В.В. Бутузов, М.В. Бурса, А.Г. Остапенко,
А.О. Калашников, Г.А. Остапенко

ИНФОРМАЦИОННЫЕ РИСКИ ФЛУД-АТАКУЕМЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

Монография

Под редакцией члена-корреспондента РАН
Д.А. Новикова

Воронеж
Издательство «Научная книга»
2015

УДК 004.056.5: 004.75
ББК 55.6
Б 93

Рецензенты:

Белоножкин В.И., д-р техн. наук (Аппарат уполномоченного представителя Президента по правам человека в Воронежской области);
Тихомиров Н.М., д-р. техн. наук (ОАО «Концерн «Созвездие», г.Воронеж)

Б 93 **Бутузов, В.В.** Информационные риски флуд-атакуемых компьютерных систем: Монография/ В.В. Бутузов, М.В. Бурса, А.Г. Остапенко, А.О. Калашников, Г.А. Остапенко; под ред. чл.-корр. РАН Д.А. Новикова. – Воронеж: Издательство «Научная книга», 2015. – 160 с.

ISBN 978-5-98222-867-3

В монографии предлагаются методики оценки и регулирования рисков флуд-атакуемых систем. Разработанное методическое обеспечение ориентировано на широкий спектр компьютерных систем. Оно может использоваться в качестве базы для дальнейших исследований сетевых структур, подвергающихся разнообразным деструктивным воздействиям типа «отказ в обслуживании».

Табл. 5. Ил. 49. Библиогр.: 109 назв.

УДК 004.056.5: 004.75
ББК 55.6
Б 93

ISBN 978-5-98222-867-3

ВВЕДЕНИЕ

Флуд (англ. flood — наводнение, затопление) — это поток сообщений в интернет-форумах и чатах, занимающие большие объемы или не несущие никакой полезной информации. Технический флуд представляет собой атаку с большим количеством запросов, приводящую к отказу в обслуживании [86].

Для организации флуд-атаки на систему мгновенного обмена сообщениями, как правило, используется вредоносная программа IM-Flooder, функцией которой является «забивание мусором» (бесполезными сообщениями) каналов системы мгновенного обмена сообщениями [85]. Однако самые популярные флуд-атаки – это атаки организованные с помощью ботнетов [75, 77, 79, 81], которые являются одним из самых прибыльных способов монетизации ботнетов [75, 82, 83], а их исполнителем может выступать как один человек, так и организованная группировка злоумышленников.

Некоторые флуд-атаки создают мгновенный аварийный отказ работы клиента. Другие просто «подвешивают» его. Создается настолько большой массив данных, что с ним не справляется центральный процессор. Это вызывает нестабильную работу или даже «зависание» всего компьютера.

Традиционный сценарий флуд-атаки состоит в затоплении выбранного пользователя огромным количеством сообщений. Все самые распространенные IM-системы передачи сообщений содержат некую встроенную защиту от такого типа атак, что позволяет жертве игнорировать некоторых конкретных пользователей. Однако имеется много инструментальных средств, позволяющих использовать множество учетных записей одновременно, или автоматически создавать необходимое количество учетных записей, чтобы преодолеть порог, с которого уже возможна флуд-атака.

Нередко флуд-атаки имеют своей целью:

– распространение нежелательной рекламы (спама) [75, 79], рассылаемой через каналы электронной почты;

– целенаправленное насыщение канала передачи данных и почтовых серверов, в результате этого может произойти отказ в работе системы из-за исчерпания системных ресурсов – процессора, памяти или каналов связи [82, 83, 84];

– отправку фиктивных предложений компаниям, с целью замедлить работу компании, так как сотрудники будут вынуждены просматривать и реагировать на ложные сообщения [76];

– проведение фишинговых атак и распространения вредоносных программ [80];

– организацию Distributed Spam Distraction (DSD) [82], т.е. рассылки нежелательных сообщений с целью отвлечения внимания.

– отказ почтового сервера, организованный с помощью вредоносной программы Email-Flooder, что несет в себе серьезную техническую, экономическую и даже социальную угрозу.

Актуальность флуд-угрозы наглядно подтверждают факты, собранные в Приложении 1.

Таким образом, флуд-атаки [75-84] представляют реальную опасность и приносят значительные ущербы для информационных систем различного профиля. В этой связи проблема оценки информационных рисков и управления ими для флуд-атакуемых систем приобретает особую актуальность.

В настоящей монографии предлагается рассмотреть эту проблему для наиболее распространенных IM-флудов, DNS-флудов, SMS-флудов и «почтовых флудов».

Содержание

Научное издание

Бутузов Владимир Вячеславович
Бурса Максим Васильевич
Остапенко Александр Григорьевич
Калашников Андрей Олегович
Остапенко Григорий Александрович

ИНФОРМАЦИОННЫЕ РИСКИ ФЛУД-АТАКУЕМЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

Монография

Издание публикуется в авторской редакции

Дизайн обложки С.А.Кравец

Подписано в печать 24.02.2015. Формат 60x84 1/16.
Усл. печ.л. 10,0. Заказ 000. Тираж 500 экз.

ООО Издательство «Научная книга»
394077, Россия, г.Воронеж, ул. 60-й Армии, 25-120
http://www.sbook.ru/

Отпечатано с готового оригинал-макета
в ООО «Цифровая полиграфия»
394036, г. Воронеж, ул. Ф. Энгельса, 52.
Тел.: (473)261-03-61