The International Scientific Association
"SCIENCE & GENESIS"
www.science-genesis.com

"GLOBAL SCIENTIFIC UNITY 2014"

26-27 September 2014 Prague (Czech Republic)

Volume I

Prague 2014

ISBN 9789665326823

The European Scientific and Practical Congress **"Global scientific unity 2014"**
Published by order of the Scientific Presidium of the Council of the International Scientific Association "Science & Genesis".

Scientific and practical edition: Copenhagen, Denmark, 18 July 2014. Publishing Center of The International Scientific Association «Science & Genesis», Copenhagen, 2014, p. 229.

"Management of the scientific potential of countries and regions" is a scientific edition, focused upon the academic perspectives of science. While striving for a balance of theory and application, edition is ultimately dedicated to developing theoretical constructs. Its strategies are to invite and encourage offerings from various disciplines; to serve as a forum through which these may interact; and thus to expand frontiers of knowledge in and contribute to the science. In this role, editions both structures and is structured by the research efforts of a multidisciplinary community of scholars.
Benefits to authors
We also provide many author benefits, such as free PDFs, a liberal copyright policy, special discounts on r publications and much more.
Please see our Guide for Authors for information on article submission. If you require any further information or help, please visit our support pages:
www.science-genesis.com

Theses of reports are presented in author's edition as of international and national legislation on the date of the Congress.
Published in author's edition. Editorial department is not responsible for the contents.

Editorial opinion may be different from the views of the authors. Please, request the editors' permission to reproduce the content published in the journal.

6. Сеженюк ЭЛ. Информационная культура общества и прогресс информатики // Научная и техническая информация. — Сер.1.— 1994. -г №1. — С. 1—8.
7. Скипор И.Л. Лингвистическое обеспечение функционирования автоматизированной библиотечной сети : автореф. дис на соиск. учен. степ. канд. пед. наук : 05.25.03 / И.Л. Скипор. – Новосибирск, 2000. – 20 с.
8. Скипор И.Л., Сбитнева Е.А. Лингвистическое обеспечение корпоративных библиотечно-информационных систем и сетей // Научные и технические библиотеки. . – 2004. – № 4. – С. 28–41.
9. Сукиасян Э.Р. Логика развития информационно-поисковых языков // Научные и технические библиотеки. – 2004. – № 4. – С. 15–27.
10. Тихонова Л.Н. Система научных коммуникаций и библиотеки // Зональное совещание «Электронные ресурсы по культуре: продвижение в культурную среду Северо-Запада России. Архангельск, 27—28 сент. 2006 г. — Архангельск, 2006.

Гвозденко М.В.
ст. викладач
Національний юридичний університет
імені Ярослава Мудрого
Кафедра інформатики та обчислювальної техніки
м.Харків, Україна
Чобу Я.В.
студент
Національний юридичний університет
імені Ярослава Мудрого
Міжнародно-правовий факультет
м.Харків, Україна

ТЕХНІЧНІ ТА ПРОГРАМНІ ЗАСОБИ ВИЯВЛЕННЯ ДЖЕРЕЛА DDOS АТАКИ

DDoS атаки – зростаюча проблема, яка впливає на всіх користувачів мережі. Один із способів пом'якшити атаку, це простежити IP адресу джерела атаки. Відомості про джерело атаки дозволяють жертві зменшити негативні наслідки атаки, а також викрити інформацію, необхідну для пошуку зловмисника.

Питання представлені в контексті нового підходу до зворотнього відстеження IP (IP traceback), заснованому на використанні автономних систем, а не окремих маршрутизаторів.

Не буде зайвим описати ті основні моменти, які закладені в інфраструктуру інтернету і протоколу доставки повідомлень. "Піонери інтернету" припускали, що кожен, хто захоче відправити якусь інформацію, захоче також отримати відповідь і надасть інформацію про себе. Тому в IP протокол не було вбудовано ніяких заходів захисту, перевіряючих коректність адреси відправника. У підсумку це стало причиною появи багатьох загроз, не останньою з яких є DDoS атака. Один із способів протистояння DDoS атакам – зворотнє відстеження справжньої IP адреси джерела атаки. Однак цей метод піднімає велику кількість технічних, суспільних і правових питань, які і будуть розглянуті далі.

DDoS атака – це навмисна дія, мета якого полягає в тому, щоб перешкодити нормальному використанню інтернет-ресурсів. Основна ідея DDoS атаки лежить в тому, щоб вичерпати ресурси цілі і змусити її відповідати на величезну кількість помилкових запитів, при цьому запити звичайних користувачів залишаться без відповіді або будуть оброблятися дуже довго. Хоча й існують різні типи DDoS атак, основною передумовою служить величезна кількість підконтрольних зловмиснику комп'ютерів, які шлють потік пакетів жертві. Зіткнувшись із цим, ресурси жертви переповнюються і відбувається різке уповільнення швидкості трафіку.

Поширення легкодоступних і все більш складних ботнетів породило явище, яке було названо "злочинною економікою": підпільні спільноти, які наймалися для здійснення кримінально караних кібердій за грошову винагороду. Це включало, серед іншого, маніпуляції з курсами акцій, атаки на конкурентів і вимагання грошей під загрозою DDoS атаки. Основною проблемою у зниженні частоти та інтенсивності DDoS атак є відсутність надійного механізму визначення адреси первісного відправника пакетів. Без такого механізму зловмисники можуть не боятися бути вирахуваними і притягнутими до юридичної відповідальності. Крім того, будь-яка участь провайдерів у відстеженні та наданні такої інформації може коштувати додаткових витрат і юридичних проблем [1].

DDoS атаки наносять величезні збитки власникам сайтів та незручності інтернет-користувачам. Через перевантаження ресурсів серверу збільшується час обробки запиту від користувачів, що призводить до виходу зі строю обладнання та до недоступності сервісу. Такі

наслідки можуть використовуватися для того, щоб вивести з ладу сайт конкурента, тобто у нечесному бізнесі. Атаки цього типу можуть проводитися на відомі ресурси задля того, щоб зробити інформацію, що є на них, недоступною для користувачів. Найбільш часто атакуються сайти, пов’язані з інтернет-торгівлею. За частотою атак після них йдуть ігрові сайти та сайти банків. В останній час значно збільшилося число атак на сайти державних та політичних установ. Інтернет – це з’єднання різних мереж, які належать різним суб’єктам і адмініструються різними людьми. Ці мережі взаємодіють для пересилання пакетів даних від відправника до одержувача. Шлях від відправника до одержувача може проходити через різні проміжні мережі. Кожна мережа оперує своєю безліччю маршрутизаторів, які передають пакети далі за маршрутом, аж до пункту призначення [3].

Мережа, яка контролюється і адмініструється незалежним і автономним суб’єктом, називається автономною системою (АС). Автономними системами можуть бути приватні організації, місцеві інтернет-провайдери або ж великі магістральні провайдери. Для даної роботи найбільш важливою характеристикою АС є їх підконтрольність і відповідальність. Якщо джерело DDoS атаки може бути простежено аж до його АС, то організація зможе зупинити DDoS атаку і притягнути до відповідальності атакуючого.

Інтернет не був розроблений з урахуванням функціональності безпеки. Одним із наслідків цього є припущення, що поле IP адреси відправника пакетів є IP адресою комп’ютера, який цей пакет надіслав. Ця адреса найчастіше не перевіряється на дійсність. Таким чином, IP адреса відправника може бути змінена без необхідних повноважень і відповідальності, що дає можливість зловмиснику отримати анонімність шляхом підміни (spoofing) своєї IP адреси. Це робить IP адресу марною для виявлення відправника. Теоретично одним із способів визначення джерела фальсифікації може бути зворотнє простежування (traceback) маршруту аж до відправника. Зворотнє відстеження можливо, якщо монітори вздовж шляху IP пакета зберігають інформацію про заголовок IP пакета (запис у журнали), або якщо маршрутизатори додають інформацію в заголовок пакета (маркування пакетів).

Попередні дослідження в області зворотнього відстеження були сконцентровані на різних методиках ведення журналів та маркування пакетів. Однак, враховуючи поточні обсяги трафіку, швидкість маршрутизації та вимоги до сховищ з даними, жоден з цих методів не є можливим для широкого розгортання. Маркування заголовків па-

кетів вимагало б змінної структури заголовка IP пакетів, що знизило б продуктивність і ефективність обладнання. Пакетне маркування також потребує зміни структури IP протоколу, що можливо в теорії, але практично не піддається реалізації на практиці.

Альтернативою пакетному маркуванню могло б послужити зберігання журналів пакетів на маршрутизаторах. З'єднання маршрутизаторів зазвичай використовуються в магістральних мережах, де швидкість доходить до 10 Гбіт/с, або приблизно 1.25 мільйонів пакетів на секунду. З такою швидкістю 10 хвилин роботи буду вимагати 750 Гбайт сховища журналів. Стає ясно, що це надмірна вимога, яка буде обходитися занадто дорого. Крім того, сортування та пошук даних займатиме велику кількість обчислювальних потужностей. Цей недолік призвів дослідників до методу вибіркового аналізу для зменшення розміру журналу. Цей метод добре працює при DoS атаках, коли один хост посилає велику кількість пакетів жертві. Проте, DDoS атака передбачає використання великої кількості зомбі-комп'ютерів. Малоймовірно, що вибірка буде включати в себе всі зомбі-машини, що беруть участь в атаці.

Сучасні дослідження припускають використання фільтрів Блума для зменшення кількості зберігання даних [2]. Ці фільтри працюють за таким принципом: є послідовність з певної кількості бітів (нехай буде 100 бітів). Спочатку всі вони обнулені. Маршрутизатор бере заголовок IP пакета і пропускає його через хеш-функцію. На виході виходить якесь число, припустимо, 56. Маршрутизатор встановлює 56-й біт в одиницю. Потім цей же заголовок "пропускає" через іншу хеш-функцію, яка повертає, наприклад, 83. 83-й біт встановлюється в одиницю. І так для заголовків інших пакетів. Звичайно, не виключена ймовірність помилкового спрацьовування (особливо, якщо таблиця мала), проте ніколи не буде ситуації, що пакет був на цьому маршрутизаторі, а в таблиці це не знайде відображення. Для визначення джерела DDoS атаки маршрутизатор "проганяє" заголовок пакета через кілька хеш-функцій. Якщо по позиціях, повернутим цими функціями, стоять одиниці, то з деякою часткою ймовірності можна сказати, що пакет тут був. Далі маршрутизатор звертається до попереднього маршрутизатора, і той теж рахує хеші для заголовка. І так далі, аж до відправника. Цей метод гарний тим, що дозволяє в кілька разів знизити кількість необхідної пам'яті для зберігання журналів. Але є й недоліки. По-перше, апаратними засобами підрахунку повинен бути забезпечений кожен маршрутизатор. Враховуючи, що основу інтернету становлять не менше 100 000 маршрутизаторів, це недоцільно.

По-друге, жодна організація не має повного контролю над інтернетом, що унеможливлює повномасштабне розгортання даної системи.

Таким чином були визначені основні вимоги до зворотного відстеження IP адреси.

Проект автономних систем (АС) мислиться як єдина глобальна мережа, а не як з’єднання окремих дрібних мереж. Ми відстежуємо пакети через автономні мережі, а не через окремі маршрутизатори. Підхід на основі АС-мереж ґрунтується на двох спостереженнях. По-перше, підміна заголовків IP пакетів відбувається на індивідуальному комп’ютері, а не на індивідуальному маршрутизаторі. По-друге, повний шлях, який проходить пакет через всі маршрутизатори, не грає ролі. Нам тільки потрібно знати шлях через відповідні АС. Іншими словами, для зворотного відстеження немає необхідності ідентифікувати кожен маршрутизатор на шляху пакета [4].

Відповідно до цього підходу, обладнання, що виконує функції журналу, поміщується на маршрутизатор, який знаходиться на “кордоні” даної АС і пов’язує її з іншою АС. Це обладнання являє собою пасивний пристрій, який працює приблизно як прослуховування на телефонній лінії. Монітор журналу використовує оптичне перехоплення для збору даних з пакетів, що надходять на “прикордонний” маршрутизатор. Використання оптичного перехоплення гарантує, що монітор не впливає на швидкість роботи мережі. Монітор застосовує односторонній хеш-алгоритм до інформації в заголовку пакета. Кінцевим підсумком хешування будуть таблиці для фільтра Блума. Монітор зберігає тільки ці таблиці, все інше відкидається. Фільтри Блума добре підходять для моніторингу високошвидкісних мереж через ефективне стиснення даних в них, зводячи до мінімуму вимоги до розміру сховища і прискорюючи пошук необхідної інформації в них.

Кожна АС також повинна буде мати окремий сервер, який буде працювати з журналом, запускати алгоритм зворотного відстеження і взаємодіяти з такими ж серверами інших АС. Щоб визначити джерело, якщо пакет пройшов її мережу, сервер-монітор АС-мережі посилає запити всім подібним серверам на інших “прикордонних” маршрутизаторах (“Ви бачили цей пакет? Якщо так, то звідки він?”), кожен з яких у свою чергу шукає його в своїх таблицях. Якщо монітор відповідає ствердно, то сервер-монітор знає, де пакет “увійшов” в мережу і знає попередню АС на шляху. Процес повторюється на інших АС аж до знаходження відправника.

Для більш чіткого розуміння розглянемо наступний приклад. Потерпілий X підключений до автономних мереж A, B і C. X виявив

пакет атаки і відправляє запит зворотного відстежування в мережі A, B і C. Мережа A відповідає, що "бачила" цей пакет. Процедура повторюється в АС A, яка розсилає запити по мережах, з якими пов'язаний її сервер-монітор. І так до виявлення джерела або до межі розгортання АС. Джерело ідентифікується тоді, коли воно виявляється як "межа" мережі, тобто мережа, яка не має трафіку від інших мереж.

Слід зазначити, що цей підхід ефективний навіть за часткового розгортання АС з сервером зворотного відстежування. Для прикладу розглянемо ілюстрацію, у якій відсутній АС з сервером зворотного відстежування. Ви можете пропустити АС A і запросити наступну в необхідному напрямку АС безпосередньо. Це можливо тому що дані топології АС є загальнодоступними, бо це необхідно для функціонування протоколу маршрутизації BGP. Якщо попередня АС відповіла негативно, це означає, що A є джерело. Якщо одна з попередніх АС відповіла ствердно, процес триває як описано вище.

Моделювання підтвердило логіку, що лежить в основі підходу АС із зворотнім відстежуванням. Було розроблено необхідне обладнання, яке проходить тестування. Однак будь-який запропонований метод зворотнього відстеження IP слід оцінювати не тільки з технічної точки зору, але і в світлі практичних міркувань, з якими зіткнуться інтернет-провайдери при розгортанні даних систем. Попередні дослідження визначили вимоги, яким повинна відповідати система зворотного відстеження IP щоб бути ефективною:

1. Сумісність з існуючим обладнанням і протоколами.

АС із зворотнім відстежуванням не потребує модифікації існуючих маршрутизаторів, протоколів або пакетів.

2. Незначні розміри службового трафіку

АС із зворотнім відстежуванням використовує метод оптичного перехоплення даних про пакети, що гарантує безвідмовність роботи мережі і відсутність впливу на пропускну здатність.

3. Підтримка поступового впровадження.

АС із зворотнім відстежуванням не вимагають повного впровадження по всьому інтернету, щоб бути ефективними. Мережі, які не є учасниками АС, можуть пропускатися, і при зворотньому відстежуванні запити підуть на сусідні мережі. Крім того, ці системи масштабуються. У середньому, шлях в Інтернеті містить 15-19 маршрутизаторів, але тільки 3-4 з них включені в АС із зворотнім відстежуванням.

4. Мінімальна витрата часу і ресурсів.

Інформація збирається на серверах, які підключені до "прикордонних" маршрутизаторів, які підключені до своїх "сусідів". Так як

внутрішні маршрутизатори не беруть участь в даній системі, витрати, пов’язані з розгортанням, мінімальні.

5. Ефективність проти DDoS атак.

В цілому, відстеження IP на основі хеш-функцій вважається ефективним проти масованих DDoS атак. Зокрема, АС із зворотнім відстежуванням використовують існуючі системи виявлення вторгнень (IDS) для виявлення ознак DDoS атаки. Запити зворотнього відстежування можуть бути ініціалізовані або системою виявлення вторгнень, або оператором мережі вручну. Після первісного запиту процес йде в автоматичному режимі, в результаті чого процес ідентифікації джерела відбувається в реальному часі.

Ці питання – це лише верхівка айсберга, при якій доведеться зіткнутися при реальному впровадженні цієї системи. Існує широкий спектр організаційних, політичних, правових і соціальних питань, які повинні бути прийняті до уваги.

Література:

1. Лукацкий А. В. Предотвращение сетевых атак: технологии и решения / А. В. Лукацкий. – СПб. : Экспресс Электроника, 2006. – 268 с.
2. Терновой О.С. Раннее обнаружение DDOS-атак методами статистического анализа / Пер- спективы развития информационных технологий. – Новосибирск: Сибпринт, 2012. – С. 201–212.
3. Обзор механизмов реализации и обнаружения атак [Электронный ресурс]. – Режим доступа : http://comp-bez.ru/?p=778
4. Denial of Service Attacks // [Электронный ресурс]. – Режим доступа: http://www.cert.org/tech_tips/denial_of_service.html

“GLOBAL SCIENTIFIC UNITY 2014”
26-27 September 2014 Prague (Czech Republic)

The European professional scientific publication
Collection of scientific articles and theses
According to the results of International Scientific and Practical Congress

The International Scientific Association “Science & Genesis”
Chief Editor Geldof S.
Page planner: Becker T.
Copy editor: Hartmann D.
Graphic designer: Ochmann O.
Contact phone: +38067-29-79-439
E-mail: info@science-genesis.com
www.science-genesis.com