УДК 681.3:621.394

© 2009 р. С.М. Цирульник, Д.В. Кисюк, Т.О. Говорущенко[1]

Вінницький національний технічний університет, м. Вінниця;
[1] Хмельницький національний університет, м. Хмельницький

DDOS-АТАКИ Й МЕТОДИ БОРОТЬБИ З НИМИ

В статті описано природу DDOS-атак, а також наведено приклади масштабних DDOS-атак, які надовго вивели з роботи певні важливі сервери. Розглянута актуальність даної тематики. Проаналізовано мету й завдання DDOS-атаки, а також різні технології й види DDOS-атак. Описано відомі методи й засоби захисту від DDOS-атак та зроблено висновки про рішення щодо виявлення DDOS-атак та боротьби з DDOS-атаками.

In the article DDOS-attacks nature was described and scale DDOS-attacks examples, which disable certain important servers, were sited. Present subjects topicality was considered. DDOS-attacks goal and tasks and DDOS-attacks different technologies and kinds were analyzed. Known techniques and means of DDOS-attacks guard were described and the conclusions about decision concerning DDOS-attacks finding and fighting against DDOS-attacks were made.

Вступ

DDOS-атаки раніше використовувались для перевірок пропускної здатності мережі. Найбільш ефективним у цьому випадку є використання ICMP-пакетів (Internet control messaging protocol), тобто пакетів, що мають помилкову структуру. На обробку такого пакета потрібно більше ресурсів, після рішення про помилковість пакет відправляється назад, отже досягається основна мета – "забивається" трафік мережі [1]. Але зловмисники досить швидко усвідомили шкідливий потенціал цієї технології. У 1997 році за допомогою DDOS-атаки був майже на добу виведений з ладу сайт Microsoft. У 1999 році зловмисники зламали сервери таких великих компаній, як Yahoo, CNN, eBay [2]. Жовтень 2002 року ознаменувався найбільшою атакою на кореневі сервери Інтернету. Тоді жертвою хакерів стали сім із тринадцяти серверів [2]. Так, у травні 2008 року відбулася блокада естонських державних інтернет-порталів, у липні 2008 постраждали сайти держкомісії Литви зі службової етики, де на головній сторінці з'явилися зображення радянської символіки, недавно забороненої в країні [3].

20 липня 2008 року сайт президента Грузії піддався розподіленій DDOS-атаці. На інтернет-портал надійшла велика кількість TCP, ICMP і http-пакетів. Одним з повідомлень в отриманих пакетах була фраза "win+love+in+Rusia". DDOS-атака зробила сайт недоступним більш ніж на 24 години [3]. Основна хвиля кібервійни інтернет-порталів почалася ж із введенням військ Росії й Грузії на територію Південної Осетії. 8 серпня були атаковані сайти Міністерства закордонних справ Грузії, на головній сторінці якого з'явився колаж із зображень Гітлера й Саакашвілі й ряд інших урядових ресурсів. Тривалий час був недоступний сайт парламенту Грузії. Також був зламаний і практично знищений один із провідних грузинських інтернет-ресурсів "Грузія online".

10 серпня 2008 року став недоступний сайт російського інформаційного агентства "Риа-Новости". 11 серпня під блокаду потрапили сайти інформаційних агентств ИТАР ТАСС і REGNUM. Якийсь час був також недоступний російський ресурс новин Lenta.Ru. 11 серпня 2008 року сайт президента Грузії перенесений на сервери американської компанії Tulip Systems з метою захисту від хакерів, які, починаючи з 10 серпня, здійснюють DDOS-атаки на ресурс [4, 5].

Актуальність даної тематики

З погляду інформаційної безпеки зловмисник може реалізувати такі погрози [6]:

– модифікація інформації при передачі її по мережі або в процесі обробки й зберігання на комп'ютері користувача;
– порушення конфіденційності інформації;
– знищення інформації;
– порушення працездатності комп'ютера ("denial of service");

– несанкціоноване використання ресурсів комп'ютера;
– запис довільних даних на локальний комп'ютер;
– роздратування користувача.

Однією із найнебезпечніших погроз є віртуальні DDOS-атаки. Непрямі збитки від однієї подібної атаки можуть становити сотні тисяч доларів у день.

Мета й завдання DDOS-атаки

DOS-атака (Denial of Service - "відмова в обслуговуванні") і DDOS-атака (Distributed Denial of Service – "розподілена відмова обслуговування") – це різновиди атак зловмисника на комп'ютерні системи. Їхньою метою є створення таких умов, при яких легітимні (правомірні) користувачі системи не можуть одержати доступ до надаваних системою ресурсів, або цей доступ ускладнений.

Наприклад, вони особливо небезпечні для компаній, які пов'язані з телекомунікаційним ринком і просто не можуть собі дозволити стати жертвами зловмисників. Компанії несуть цілком відчутні фінансові збитки, як прямі, так і непрямі. Заблокований сайт для організації означає втрачену вигоду, а витрати на відбиття атаки або звертання до сторонніх сервіс-провайдерів досить відчутні для бюджету. Захист від DDOS-атак особливо важливий для інтернет-магазинів, ресурсів новин та інших компаній, діяльність яких передбачає постійні звернення користувача до ресурсу.

У випадку ж з віртуальною війною DDOS-атаки наносять більш значні іміджеві втрати, ніж матеріальні [1, 2, 7].

Зміст атаки на офіційні сайти владних органів очевидні – продемонструвати слабкість структур безпеки. Якщо такі атаки будуть вестися на DNS-сервери і поштові сервери, то у держустанов із засобів зв'язку залишаться лише телефон і факс.

Якщо на початку DDOS-атаками "бавилися" більше заради слави або з почуття помсти, то зараз цей бізнес приносить своїм організаторам цілком відчутні прибутки. Наприклад, DDOS-атаки використовуються для шантажу, у цих випадках злочинна група обіцяє припинити потік *flood* в обмін на деяку кількість готівки. Проте, відомо, що більшість онлайн-казіно й офшорних компаній платять хакерам превентивно.

DDOS-атака може використовуватися і як прикриття для запуску інших шкідливих програм, за допомогою яких зловмисник може викрасти конфіденційні дані, які потім продаються конкурентам.

Технологія й види DDOS-атак

Схематично DDOS-атака виглядає приблизно так: на обраний в якості жертви сервер навалюється величезна кількість помилкових запитів з безлічі комп'ютерів з різних кінців світу. У результаті сервер витрачає всі свої ресурси на обслуговування цих запитів і стає практично недоступним для звичайних користувачів. Цинічність ситуації полягає в тому, що користувачі комп'ютерів, з яких направляються помилкові запити, можуть навіть не підозрювати про те, що їхня машина використовується хакерами. Програми, встановлені зловмисниками на цих комп'ютерах, прийнято називати "зомбі". Відомі безліч шляхів "зомбіювання" комп'ютерів – від проникнення в незахищені мережі до використання програм-троянів [7, 8]. Цей підготовчий етап є для зловмисника найбільш трудомістким.

Найчастіше зловмисники при проведенні DDOS-атак використовують трьохрівневу архітектуру (рис.1), що називають "кластер DDOS". Така ієрархічна структура містить:
– консоль керування (їх може бути декілька), тобто той комп'ютер, з якого зловмисник подає сигнал про початок атаки;
– головні комп'ютери. Це ті машини, які одержують сигнал про атаку з консолі керування й передають його агентам -"зомбі". На одну керуючу консоль залежно від масштабності атаки може доводитися до декількох сотень головних комп'ютерів;

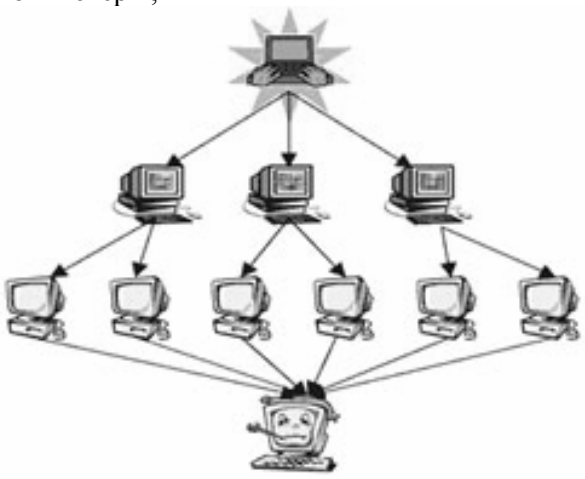

Рис. 1. Трирівнева архітектура для проведення DDOS-атак

– агенти – безпосередньо самі "зомбі"-комп'ютери, що своїми запитами атакують вузол-мішень.

Простежити таку структуру у зворотньому напрямку практично неможливо. Як відомо, і комп'ютери-агенти, і головні комп'ютери є також потерпілими в даній ситуації й називаються "скомпрометованими". Така структура робить практично неможливим відстежити адресу вузла, що організував атаку.

Інша небезпека DDOS полягає в тому, що зловмисникам не потрібно мати якісь спеціальні знання й ресурси. Програми для проведення атак вільно поширюються в мережі. За роки це програмне забезпечення постійно модифікувалося й до теперішнього часу фахівці з інформаційної безпеки виділяють наступні види DDOS-атак [1, 2, 6]:

1.*UDP flood* – відправлення на адресу системи-мішені безлічі пакетів UDP (User Datagram Protocol). Цей метод використовувався на ранніх атаках і в цей час вважається найменш небезпечним. Програми, що використовують цей тип атаки легко виявляються, тому що при обміні головного контролера й агентів використовуються нешифровані протоколи TCP і UDP.

2.*TCP flood* – відправлення на адресу мішені безлічі TCP-пакетів, що також приводить до "зв'язування" мережних ресурсів.

3.*TCP SYN flood* – відправлення великої кількості запитів на ініціалізацію TCP-з'єднань із вузлом-мішенню, якому в результаті доводиться витрачати всі свої ресурси на те, щоб відслідковувати ці частково відкриті з'єднання.

4.*Smurf-атака* – ping-запити ICMP (Internet Control Message Protocol) за адресою спрямованого широкомовного розсилання з використанням у пакетах цього запиту фальшивої адреси джерела, яка в результаті виявляється мішенню атаки.

5.*ICMP flood* – атака, аналогічна Smurf, але без використання розсилання.

Природно, найнебезпечнішими є програми, що використовують одночасно кілька видів описаних атак. Вони одержали назву *TFN і TFN2K* і вимагають від хакера високого рівня підготовки [8].

Однією з останніх програм для організації DDOS-атак є *Stacheldracht*, що дозволяє організовувати всілякі типи атак і лавини широкомовних ping-запитів із шифруванням обміну даними між контролерами й агентами.

Захист від DDOS-атак

З погляду інформаційного захисту DDOS-атаки є однією із найскладніших мережевих погроз, тому вживання ефективних заходів протидії є винятково складним завданням для організацій, діяльність яких залежить від інтернету. Міри протидії DDOS-атакам можна розділити на пасивні й активні, а також на превентивні й реакційні [9]. Розглянемо основні методи.

Запобігання. Профілактика причин, що спонукують тих або інших осіб організовувати DDOS-атаки. Дуже часто атаки є наслідками особистої образи, політичних, релігійних розбіжностей, що провокує поводження жертви.

Розосередження. Побудова розподілених і резервних систем, які не припинять обслуговувати користувачів навіть якщо деякі їхні елементи стануть недоступні через атаку.

Відхилення. Відвести безпосередню ціль атаки (доменне ім'я або IP-адресу) подалі від інших ресурсів, які часто піддаються впливу разом з безпосередньою ціллю.

Фільтрація. Фільтрація трафіку на маршрутизаторах – поки найпоширеніший метод протидії. Фільтри варто вводити можливо ближче до джерела *flood*. Міжмережеві екрани й спеціалізовані *antiflood* засоби фільтрації – найбільш ефективна міра, але й найбільш дорога. Наприклад, програмний засіб Ados [10] є динамічним фільтром TCP-пакетів, здатним блокувати в реальному часі доступ до вебсерверу з IP-адрес, що генерують інтенсивний потік HTTP-запитів. Знизити витрати можна, розділяючи такі системи між багатьма клієнтами (фільтрація на вимогу).

Нарощування. Якщо *flood* спрямований на вичерпання ресурсів, самий примітивний спосіб протидії *flood* – нарощування своїх ресурсів, щоб супротивник не зміг їх вичерпати.

Сучасні засоби захисту від DDOS-атак дозволяють із досить високим ступенем ефективності виявити атаку й зменшити або запобігти збитку ресурсам операторів і їхніх клієнтів. Компанія "NVisionGroup" пропонує комплексне рішення для захисту від DDOS-атак на основі технології Cisco Clean Pipes [11], що забезпечує оперативну реакцію на DDOS-атаки, легко масштабується, має високу надійність і швидкодію.

Технологія Cisco Clean Pipes припускає використання модулів Cisco Anomaly Detector і Cisco Guard, а також різні системи статистичного аналізу мережевого трафіку, засновані на да-

них, одержуваних з маршрутизаторів за протоколом Cisco Netflow. При цьому Anomaly Detector і системи статистичного аналізу трафіку виступають як системи виявлення DDOS-атак, а Cisco Guard як засіб протидії вже виявленій атаці. У загальному випадку технологія Clean Pipes припускає наявність етапу тестування (навчання), що проводиться в період відсутності DDOS-атак на ресурс, що захищається. На цьому етапі пристрої виявлення визначають і запам'ятовують, який трафік для ресурсу, що захищається, є нормальним. Ситуація, при якій поточний трафік на ресурс, що захищається, різко відрізняється від нормального, уважається DDOS-атакою. При виявленні DDOS, система виявлення повідомляє оператору та активує підсистему захисту Cisco Guard.

Висновки

DDOS-атаку дуже складно виявити й запобігти, оскільки "шкідливі" пакети не відрізняються від "легітимних". Мережеві пристрої й традиційні технічні рішення для забезпечення безпеки мережевого периметру, такі як міжмережеві екрани й системи виявлення вторгнень (IDS), є важливими компонентами загальної стратегії мережевої безпеки, однак самі ці пристрої не забезпечують повного захисту від DDOS-атак. Міжмережеві екрани дозволяють або забороняють проходження мережевого трафіку на підставі аналізу різних полів мережевих пакетів. Але DDOS-атака може бути успішно реалізована в рамках дозволених міжмережевим екраном потоків трафіка. Оскільки трафік DDOS-атаки – це звичайні мережеві пакети, кожен з яких окремо собою атаку не представляє, то система IDS не виявить таку атаку. У деяких випадках, при проведенні таких атак використовується підміна IP-адрес джерела, через що стає неможливою ідентифікація шкідливого трафіку від конкретного джерела.

Для боротьби з DDOS-атаками необхідно використовувати комбіновані рішення: на рівні сервера, на рівні сервісів сервера, на рівні мережі, на рівні провайдера, на рівні апаратури, на рівні адміністраторів сервера.

СПИСОК ЛІТЕРАТУРИ

1. *Андрончик А.Н. и др.* Защита информации в компьютерных сетях. Практический курс. – Екатеринбург: УГТУ-УПИ, 2008. – 248 с.
2. *Мельников В.П. и др.* Информационная безопасность и защита информации. - М.:Академия, 2008. – 336 с.
3. DDos-война: кто стравливает Россию и Грузию? // Cnews.ru, 18 августа 2008 г. — *http://www.cnews.ru/reviews/index.shtm?2008/08/18/313221*
4. Война: российские СМИ под шквалом DDoS-атак // Cnews.ru, 11 августа 2008 г. — *http://www.cnews.ru/news/top/index.shtml?2008/08/11/311644*
5. Российско-грузинский DDoS-конфликт // Приложение к газете "Коммерсантъ" № 225(4042) от 10.12.2008. — *http://www.kommersant.ru/doc.aspx?*
6. *Расторгуев С. П.* Информационная война – М: Радио и связь,1999. – 416 с.
7. *Чирилло Дж.* Обнаружение хакерских атак. Для профессионалов. — СПб.: Питер, 2002. — 864 с.
8. Удар издалека // Спецвыпуск: Хакер, номер #048, стр. 048-030-3. – *http://www.xakep.ru/magazine/xs/048/030/1.asp*
9. 100% защита от DDoS// SysAdmin Online-Безопасность, 8 января 2008 г. – *http://sysadminonline.ru /100-zaschita-ot-ddos/*
10. Программная Анти-DDOS защита. Недорогой способ отражения большинства DDOS атак // Офіційна сторінка програмного забезпечення ANTIDDOS. – *http://antiddos.ru*
11. Защита от DoS-атак компании MacHoster.Ru // Офіційна сторінка компанії MacHoster. – *http://machoster.ru/index.php?newsid=8*

S.M. Cirulnik, D.V. Kysuk, T.O. Govorushchenko.
DDOS-attacks and Techniques of Fight Against Them

С.М. Цирульник, Д.В. Кисюк, Т.О. Говорущенко
DDOS-атаки и методы борьбы с ними

В статье описана природа DDOS-атак, а также приведены примеры масштабных DDOS-атак, которые надолго вывели из строя некоторые важные серверы. Рассмотрена актуальность данной тематики. Проанализированы цель и задание DDOS-атаки, а также разные технологии и виды DDOS-атак. Описаны известные методы и средства защиты от DDOS-атак и сделаны выводы о решениях относительно выявления DDOS-атак и борьбы с DDOS-атаками.