УДК 004

Классификация методов проведения DDoS-атак

Дмитрий КОВАЛЕВ

Dmitry A.KOVALIEV

Ковалев Дмитрий Алексеевич *– инженер, аспирант кафедры «Вычислительные системы и сети» Московского государственного университета путей сообщения (МИИТ).*

Описание атак типа «распределенный отказ в обслуживании» (DDoS-атака) в сети Интернет. Классификация по направленности и механизмам реализации. Типовые способы и опора на иерархичность обобщенной структуры. Предложенная в статье иерархическая классификация является универсальной, если иметь в виду механизмы проведения DDoS-атак, и достаточной для понимания процесса их организации. Она способна служить базисом при разработке средств обнаружения и идентификации DDoS-атак по определенным протоколам уровня приложений, что придает ей значимость не только с аналитической точки зрения, но и с практической.

Ключевые слова: транспорт, система управления, процессинг, Интернет, отказ в обслуживании, DDoS-атаки, классификация, иерархичность структуры, безопасность.

Проблематика защиты от DDoS-атак остается одной из самых актуальных на современном этапе развития Интернета. Каждая компания, чья деятельность связана с глобальной сетью, может стать жертвой DDoS-атак. Главной их целью является обеспечить недоступность целевого ресурса для легитимных пользователей.

Согласно Computer Incident Advisory Capability (CIAC), первые DDoS-атаки были зафиксированы в 1999 году, а уже в 2000-м осуществлен крупномасштабный налет на Yahoo.com, вследствие которой компания понесла значительные убытки. 20 октября 2002 года последовала крупная DDoS-атака на тринадцать корневых DNS-серверов. К 2010 году максимальная мощность интервенций, по данным компании Arbor Networks [1], составила 100 гигабит в секунду.

С развитием различных электронных сервисов проблематика DDoS-атак становится все более актуальной и на транспорте. 16 июля 2010 года было организовано нападение на сайт ОАО «Аэрофлот», который обслуживается процессинговой системой «Ассист». Последствием атаки стала полная недоступность сервиса покупки электронных билетов через сайт авиаперевозчика в течение нескольких дней. Для «Аэрофлота»

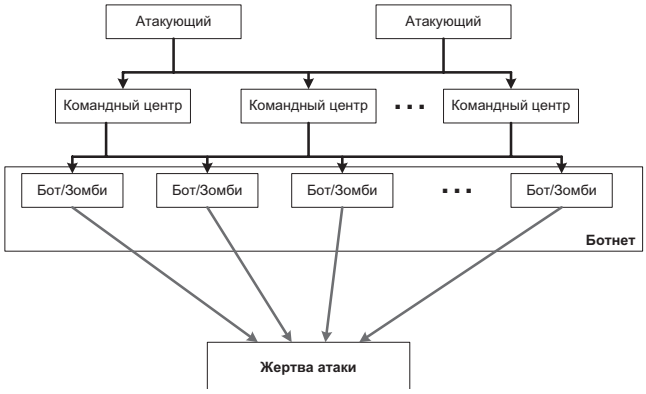

Рис. 1. Общая структура реализации DDoS-атак.

материальный ущерб превысил 146 миллионов рублей [7].

1. ОРГАНИЗАЦИЯ АТАК

Для DDoS-атаки злоумышленник организует сеть из скомпрометированных ранее компьютеров и серверов-ботнет, деятельность которых контролируется с помощью специализированных центров управления – командных центров. С помощью такого центра отдаются команды ботам на атаку, после чего на целевом ресурсе фиксируется лавинообразное увеличение объема вредоносного трафика. Пользователь скомпрометированного компьютера зачастую не подозревает, что в данный момент его аппарат является частью агрессии. Общая структура реализации DDoS-атаки представлена на рис. 1.

2. ЗАЩИТА ОТ DDoS-АТАК

Основными этапами защиты и предупреждения DDoS-атак служат:

- этап мониторинга;
- этап обнаружения атаки;
- этап противодействия атаке.

Механизмы мониторинга выполняют контроль над сбором статистических данных и построение необходимых статистических профилей нормального поведения различных параметров сетевого трафика для объекта мониторинга. Объектом мониторинга является часть анализируемого трафика, соответствующая определенным критериям. Критериями предназначены служить диапазоны IP-адресов, трафик к определенным сервисам или приложениям (HTTP, DNS, FTP и другие). Статистические данные механизма мониторинга могут содержать в себе параметры (сигнатуры) уже существующих типов атак.

На этапе обнаружения атаки осуществляется сравнение текущих параметров проходящего трафика со статистическими параметрами. Обнаружение DDoS-атаки происходит путем исследования отклонений текущего трафика от нормального профиля его прохождения.

Второй основной задачей на этапе обнаружения атаки становится классификация аномалий. На основании классификации выбирается определенный набор контрмер, требуемый для подавления атаки, а также устанавливаются вероятные ее источники. Классификация аномалий входит в число приоритетных задач в механизмах противодействия DDoS-атакам.

Механизмы противодействия представляют совокупность контрмер, направленных на блокировку и выделение нелегитимного трафика из его общего потока. Процесс применения набора контрмер для текущего трафика объекта называют очисткой и смягчением трафика атаки.

3. ТИПОВЫЕ СПОСОБЫ КЛАССИФИКАЦИИ

С момента появления первых DDoS-атак было разработано множество механизмов их классификации, которые опираются на различные критерии [2–6]:

- тип ресурса, на который направлена атака;
- тип протокола, используемый для реализации атаки;
- по типу используемых уязвимостей;
- по виду воздействия;
- по мощности и динамике атаки;
- по степени автоматизации.

Наиболее подробно классификация DDoS-атак рассмотрена в работах Мирковича, Мартина [4], Асосхех и Рамезани [3].

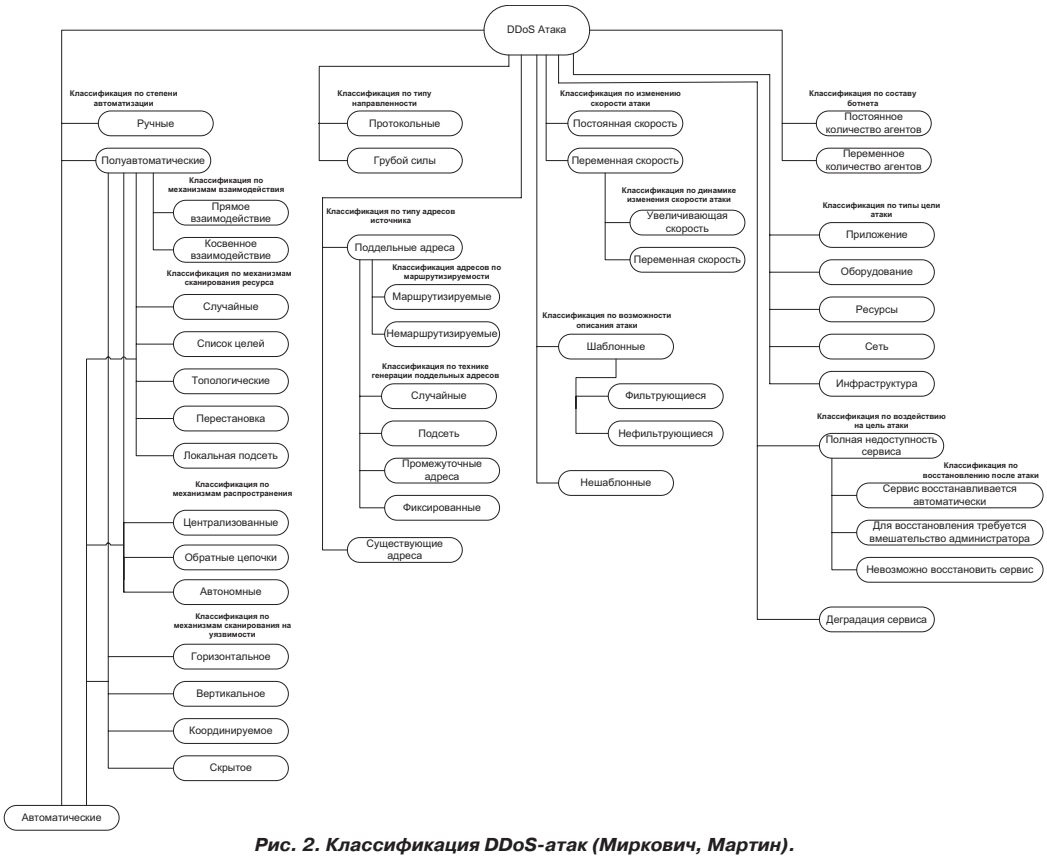

Рис. 2. Классификация DDoS-атак (Миркович, Мартин).

В них выстраивается систематика механизмов реализации DDoS-атак на основе различных критериев классификации. На рис. 2 представлена классификация DDoS-атак, предложенная Мирковичем и Мартином:

Данная классификация описывает обобщенную структуру и методику проведения DDoS-атак, но в связи со своей сложностью и разобщенностью не подходит для реализации ее в механизмах обнаружения и предотвращения атакующих действий.

4. ИЕРАРХИЧЕСКАЯ КЛАССИФИКАЦИЯ DDoS-АТАК

На рис. 3 представлена предлагаемая схема иерархической классификации DDoS-атак. Основными аспектами при составлении данной классификации были:

- направленность DDoS-атаки;
- обобщенная структура механизмов проведения DDoS-атак.

Направленность DDoS-атаки заключается в выборе злоумышленником типа ресурса или протокола, на который должна быть нацелена агрессия. На первоначальном уровне классификации все атаки разделяются на два вида, в зависимости от типа ресурса, на который совершается нападение.

Главной целью DDoS-атак на сетевые ресурсы является переполнение выделенной полосы пропускания сетевого трафика жертвы. При реализации плана агрессии определяющим фактором служит выбор протокола для проведения атаки:

- При DDoS-атаке по протоколу TCP с жертвой устанавливается множество TCP-сессий, в рамках которых передается большое количество случайно сгенерированных данных, либо просто посылается множество TCP-сегментов большого размера без установления соединения.
- При DDoS-атаке по протоколу UDP или ICMP жертве посылается множество UDP-сегментов, либо ICMP-пакетов большого размера.
- При DDoS-атаке по остальным протоколам жертве посылается множество пакетов большого размера с различным содержанием параметров заголовка пакета и случайно сгенерированными данными в его теле.

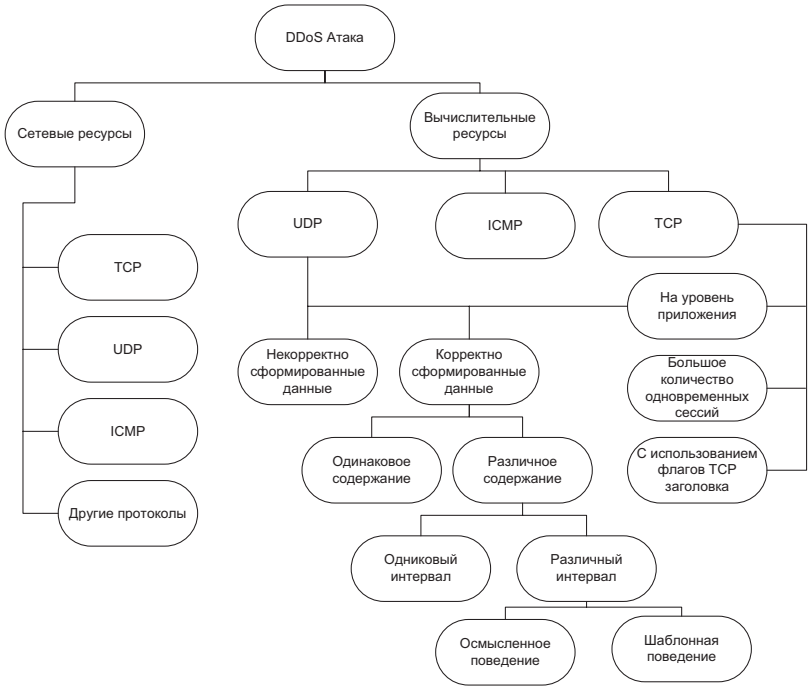

Рис. 3. Классификация DDoS-атак по их направленности и механизмам реализации.

Методы DDoS-атак, направленных на исчерпание вычислительных ресурсов, зависят от работающих на оборудовании жертвы сервисах и приложениях, а также используемых ими коммуникационных протоколов. Исходя из классификации, далее данный тип атак разделяется на три подтипа в зависимости от протокола, с помощью которого реализуется атака.

При осуществлении DDoS-атаки по протоколу ICMP жертве посылается большое количество ICMP-пакетов, при этом вычислительные ресурсы объекта атаки тратятся на их обработку.

DDoS-атаки на вычислительные ресурсы по протоколу TCP реализуются по трем основным направлениям:

- С жертвой устанавливается большое количество одновременных TCP-сессий, в рамках которых данные либо не передаются совсем, либо передаются малыми партиями.
- При проведении атак с использованием TCP-флагов жертве посылается большое количество TCP-сегментов (чаще всего с поддельных IP-адресов) с различными комбинациями поля флагов. Наиболее известный пример реализации данного типа атак – на установление соединений – SYN-food.
- Атаки на уровень приложений непосредственно предполагают исчерпание вычислительных ресурсов жертвы за счет обработки большого количества нелегитимного трафика.

DDoS-атаки по протоколу UDP аналогичны по своему воздействию атакам на приложения по протоколу TCP, с той разницей, что приложение должно использовать в своей работе протокол UDP.

Дальнейшая классификация DDoS-атак, направленных на приложения, зависит только от сложности организации механизмов их проведения.

DDoS-атаки с некорректно сформированными данными характеризуются неправильным заполнением полей заголовка или данных запроса на уровне приложений.

Такие же операции с корректно сформированными данными различаются по динамике изменения их содержания в течение атаки – они либо не меняются, либо нелегитимный трафик несет в себе меняющиеся со временем данные. Причем данные от определенного источника атаки могут поступать как с одинаковыми, так и различными по времени частотными интервалами.

При шаблонном поведении информация, посылаемая источником DDoS-атаки приложению, генерируется на основе заранее определенного образца.

При осмысленном поведении источник DDoS-атаки ведет себя максимально прибли-

женно или практически не отличается от легитимных источников трафика. Данный тип считается самым сложным механизмом как для реализации DDoS-атак, так и организации противодействия.

ЗАКЛЮЧЕНИЕ

Предложенная в статье иерархическая классификация является универсальной, если иметь в виду механизмы проведения DDoS-атак, и достаточной для понимания процесса их организации. Иерархичность может качественно сократить время анализа в ходе решения типовых задач, связанных с защитой объекта и предупреждением злоумышленных посягательств. Классификация такого рода способна служить базисом при разработке средств обнаружения и идентификации DDoS-атак по определенным протоколам уровня приложений, что придает ей значимость не только с аналитической точки зрения, но и с практической.

ЛИТЕРАТУРА

1. Roland Dobbins, Carlos Morales. Worldwide Infrastructure Security Report. 2010 Report www.arbornetworks.com

2. Nirbhay Ahlawat, Chetan Sharma, Classification and Prevention of Distributed Denial of Service Attacks // International Journal of Advanced Engineering Sciences and Technologies. 2011, Vol 3, No. 1, 052–060.

3. Abbass Asosheh, Naghmen Ramezani, A Comprehensive Taxonomy of DDoS Attacks and Defense Mechanism Applying in a Smart Classification // Wseas Transactions on Computers. April 2008, Vol. 7, No 4.

4. J. Mirkovic, J. Martin, et al., A Taxonomy of DDoS Attacks and DDoS Defence Mechanisms // Computer Science Department, University of California, 2002.

5. Christos Douligeris, Aikaterini Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art // Computer Networks 44, 2004, pp 643–666.

6. T. Subbulakshmi, S. Mercy Shalinie, A. Ramamoorthi, Detection and Classification of DDoS Attacks Using Machine Learning Algorithms in: European Journal of Scientific Research. 2010, Vol.47, No.3.

7. Дело о DDoS-атаке н а «Аэрофлот» вернули в прокуратуру: такого обвинения не существует // Газета.Ru, 2012. http://www.gazeta.ru/social/news/2012/06/13/n_2387569.shtml (последний доступ 03.03.2013).

CLASSIFICATION OF THE METHODS OF DDOS-ATTACKS

Kovaliev, Dmitry A. *– engineer, Ph.D. student at the department of compution systems and networks of Moscow State University of Railway Engineering (MIIT), Moscow, Russia.*

The article describes Internet distributed denial of service- attacks (DDoS-attacks) and proposes classification of such offences by the objectives and tools of realization, making distinction between typical methods and those based on the hierarchy of generalized structure.

The hierarchical classification proposed in the article can be considered to be universal from the point of view of DDoS-attacks mechanisms and sufficient for understanding of the processes of their organization. The hierarchy-based approach can significantly reduce the time of analysis during solving typical problems, necessary for the protection of a system and for neutralization of malicious attempts. Such classification can serve as a basis for engineering of the tools of detection and identification of DDoS-attacks in certain protocols at application level which makes it not only analytic but practically oriented as well. See the modern electronic service systems for customers in the transport sphere it can be useful for the protection of this sector too.

Key words: transport, control system, processing, Internet, denial of service, classification, DDoS-attacks, hierarchical structure, security.

REFERENCES

1. Roland Dobbins, Carlos Morales, Worldwide Infrastructure Security Report. 2010 Report. www.arbornetworks.com (last accessed 20.06.2012).

2. Nirbhay Ahlawat, Chetan Sharma. Classification and Prevention of Distributed Denial of Service Attacks // *International Journal of Advanced Engineering Sciences and Technologies*, 2011, Vol 3, No. 1, 052–060.

3. Abbass Asosheh, Naghmen Ramezani, A Comprehensive Taxonomy of DDoS Attacks and Defense Mechanism Applying in a Smart Classification in: Wseas Transactions on Computers. April 2008, Vol. 7, No 4.

4. J. Mirkovic, J. Martin, et al. A Taxonomy of DDoS Attacks and DDoS Defence Mechanisms in: Computer Science Department, University of California, 2002.

5. Christos Douligeris, Aikaterini Mitrokotsa. DDoS attacks and defense mechanisms: classification and state-of-the-art in: *Computer Networks,* 44, 2004, pp 643–666.

6. T. Subbulakshmi, S. Mercy Shalinie, A. Ramamoorthi. Detection and Classification of DDoS Attacks Using Machine Learning Algorithms in: *European Journal of Scientific Research*, 2010, Vol. 47, No.3.

7. The case of DDoS-attack on «Aeroflot» is returned to the public procurator's office: there is no charge like this [Delo ob DDoS-atake na Aeroflot vernuli v prokuraturu: takogo obvineniya ne suschestvuet]. Gazeta.Ru, 13.06.2012. http://www.gazeta.ru/social/news/2012/06/13/n_2387569.shtml (last accessed 03.03.2013).

Координаты автора (contact information): Ковалев Д. А. (Kovaliev, Dmitry A.) – rabbit.dm@gmail.com
Статья поступила в редакцию / received 29.06.2012
Принята к публикации / accepted 02.11.2012