Что такое DNS и как это работает?

Андриченко Никита Андреевич
Andrichenko Nikita Andreevich
студент института кибернетики,
кафедры компьютерной и информационной безопасности,
Московский Институт Радиотехники Электроники и Автоматики
(Московский Технологический Университет),
Россия, г. Москва
E-mail: willon95@gmail.com

Лубова Елена Сергеевна
Lubova Elena Sergeevna
студент института кибернетики,
кафедры компьютерной и информационной безопасности,
Московский Институт Радиотехники Электроники и Автоматики
(Московский Технологический Университет),
Россия, г. Москва
E-mail: helen.95@inbox.ru

Аннотация: *в данной статье рассматривается «система доменных имен» (DNS), механизм ее работы, хакерские атаки, которым она подвержена, и современный механизм защиты.*

Ключевые слова: *домен, DNS, ip-адрес, сервер, хакерская атака.*

Что такое DNS?

Domain Name System (DNS) переводится как «Система доменных имен» является одной из основных частей Интернета, однако большинство людей, вероятно, не понимают, что они используют ее каждый день, выполняя свою работу, используя планшеты и смартфоны или проверяя электронную почту.

По сути DNS- это каталог имен, которые соответствуют некоторым номерам. Этими номерами являются IP-адреса, которые компьютеры используют для связи друг с другом. Описывая систему DNS обычно используют аналогию со списком контактов в смартфоне или телефонной книгой, где имена людей сопоставляются с их телефонными номерами или адресами электронной почты.

Когда Интернет был очень и очень мал, людям было просто сопоставить конкретные IP-адреса с конкретными компьютерами в сети, но это продолжалось недолго, поскольку все больше устройств и людей присоединялось к быстро растущей глобальной сети. Для устройств стали использоваться наименования, чтобы людям было легче подключаться к ним в Интернете, ведь для большинства людей запоминание слов проще, чем запоминание определенных наборов чисел.

Как работает DNS?

Каталог DNS имеет распределенный характер, он распространен по всему миру и хранится на серверах доменных имен, которые регулярно взаимодействуют друг с другом. DNS-информация распределяется между большим количеством серверов, а также локально кэшируется на клиентских компьютерах. Скорее всего, вы используете поисковик google.com несколько раз в день. Вместо того, чтобы ваш компьютер каждый раз запрашивал от DNS-сервера ip-адрес для сайта google.com, информация о соответствии имени сайта ip-адресу единожды сохраняется на компьютере и используются при всех дальнейших посещениях этого сайта. Дополнительное кэширование может происходить на маршрутизаторах, используемых для подключения

к Интернету, а также на серверах Интернет-провайдера пользователя.

К концу 2017 года было насчитано более 332 миллионов доменных имен. Каждый именованный сайт может соответствовать более чем одному ip-адресу. Фактически, некоторым сайтам соответствуют сотни и более ip-адресов. Например, сервер, к которому обращается ваш компьютер по адресу www.google.com, вполне может отличаться от сервера, доступного кому-то в другой стране, использующему то же имя сайта в своем браузере.

Механизм DNS основан на иерархическом принципе, который обеспечивает хранение и поддержание данных о доменных именах. Чтобы проиллюстрировать работу системы доменных серверов, предположим, что вы ввели в браузере адрес «www.facebook.com». Запрос на получение ip-адреса для сайта facebook от браузера поступает известному DNS-серверу, который обычно находится под управлением вашего или стороннего провайдера. Однако DNS-сервер может не иметь информацию об ip-адресе запрошенного вами сайта. В таком случае запрос переходит к корневому серверу, который содержит полную информацию обо всех доменах верхнего уровня, таких как .com, .net, .org, включая домены стран, такие как .ru (Россия) или .uk (Великобритания). Корневые серверы расположены по всему миру, таким образом, система обычно направляет запрос к самому близкому территориально корневому серверу. Корневой сервер перенаправляет запрос к DNS-серверу, который хранит информацию о доменах второго уровня, принадлежащих верхнему домену, т.е. слова в адресе, вводимые перед .com или .ru (Для facebook.com —"facebook«). Затем запрос переходит к серверу доменных имен, который хранит запись о сайте и его ip-адресе. Как только ip-адрес обнаружен, его передают обратно клиенту, который теперь может использовать его, чтобы посетить веб-сайт. Весь этот процесс занимает миллисекунды.

Система DNS работает вот уже на протяжении 30 лет и большинство людей воспринимают ее как должное. Однако вопросы безопасности не учитывалась при построении системы и хакеры, в полной мере воспользовавшись этим, создали множество атак. Ниже описаны некоторые разновидности этих атак.

DNS reflection attacks- «атаки отражением» могут затопить жертву сообщениями большого объема от DNS-серверов. Атакующие запрашивают большие DNS-файлы со всех доступных DNS-серверов, которые могут найти, используя при этом поддельный ip-адрес жертвы. Когда эти DNS-сервера отвечают, жертва получает поток непроверенных данных, которые переполняют ее компьютер.

DNS cache poisoning- «атаки отравлением кэша» могут перенаправлять пользователей на вредоносные веб-сайты. Происходят, когда хакерам удается вставить ложные адресные записи в DNS. Когда потенциальная жертва запрашивает ip-адрес для одного из отравленных сайтов, DNS в ответе присылает ip-адрес для другого сайта, который контролируется злоумышленником. После перенаправления на поддельный веб-сайт, посетитель не будет информирован о подмене и рискует раскрыть свои пароли или пострадать от загрузки вредоносных программ.

DNS resource exhaustion- «атаки на истощение ресурсов» могут засорять DNS-инфраструктуру провайдеров, блокируя клиентам доступ к сайтам в Интернете. Злоумышленник отправляет большое количество запросов через известные открытые DNS-сервера, которые находятся в сети Интернет-провайдера. Каждый запрос будет содержать уникальный, случайно сгенерированный и несуществующий поддомен ранее зарегистрированного домена (например, dsfbdb.www.200fs.com, afbgfnx.www.200fs.com). DNS-сервер должен обработать каждый запрос, временно сохраняя его у себя в кэш-памяти, затем отправить другому DNS-серверу, при этом расходуя свои вычислительные ресурсы. По мере проведения атаки увеличивается количество запросов с машин атакующего. В конце концов целевой DNS-сервер подавляется под нагрузкой

либо от истощения системных ресурсов, либо от перегрузки сети, либо от того и другого.

Что такое DNSSec?

DNS Security Extensions- «Расширения безопасности DNS» — это попытка обеспечить более безопасную связь между различными уровнями DNS-серверов. Технология была разработана Internet Corporation for Assigned Names and Numbers (ICANN), организацией, отвечающей за систему DNS.

ICANN узнала о слабых сторонах связи между DNS-серверами, которые могут позволить злоумышленникам захватывать запросы. DNSSEC задействует механизм шифрования и дополняет DNS-запросы цифровой подписью, что гарантирует достоверность полученных данных. Создается цепочка доверия и на каждом шаге обмена DNS-информацией между серверами и клиентами проверяется целостность сообщений, чтобы пользователь был уверен в том, что соединение в браузере установлено с правильным веб-сайтом. Кроме того, DNSSec может определить, существуют ли имена доменов или нет. Эта функция также важна для обеспечения доверия в Интернете.

По мере создания большого количества доменных имен и непрерывного роста числа устройств, подключающихся к сети Интернет при помощи «Интернета вещей» и других интеллектуальных систем, важно поддерживать экосистему DNS в исправном и работоспособном состоянии.

Литература:

1. Cricket Liu, Paul Albitz «DNS and BIND» — O'Reilly, Fifth Edition, May 2006; ISBN 0596100574, 648 pages.