https://habr.com/ru/post/301096/. – Дата доступа: 8.02.2020.

АТАКИ С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА DNS И СРЕДСТВА ПРОТИВОДЕЙСТВИЯ ИМ

Коляго Н.Р.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Одинец Д.Н. – канд. техн. наук

Данная работа содержит описание самых распространенных атак как на саму инфраструктуру DNS, так и с использованием архитектуры DNS, а также описывает существующие способы им противодействовать.

Протокол DNS разрабатывался с идеей, что инфраструктурой может пользоваться кто угодно, никакой аутентификации пользователя или шифрования данных не предусмотрено. Кроме того, он реализован с помощью протокола UDP, что позволяет более быстро обмениваться данными. Однако, именно эти особенности делают возможными большинство типов атак как на сам DNS, так и с использованием DNS.

Атаки с использованием инфраструктуры DNS в основном относятся к DoS атакам. К ним можно отнести «отраженные» атаки и «отраженные» атаки с усилением. Злоумышленник посылает на DNS сервер множество DNS запросов, в которых подменен IP адрес источника на IP адрес жертвы. В ответ сервер посылает множество ответов в адрес жертвы, чем вызывает трату ее ресурсов на обработку пришедших пакетов. Усиление же заключается в том, что запросы подбираются так, чтобы

ответ был значительно больше, чем сам запрос. Это вызывает еще большую трату ресурсов.

Эффективных способов защититься от таких атак нет, даже при настроенном файрволле интернет-канал до него все равно будет занят мусорными пакетами, будут тратиться вычислительные ресурсы на отсеивание пакетов, а также придется заблокировать функционал DNS в целом.

Кроме DoS атак с помощью DNS можно произвести разведывательную атаку. Обычно, она является частью какой-то другой, более долгосрочной атаки. Например, с помощью DNS возможно получить информацию, на каком конкретно программном обеспечении работает сервер, а затем использовать уже специфичную для этого программного обеспечения атаку. Сервисы, позволяющие получать такую информацию, находятся в открытом доступе в сети Интернет.

Защититься от разведывательных атак можно только не допуская хранения чувствительной информации в системе DNS.

Самыми известными следствиями отсутствия какой-либо проверки авторитетности источников DNS пакетов являются атаки неавторизованного обновления и отравление кэша.

Обновление записей в реальном времени или по запросу является основной функцией DDNS (Dynamic DNS). Определенный тип запроса позволяет добавить или удалить ресурсную запись. Однако, изначальный механизм проверки источника был очень простым: IP адрес сверялся с хранящимся на сервере списком авторитетных источников. Злоумышленник, подменив адрес в пакете, мог добавить на сервер новую запись либо обновить существующую.

Отравление кэша (атака Каминского)[1] является атакой на рекурсивный сервер. Злоумышленник запрашивает у сервера несуществующий поддомен домена, который будет подменен. Сервер отправляет запрос на авторитетный сервер. Злоумышленник посылает на рекурсивный сервер множество подделанных ответов. С некоторой вероятностью один из них дойдет раньше реального ответа и будет принят. Пользователь, запросив IP подмененного хоста, получит тот IP, который задал злоумышленник.

Кроме этого, DNS трафик может быть модифицирован налету Интернет-провайдером.

Для защиты от таких атак были разработаны расширения DNSSEC (только аутентификация источника и проверка целостности, отсутствие шифрования данных для обеспечения обратной совместимости) и экспериментальный протокол DoH (DNS over HTTPS), который обеспечивает шифрование данных при передаче запросов и ответов между звеньями цепочки DNS.

Также, DNS-серверы уязвимы перед DoS атаками случайного поддомена и NXDOMAIN атаками. Они заключаются в посыле на сервер большого числа запросов на несуществующие поддомены (авторитетный сервер вынужден осуществлять более глубокий поиск соответствия) или несуществующие домены (рекурсивный сервер вынужден обращаться к авторитетному). При этом ресурсы сервера тратятся на заведомо бесполезный поиск соответствия. От таких атак невозможно полностью защититься, можно лишь смягчить последствия путем оптимизации программного кода сервера и фильтрации запросов.

Список использованных источников:

1. S. Son, The Hitchhiker's Guide to DNS Cache Poisoning [Electronic resource] / S. Son, V. Shmatikov // Cornell University. – Mode of access: https://www.cs.cornell.edu/~shmat/shmat_securecomm10.pdf. – Date of access: 15.03.2020

2. DNS Amplification Attack Detection and Mitigation via sFlow with Security-Centric SDN/ A. Atan [et al.] // IMCOM '17, Beppu, Japan, January, 2017 – P. 1–7.