SkyDNS

Тайные туннели Интернета

Недооцененные уязвимости DNS протокола

SkyDNS

Павел Евтихов

руководитель отдела внедрения

DNS-туннель

Метод передачи данных между двумя точками, например, между компьютером и сервером, через протокол DNS.

Чем опасен DNS-туннель?

Рабочий инструмент для полноценной утечки данных

Остается как бэкдор для дальнейших атак: слежка, кража, вредительство

«DNS-туннели нас не смогут нас коснуться»

Убеждение подавляющего большинства компаний. Некоторые убеждены, что они защищены по белым спискам.

100%

Компаний, которые обратились к нам
за диагностикой, – не защищены от DNS-туннелей

DNS – слепая зона

Компании забывают мониторить трафик

Внедрить легко

Даже если вы считаете, что ваша сеть защищена, в нее легко смогут внедрить DNS-туннели.

Почему DNS-туннель легко внедрить?

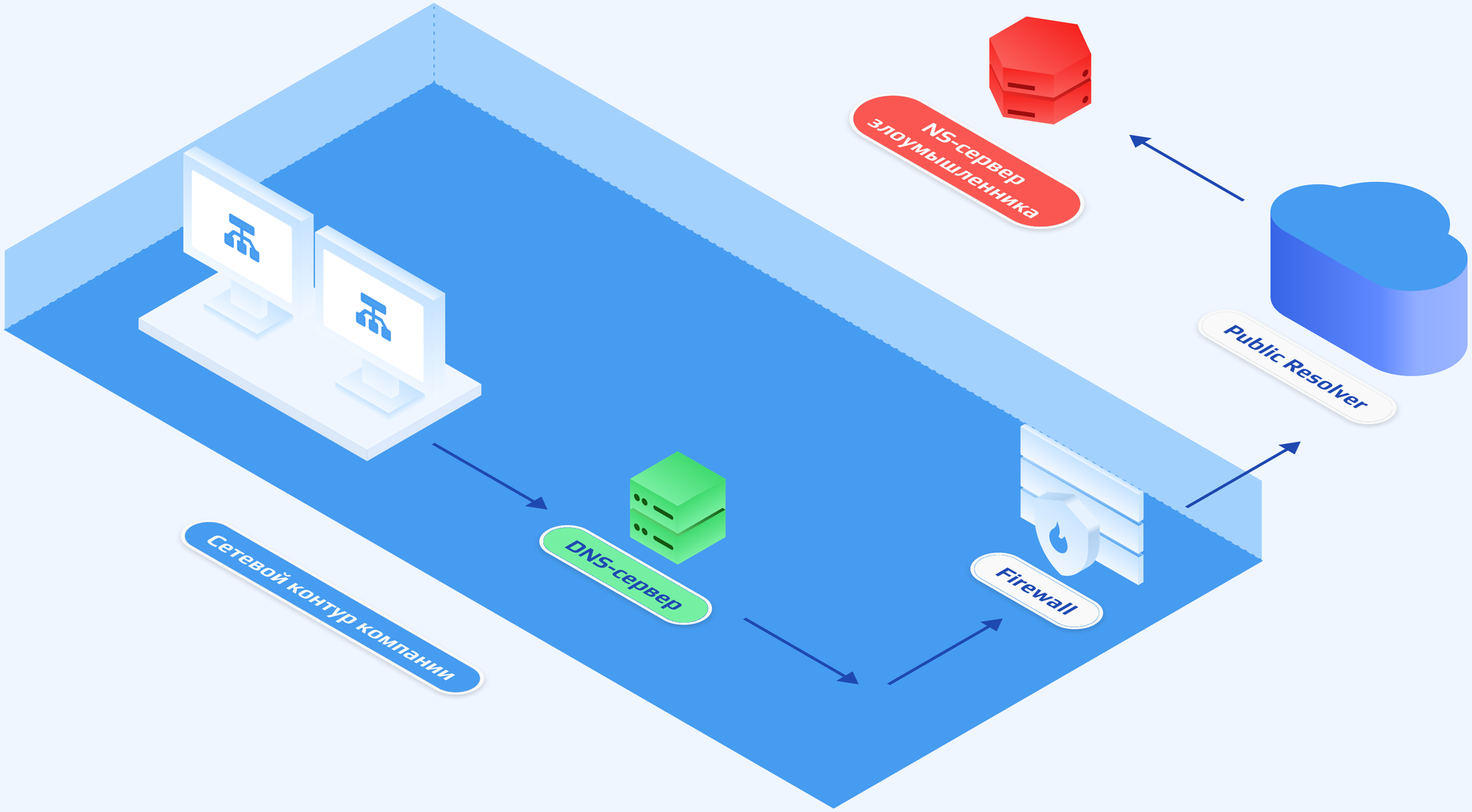
Злоумышленники не изобретают велосипед,
а используют
готовое решение

Создается в один клик на базе open-source решений

Некоторые open-source решения для DNS-туннелирования

Решение	Описание
Iodine	Позволяет туннелировать IPv4 данные через DNS-сервер. Это может быть полезно в ситуациях, когда доступ в интернет ограничен межсетевым экраном.
DNSStager	Позволяет скрытно управлять скомпрометированными системами, поддерживая динамическую загрузку и выполнение вредоносного кода через легитимный на вид DNS-трафик.
dnscat2	Предназначен для создания зашифрованного канала командования и управления (C&C) через DNS протокол. Состоит из клиента и сервера.
Sliver	Привлекает хакеров благодаря сложности обнаружения, поддержке шифрования и способности передавать TCP и UDP-трафик через легитимные DNS-запросы.
dnstt	Используется несколькими VPN-сервисами. Реализует протокол поверх DNS запросов и ответов, обладает функциями безопасности, такими как шифрование и аутентификация, и использует TXT-записи для кодирования данных в DNS-ответы.
Heyoka	Proof of Concept инструмента эксфильтрации, который использует поддельные DNS-запросы для создания двунаправленного туннеля.
Chisel	Open source инструмент туннелирования, написанный на Golang.

Схема DNS-трафика



Примеры туннелирования

Любая полезная нагрузка может быть передана прямо в самом домене в виде текста

Время	Домены
2025-03-11 03:26	520a01ae0d45a87245bcc9007244ce0d55.
2025-03-11 03:26	5ce401ae0da1df056524d90071981ef781.
2025-03-11 03:26	bfd501ae0d857336d9689b00705737557c.
2025-03-11 03:26	8bb101ae0dc461acd325fe006fddb27a6f.
2025-03-11 03:26	16ae01ae0ddea94434ac7d006e32a04999.
2025-03-11 03:26	b3b701ae0d56b1314e546b006d694e964d
2025-03-11 03:26	9a8c01ae0dbae7f66cf095006cf982fe55.
2025-03-11 03:26	9a8c01ae0dbae7f66cf095006cf982fe55.
2025-03-11 03:26	9f9901ae0d8078a34b957b006b38525fcb.
2025-03-11 03:26	6a7101ae0d299a12998ecb006a5359f765.

```
Autodetecting DNS query type (use -T to override).iodine: Received unsupported encoding
.iodine: Received unsupported encoding
.....iodine: Received unsupported encoding
.iodine: Received unsupported encoding
....iodine: Received unsupported encoding
.iodine: Received unsupported encoding
```

Iodine проверяет какие типы DNS-пакетов вообще подходят для полезной нагрузки

Проверяем максимально возможный размер полезной нагрузки в пакете

```
Autoprobing max downstream fragment size... (skip with -m fragsize)
768 not ok.. 384 not ok.. 192 ok.. 288 not ok.. 240 not ok.. 216 not ok.. 204 ok.. 210 ok.. 213 ok.. 214 ok.. will use 214-2=212
Setting downstream fragment size to max 212...
```

```
root@[redacted]:~# wget http://[redacted].ru/test.csv
--2025-02-02 17:18:45--  http://[redacted].ru/test.csv
Resolving [redacted].ru ([redacted].ru)... [redacted].52.251
Connecting to [redacted].ru ([redacted].ru)|[redacted].52.251|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://[redacted].ru/test.csv [following]
--2025-02-02 17:18:46--  https://[redacted].ru/test.csv
Connecting to [redacted].ru ([redacted].ru)|[redacted].52.251|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10535496 (10M) [application/octet-stream]
Saving to: 'test.csv.2'

test.csv.2                          100%[=============================================================================>]  10.05M  10.0MB/s    in 1.0s
```

Передали файл 10Мб за 1 секунду

В случае если мы на файрволе заблокировали абсолютно все неизвестные исходящие подключения, скорость значительно снизижается, но туннель продолжает работать

```
Saving to: 'test.pdf.5'

test.pdf.5                          100%[=============================================================================>]  96.84K  12.8KB/s    in 67s

2025-02-14 13:17:23 (1.44 KB/s) - 'test.pdf.5' saved [99162/99162]
```

200+

мегабит в секунду – возможная скорость передачи информации через туннель

Бесплатные лайфхаки для замедления DNS-туннелей

Можно закрыть 53 порт – скорость передачи информации уменьшится в 1000 раз

Анализируйте DNS-трафик – поможет лучше понять, что происходит в сети

SkyDNS

Павел Евтихов

Руководитель отдела внедрения

+7 922 222 15 84

p.evtikhov@skydns.ru

www.skydns.ru