



Невидимые
туннели Интернета:
как атаки годами
живут в тени DNS





Павел Евтихов

руководитель отдела внедрения



Злоумышленники могут оставаться незамеченными годами

51 мин

Средняя продолжительность кибератаки на российские компании в 2024 году

[Исследование компании «Информзащита», 2024](#)

249 дней

Столько в среднем злоумышленники находятся в инфраструктуре компании-жертвы до их обнаружения

[IBM Data Breach Report, 2025](#)

3 года

Длилось самое долгое пребывание злоумышленников в инфраструктуре

[Отчет Positive Technologies, 2023](#)



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



Чем опасен DNS-туннель?

- **Внедрить легко.** Существует множество готовых open-source решений
- **Обнаружить сложно.** Маскируется под легитимный трафик и сливается с фоновым «шумом» сети
- **Заблокировать ещё сложнее.** 100% компаний, который обращались к нам, не имели возможности блокировать DNS-туннели на лету

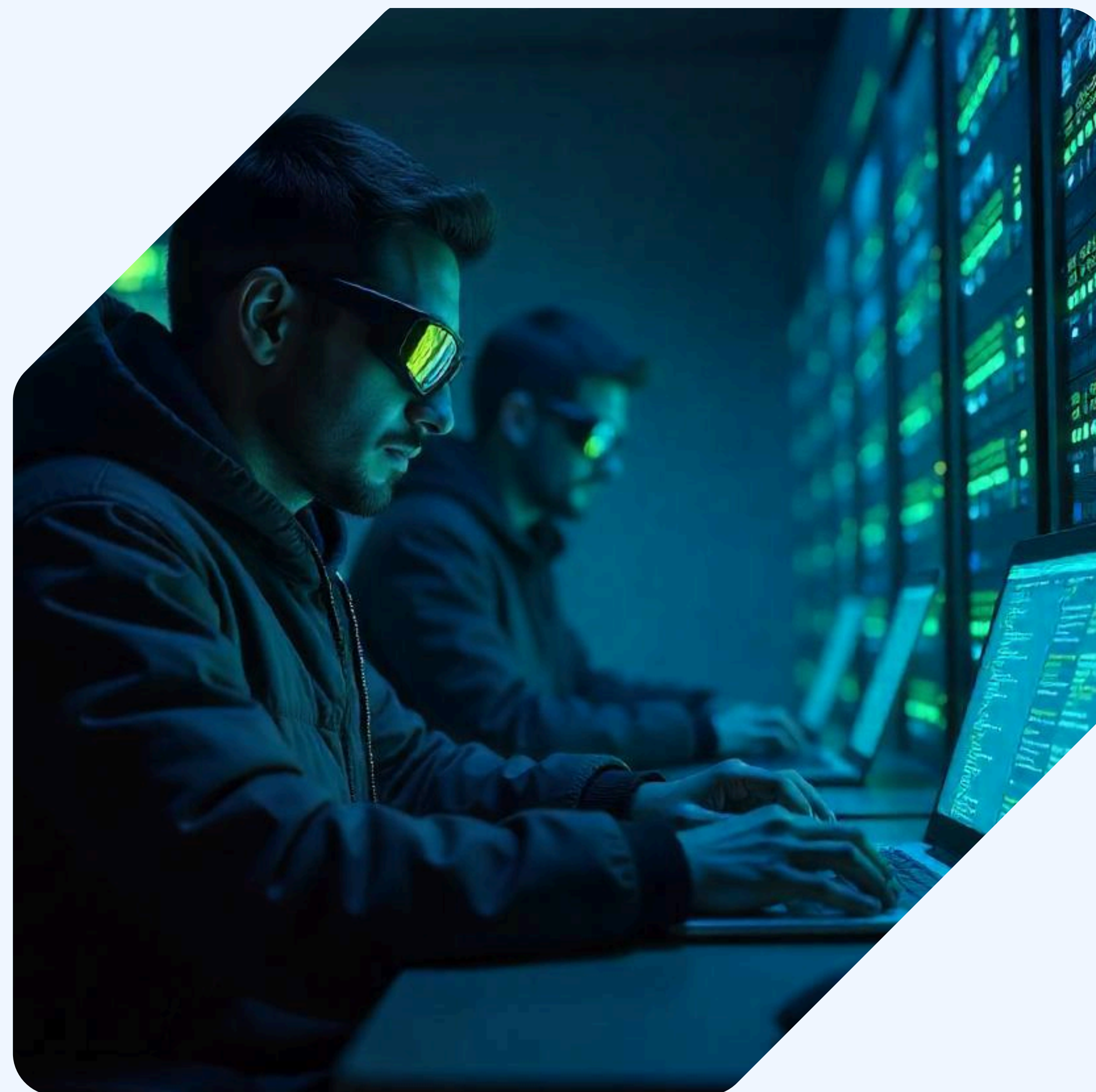
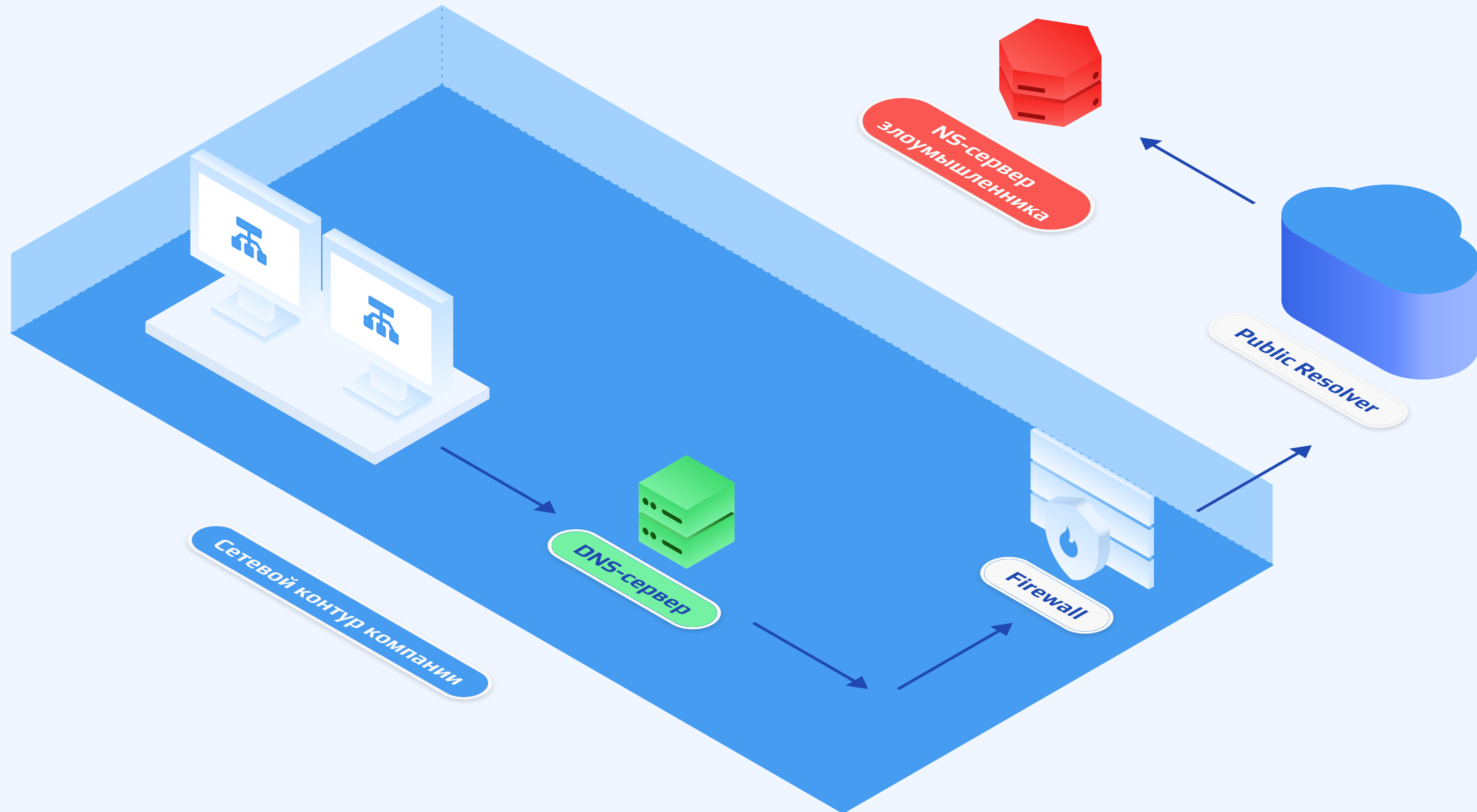


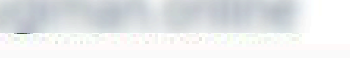
Схема DNS-трафика



Схема DNS-туннеля



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

Обнаруженные туннели	
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	16ae01ae0dde94434ac7d006e32a04999. 
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. 
Showing 301-310 of 465	
< 1 ... 30 31 32	



```
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

```
Server switched to lazy mode
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@kali:~# wget http://192.168.1.100/test.csv
--2025-02-02 17:18:45-- http://192.168.1.100/test.csv
Resolving 192.168.1.100 (192.168.1.100)... 192.168.1.52.251
Connecting to 192.168.1.100 (192.168.1.100)|192.168.1.52.251|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://192.168.1.100/test.csv [following]
--2025-02-02 17:18:46-- https://192.168.1.100/test.csv
Connecting to 192.168.1.100 (192.168.1.100)|192.168.1.52.251|: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 фаерволе заблокировали абсолютно все неизвестные исходящие подключения, скорость значительно снижается, 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]
```



Бесплатные лайфхаки для замедления DNS-туннелей

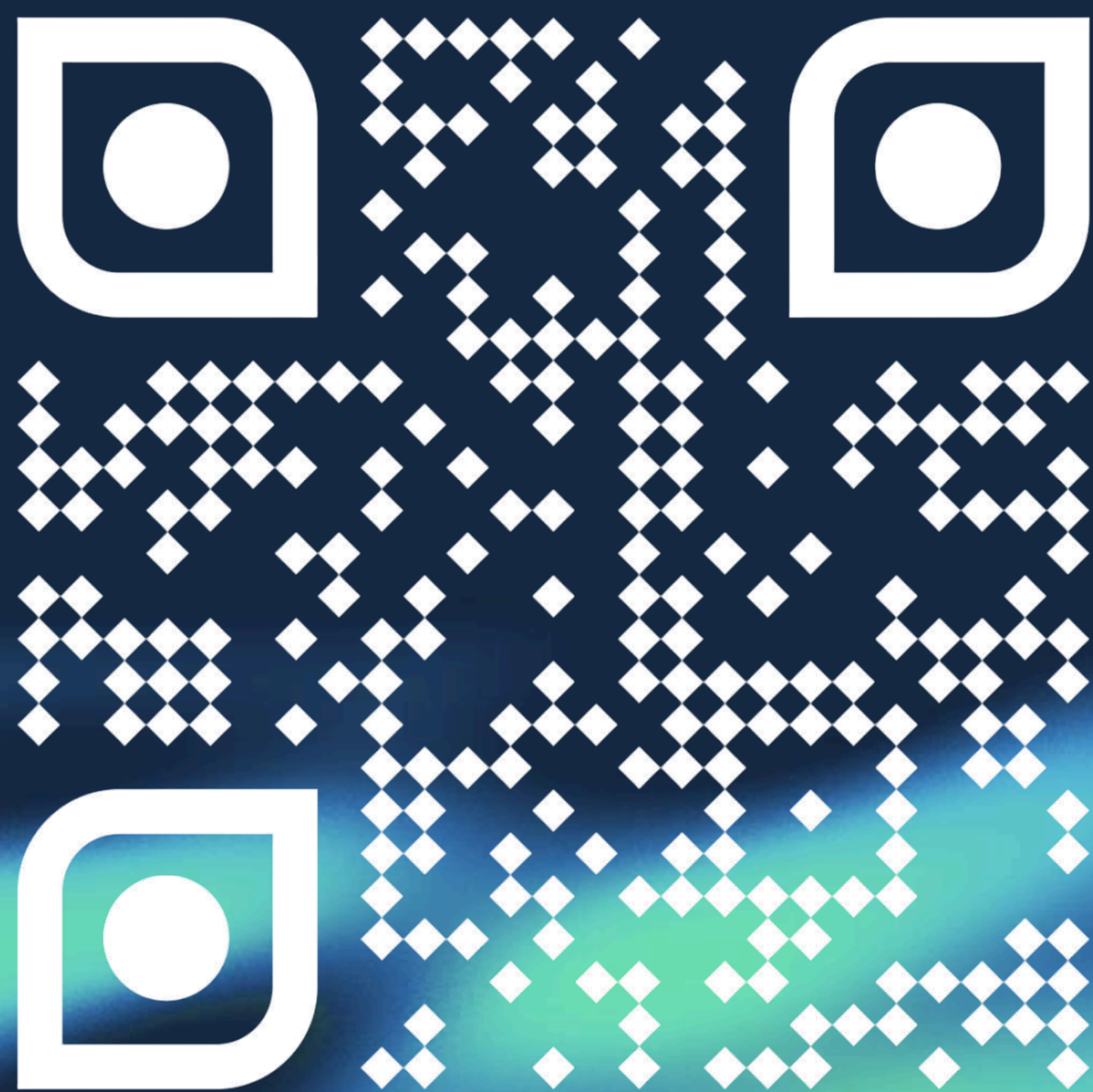
Можно закрыть 53 порт – скорость передачи информации уменьшится в 1000 раз



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



Проверьте, можно ли унести данные из вашей сети через DNS-туннели



Внимание! Утилита подписана нашим сертификатом безопасности и является диагностическим инструментом



Диагностическая утилита

DNS Tunnel Test

Шаг 1

Определяет, какой туннель можно использовать и какого размера файл можно передать в DNS-запросе.

Шаг 2

Находит типы DNS-запросов для организации туннеля, по которому будет передан ваш текстовый файл.

Шаг 3

Передаёт файл на сервер SkyDNS и закрывает туннель.

Шаг 4

Сервер собирает файл воедино и предоставляет ссылку на скачивание этого файла с сервера SkyDNS.

Файл передан через вашего поставщика DNS-услуг = высока вероятность утечки данных из вашей корпоративной сети



Будьте в курсе всех новостей и
подписывайтесь на ТКК



www.skydns.ru



Ответим на все ваши вопросы.
Связаться с нами просто:

 www.skydns.ru

 +7 800 333 33 22

 sales@skydns.ru

 г. Екатеринбург, ул. Токарей, д. 40,
офис 380

 Информация об обновлениях сервиса
в нашем [Телеграм-канале](#)