УДК 004.4

В.Д. Погребенник, П.Т. Хромчак
Національний університет "Львівська політехніка",
кафедра захисту інформації

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ЗА ДОПОМОГОЮ СИСТЕМ РЕЙТИНГУ ВІДПРАВНИКА

Описано механізм роботи системи рейтингу відправника та формування довірених відносин під час встановлення з'єднання між двома хостами. Наведено практичні аспекти реалізації такої системи на прикладі роботи поштового серверу.

Ключові слова: інформаційні ресурси, поштовий сервер.

The mechanism of sender rating system and establishing of trustworthy relations in the process of connecting between 2 ends is described. The practical aspects of such system realisation is provided on the basis of mail server.

Key words: informative resources, MTA.

Вступ. В умовах обмеженості інформаційних ресурсів, які можуть бути використані для опрацювання інформаційних потоків в користувацьких, а також серверних аплікаціях та сервісах, постає потреба їх заощадження та підвищення ефективності. Використання системи довіреності, заснованої на рейтингу відправника, дає змогу значно заощаджувати обчислювальні ресурси за рахунок відсіювання шкідливого потоку даних на стадіях ініціалізації з'єднання без залучення сервісів, що працюють вище транспортного рівня моделі OSI.

У статті розглянуто питання захисту інформаційних ресурсів поштових серверів від спам-повідомлень, що можуть бути згенеровані ботнет-мережами [1]. Також наведено огляд існуючих технологій систем рангування та приклад практичної реалізації такого сервісу рейтингу відправника з використанням відкритого програмного забезпечення на базі ОС Linux.

Метою роботи є висвітлення основних аспектів роботи системи рейтингу відправника та показ практичних аспектів її застосування з метою відсіювання шкідливого трафіку на підході до опрацювання цих даних прикладними сервісами та програмами, що є чутливими до ресурсів.

Опис роботи системи рейтингу відправника. Принципи наповнення бази рейтингу відправника (далі БРВ) доволі істотно розрізняються між собою. Як правило, вона містить ip-адреси відомих або потенційних джерел спаму, вірусів, експлойтів та іншого виду шкідливого програмного забезпечення, зокрема: відкриті транслятори пошти (open relays) або машини, що розсилають відомі троянські програмами та віруси, зомб- мережі, а також ip-адреси, котрі мають стосунок до аномальної DdoS-активності. Також організації, що наповнюють ці списки, проводять тестування комп'ютерів і виявляють наявність можливості загроз розсилання спаму з тих або інших віддалених джерел. Процес наповнення передбачає дослідження інформаційної інфраструктури віддалених хостів з метою формування рейтингу відправника. Оскільки таке поняття, як "інфраструктура" чітко визначити неможливо, то внесення адрес робиться відповідно до внутрішньої політики організації, що формує базу [2]. Важливим є також те, що у базу заносяться не тільки ті хости, з яких здійснюється розсилання спаму, а також мережі, які використовуються для підтримки і хостингу шкідливих ресурсів – поштових серверів, web-сайтів, DNS і т.п.

Загальну схему етапів встановлення довірених відносин між відправником та обчислювальним вузлом зображено на рис. 1.

Рис. 1. Етапи встановлення довірених відносин між відправником та обчислювальним вузлом

Відправник характеризується парою ip-адреса/порт, з якої відбувається встановлення з'єднання з активним сокетом обчислювального вузла. Після етапу "потрійного рукостискання" (обміну повідомленнями SYN, SYN/ACK, ACK), обчислювальний вузол ініціює запит до системи БРВ з метою визначення рейтингу відправника. БРВ містить велику кількість записів у вигляді пар ip-адреса відправника/рейтинг. У відповідь на запит система БРВ повертає значення рейтингу відправника.

Розрізняють плоскі та багаторангові БРВ. Плоскі БРВ у відповідь на запит повертають один з двох можливих рейтингів:

– надійний відправник

– ненадійний відправник

Така система не дає змоги створити шкалу градацій рейтингу, тому у випадку, якщо результат буде негативним, з'єднання розривається. Така БРВ не має гнучкої системи встановлення довірених відносин. Прикладом таких баз є XBL (Exploits Block List) та RBL (Real-time Blackhole Lists) – бази, що формуються організацією Spamhaus.

Натомість багаторангова база дає змогу здійснювати подальші маніпуляції зі з'єднанням, піддаючи його тій чи іншій політиці обмежень, базованій на рейтингу. Записи багаторангової БРВ містять шкалу градації в числовому діапазоні, що характеризує з певним коефіцієнтом рейтинг відправника. Прикладом такої бази є SBRS (Sender Base Reputation Score), котра наповнюється організацією IronPort та розповсюджується під торговою маркою IronPort Reputation Filters .

DNSBL

DNSBL – DNS blacklist або DNS blocklist – списки хостів, які зберігаються за допомогою архітектури DNS. Раніше такі списки називалися RBL, Real – time Blackhole List, але зараз ця назва є торговою маркою, що належить компанії MAPS LLC.

Розрізняють такі типи DNSBL:

– списки відкритих релеїв – це база поштових серверів, які неправильно сконфігуровані і які дають змогу пересилати через себе поштові повідомлення для усіх охочих. Як правило, ці хости автоматично скануються в Інтернеті, тому потрапляння такого хоста до рук людей, що розсилають спам-повідомлення, відбувається дуже швидко (не більше 4 днів). При використанні цих списків існує найменша небезпека блокування звичайної пошти,

оскільки сервер потрапляє в список, тільки після перевірки його спеціальним поштовим роботом;

- списки спам серверів – база цих серверів, через які було помічено проходження спам-повідомлень. Ці списки складають на основі свідчень користувачів, що отримали спам з якого-небудь сервера, тому вони можуть містити застарілу або просто невірну інформацію;
- список Dialup-адрес – список ip-адрес провайдерів, які використовуються ними для організації сервісу віддаленого доступу;
- список відкритих HTTP/Socks проксі-серверів без контролю доступу, що дають змогу будь-якому користувачеві здійснювати неавторизовані дії, приховуючи свою реальну ip-адресу (незаконні дії – цене лише розсилання спаму, але й інша шкідлива активність [3]).

DRBL

DRBL (Distributed Realtime Blocking List) – принцип формування БРВ, який є розподіленим і дає змогу організаціям і приватним особам не просто збирати свою базу БРВ, але і обмінюватися цими списками з колегами. Кожен учасник (node) має у своєму розпорядженні усі доступні йому можливості складання списків ip, що блокуються, для публікації їх за допомогою DRBL (своя DRBL зона).

У DRBL-зоні прийнято публікувати інформацію про хости, які учасник обміну блокує на своїх сервісах. Так, наприклад, відбувається опрацювання поштової кореспонденції на стороні сервера, де виявлений спам не просто не пропускається в поштові скриньки користувачів, але і ip-адреси джерел цього спаму одразу публікуються в DRBL зоні провайдера. Поштові сервери інших компаній, налаштовані на роботу з цією DRBL-зоною, зможуть скористатися цією інформацією і відкинути листи від джерела спаму ще до їх приймання, без додаткового опрацювання спам-повідомлень. Такий підхід дозволяє значно понизити накладні витрати сервера на обробку спам-повідомлень для усіх учасників мережі.

DRBL передбачає критерії оцінки ваги інформації, отриманої від кожної конкретної DRBL зони, що дає змогу не блокувати усе підряд, а довіряти інформації, що була отримана з різних джерел. Ефективність опублікованого за допомогою DRBL зони списку ip-адрес тим вища, чим динамічніше учасник заносить в список нові ip-адреси, які є, на його думку, джерелами спаму і видаляє звідти застарілі.

Інтерфейс звернення до БРВ. На рис. 2 зображено узагальнений інтерфейс звернення до БРВ.

Рис. 2. Узагальнений інтерфейс звернення до БРВ

Для перевірки рейтингу ip-адреси відправника через будь-який DNSBL-список потрібно вказати ip, що перевіряється, в форматі DNS PTR (задом наперед) і додати ім'я домену DNSBL сервера. Якщо відповідь буде отримана, то ця адреса заблокована, тобто знаходиться в списку.

Отримана ip-адреса може бути будь-якою, важливий лише факт її наявності у відповіді на запит. Саме тому ip-адресу можна використати для опису типу джерела, в якому здійснювався пошук. Наприклад, якщо у відповідь повернуте значення дорівнює 127.0.0.1 – то це веб-адреса, що

збігається з типом відкритого релею, 127.0.0.2 – джерело ботнет-активності тощо. Також додатково в файлі зон пропагуються записи типу TXT RR, які містять текстову інформацію про ip-адреси.

Так, наприклад, для ip-адреси відправника 172.22.16.22 результати пошуку по базі БРВ від abuseat.org будуть різні, якщо хост має позитивний або негативний рейтинг. Для перевірки рейтингу скористаємось утилітою dig, або nslookup. Результати перевірки рейтингу для тестового хоста наведено в табл. 1.

Таблиця 1

Результати перевірки рейтингу для тестового хоста

Негативний рейтинг (Існує запис про хост в базі)	Позитивний рейтинг (Запис про хост відсутній)
;; QUESTION SECTION: ;22.16.22.172.abuseat.org. IN A ;; ANSWER SECTION: 22.16.22.172.abuseat.org. 86332 IN A 127.0.0.2	;; QUESTION SECTION: ;22.16.22.172.spamcop.net. IN A

Результат запиту в першому випадку становить 127.0.0.2, що сигналізує про негативний рейтинг відправника в вищенаведеній базі. Якщо запис про ресурси в службі DNS даного сервісу містить додаткову інформацію, то її можна отримати, сформувавши запит з використанням утиліти host. Результат отриманий в процесі пошуку TXT RR наведено в табл. 2.

Таблиця 2

Результати пошуку TXT RR запису для відправника 172.22.16.22

22.16.22.172.abuseat.org descriptive text "030311:Seems it is spammer" 22.16.22.172.abuseat.org has address 127.0.0.2

Прикладні аспекти реалізації БРВ. Припустимо, що потрібно реалізувати зв'язку роботи сервісів SMTP (поштовий сервер) та DNSCACHE БРВ з подальшою фільтрацією відправників згідно з цією базою.

Для практичної імплементації сервісу БРВ скористаємось програмним комплексом djbdns, що працює в сімействі ОС GNU/Linux.

Також як поштовий сервер було вибрано MTA QMAIL, який приймає з'єднання на 25 портів. Під час встановлення зв'язку поштовий сервер звертається до DNSBL і перевіряє наявність ip-адреси клієнта, від якого він приймає повідомлення. При позитивній відповіді вважається, що відбувається спроба приймання спам-повідомлення. Серверу відправника посилається повідомлення про помилку типу 5xx, і повідомлення не приймається. Поштовий сервер відправника генерує т. зв. "відмовну квитанцію" (bounce-повідомлення) клієнту-відправнику про те, що повідомлення не було доставлено [4].

Основні етапи налаштування сервісу БРВ:

Етап 1. Налаштування серверу RBLDNS з двома зонами.

Під час роботи серверу RBLDNS працює дві зони DNS. Перша – RBL-зона, що містить інформацію про ip, які мають негативний рейтинг. Друга зона – WHT-зона (біла зона), що містить запис про ip-адреси відправників, для яких рейтинг повинен бути визначений як позитивний, незважаючи на результати, які отримані через інші вузли мережі DNSBL.

Налаштування вищезазначених зон:

rbldns-conf rbldns dnslog /etc/rbldns/black 127.0.0.2 rbl.pl.org.ua

rbldns-conf rbldns dnslog /etc/rbldns/white 127.0.0.3 whitelist.pl.org.ua

Так, якщо рейтинг негативний чи позитивний, то значення, що буде одержане у відповідь, становитиме 127.0.0.2 або 127.0.0.3 відповідно.

Етап 2. Налаштування серверу DNS серверу dnscache для обслуговування вищезазначених зон.

Основний сервер імен, який буде обслуговувати запити від клієнтів, це dnscache сервер:

cd /run/dnscache/root/servers
echo 127.0.0.2 > rbl.pl.org.ua
echo 127.0.0.3 > whitelist.pl.org.ua
svc -h /run/dnscache

Етап 3. Пропагування записів в файлах зон DNS.

Процес пропагування записів в файлі зон DNS сервера достатньо простий та не потребує складних маніпуляцій з RR (Resource Records) записами:

cd /etc/rbldns/rbl/
echo 192.168.0.1 >> data
make

У даному випадку ір-адреса відправника 192.168.0.1 буде зазначена з негативним рейтингом.

Етап 4. Запуск прикладного сервісу.

Запуск прикладного сервісу здійснюють з використанням проміжного сервісу, котрий виконує функції тунелювання та перевірки безпосереднього рейтингу клієнта. Як такий сервіс було вибрано ПЗ tcpserver [4].

Запуск поштового серверу:

*tcpserver -R -v -p -x /var/qmail/control/tcp.smtp.cdb -u $QMAILUID -g $QMAILGID *
*mail.pl.org.ua smtp /usr/local/bin/rblsmtpd -a whitelist.pl.org.ua *
-r rbl.pl.org.ua -r relays.ordb.org -r bl.spamcop.net qmail-smtpd,

де як БРВ бази вибрано дві локальні whitelist.pl.org.ua та rbl.pl.org.ua, які дають змогу здіснювати маніпуляції над відправниками індивідуально та дві БРВ bl.spamcop.net, relays.ordb.org як сервіси рейтингу відправника, які не було зазначено в перших двох зонах.

Етап 5. Перевірка рейтингу відправника.

Перевірити роботу створених баз можна, використовуючи утиліту dnsip або nslookup:
dnsip 1.0.168.192.rbl.pl.org.ua

Висновки. За допомогою системи БРВ за різними підрахунками вдається відфільтрувати близько 75 відсотків шкідливого трафіку на підході до сервісів та прикладних програм без залучення основного обчислювального потенціалу серверного обладнання [5]. З погляду прикладного аспекта впровадження такої системи в корпоративну мережу провайдера найкращими є багаторангові БРВ, які дають змогу здійснювати більш гнучкі маніпулятивні дії з трафіком за внутрішніми правилами та політиками інформаційної безпеки.

Також, враховуючи динаміку зміни RR записів в файлах-зон DNS-серверів, слід пам'ятати про згладжену стратегію відсіювання відправників, засновану на власних записах та поєднання БРВ із іншими механізмами встановлення автентичності відправника такими як DK/DKIM, та SPF/SIDF у випадку роботи поштових серверів.

1. Погребенник В.Д., Хромчак П.Т. Розроблення моделі системи виявлення центрів управління ботнет-мережами / П.Т. Хромчак // Вісник Нац. ун-ту "Львівська політехніка". – 2009. – № 639: Автоматика, вимірювання та керування. – С. 117–123. 2. Хромчак П.Т. Концепція моделі виявлення IRC-орієнтованих ботнет-мереж / П.Т. Хромчак // Комп'ютерні науки та інженерія: Матеріали IV Міжнар. конф. молодих вчених CSE-2010. – Львів: Вид-во Львівської політехніки, 2010. – С. 374–375. 3. Wenke Lee, Cliff Wang, David Dagon, Botnet Detection Countering the Largest Security Threat. – New York: Springer, 2008. – 167 p. 4. Chris Wilkes. How to setup own private RBL list / http:// ladro.com/docs/dns/rblsmtpd.html 5. *http://www.ironport.com/products/ironport_senderbase_network. html*