ОБНАРУЖЕНИЕ ПЕРЕДАЧИ НЕСАНКЦИОНИРОВАННОГО ТРАФИКА ПОСРЕДСТВОМ ТУННЕЛИРОВАНИЯ DNS

Калабухов Е.В.[1], Недведский А.Ю.[2], Масензов В.В.[3], Якубович Ф.В.[4]

[1]Калабухов Евгений Валерьевич – старший преподаватель;
[2]Недведский Александр Юрьевич – магистрант;
[3]Масензов Вадим Валерьевич – магистрант;
[4]Якубович Федор Владимирович – магистрант,
кафедра информатики,
Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Аннотация: *DNS – это один из основных сетевых протоколов. Он предназначен для обеспечения работы с доменными именами. Существуют специальные инструменты, которые позволяют настроить туннель на основе протокола DNS. И так как этот протокол не предназначен для передачи пользовательского сетевого трафика ему часто не уделяется достаточного внимания при защите сети от несанкционированных действий. В данной работе будут рассмотрены некоторые инструменты, предназначенные для установления туннеля, на основе протокола DNS и предложены варианты обнаружения передачи несанкционированного трафика посредством туннелирования DNS.*
Ключевые слова: *DNS, туннелирование DNS, сетевые протоколы, компьютерные сети, безопасность компьютерной сети.*

DNS (Domain Name System) – система, используемая для получения информации о доменных именах. Чаще всего используется для получения IP адреса хоста по его имени. Поскольку DNS не предназначен для передачи данных, чаще всего он не рассматривается сетевыми администраторами как средство для передачи вредоносных сообщений. Поэтому в большинстве сетей DNS не подвергается контролю и фильтрации межсетевыми экранами.

Туннелирование DNS – это техника, которая может быть использована для обхода межсетевых экранов и получения доступа к ресурсам сети. Она предполагает инкапсуляцию данных в обычные DNS пакеты. Одним из примеров использования этой техники является передача несанкционированного трафика с целью контроля над ботнетом, что предполагает использование незащищённого канала связи. Таким образом, туннелирование DNS представляет серьезную угрозу безопасности сети.

Существуют специальные инструменты для настройки туннеля на основе протокола DNS. Все эти инструменты используют похожие техники и отличаются только способом кодирования данных и типом используемых полей пакета DNS. Ключевыми компонентами, которые применяются всеми инструментами для туннелирования DNS, являются: специальный домен или субдомен; сервер, на котором установлена серверная часть утилиты для туннелирования; кодировка, используемая для кодирования данных. Существуют также коммерческие предложения по предоставлению сервиса «VPN over DNS». Пользователю остается только установить клиентскую часть утилиты для туннелирования, что значительно упрощает настройку и использование туннеля. Ниже приведено краткое описание некоторых инструментов для туннелирования DNS.

Heyoka – специальная утилита, создающая двунаправленный туннель, который может использован для эксфильтрации данных. Heyoka использует EDNS для передачи DNS пакетов большого размера (более 512 байт). Также она использует технику спуфинга для рассылки DNS запросов с различных IP адресов.

DNScat – еще одна утилита для создания двунаправленного канала передачи данных на основе протокола DNS. Она может использовать A и CNAME поля пакета DNS. Другая версия этой утилиты, может использовать A, AAAA, CNAME, NS, TXT и MX поля.

Большинство инструментов для туннелирования полагаются на тот факт, что DNS трафик чаще всего просто не подвергается анализу. Всю технику по обнаружению передачи несанкционированного трафика посредством туннелирования DNS можно разделить на две категории: технику, построенную на основе анализа содержимого пакетов DNS и технику, основанную на анализе количества и частоты DNS запросов.

Одна из техник предполагает анализ размеров DNS запросов и ответов. В статье «The six most dangerous new attack techniques and what's coming next?» [1] автор определят методы для обнаружения подозрительного DNS трафика на основе анализа соотношения между размером DNS запроса и DNS ответа. Обычно, инструменты для туннелирования DNS с целью увеличения пропускной способности пытаются использовать максимально возможные размеры DNS пакетов, что можно считать признаком использования туннеля.

Также DNS туннели могут быть обнаружены при помощи анализа энтропии доменных имен, передающихся в DNS пакете [2]. Обычные DNS имена, как правило, состоят из слов английского языка. Закодированные же данные (инструменты для туннелирования кодируют данные, которые помещают в DNS пакет) имеют высокую энтропию и DNS имена, имеющие высокую энтропию, могут служить признаком использования туннеля.

Список литературы

1. *Sqoudis E.* The six most dangerous new attack techniques and what's coming next? [Electronic resource], 2012. URL: https://blogs.sans.org/pentesting/files/2012/03/RSA-2012-EXP-108-Skoudis-Ullrich.pdf (date of access: 26.05.2017).
2. Van Horenbeeck T. DNS Tunneling [Electronic resource], 2006. URL: http://www.daemon.be/maarten/dnstunnel.html (date of access: 26.05.2017).