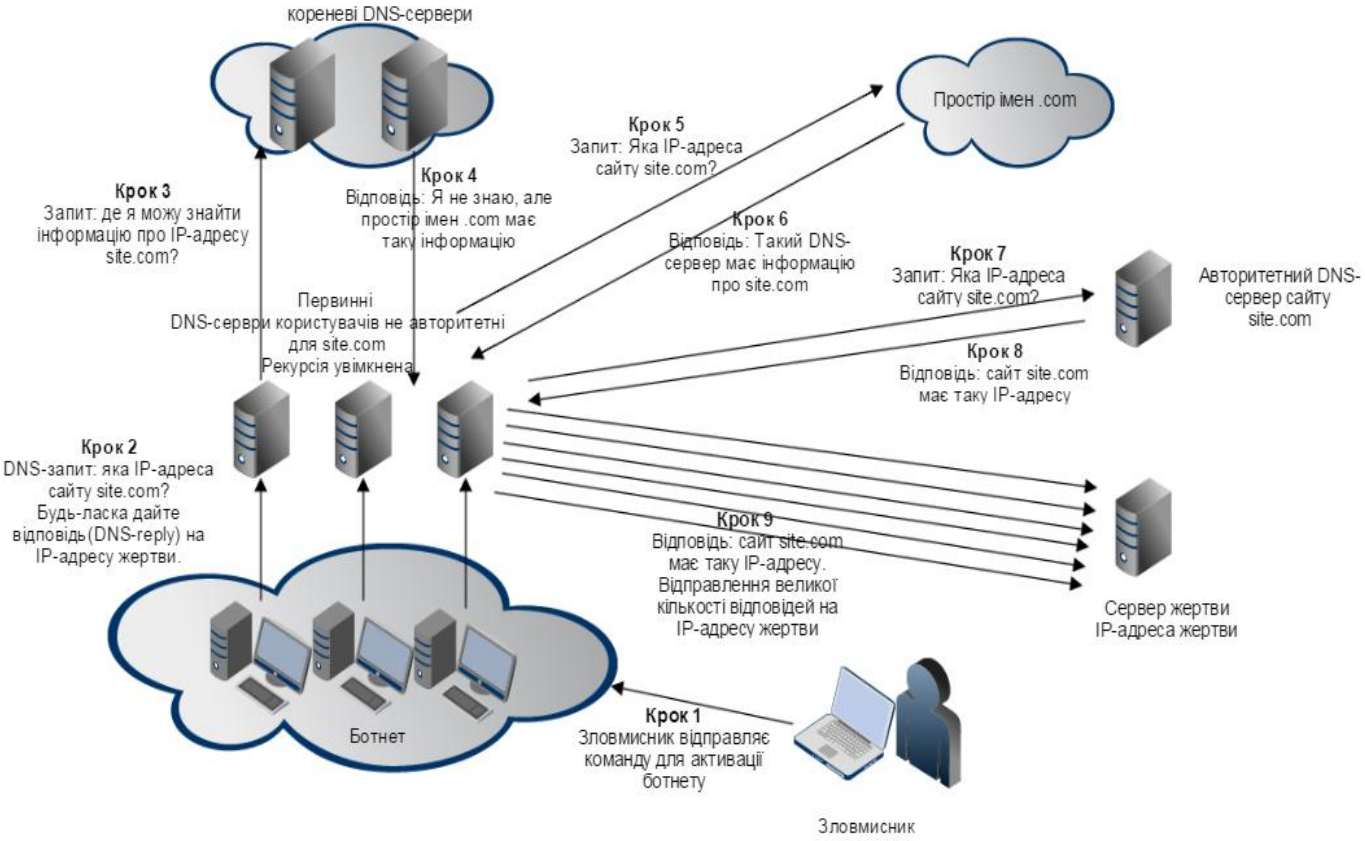

Рис. 1 Атака DNS-amplification

Суть атаки полягає в тому, що зловмисник посилає DNS-запит (DNS-request) пошуку IP-адреси доменного імені до відкритого DNS-серверу із заміною дійсної IP-адреси джерела запиту IP-адресою жертви атаки. Робота DNS базується на використані UDP-протоколу, який не вимагає встановлення з'єднання і працює без збереження стану про з'єднання, тому є можливою підміна IP-адреси. Коли DNS-сервер відправляє DNS-відповідь, вона приходить на IP-адресу жертви. Зазвичай, зловмисники у своїх запитах запитують про якомога більшу кількість доменів DNS-зони для максимізації ефекту підсилення. У більшості атак цього типу підроблені запити, надіслані зловмисниками, відносяться до типу "ANY". На такий запит приходить DNS-відповідь, яка включає у себе всю відому інформацію про DNS-зону. Оскільки розмір DNS-відповіді набагато більший за DNS-запит (так стандартний DNS-запит – 60 байт, DNS-відповідь – 200 байт і більше),

атакуючий може значно збільшити розмір трафіка, спрямованого на IP-адресу жертви (в середньому коефіцієнт підсилення 30-60, але можливо достигнути і більших показників). Використовуючи бот-мережу, зловмисник може згенерувати велику кількість підроблених DNS-запитів і, таким чином, з легкістю створити велику кількість трафіку. Крім того, оскільки у DNS-відповідях приходять безпечні дані з авторитетних серверів, надзвичайно важко запобігти таким типам атак.

Зазвичай, у атаках типу DNS-amplification використовуються DNS-сервери, які некоректно налаштовані і дозволяють приймати рекурсивні запити від будь-якого клієнту в Інтернеті. Також, у таких атаках можуть використовуватись і авторитетні сервери, в яких відключена рекурсія, бо вони також повертають відповідь, яка містить інформацію про обслуговуючу зону, або помилку, тому можливо досягти ефекту підсилення. Навіть коректно налаштований DNS-сервер може використовуватись у DDoS атаках, але коефіцієнт підсилення буде значно менший.

2. Рекомендації

2.1 Перевірка DNS-серверу на предмет некоректного налаштування

Є декілька організацій, які пропонують безкоштовні веб-інструменти сканування для перевірки того, чи працює DNS-сервер в режимі "open resolver":

http://openresolverproject.org/
http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl/
http://www.dnsinspect.com/
http://openresolver.com/

Механізм виявлення:

У рекурсивному DNS-запиті клієнт відправляє запит до локального DNS-серверу з питанням про IP-адресу ім'я домену, після чого DNS-сервер виконує всі необхідні запити від імені клієнта і повертає відповідь, яка містить потрібну інформацію про домен, або помилку. Показником того, що DNS-сервер - вразливий до участі у DDoS атаках є те, що сервер відправляє DNS-відповіді будь-якому клієнту в Інтернеті з інформацією про домен, для якого цей сервер не є авторитетним (non authoritative).

2.2 Рекомендації щодо усунення вразливості до атак типу DNS-amplification

За даними "Open DNS Resolver Project" із 27 мільйонів відомих DNS-серверів в Інтернеті, приблизно 25 мільйонів мають вразливості до участі у DDoS атаках. Позбавитися такої вразливості дуже складно, але можливо зменшити коефіцієнт підсилення до мінімуму методом коректного налаштування свого DNS-серверу, тобто заборонити серверу відповідати на рекурсивні запити, які надходять з мережі Інтернет, і відповідати тільки на запити клієнтів своєї підмережі.

Перевірка IP-адреси джерела запиту

Оскільки DNS-запити, які відправляються з контрольованих зловмисником ботів, повинні мати підмінену вихідну IP-адресу, першим кроком до зменшення ефективності атак DNS-amplification є відхилення Інтернет-провайдерами будь-якого DNS-трафіку з підроблених адрес. "The Network Working Group of the Internet Engineering Task Force" розробила документи "Best Current Practice 38" [7] та "Best Current Practice 84" [8], які описують, як Інтернет-провайдери можуть фільтрувати трафік в своїй мережі для відхилення пакетів з підробленою IP-адресою. Рекомендації, надані в цих документах, стосуються перевірки пристроями маршрутизації відповідності вихідної IP-адреси пакету з IP-адресою інтерфейсу, який його передав. Якщо IP-адреси не відповідні, то пакет, очевидно, має підроблену вихідну IP-адресу.

Нижче наведені рекомендації щодо налаштування найбільш поширених DNS-серверів: BIND9 та Microsoft DNS Server. Якщо ви працюєте з іншим DNS-сервером, будь-ласка зверніться до документації Вашого постачальника для докладної інформації про конфігурацію.

Відключення рекурсії

Багато функціонуючих в Інтернеті DNS-серверів працюють виключно для представлення інформації про ім'я одного домену. У цих системах, DNS для приватних клієнтських систем може бути забезпечена за допомогою окремого DNS-сервера і авторитетний сервер діє тільки, як джерело інформації про свою DNS-зону для зовнішніх клієнтів. Таким серверам не потрібно підтримувати обробку рекурсивних запитів про області імен інших DNS-серверів. Тому рекомендується налаштувати такий сервер з вимкнутою рекурсією.

BIND9

В файлі /etc/bind/named.conf [11]

```
options {
    allow-query-cache { none; };
    recursion no;
};
```

Microsoft DNS Server

Використовуючи інтерфейс Windows: [9]
1) Відкрийте DNS (Start->Control Panel->Administrative Tools->DNS)
2) Правий клік мишки на DNS-сервер та обрати Properties (Свойства)
3) Натиснути на вкладку Advanced.
4) В Server Options обрати позначку "Disable recursion", натиснути ОК.

Використовуючи командну строку:
1) Ввести dnscmd*Ім'яСерверу*/Config/NoRecursion {1|0}

Обмеження рекурсії для авторизованих клієнтів

Для DNS-серверів, які розгорнуті в межах організації, або постачальника послуг Інтернету, сервер повинен бути налаштований для виконання рекурсивних запитів тільки від авторизованих клієнтів. Ці запити, зазвичай, повинні надходити тільки від клієнтів в зоні мережевих адрес організації. Ми рекомендуємо щоб усі адміністратори серверів обмежили прийняття рекурсивних запитів DNS-сервером тільки від клієнтів мережі організації.

BIND9

В файлі /etc/bind/named.conf [10]

```
acl corpnets { 192.168.1.0/24; 192.168.2.0/24; }; (Діапазон IP-адрес)
options {
  allow-query { any; };
  allow-recursion { corpnets; };
};
```

Microsoft DNS Server

В Microsoft DNS Server немає можливості обмеження рекурсивних запитів в певному діапазоні IP-адрес. Для наближення до функціональності списку контролів доступу BIND, Microsoft DNS Server повинен бути встановлений на окремому кеш-сервері який оброблює рекурсивні запити. На цьому окремому сервері повинні бути налаштовані правила брандмауера для блокування доступу до нього адрес, які не належать організації.

Обмеження кількості DNS-відповідей(Response Rate Limiting)

В BIND9 існує можливість обмежити максимальну кількість відповідей в секунду, яка відправляється одному клієнту з DNS-сервера. Ця функція призначена для використання тільки на авторитетних DNS-серверах, бо вона впливає на роботу рекурсивних серверів. Для забезпечення найбільш ефективного захисту рекомендується встановлювати авторитетний DNS-сервер і сервер, який оброблює рекурсивні запити на різних системах. На авторитетному сервері встановлюється обмеження кількості відповідей (RRL), а на рекурсивному сервері використовується обмеження рекурсії для клієнтів своєї підмережі. Це знизить ефективність атак типу DNS-amplification, за рахунок зменшення кількості трафіку, який надходить від якогось одного авторитетного DNS-сервера, не впливаючи на обробку внутрішніх рекурсивних запитів.

Попередження: Використання RRL підвищує ризик до ураження атаками типу "DNS cache poisoning".

BIND9

RRL підтримується в версії BIND 9.9.4 і пізніших.

```
rate-limit {
   responses-per-second 5;
   window 5;
};
```

Microsoft DNS Server

Дана функція відсутня.

3. Корисні посилання

[1] https://en.wikipedia.org/wiki/Domain_Name_System

[2] https://en.wikipedia.org/wiki/Name_server

[3] http://openresolverproject.org/

[4] http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl/

[5] http://www.dnsinspect.com/

[6] http://openresolver.com/

[7] http://tools.ietf.org/html/bcp38

[8] https://tools.ietf.org/html/bcp84

[9] http://technet.microsoft.com/en-us/library/cc787602.aspx

[10]http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch07.html#Access_Control_Lists

[11] http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.ch03.html#id2567992

[12] https://www.us-cert.gov/ncas/alerts/TA13-088A

Зміни до документу

- 26.11.2014: Перший випуск.