УДК. 004.94

И. В. Котенко, А. М. Коновалов, А. В. Шоров

ИССЛЕДОВАНИЕ БОТ-СЕТЕЙ И МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ ИМ НА ОСНОВЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ

Предлагается подход к исследованию бот-сетей и механизмов защиты от их воздействия, основанный на применении методов имитационного моделирования. Представлены общая формальная модель бот-сети и механизмов защиты, среда моделирования и результаты экспериментов.

Ключевые слова: *бот-сети, модели атак, модели механизмов защиты, имитационное моделирование, агентно-ориентированное моделирование.*

Введение. В настоящее время в сети Интернет наблюдается очевидная тенденция к распространению злоумышленниками так называемых бот-сетей. Бот-сети (от англ. botnet — ro*bot* и *net*work), по существу, позволяют объединить в самостоятельную сеть вычислительные мощности большого количества уязвимых хостов. Целью данного объединения является выполнение таких действий, как, например, поиск уязвимых хостов, реализация атак типа „распределенный отказ в обслуживании“ (DDoS), рассылка „спама“, получение конфиденциальной информации. Функционирование бот-сетей характеризуется одновременными действиями большого количества бот-агентов в интересах злоумышленника. В большинстве случаев злоумышленник получает полный контроль над ресурсами инфицированного компьютера и может их беспрепятственно использовать.

Таким образом, исследование бот-сетей и механизмов защиты от их воздействия является актуальной проблемой. Одна из важнейших задач при решении данной проблемы — исследовательское моделирование бот-сетей и механизмов защиты в целях разработки эффективных методов и средств обнаружения этих сетей и противодействия им. В настоящей статье предложен подход к исследованию данной проблемы, базирующийся на объединении агентно-ориентированного моделирования и методов имитационного моделирования дискретных событий, сетевых событий и протоколов.

Проводимые в настоящее время исследования можно разделить на две категории. В первую категорию входят исследования, непосредственно посвященные разработке методов выявления бот-сетей и методов противодействия им. Например, выявление бот-сетей может быть основано на распознавании коллективных действий бот-агентов в сети [1], определении сигнатур коммуникационного трафика, инициируемого бот-агентами [2, 3], и обнаружении атак, проводимых бот-сетями [4, 5]. Ко второй категории относятся исследования, связанные с изучением бот-сетей [6, 7], в частности с выявлением и описанием их функций, а также измерением параметров их функционирования [8].

Одним из наиболее опасных типов атак, которые могут выполнять бот-сети, является „распределенный отказ в обслуживании“. Традиционные механизмы защиты от атак данного типа реализуются на основе последовательного выполнения двух процедур — распознавания атаки, выполняемой бот-сетью, и противодействия этой атаке. Процедура распознавания атаки основывается на поиске аномалий сетевого трафика и может быть решена различными методами (например, статистическими, методом сигнатурного поиска и т.п.).

Общая формальная модель бот-сети и механизмов защиты. Общую модель бот-сети и механизмов защиты будем описывать с использованием формальных теоретико-множественных конструкций.

Представим общую модель бот-сети и механизмов защиты в виде кортежа $Q =< N, L, S, O >$, где N — множество узлов (хостов) вычислительной сети, L — множество связей между узлами вычислительной сети, S — сценарий реализации атаки, O — параметр, характеризующий действия пользователя.

Множество N узлов зададим в виде кортежа элементов: $N =< T, R, P, F >$, где T — множество типов оборудования, соответствующее узлу вычислительной сети; R — множество функциональных ролей узла; P — множество компонентов программного обеспечения, используемого узлами; $F : R \to P$ — функция, реализующая отображение множества функциональных ролей узла на множество компонентов программного обеспечения (ПО).

Программным и/или аппаратным компонентом ПО, является протокол, реализующий набор правил и позволяющий осуществлять соединение и обмен данными между двумя и более включенными в сеть устройствами.

Множество связей L между узлами вычислительной сети в контексте различных протоколов описывается следующим образом: считается, что узлы a, b сети связаны посредством некоторого протокола, если существует хотя бы одна непустая конечная последовательность с начальным узлом a и конечным узлом b, через которые будет проходить сообщение.

Сценарий реализации атаки $S =< S_B, S_D, S_K >$ содержит сценарии S_B функционирования бот-сети, сценарии S_D сдерживания бот-сети и противодействия атакам, а также сценарии S_K легитимной деятельности вычислительной сети. Каждый из сценариев S_B, S_D или S_K, в свою очередь, содержит множество подсценариев, цель сценария, алгоритм достижения цели, узлы, вовлеченные в сценарий; при этом может быть осуществлено разделение узлов на группы $H_i \subset N$, где i — номер группы, соответствующий исполняемым ролям или другим признакам.

Процесс детализации каждого из сценариев S_B, S_D, S_K можно итеративно продолжить. В этом случае каждый промежуточный сценарий становится объектом последующей декомпозиции. Сценарии S_B содержат подсценарии распространения бот-сети, управления ею и реализации атак. Сценарии S_D содержат подсценарии противодействия распространению бот-сети, противодействия управлению ею и противодействия реализации атак. Сценарии S_K предназначены для генерации шаблонов легитимного трафика.

Параметр O, характеризующий действия пользователя, необходим для оценки эффективности функционирования бот-сети и механизмов защиты.

Рассмотренная общая формальная модель бот-сети и механизмов защиты используется для построения имитационных моделей.

Среда моделирования. В настоящее время авторами используется и постоянно модернизируется многоуровневая инструментальная среда имитационного моделирования сетевых процессов для приложений в области защиты информации. Среда моделирования представляет собой программный комплекс, включающий в качестве нижнего уровня систему моделирования дискретных событий, а также ряд компонентов, реализующих сущности более высокого уровня.

Архитектура среды моделирования содержит четыре основных компонента:

— базовую систему имитационного моделирования (Simulation Framework);

— модуль имитации сети Интернет (Internet Simulation Framework);

— подсистему агентно-ориентированного моделирования (Agent-Based Framework);

— модуль процессов предметной области (Subject Domain Library), включающий сценарий реализации атаки в общей формальной модели бот-сети и механизмов защиты.

С использованием симулятора OMNeT++, библиотек INET Framework, ReaSE, а также собственных программных компонентов представленная архитектура была реализована в виде

модели противоборства команд интеллектуальных агентов при многоагентном моделировании бот-сетей, атак типа „распределенный отказ в обслуживании“ и механизмов защиты от воздействия бот-сети.

Параметры моделирования. Для проведения экспериментов было проведено моделирование вычислительных сетей, состоящих из 5—10 автономных систем. Каждая автономная система содержит примерно 300 конечных узлов. Оборудование узлов представлено типами „маршрутизатор“ и „хост“. Оборудование типа „хост“ представлено следующим множеством функциональных ролей: web-сервер, web-клиент, почтовый сервер, сервер мультимедийного контента, сервер „командный центр“, „уязвимый сервис“, „мастер“, IP-фильтр.

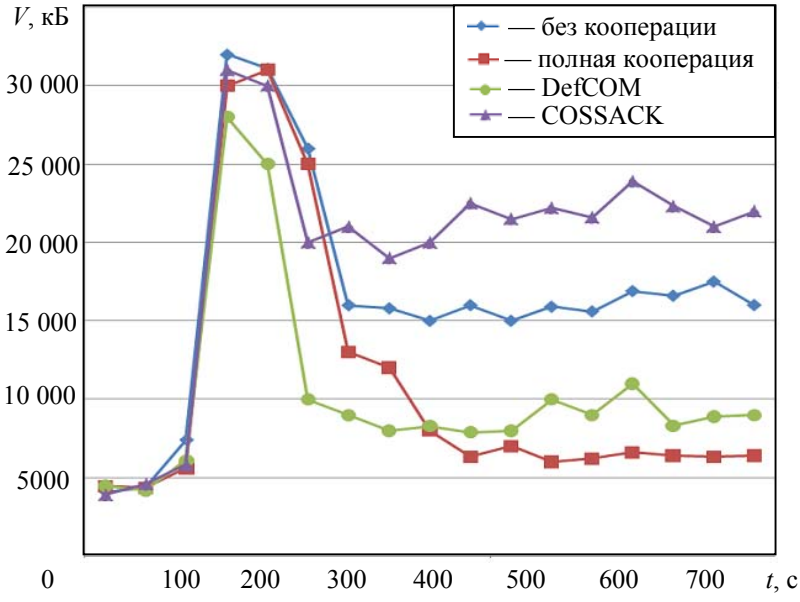
Команда интеллектуальных агентов атаки представлена агентами следующих типов: „мастер“, „командный центр“, „цель“, „зомби“. В ходе экспериментов определялись один агент „мастер“, один или несколько агентов „командный центр“ и множество агентов с уязвимым программным обеспечением, которые потенциально могут обратиться в „зомби“.

Команда интеллектуальных агентов защиты представлена следующими общими классами агентов: первичной обработки информации („сенсор“); вторичной обработки информации („сэмплер“); обнаружения атаки („детектор“); фильтрации („фильтр“); „расследования“; управления нагрузкой на коммуникационные каналы („ограничитель“).

Одним из примеров реализованных сценариев атаки, выполняемой бот-сетью, является атака типа UDP Flood, проводимая по отношению к некоторому узлу (подсети), IP-адрес которого (которой) указывается агентом „мастер“.

В ходе исследований было реализовано несколько сценариев сдерживания бот-сети и противодействия атакам DDoS: сценарий, реализуемый без кооперации интеллектуальных агентов защиты [9], с кооперацией типа DefCOM [10], с кооперацией типа COSSACK [11] и с полной кооперацией [9].

Результаты экспериментов. Оценка результатов реализации сценариев атак и сценариев защиты проводилась по следующим параметрам:



— количеству принадлежащих атакующему трафику входящих пакетов до и после фильтрации, выполняемой командами, защищающими атакуемую сеть (узел);

— количеству ошибок первого и второго рода (оценки false positive — FP — и false negative — FN), характеризующих результаты обнаружения атак командами интеллектуальных агентов защиты.

Результаты процесса фильтрации оценивались по значениям FP и FN. Например, значения этих оценок в одном из экспериментов, при исследовании сценария защиты, реализуемого без кооперации агентов, были следующими: FP=0,002, FN=0,09.

На рисунке представлен график, демонстрирующий уровень трафика атаки внутри атакуемой подсети при использовании различных сценариев сдерживания бот-сети и противодействия атакам.

Как показали результаты экспериментов, сценарий, реализуемый при полной кооперации агентов, наиболее эффективен при защите от DDoS-атак, следующим по эффективности является метод DefCOM, а затем — защита без кооперации агентов и метод COSSACK.

Заключение. Рассмотрен подход к исследовательскому моделированию бот-сетей и механизмов защиты от их воздействия в сети Интернет. Представлены общая формальная модель бот-сети и механизмов защиты, архитектура разрабатываемой среды моделирования, предназначенной для анализа бот-сетей, и ее программная реализация. Проведенные эксперименты показали применимость предложенного подхода для моделирования бот-сетей и механизмов защиты.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (проект № 10-01-00826) и программы фундаментальных исследований Отделения нанотехнологий и информационных технологий РАН (проект № 3.2), а также при частичной финансовой поддержке, осуществляемой в рамках проектов Евросоюза “SecFutur”, “Massif” и др.

СПИСОК ЛИТЕРАТУРЫ

1. *Gu G., Perdisci R., Zhang J., Lee W.* BotMiner: Clustering analysis of network traffic for protocol- and structure-independent botnet detection // Proc. of the 17th USENIX Security Symp. (Security’08). San Jose, CA, 2008.
2. *Goebel J., Holz T.* Rishi: Identify bot contaminated hosts by IRC nickname evaluation // Proc. of the 1st Workshop on Hot Topics in Understanding Botnets (HotBots’07). Cambridge, MA, 2007.
3. *Binkley J., Singh S.* An algorithm for anomaly-based botnet detection // Proc. of the 2nd Conf. on Steps to Reducing Unwanted Traffic on the Internet (SRUTI’06). San Jose, CA, 2006.
4. *Chen S., Song Q.* Perimeter-based defense against high bandwidth DDoS attacks // IEEE Transact. on Parallel and Distributed System. 2005. Vol. 16. N. 7.
5. *Mirkovic J., Dietrich S., Dittrich D., Reiher P.* Internet Denial of Service: Attack and Defense Mechanisms. NJ: Prentice Hall PTR, 2004.
6. *Dagon D., Gu G., Lee C., Lee W.* A taxonomy of botnet structures // Proc. of the 23rd Annual Computer Security Applications Conf. (ACSAC’07). Florida, 2007.
7. *Gianvecchio S., Xie M., Wu Z., Wang H.* Measurement and classification of huamans and bots in Internet chat // Proc. of the 17th USENIX Security Symp. (Security’08). San Jose, CA, 2008.
8. *Bailey M., Cooke E., Jahanian F.* et al. A survey of botnet technology and defenses // Proc. of the Cybersecurity Applications & Technology Conf. for Homeland Security. Washington, DC: IEEE Computer Society, 2009.
9. *Kotenko I., Ulanov A.* Packet level simulation of cooperative distributed defense against Internet attacks // Proc. of the 16th Euromicro Intern. Conf. on Parallel, Distributed and Network-Based Processing (PDP 2008). Toulouse: IEEE Computer Society, 2008.
10. *Mirkovic J., Robinson M., Reiher P., Oikonomou G.* Distributed defense against DDOS attacks // Univ. of Delaware, CIS Department Technical Report. 2005. N 2.
11. *Papadopoulos C., Lindell R., Mehringer I.* et al. COSSACK: Coordinated suppression of simultaneous attacks // DISCEX — DARPA: Information Survivability Conference and Exposition. 2003.

Сведения об авторах

Игорь Витальевич Котенко — д-р техн. наук, профессор; СПИИРАН, лаборатория проблем компьютерной безопасности; E-mail: ivkote@comsec.spb.ru

Алексей Михайлович Коновалов — аспирант; СПИИРАН, лаборатория проблем компьютерной безопасности; E-mail: konovalov@comsec.spb.ru

Андрей Владимирович Шоров — аспирант; СПИИРАН, лаборатория проблем компьютерной безопасности; E-mail: ashorov@comsec.spb.ru

Рекомендована СПИИРАН

Поступила в редакцию
09.07.10 г.