004.773

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

О.И. БАРСУКОВ, Р.М. ПАСЕЧНИК

Кубанский государственный технологический университет,
350075, Российская Федерация, г.Краснодар, ул. Московская,2

В статье приведены результаты анализа практики и эффективности использования DNS-запросов при реализации скрытых каналов передачи информации. Использование стандартных DNS-запросов позволяет обходить стандартные системы межсетевого экранирования, обнаружения и предотвращения вторжений. в результате проведенных исследований, было выявлено, что реализация скрытого канала передачи данных, используя в качестве среды передачи данных DNS-запросы, возможна. Исследованный скрытый канал передачи данных можно нейтрализовать, применив дополнительные средства защиты информации.

Ключевые слова: скрытые каналы, DNS-запрос, туннелирование, инкапсуляция, сети передачи данных.

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[1].

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

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:

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 .

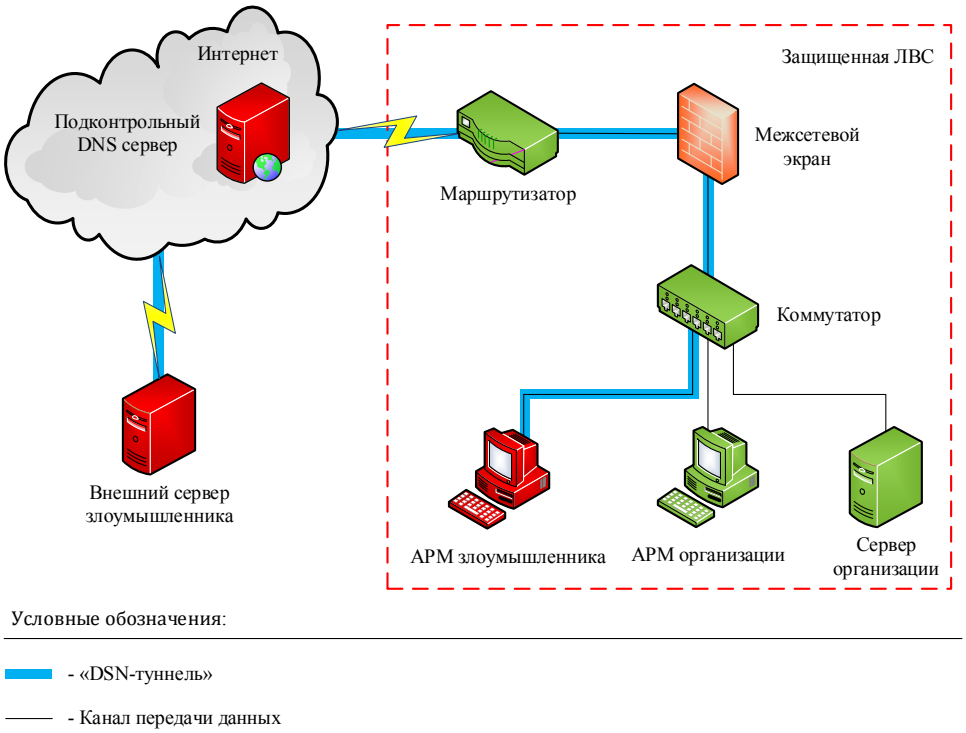

Рисунок 1 – Пример схемы сети реализации скрытого канала

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

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

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

– в случае подтверждения авторитарным DNS-сервером полученного запроса – осуществляется создание «DNS-туннеля» между АРМ злоумышленника и сервером злоумышленника (при этом, между сервером злоумышленника и авторитарным DNS-сервером «DNS-туннель» существует постоянно);

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

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

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.

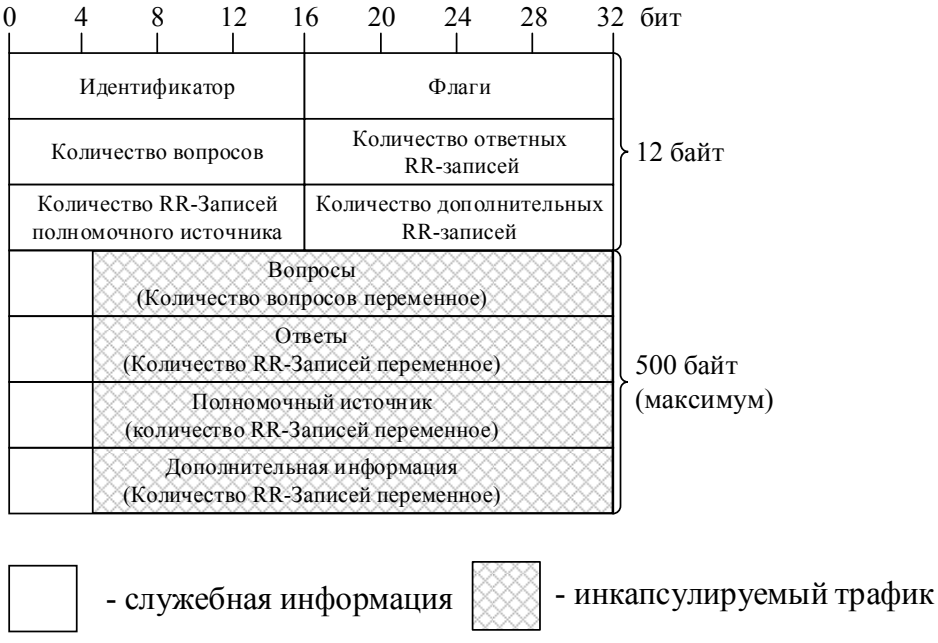

Рисунок 2 – Структура DNS-запроса

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 дополнительные 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.

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.

REFERENCES

1. GOST R 53223.1-2008. Informacionnaja tehnologija. Zashhita informacionnyh tehnologij i avtomatizirovannyh sistem ot ugroz informacionnoj bezopasnosti, realizuemyh s ispol'zovaniem skrytyh kanalov. Chast' 1. Obshhie polozhenija. – Vved. 2009-09-30. – M. : Izd-vo standartov, 2008, 12 s.

2. GOST R 53223.2-2009. Informacionnaja tehnologija. Zashhita informacionnyh tehnologij i avtomatizirovannyh sistem ot ugroz informacionnoj bezopasnosti, realizuemyh s ispol'zovaniem skrytyh kanalov. Chast' 2. Rekomendacii po organizacii zashhity informacii, informacionnyh tehnologij i avtomatizirovannyh sistem ot atak s ispol'zovaniem skrytyh kanalov. – Vved. 2009-12-01. – M. : Izd-vo standartov, 2008, 12 s.

3. Bezukladnikov I.I. Skrytye kanaly v raspredelennyh avtomatizirovannyh sistemah / Bezukladnikov I.I., Kon E.L. – Ufa: UGATU, 2010. - s. 245 – 250.

DNS-QUERY AS COVERT INFORMATION CHANNEL ENVIRONMENT

O.I. BARSUKOV, R.M. PASECHNIK

Kuban State Technological University,
2, Moskovskaya st., Krasnodar, Russian Federation, 350072

The results of practices and efficient use of DNS-queries in the implementation of covert channels analysis of communication are given in article. Using standard DNS-queries allows to bypass the standard system firewall, intrusion detection and prevention. as a result of the research, it was found that the implementation of the hidden data transmission channel, using a data transmission medium DNS-request is possible. Explore the hidden data channel can be neutralized by applying additional security information.
Keywords: covert channels, DNS-query, tunneling, encapsulation, data network.