SkyDNS

Как меняется ландшафт DNS-угроз: данные и выводы для CISO

Ландшафт киберугроз постоянно меняется, и часть этих изменений заметна в DNS-трафике еще на этапе обращения к домену. Анализ телеметрии SkyDNS за май и июнь 2026 года показал рост DNS-туннелирования, Botnets & C2 и числа недавно зарегистрированных доменов.

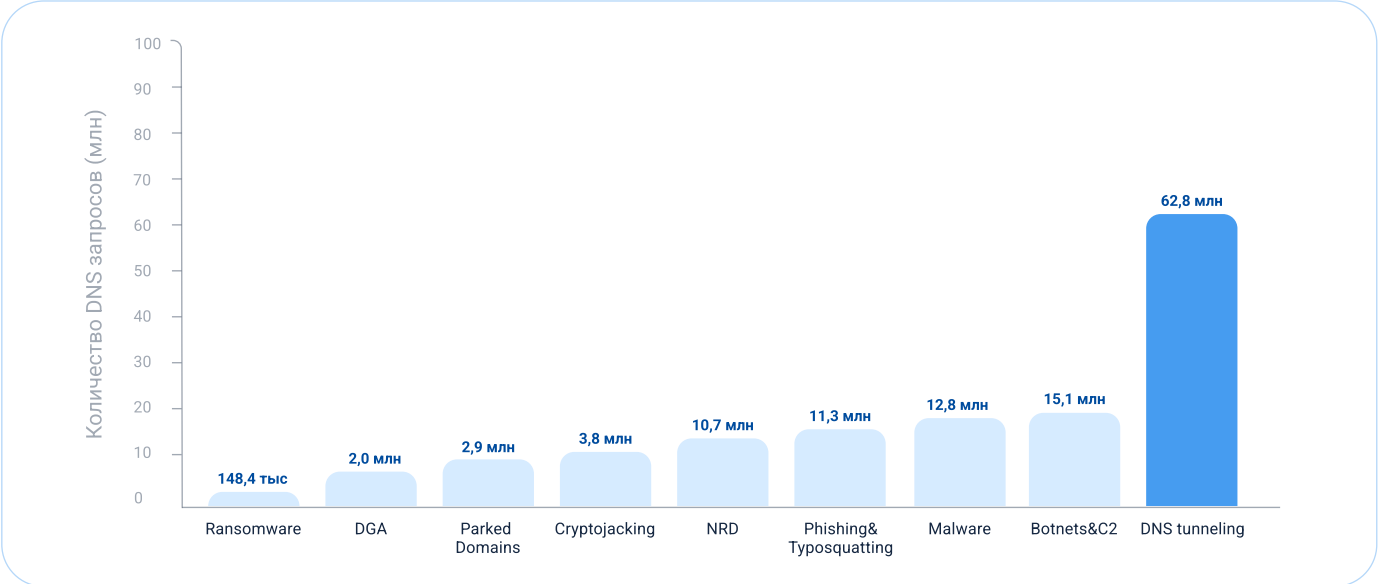
При этом динамику запросов важно оценивать в контексте: на нее влияют активность и блокировка вредоносной инфраструктуры, поведение зараженных устройств и изменения в механизмах детектирования.

Структура	Цифры	DNS
угроз быстро меняется. Может моментально вырасти одна активность и снизиться другая	важны в контексте. Рост запросов не всегда означает рост атак, а снижение не гарантирует уменьшения риска	помогает быстрее расследовать угрозы. Важно связать подозрительный домен с устройством, контекстом и дальнейшим действием

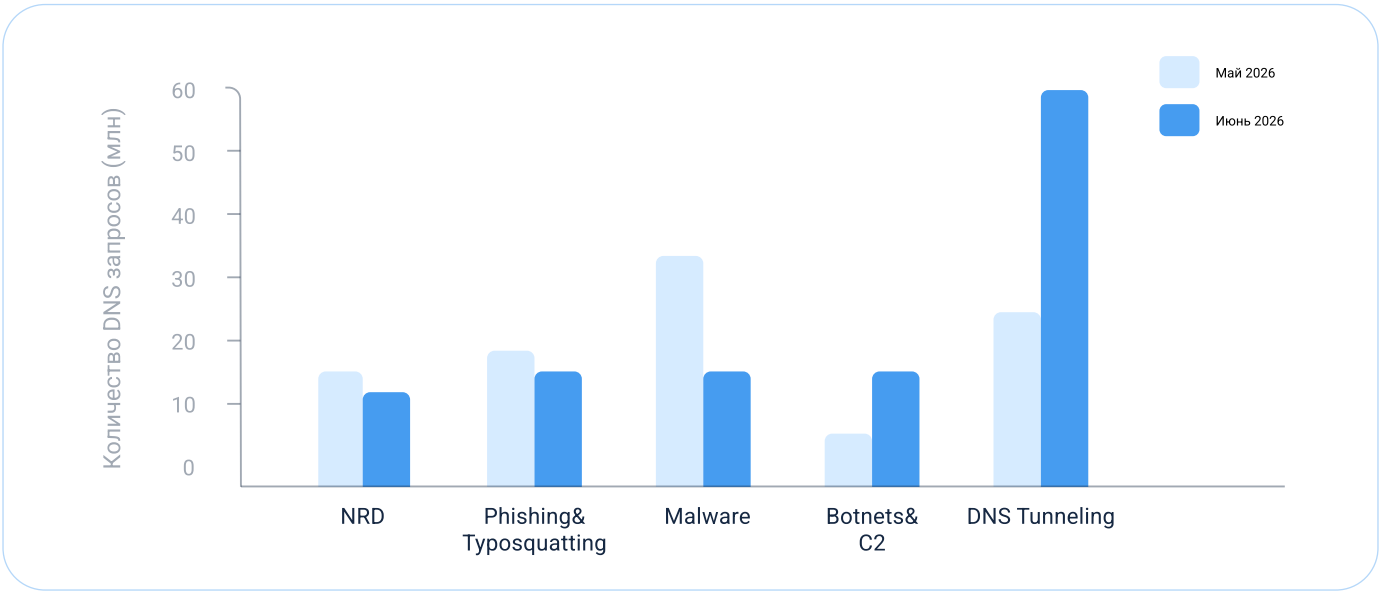
DNS-угрозы в июне: главное в цифрах

В июне в девяти анализируемых категориях SkyDNS зафиксировано около 121,5 млн DNS-запросов.

Наиболее крупной категорией стал DNS tunneling: 62,8 млн запросов. Еще 15,1 млн пришлось на Botnets & C2, 12,8 млн на Malware, 11,3 млн на Phishing & Typosquatting и 10,7 млн на NRD (недавно зарегистрированные домены).



Эта динамика показывает, что ландшафт наблюдаемой DNS-активности не просто растет или снижается. Меняется его структура, причем причины изменений в разных категориях могут существенно отличаться.



Изменения в категориях угроз

DNS tunneling вышел на первое место по числу запросов

Число запросов с признаками DNS-туннелирования выросло с 26,1 млн в мае до 62,8 млн в июне, а уникальных доменов — со 114,3 до 209,2 тыс.

Однако часть роста связана с ужесточением правил детектирования, поэтому для CISO важнее быстро определить источник запросов и необходимость расследования.

Botnets & C2: больше запросов при прежнем числе доменов

Число запросов в категории Botnets & C2 выросло с 7,8 до 15,1 млн, а число уникальных доменов почти не изменилось: 61 903 в мае и 61 812 в июне.

Это может указывать на активные обращения к известной инфраструктуре, поэтому команде ИБ важно связать C2-сигнал с устройством или сегментом сети.

Malware и phishing снизились

Количество запросов категории Malware сократилось с 33,9 до 12,8 млн, Phishing & Typosquatting — с 17,8 до 11,3 млн. Также снизились Cryptojacking, Parked Domains и DGA.

Но снижение телеметрии не означает автоматического снижения риска. На показатели влияют жизненный цикл вредоноса, блокировка доменов и изменения самих кампаний.

Ransomware: небольшой объем, высокий приоритет

Количество запросов, связанных с ransomware, выросло с 127,8 до 148,4 тыс.

На фоне других категорий объем небольшой, но здесь особенно хорошо видно, что частота и критичность события — разные вещи. Даже единичный сигнал, связанный с ransomware, может требовать высокого приоритета

Новых доменов стало больше

Число уникальных недавно зарегистрированных доменов выросло с 2 451 до 3 748, или на 53%, хотя количество запросов к ним немного снизилось.

Молодой домен сам по себе не является угрозой, но вместе с другими признаками помогает выявлять фишинг, временную инфраструктуру и обход политик.

Какие вредоносные семейства проявились в DNS-трафике

В DNS-телеметрии выявлялась инфраструктура, связанная с несколькими вредоносными семействами. **Lumma Stealer** используется для кражи учетных данных, а **BrockenDoor**, связанный с **BO Team / Black Owl**, для закрепления и удаленного управления скомпрометированными системами.

В категории C2 выделялись **P2PInfect** с peer-to-peer архитектурой и активностью в Redis, облачных и Kubernetes-средах, а также шпионский инструмент **XDSpy**. В DGA-трафике фиксировались **Vobfus**, **QSnatch** и **Ngioweb**: **QSnatch** атакует QNAP NAS и использует DGA для связи с C2, **Ngioweb** связан с ботнетной и прокси-инфраструктурой. Такие доменные индикаторы помогают команде ИБ искать источник подозрительной активности внутри сети.

Что эта динамика говорит CISO

Данные за май и июнь показывают, что ландшафт DNS-угроз нельзя описать одним показателем. В одной категории одновременно растут число запросов и количество доменов. В другой запросов становится почти вдвое больше при неизменном наборе доменной инфраструктуры. В третьей количество запросов сокращается, хотя разнообразие доменов растет.

Кроме того, на статистику могут влиять изменения детектирования, как в случае с DNS tunneling. Поэтому ценность DNS-телеметрии заключается не только в количестве обнаруженных событий.

Для CISO важнее, может ли команда быстро ответить:

- какое устройство создало подозрительный запрос;
- к какому домену оно обращалось;
- какой риск связан с этим доменом;
- как часто повторяется активность;
- есть ли связанные события в других средствах защиты;
- какое действие необходимо после обнаружения.

То есть из DNS-сигнала должна складываться понятная цепочка. В таком виде DNS становится не просто источником блокировок, а данными для расследования.

Домен → риск → источник → контекст → действие

SkyDNS

Что происходит во внешнем ландшафте угроз

1 Цепочки поставок остаются привлекательной целью

В июне группа World Leaks заявила о компрометации Tata Electronics и публикации более 200 тыс. файлов общим объемом свыше 630 ГБ. В массиве, по заявлениям атакующих, присутствовали документы, связанные с крупными технологическими компаниями.

Еще один пример — кампания IronWorm в npm-экосистеме. Она затронула 36 пакетов и использовала postinstall-скрипты для запуска вредоносных компонентов. Подобные инциденты показывают, что поверхность риска компании давно не заканчивается собственной инфраструктурой. В нее входят поставщики, подрядчики, программные зависимости и общие сервисы.

2 Кража данных остается самостоятельной целью

Заметная часть крупных инцидентов связана с предварительным выводом информации.

Группа FulcrumSec заявила о похищении более 1,3 ТБ данных у Novo Nordisk и требовании выкупа в размере $25 млн. Компания подтвердила факт киберинцидента, но не заявленный злоумышленниками масштаб.

ShinyHunters сообщали о краже 3,1 ТБ данных у NAIC через PeopleSoft. При этом публичные заявления атакующих и подтвержденные организацией последствия различались.

3 Учетные данные остаются ценным активом

В Have I Been Pwned был добавлен массив Stealer Logs примерно с 56 млн уникальных email-адресов и 124 млн уникальных паролей, собранных из логов инфостилеров. Для корпоративной безопасности это означает, что компрометация может начинаться далеко за пределами периметра организации. Инфостилер на отдельном устройстве крадет учетные данные, после чего они могут использоваться уже для доступа к корпоративным системам.

4 Последствия старых компрометаций никуда не исчезают

Еще один заметный эпизод связан с FortiBleed. В публичном доступе оказались действующие административные учетные данные для интернет-доступных устройств Fortinet FortiGate. По данным, приведенным в брифинге, речь шла о десятках тысяч устройств в 194 странах. При этом ключевой риск был связан не с появлением новой уязвимости, а с сохранением ранее скомпрометированных учетных данных.

Это важный принцип для команды ИБ: устранение уязвимости еще не всегда означает устранение последствий компрометации. После инцидента необходимо отдельно проверять и отзывать пароли, ключи, токены и др. средства доступа.

SkyDNS

Что важно учитывать CISO

Если сопоставить DNS-телеметрию и события внешнего ландшафта, можно выделить несколько общих выводов.

Структура угроз быстро меняется

Сегодня в наблюдаемом трафике доминирует одна категория, через месяц соотношение может выглядеть совершенно иначе

Объем события нельзя оценивать отдельно от контекста

Рост не всегда означает аналогичный рост числа атак, а снижение не гарантирует уменьшения риска

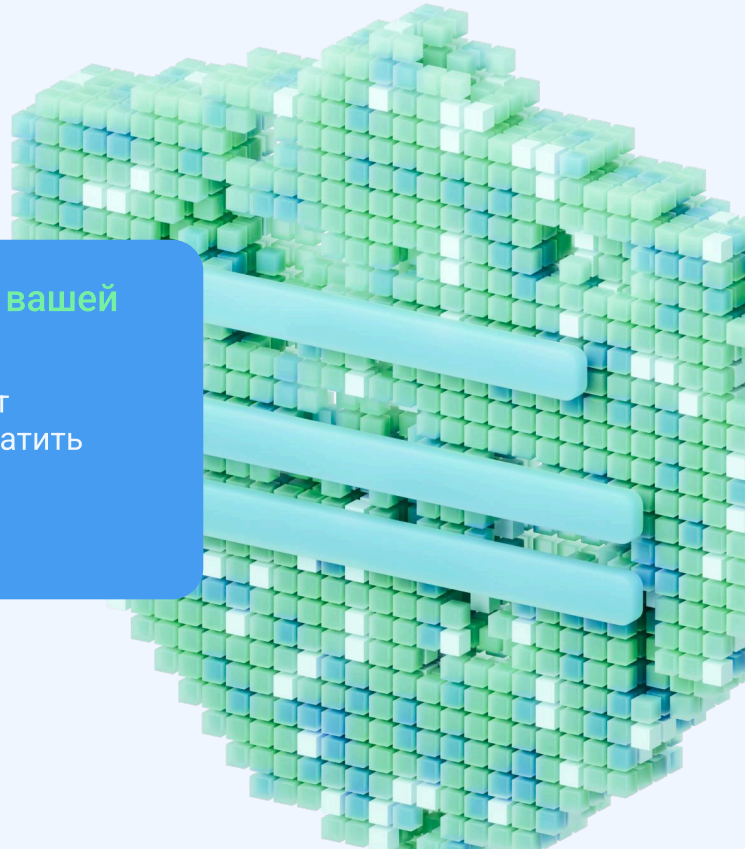
DNS помогает заранее увидеть угрозу

Особенно это актуально для C2, DGA, недавно зарегистрированных доменов, фишинга и подозрительных DNS-паттернов

Поэтому вопрос для CISO заключается не только в том, блокируются ли опасные домены. Важно понимать, насколько управляем сам DNS-слой: видит ли команда запросы из разных сегментов инфраструктуры, может ли связать событие с конкретным источником, попадают ли DNS-сигналы в общий процесс мониторинга и расследования и понятно ли, какое действие необходимо после обнаружения.

Чем быстрее команда может пройти путь от подозрительного домена до устройства и контекста события, тем больше практической ценности дает DNS-телеметрия.

DNS в этом случае становится дополнительным уровнем наблюдения, который помогает раньше увидеть риск и быстрее перейти к расследованию.



Хотите понять, какие DNS-риски есть в вашей инфраструктуре?

Оставьте заявку, и наши специалисты помогут разобраться, на какие DNS-сигналы стоит обратить внимание и как выстроить защиту.

Оставить заявку