Слепые зоны инфраструктуры

Что можно увидеть через анализ DNS-трафика

SkyDNS — признанный лидер в защите DNS

ТОП-1

по импортозамещению согласно рейтингу «Лидеры цифровизации» 2025

1500+

компаний из промышленности, финансов, транспорта и ритейла уже под нашей защитой

15 лет

совершенствуем собственный центр аналитики угроз на базе AI и ML

ТОП-10

самых быстрых DNS-резолверов в мире по независимым оценкам

ТОП-5

по устойчивости DNS-резолверов — доверие миллионов пользователей

- Член ассоциации разработчиков ПО РУССОФТ
- Обладатель сертификата AM Test Lab
- Включены в Единый реестр российского ПО

RUS SOFT

20 ТОП Российских SaaS-компаний

Минкомсвязь России

www.amtestlab.ru CERTIFIED AM TEST LAB

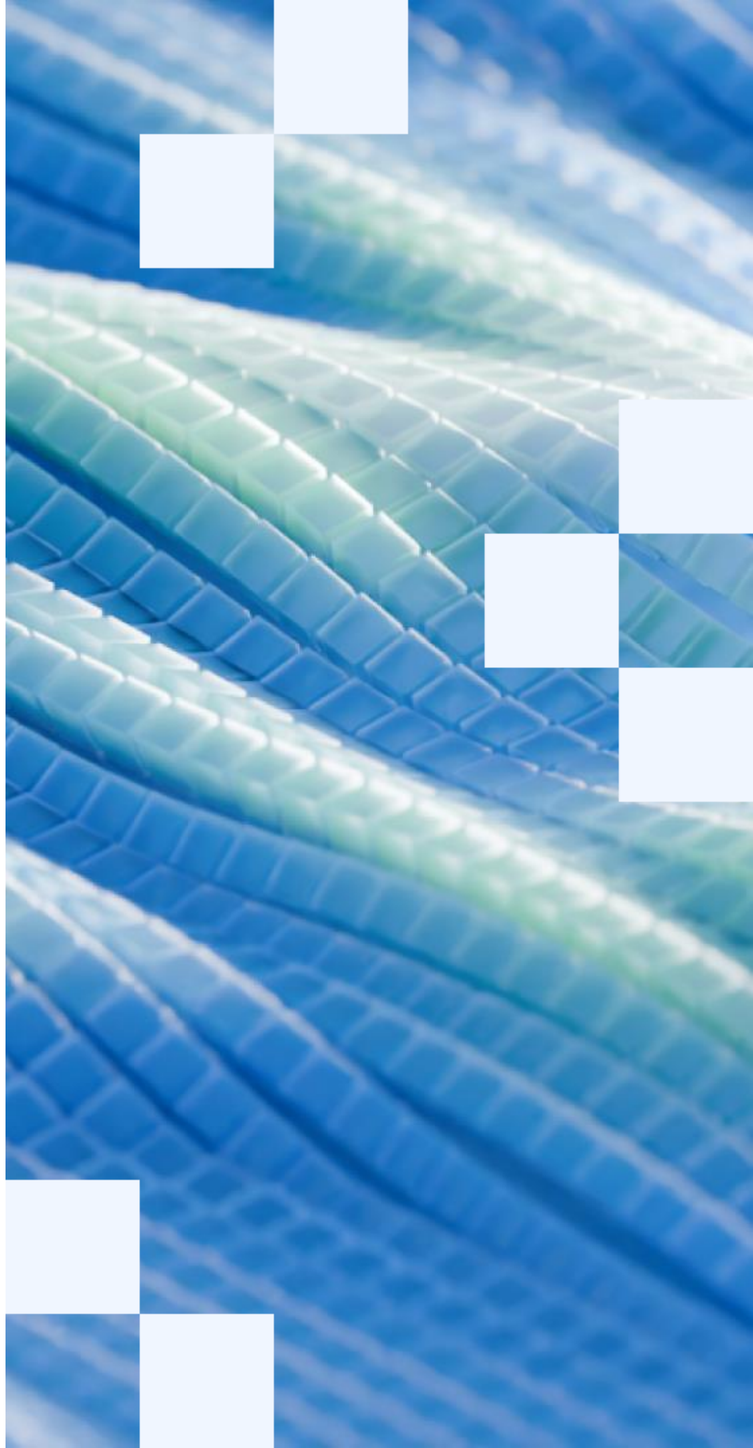
Слепые зоны сети

EDR & AV

Работают только на устройствах с установленными агентами; виртуальные среды и IoT-сегменты вне зоны видимости, инциденты не фиксируются

NGFW

Фиксирует только аномалии в объеме трафика, не различает DGA-паттерны, а C&C-запросы могут выглядеть легитимно



Злоумышленники могут оставаться незамеченными годами

51 мин

Средняя продолжительность кибератаки на российские компании в 2024 году
«Информзащита», 2024

249 дней

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

Кейс 1

Туннели — не вымысел

- Выявлен аномальный поток DNS-запросов к большому количеству доменов
- Домены второго и первого уровня оставались неизменными, а третий уровень постоянно менялся
- Изменяющийся поддомен — хаотичный набор символов от a до f, что характерно для кодирования данных в 16-ричном формате
- Сеть клиента не имела прямого доступ к сети Интернет, только к домен-контроллеру
- Через такой канал был выведен файл размером 15 Кб, но возможна передача и больших объемов данных

Возможные туннели

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

Showing **301-310** of **465**

< 1 ... 30 31 3

Кейс 2

Признаки активности ботнет-сети

- Несколько тысяч доменов с неизменными первыми двумя уровнями и постоянно меняющимся третьим уровнем указывали на аномальную DNS-активность

- К каждому домену фиксировалось всего 2–4 запроса, но на головной домен второго уровня пришлось 892 обращений

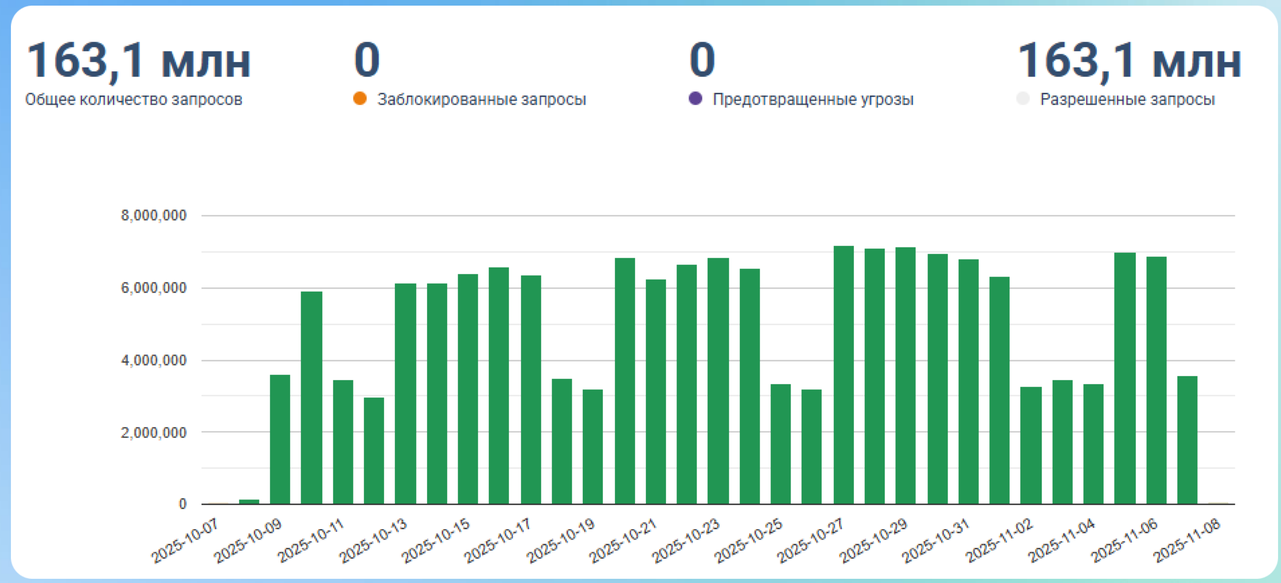
Домены	Категории	Запросы
chesselo2000.cfd	Botnets & C2, Недавно зарегистрированные домен...	892
fIyWd2A.chesselo2000.cfd	Недавно зарегистрированные домены	4
1pfyzFquX.chesselo2000.cfd	Недавно зарегистрированные домены	4
ZpqVD.chesselo2000.cfd	Недавно зарегистрированные домены	4
n8pv3X.chesselo2000.cfd	Недавно зарегистрированные домены	4
x6pnLyCGSP9lFgrB.chesselo2000.c...	Botnets & C2, Недавно зарегистрированные домен...	3
jwTOEaHJK2sFcOm.chesselo2000....	Недавно зарегистрированные домены	3
LmZK0wNY37.chesselo2000.cfd	Botnets & C2, Недавно зарегистрированные домен...	3
Hv2xD2t0EI3J1.chesselo2000.cfd	Недавно зарегистрированные домены	3
IJdt0j4wm4.chesselo2000.cfd	Botnets & C2, Недавно зарегистрированные домен...	3

Показаны 1-10 из 1000

Кейс 2

Признаки активности ботнет-сети

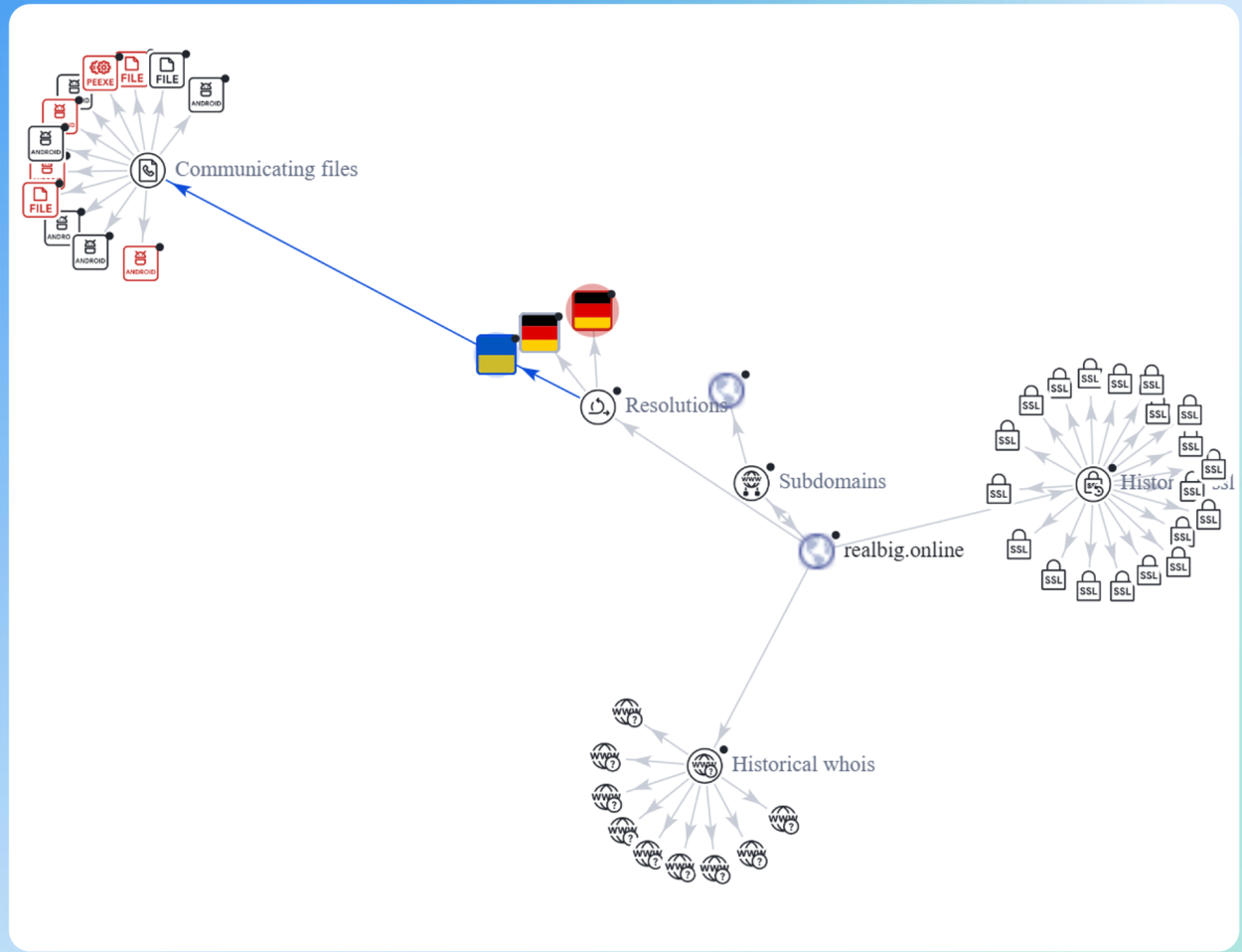
- При общем объеме 163 млн DNS-запросов эта активность оказалась частью коммуникации ботнет-сети
- Вероятно, уникальные поддомены соответствовали отдельным зараженным хостам



Кейс 3

Украинская APT-группировка

- У клиента зафиксировано большое количество запросов к конкретному домену
- Домен использовался для доставки обцированных скриптов, сбора данных и обхода ad blocker-ов
- Анализ артефактов показал, что инфраструктура могла использоваться не только для трекинга, но и для более агрессивной вредоносной активности
- Среди связанных объектов были обнаружены пересечения с инфраструктурой, используемой троянами, шифровальщиками и C2-цепочками
- Несмотря на внешний вид обычных парковочных доменов, такие запросы вели в потенциально опасную инфраструктуру



Кейс 4

Майнинг из самого неожиданного источника

- У клиента зафиксировано большое количество запросов к доменам, которые попали в категорию Cryptojacking
- Такая активность могла выглядеть как обычный cryptojacking, однако дополнительные запросы к криптообменникам и крупному форуму по майнингу показали, что речь идет не о браузерном сценарии или действиях вредоносного ПО

Домены	Категории	Запросы
2miners.com	Cryptojacking	2 942
zeph-eu.kryptex.network	Cryptojacking	1 302
zeph-ru.kryptex.network	Cryptojacking	1 272
rvn-eu2.nanopool.org	Cryptojacking	927
xmr-ru.kryptex.network	Cryptojacking	840
xmr-eu2.nanopool.org	Cryptojacking, Сайты для взрослых, Финансы и фин...	820
nanopool.org	Cryptojacking	528
okxac.okpool.top	Cryptojacking	491
okxcab.okpool.top	Cryptojacking	390
etc-eu2.nanopool.org	Cryptojacking	261

Домен donate связан не с майнинговыми пулами, а использует XMRig как часть своей модели работы. Такие запросы указывают на запуск стационарного майнера внутри сети

Домены	Категории	Запросы
donate.ssl.xmrig.com	Cryptojacking	30
donate.v2.xmrig.com	Cryptojacking	1

Домены	Категории	Запросы
changelly.com	Cryptojacking	243
cryptonator.com	Cryptojacking	10
emcd.io	Cryptojacking	18
miningclub.info	Cryptojacking	21

Криптообменники и крупный форум о майнинге. Такая активность характерна не для вредоносного ПО, а для человека внутри сети. Вывод: есть сотрудник, использующий ресурсы компании для майнинга

DNS — источник полезных сигналов

Однако DNS-трафик слишком масштабен для ручного анализа — угрозы в нем остаются незамеченными

Единая интеллектуальная система анализа DNS-угроз

В реальном времени обрабатывает и взвешивает данные из десятков источников



Преимущества решения SkyDNS

Блокировка угроз в динамике: система мгновенно реагирует на подозрительные ресурсы

Непрерывная адаптация защиты к новым угрозам с помощью AI/ML-алгоритмов

Быстрая интеграция за 15 минут: просто смена резолвера, инфраструктура не меняется



Просто смена внешнего резолвера

Без изменений сети

работает вне вашей инфраструктуры, без нового ПО или оборудования, достаточно смены IP внешнего резолвера

Полная приватность

передается только публичная информация, которая и до этого покидала сеть

Максимальная безопасность

поставляется полностью очищенный DNS-трафик

Высокая скорость и отказоустойчивость

распределённая BGP Anycast сеть с серверами в разных регионах обеспечивает мгновенный отклик

