6. Security threat modeling and analysis: a goal-oriented approach. Ebenezer A. Oladimeji, Sam Supakkul, Lawrence Chung//Режим доступа: - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10 .1.1.103.2997&rep=rep1&type=pdf

7. Миронов В. В., Носаль И.А. Моделирование и оценка системы обеспечения информационной безопасности на примере ГОУ ВПО «СыктГУ» // Информация и безопасность. 2011. № 2. С. 209–211.

8. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена зам.директора ФСТЭК России от 14.02.2008

9. ГОСТ Р ИСО/МЭК ТО 13335-3 – 2007 Руководство по управлению безопасностью информационных технологий. Часть 3. Методы управления безопасностью информационных технологий; Введ. 01.09.2007. – М.: Стандартинформ, 2006 -49с.

10. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с. // Хоффман, Л. Д. Современные методы защиты информации / Л. Д. Хоффман; под ред. В.А. Герасименко. М.: Сов. радио, 1980. — 264 с.

Р.М. Пасечник, О.И. Барсуков

ИСПОЛЬЗОВАНИЕ DNS-ЗАПРОСОВ В КАЧЕСТВЕ СРЕДЫ РЕАЛИЗАЦИИ СКРЫТОГО КАНАЛА ПЕРЕДАЧИ ИНФОРМАЦИИ

(Кубанский государственный технологический университет)

В настоящее время одной из актуальных угроз обеспечения информационной безопасности в автоматизированных системах является использование злоумышленниками скрытых каналов передачи информации в открытых компьютерных системах (в том числе в сетях связи общего пользования). Необходимо констатировать факт, что проблематике использования скрытых каналов в сетях передачи данных не уделяется необходимого внимания.

В данной статье рассматривается вопрос использования DNS-запросов в качестве среды для создания нетрадиционного (скрытого) канала передачи информации. Реализация данного способа передачи данных основывается на технологии «туннелирования» TCP/IP трафика по средству DNS-запросов, т.е. инкапсуляции TCP/IP трафика в DNS-запросы.

В настоящий момент, данный метод рассматривается мировым ИТ-сообществом только с целью получения доступа в глобальную сеть Интернет через Wi-Fi сети в обход авторизации пользователей на web-форме*.

Помимо безвредного, на первый взгляд, доступа в сеть Интернет (но уже по сути являющимся правонарушением), данной технологией могут пользоваться злоумышленники, для достижения таких целей как:

* Такой метод авторизации в основном применяется для обеспечения коммерческого доступа в сеть Интернет в аэропортах, гостиницах и др. общественных местах

– передача конфиденциальных данных из защищенного контура организации, минуя установленные на периметре локальной вычислительной сети организации средства и системы защиты информации;
– установка вредоносного программного обеспечения внутри защищенного контура организации;
– управление элементами ботнет-сетей для организации DDoS-атак (распределенная атака, направленная на нарушение такой характеристики информации как «доступность»);
– и пр.

Использование стандартных DNS-запросов для реализации поставленных выше задач позволяет обходить стандартные системы межсетевого экранирования, обнаружения и предотвращения вторжений, по причине того, что инкапсулированная в DNS-трафик информация не подвергается контентному анализу и инкапсулированные в DNS-трафик TCP/IP-пакеты консолидируются за системой защиты информации (внутри защищенного контура организации).

Для реализации данного способа передачи информации необходимы следующие компоненты:
– авторитарный DNS-сервер со своим собственным доменом (данный компонент выполняет роль сервера управления в создаваемом «DNS-туннеле»);
– программное обеспечение, обеспечивающие согласованную работу с DNS-сервером (данный компонент осуществляет мониторинг входящих DNS-пакетов в фоновом режиме и поддерживает постоянный «туннель» с авторитарным DNS-сервером);
– клиентское программное обеспечение, инициирующее запросы к авторитарному DNS-серверу (данный компонент осуществляет инкапсуляцию TCP/IP-пакетов в DNS-трафик при передачи информации из защищенного контура организации, а также консолидацию TCP/IP-пакетов при получении инкапсулированного трафика)

На данный момент существует ряд свободно распространяемых (Open Source) решений для создания «DNS-туннеля», что существенно облегчает злоумышленникам возможность построения скрытого канала передачи информации.

Схема сети, в которой возможно использование DNS-запросов в качестве скрытого канала передачи информации представлена на рисунке 1.

Процедура реализации скрытого канала передачи информации по средствам DNS-запросов:

1. АРМ злоумышленника с помощью клиентского программного обеспечения осуществляет запрос на авторитарный DNS-сервер для инициализации соединения с внешним сервером злоумышленника;

2. авторитарный DNS-сервер подтверждает/отклоняет полученный запрос от АРМ злоумышленника;

3. в случае подтверждения авторитарным DNS-сервером полученного запроса – осуществляется создание «DNS-туннеля» между АРМ злоумышлен-

ника и сервером злоумышленника (при этом, между сервером злоумышленника и авторитарным DNS-сервером «DNS-туннель» существует постоянно);

4. в DNS-запросы, отправляемые с АРМ злоумышленника инкапсулируются TCP/IP-пакеты, которые консолидируются на сервере злоумышленника;

5. внешний сервер злоумышленника отправляет информацию (в виде инкапсулированного трафика) на АРМ злоумышленника, на котором он в дальнейшем консолидируется.

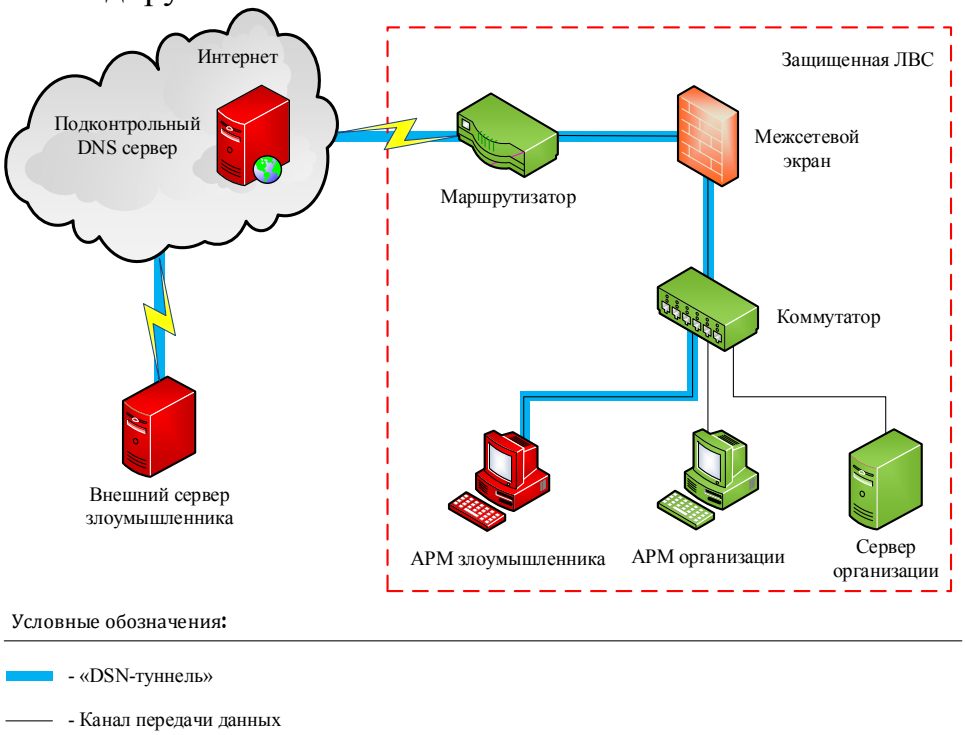

Рис. 6. Пример схемы сети реализации скрытого канала

Таким образом, АРМ злоумышленника имеет двустороннюю связь со своим сервером по средству скрытого канала передачи информации по средству «DNS-туннеля».

Так как структура DNS-запроса позволяет использовать 263 символа для имени хоста и до 63 символов для каждого субдомена, это дает возможность использовать достаточно большой объем инкапсулированного трафика.

Структура DNS-запроса, а также места расположения инкапсулированного в нем трафика представлена на рисунке 2.

Скорость передачи данных полученного скрытого канала передачи информации, определенная экспериментальным путем, достигает 110 Кб/сек и задержка при передачи информации составляет 150 мс. Данной ширины канала достаточно, например для: управления зараженным компьютером, передачи конфиденциальных данных минуя установленные средства защиты информации, чтения html-страниц и др.

Таким образом, в результате проведенных исследований, было выявлено, что реализация скрытого канала передачи данных, используя в качестве среды передачи данных DNS-запросы, возможна.. Предположительно, исследованный скрытый канал передачи данных можно нейтрализовать, применив дополни-

тельные средства защиты информации. Исследование возможностей существующих методов и средств защиты информации, а также их доработка в случае неудовлетворительных результатов, на предмет возможности противодействия скрытым каналам передачи информации данного типа является темой будущих исследований.

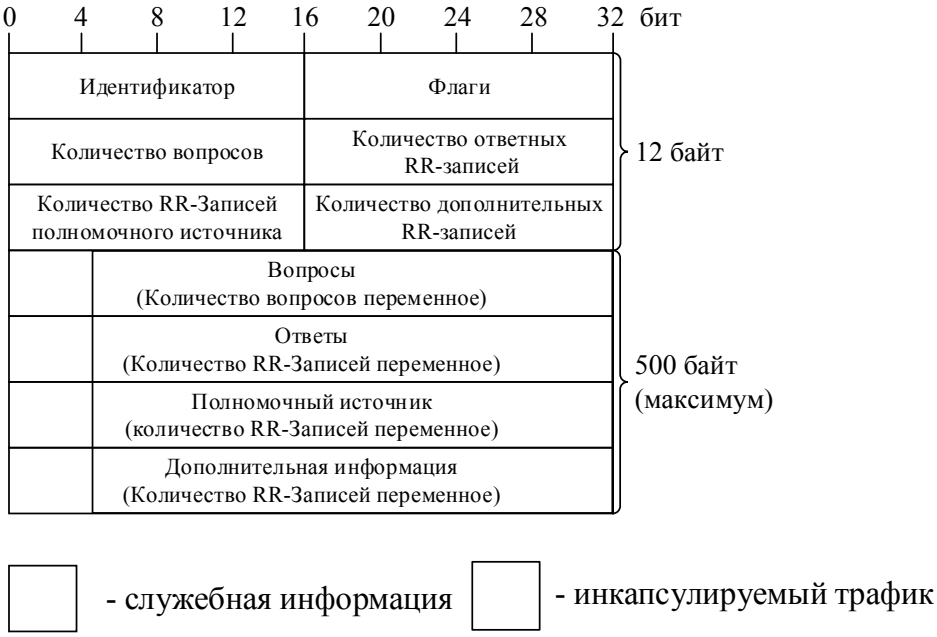

Рис. 2. Структура DNS-запроса

Литература

1. ГОСТ Р 53223.1-2008. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 1. Общие положения. – Введ. 2009-09-30. – М. : Изд-во стандартов, 2008, 12 с.

2. ГОСТ Р 53223.2-2009. Информационная технология. Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов. Часть 2. Рекомендации по организации защиты информации, информационных технологий и автоматизированных систем от атак с использованием скрытых каналов. – Введ. 2009-12-01. – М. : Изд-во стандартов, 2008, 12 с.

3. Безукладников И.И. Скрытые каналы в распределенных автоматизированных системах / Безукладников И.И., Кон Е.Л. – Уфа: УГАТУ, 2010. - с. 245 – 250.

Д.И. Тихонов, А.В. Дорфман

ПРИМЕНЕНИЕ PROGRAM SLISING В ЗАДАЧАХ REVERSE ENGINERRING

(Самарский государственный технический университет)

Reverse engineering (или обратная разработка, далее RE) –давно применяемая техника низкоуровневого исследования программ. RE в основном ис-