

---

УДК 004.056

I.B. Рубан, С.С. Серов

*Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков*

## **ИССЛЕДОВАНИЕ УДАЛЕННЫХ АТАК НА РАСПРЕДЕЛИТЕЛЬНО ВЫЧИСЛИТЕЛЬНЫЕ СЕТИ**

*Статья посвящена исследованию удаленных атак на РВС, их актуальность, типы угроз и дальнейшее исследование, современных технологий удаленных атак.*

**Ключевые слова:** распределенная система, атака, отказ в обслуживании.

### **Актуальность**

В наше время главной ценностью на планете считается информация, следовательно её, как и всякую другую ценность, человек старается сохранить от посторонних рук и глаз. Изобретение компьютера и дальнейшее бурное развитие технологий во второй половине XX века сделали проблему защиты информации настолько актуальной и острой, насколько актуальна сегодня информатизация для всего общества. Особенно актуально стоит этот вопрос в области секретной информации государства и частной коммерческой информации.

Современные вычислительные сети организаций представляют собой сложные системы, состоящие из множества компонентов. Среди этого множества компонентов можно выделить разнообразные компьютеры, системное и прикладное программное обеспечение (ПО).

Статистика нарушений показывает, что количество атак имеет тенденцию к экспоненциальному росту. Сама сеть Интернет является благодатной почвой для вторжения злоумышленников в компьютерные системы. Для получения необходимой информации, нарушители используют специально разработанные средства и скрипты, которые потом могут использовать (более слабые категории нарушителей) в проведении своих атак. Обычно новые угрозы используют неизвестные, или только что обнаруженные уязвимости.

Все угрозы, можно разделить на внешние и внутренние. Внешними угрозами являются те, которые исходят извне. Внутренние угрозы инициируются субъектом, имеющим доступ к инфраструктуре организации. Угрозы реализуются с помощью сетевых атак, или удаленных сетевых атак. Под удаленной сетевой атакой, надо понимать воздействие на программные компоненты целевой системы с помощью программных средств. На сегодняшний день в средствах массовой информации приводят факты и ошеломляющие цифры ущерба от атаки- это определяется низким и недостаточным уровнем обеспечения безопасности в компьютерных системах.

### **Основной материал**

Основной особенностью любой распределенной системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений и программно при помощи механизма сообщений. Для того чтобы защититься от атак, необходимо их изучать и классифицировать, в связи с этим не прекращаются попытки, изучить уязвимости и предотвращать их. На рис. 1 приведена классификация удаленных атак.

На данный момент существует множество типов атак, но более всего эффективный и распространенный –это ddos атака. Рассмотрим подробнее что такое Ddos атака-это атака переводится как «распределенный отказ в обслуживании». Ddos атака – сово-



Рис. 1. Классификация удаленных атак

купность действий, приводящих к перегрузке сервера, зависанию системы из-за ложных запросов и прочего. Ежегодно такие атаки, стоят различным компаниям и госструктурам миллиарды долларов и таят в себе серьезную угрозу для любой компьютерной системы. Типы таких атак нарушают или полностью блокируют обслуживание законных пользователей, сетей, систем и иных ресурсов. Результат таких атак – длительные простой системы, потерянная прибыль, большие объемы работ по идентификации атак и подготовка адекватных ответных мер.

Существует два основных типа атак, вызывающих отказ в обслуживании :

1) Когда злоумышленник посыпает жертве данные или пакеты, которые она не ожидает, и это приводит либо к остановке системы, а также к ее перезагрузке, значит, взломщик проводит **атаку ddos**, поскольку никто не сможет получить доступ к ресурсам. Таким образом, первый тип атак является наиболее разрушительным, поскольку осуществить атаку легко, а для устранения ее последствий требуется вмешательство оператора.

2) Второй (более распространенный) тип атак приводит к переполнению системы или локальной сети с помощью такого большого количества информации, которое невозможно обработать. Например, если система может обрабатывать только 40 пакетов в секунду, а взломщик отправляет 50 пакетов в секунду, то когда законные пользователи пытаются подключиться к системе, они получают отказ в обслуживании, поскольку все ресурсы заняты. При такой атаке злоумышленник должен постоянно переполнять систему пакетами. После того как он перестает заполнять систему пакетами, проведение атаки прекращается, и сис-

тема возобновляет нормальную работу. Этот тип атаки требует больших усилий со стороны взломщика, поскольку ему необходимо постоянно активно воздействовать на систему. Иногда этот тип атаки приводит к остановке системы, однако в большинстве случаев восстановление после проведения этой атаки требует минимального вмешательства человека. При проведении **DDoS-атаки** второго типа подвергшаяся нападению информационный ресурс (чаще всего это сервер) получает пакеты одновременно от большого количества машин, хозяева которых сами могут и не подозревать о происходящем. Кроме того, поскольку эти атаки проводятся с широкого диапазона IP-адресов, становится гораздо сложнее блокировать и обнаруживать нападение по той причине, что небольшое количество пакетов с каждой машины может не вызвать реакции со стороны систем обнаружения вторжений. Если атака проводится с одного IP-адреса, его можно блокировать с помощью брандмауэра. Если же задействовано 700-800 машин, то блокировать их становится чрезвычайно трудно. Причем, как правило, атака против единственной жертвы проводится с множества компьютеров, разбросанных по всему миру. Если даже проводимые с одного источника атаки **DDoS** бывает сложно предотвращать, то можно себе представить, насколько сложнее защищаться от таких атак, которые проводятся с множества машин, расположенных в разных местах. К тому же от атак **DDoS** защититься довольно сложно еще и потому, что жертва никогда не может исключить полностью возможность ее проведения. Если компьютерная система подключается к Интернету, то всегда есть вероятность того, что взломщик может отправить в нее такое количество данных, которое она будет не в состоянии обрабатывать.

На данный момент активно распространяется новый метод Ddos-атак это "HTTP-POST". Уязвимость опирается на так называемый «медленный» POST-трафик, который затруднительно дифференцировать от законного обмена данными. DDOS-атаки легко проводить в окружении многопользовательских онлайновых игр как среди распределенных компьютерных сетей, затрагивающих массу вычислительных систем.

Что интересно, «медленная» POST-технология может быть вполне адаптирована для работы с SMTP и даже DNS-серверами. Атака работает так: вредоносный код отправляет POST-заголовки с легитимно заполненными полями, касающимися размеров готовящихся к передаче данных, однако последние затем передаются на очень низких скоростях, что приводит к формированию «заторов» на серверах и связыванию их системных ресурсов. Достаточно нескольких десятков тысяч ботов, чтобы отключить сервер. Балансирующее нагрузку ПО, ныне используемое для предотвращения DDOS-атак, не эффективно против новой методики. Поэтому дальше стоит более подробно изучать этот метод работы.

#### **Какие недостатки у методов борьбы с сетевыми атаками?**

Продукты по обнаружению атак используются в качестве дополнения к существующей системе защиты информации, позволяя обнаруживать злоумышленные действия направленные против информационной системы. На сегодняшний день одной из актуальных задач в сфере информационных технологий является метод борьбы с сетевыми атаками.

Возникающие сетевые угрозы потребовали внедрения адекватных мер защиты. Традиционные технические решения для обеспечения безопасности сетевого периметра — такие, как межсетевые экраны и системы обнаружения вторжений (IDS) — сами по себе не обеспечивают защиты от DDoS-атак. Межсетевые экраны позволяют разрешить либо запретить прохождение сетевого трафика на основании анализа различных полей сетевых пакетов. Атака может быть успешно реализована в рамках разрешенных межсетевым экраном потоков трафика. А классические системы IDS, работающие по принципу сигнатурного анализа трафика. Трафик DDoS-атаки — это обычные сетевые пакеты, каждый из которых в отдельности собой атаку не представляет, и система IDS такую атаку не обнаруживает. Ведь Пользователи, компьютеры которые генерируют

паразитический трафик, как правило, даже не подозревают, что их ПК стал инструментом в руках злоумышленников. Да и практически невозможно отличить вредоносный трафик от легитимного.

#### **Выводы**

Выделим основные недостатки, по которым реализуется удаленная атака:

- 1) использование широковещательной среды передачи (например, Ethernet);
- 2) применение нестационарных алгоритмов идентификации удаленных субъектов и объектов РВС;
- 3) использование протоколов динамического изменения маршрутизации с нестационарными алгоритмами идентификации;
- 4) применение алгоритмов удаленного поиска с использованием широковещательных и направленных поисковых запросов;

5) возможность анонимного захвата одним субъектом РВС множества физических или логических каналов связи.

Итак, основными научными направлениями в разработке, борьбы с Ddos атаками являются:

- разработка эвристических методов идентификации факта возникновения сетевой атаки
- разработка методов быстрого установления источника сетевой атаки
- разработка методов быстрого блокирования источника сетевой атаки.

#### **Список литературы**

1. Секреты хакеров. Безопасность сетей - готовые решения / Мак-Клар Сьюард и др. – М.: Издательский дом «Вильямс», 2001. 722 с.
2. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий. – СПб.: БХВ-Петербург, 2001. – 624 с.
3. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, В.А. Олифер. – СПб. : БХВ-Петербург, 2001. – 978 с.
4. Таненбаум Э. Компьютерные сети / Э. Таненbaum. – СПб.: ПИТЕР, 2003. – 1120 с.
5. Ярочкин В.В., Информационная безопасность / В.В. Ярочкин. – М.: Наука, 2006. – 544 с.
6. Понятие типовой угрозы безопасности [Электронный ресурс]. – Режим доступа к ресурсу: <http://www.sources.ru/security/attack/2/03-02.html>.

Поступила в редакцию 29.03.2013

**Рецензент:** д-р техн. наук доц. К.С. Смеляков, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

#### **ДОСЛІДЕННЯ ВІДДАЛЕНИХ АТАК НА РОЗПОДІЛЬЧІЙ ОБЧИСЛЮВАЛЬНІЙ МЕРЕЖІ**

І. В. Рубан, С.С Серов

Стаття присвячена дослідженню віддалених атак на РВС, їх актуальність, типи погроз і подальше дослідження, сучасних технологій віддалених атак.

**Ключові слова:** розподілена система, атака, відмова в обслуговуванні.

#### **STUDY OF AN ATTACK AGAINST THE COMPUTER NETWORK OF DISTRIBUTION**

I.V. Ruban, S.S.Serov

The article is devoted to the study of remote attacks on the DNC, their relevance, the types of threats and further study of modern technologies of remote attacks.

**Keywords:** distributed system, attack, refuse in service