УДК 004.75

магистр П.С. Киценко
ГВУЗ «Национальный горный университет»

КАНАЛ УТЕЧКИ ИНФОРМАЦИИ В DNS СЕРВИСЕ ПРИ ИСПОЛЬЗОВАНИИ DLP

В работе проанализирован канал утечки информации, возможные методы его реализации. Предложены методы для обнаружения утечек информации.

Domain Name System (система доменных имён) компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).

Канал утечки информации в DNS может быть использован злоумышленником создания канала передачи данных между злоумышленником и инсайдером. Для этого, со стороны злоумышленника понадобится создать и поддерживать свою DNS зону (их может быть несколько). В свою очередь со стороны инсайдера необходимо сформировать необходимые данные и создать запрос на разрешение доменного имени.

В общем случае принцип работы следующий. Инсайдер формирует данные, например, разбивает на блоки и кодирует их в BASE64. Далее он добавляет эти данные, в качестве субдомена для домена(ов) злоумышленника. После инсайдер запрашивает разрешение имени у стандартного DNS сервера. После определения сервера, ответственного за зону злоумышленника, DNS сервер отправляет ему запрос на разрешение имени. Злоумышленник сохраняет запрошенное имя, и в качестве ответа может передать управляющую информацию инсайдеру. Еще одним способом передачи небольших порций информации можно использовать такой алгоритм: выставить допустимое время хранения ресурса записи в нулевое значение. На стороне злоумышленника создать ассоциативный массив субдомен/значение. Например, mail.example.com – соответствует тетраде равной семи, docs.example.org – тетраде равной трем. Таких доменов можно сделать достаточное количество, для передачи необходимого потока данных. После этого последовательно производить разрешение заранее известных

доменов. Далее злоумышленник сможет восстановить закодированную информацию.

Поскольку злоумышленнику в большинстве случаев необходимо передавать бинарные данные. Поскольку стандарт рекомендует передачу только текстовой информации, злоумышленнику необходимо произвести кодирование информации. Для этих целей может быть применено кодирование BASE32, которое гарантированно передаст информацию, избыточность передачи данных составит 83%. Если промежуточные DNS сервера сохраняют регистр символов, тогда можно использовать BASE64, избыточность составит 52%. Согласно стандарту [1], можно передавать любые байты, кроме нулевого байта, который является сервисным. Поэтому если перекодировать текст, для избавления от нулевого байта, тогда избыточность будет минимальна, и составят 15%, по сравнению с чистой передачей пакета объемом в 512 байт.

Проведя анализ наиболее распространённых систем предотвращения утечек информации [2,3], можно сделать вывод, что в них не производится за такими протоколами как DNS, ICMP. Поскольку данный метод может быть легко реализован со стороны инсайдера, следовательно, необходимо дальнейшее изучение данной уязвимости и создание методологии для обнаружения утечек данным каналом.

Перечень литературы:

1. P. Mockapetris. RFC1035. Domain names – implementation and specification [Электронный ресурс] – Режим доступа: http://www.ietf.org/rfc/rfc1035.txt

2. Eric Ouellet, Rob McMillan. Gartner Magic Quadrant for Content-Aware DLP [Электронный ресурс] – Режим доступа: http://www.gartner.com/technology/streamReprintPDF.do?id=1-16XZCGC&ct=110811&st=sb

3. Баранов А., Шабанов И. Сравнение систем защиты от утечек (DLP) [Электронный ресурс] – Режим доступа: http://www.anti-malware.ru/comparisons/data_leak_protection_2011_part1