Ландшафт DNS-угроз

Июль 2026

DNS-запрос — один из самых ранних сигналов того, что пользователь или устройство пытается обратиться к внешнему ресурсу: сайту, сервису, фишинговой странице, C2-инфраструктуре или другому подозрительному домену.

Поэтому DNS-телеметрия — это не просто статистика запросов, а дополнительный слой видимости для команды: к каким доменам обращаются устройства, откуда идут запросы, насколько часто они повторяются и с какими рисками связаны.

Июльские данные SkyDNS показывают, почему эти параметры важно смотреть вместе: количество запросов и доменов может меняться по-разному, а за одинаковой динамикой могут стоять разные сценарии — активность зараженного устройства, изменение инфраструктуры атакующих или результат реагирования.

Ранний сигнал

DNS-запрос возникает еще до соединения с внешним ресурсом и помогает раньше заметить обращение к подозрительной инфраструктуре

Источник

DNS-телеметрия помогает понять, какое устройство или сегмент сети создает подозрительные запросы и насколько часто они повторяются

Контекст

Категория домена, источник и интенсивность запросов помогают понять, что стоит за сигналом и требуется ли дальнейшее расследование

DNS-угрозы в июле: главное в цифрах

- **DGA стал главным растущим направлением июля**

число запросов выросло почти втрое — с 2,0 до 6,0 млн, при этом уникальных доменов стало меньше

- **DNS tunneling остается крупнейшей категорией**

несмотря на снижение запросов на 37%. Число уникальных доменов при этом практически не изменилось

- **Botnets & C2 сохраняет высокую интенсивность**

после устранения крупных источников заражения число уникальных доменов резко снизилось, но в июле все еще зафиксировано 12,6 млн запросов к C2-инфраструктуре

- **Ransomware-запросов стало на 33% больше**

хотя число уникальных доменов сократилось. Это показывает, что небольшой набор инфраструктуры может генерировать высокую интенсивность обращений

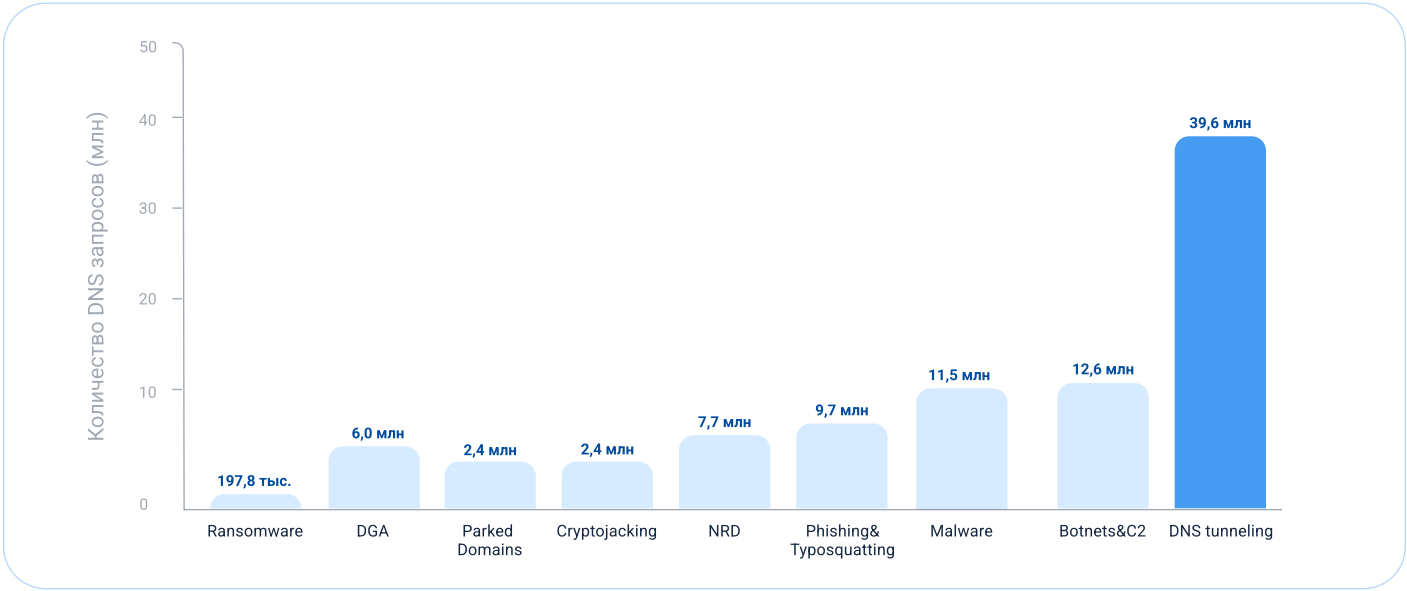
Как и прежде, сами цифры важно оценивать в контексте. На статистику влияют не только действия злоумышленников, но и изменения детектирования, жизненный цикл инфраструктуры атакующих и мероприятия по реагированию внутри организаций.

Какие вредоносные семейства проявились в DNS-трафике

В июле в девяти анализируемых категориях SkyDNS зафиксировано около 92,1 млн DNS-запросов.

Крупнейшей категорией остался DNS tunneling — 39,6 млн запросов. Еще 12,6 млн пришлось на Botnets & C2, 11,5 млн на Malware, 9,7 млн на Phishing & Typosquatting и 7,7 млн на недавно зарегистрированные домены.

Наиболее заметно на этом фоне выделяется DGA: число запросов выросло с 2,0 до 6,0 млн, то есть почти в 3 раза.



При этом по большинству остальных категорий объем обращений снизился. Такая картина показывает, что ландшафт угроз меняется не синхронно: общий спад может происходить одновременно с резким ростом отдельных типов активности.

Изменения в категориях угроз

1 DNS tunneling снизился, но остается крупнейшей категорией

Количество запросов с признаками DNS-туннелирования сократилось с 62,8 млн в июне до 39,6 млн в июле, то есть примерно на 37%.

При этом число уникальных доменов практически не изменилось: 209 171 в июне и 208 602 в июле.

Динамика DNS tunneling зависит не только от активности угроз, но и от развития механизмов их обнаружения. Поэтому снижение числа запросов в июле нельзя напрямую связывать со снижением риска. Для команды ИБ важнее понимать источник подозрительной активности и контекст каждого сигнала.

2 Botnets & C2: источников стало меньше, активность остается высокой

В июле SkyDNS зафиксировал 12,6 млн запросов к доменам категории Botnets & C2 — меньше, чем в июне, когда их было 15,1 млн. Количество уникальных доменов Botnets & C2 также снизилось: с 61 812 в июне до 2 047 в июле.

Значительная часть этого изменения связана с устранением ранее наблюдаемых источников заражения в инфраструктуре клиентов. При этом высокий объем запросов сохраняется, поэтому снижение числа доменов не означает исчезновения C2-активности.

DNS-телеметрия в таком сценарии помогает не только обнаружить подозрительное обращение, но и проверить результат реагирования: какие источники удалось устранить, какие обращения прекратились и какие сигналы продолжают появляться в сети.

3 DGA: почти трехкратный рост запросов при меньшем числе доменов

Пока большинство категорий снижалось, DGA двигался в противоположную сторону. В июле количество DNS-запросов выросло с 2 до 6 млн — сразу на 198%. При этом уникальных доменов стало меньше: 107 против 83 месяцем ранее.

Получается необычная комбинация: доменная инфраструктура не расширяется, но обращения к ней становятся значительно интенсивнее. Такая картина может возникать, например, когда зараженные устройства многократно пытаются найти доступный адрес управляющей инфраструктуры или восстановить связь с C2.

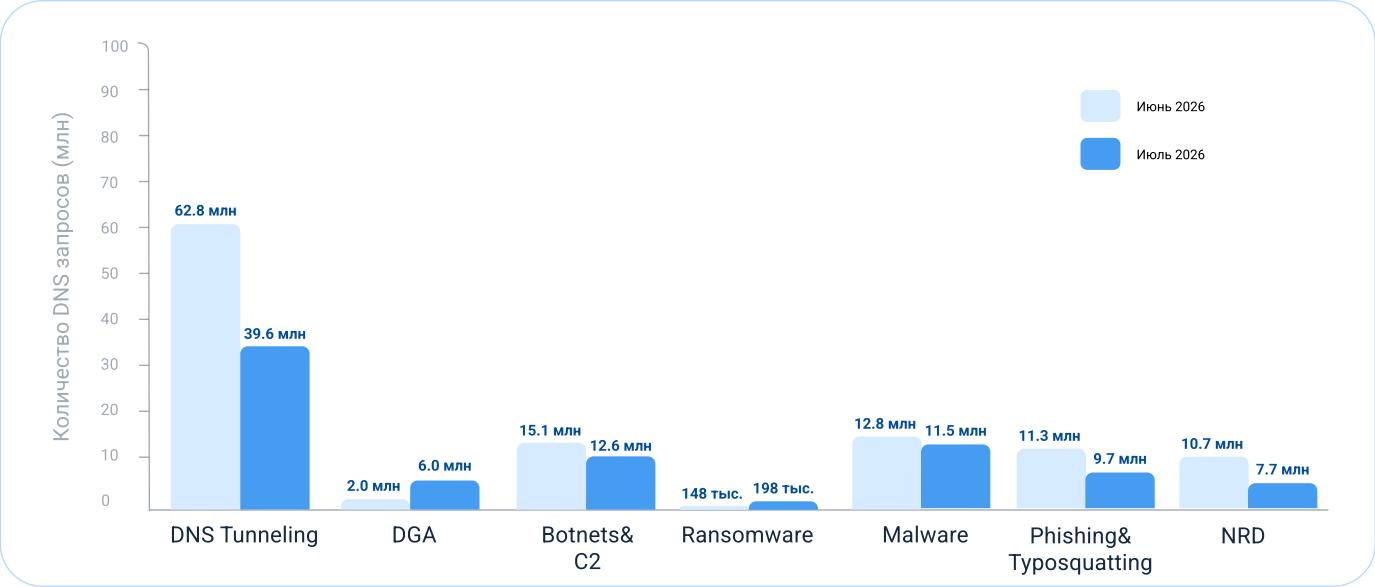
4 Ransomware: доменов меньше, запросов больше

Количество ransomware-запросов выросло с 148,4 до 197,8 тыс., или примерно на 33%.При этом число уникальных доменов снизилось с 99 до 61.

Как и в случае с DGA, небольшой набор инфраструктуры может генерировать высокую интенсивность обращений. Поэтому абсолютное число доменов не должно использоваться как единственный показатель риска.

5 Malware, phishing и NRD снизились

Malware сократился с 12,8 до 11,5 млн запросов, Phishing & Typosquatting — с 11,3 до 9,7 млн, NRD — с 10,7 до 7,7 млн. Количество уникальных доменов в этих категориях также уменьшилось.



Важно! Снижение наблюдаемой телеметрии не означает автоматического снижения риска. На показатели могут влиять блокировка и деактивация инфраструктуры, изменения отдельных кампаний, действия команд реагирования и переход атакующих на другие доменные кластеры.

Что говорит июльская динамика

Данные июля показывают, почему DNS-телеметрию нельзя оценивать только по общему количеству событий.

DNS tunneling

В DNS tunneling число запросов снизилось более чем на треть, тогда как набор уникальных доменов практически не изменился.

DGA

В DGA происходит обратная ситуация: уникальных доменов становится меньше, но интенсивность обращений увеличивается почти втрое.

Botnets & C2

В Botnets & C2 резкое сокращение числа наблюдаемых доменов связано в том числе с устранением источников заражения, однако миллионы обращений к C2-инфраструктуре продолжают фиксироваться.

Ransomware

Ransomware показывает еще один вариант той же картины: событий относительно немного, но их интенсивность растет при сокращении доменного пула.

Поэтому для команды ИБ важен не только вопрос «Сколько событий мы увидели?», но и то, что стоит за этой цифрой.

Практическая ценность DNS-телеметрии зависит от того, насколько быстро команда может ответить:

- какое устройство создает повторяющиеся подозрительные DNS-запросы;
- к какой инфраструктуре оно обращается;
- как изменяется интенсивность этих обращений;
- связан ли домен с C2, DGA, ransomware или другой ИБ-категорией;
- есть ли похожая активность в других сегментах сети;
- изменился ли риск или изменилась сама логика детектирования;
- какое действие требуется после обнаружения сигнала.

Именно здесь DNS становится практическим инструментом: он помогает не просто зафиксировать подозрительный домен, а пройти путь от сигнала к его источнику, необходимому действию и проверке результата реагирования.

Что происходит во внешнем ландшафте угроз

- **Доверенная инфраструктура становится точкой входа**

Open-source зависимости, CI/CD, support-системы, PLM-платформы, AI-агенты и сторонние интеграции все чаще становятся частью поверхности атаки.

- **DNS остается точкой риска за пределами корпоративной сети**

История с Hospitality Wi-Fi Poisoning показывает, что компрометация DNS возможна еще до подключения пользователя к корпоративной инфраструктуре.

- **Корпоративные и perimeter-системы остаются приоритетной целью**

SharePoint, ServiceNow, SD-WAN и системы управления средствами защиты привлекательны из-за широких прав, интеграций и доступа к критичной инфраструктуре.

- **Кража данных все чаще становится самостоятельной целью**

Для давления на компанию злоумышленникам необязательно останавливать процессы или шифровать системы: ценностью сами по себе становятся технические данные, R&D, учетные записи и клиентская информация.

- **GitLost: риск утечки данных через AI-агентов**

Исследователи Noma Security показали технику GitLost: специально подготовленный GitHub issue может через prompt injection заставить AI-агента с избыточными правами прочитать данные приватного репозитория и передать их во внешний канал. Этот кейс показывает, что права и каналы вывода AI-агентов нужно контролировать так же строго, как сервисные учетные записи.

Киберинциденты месяца

Июль показал, насколько разными могут быть точки входа в корпоративную инфраструктуру. В заметных инцидентах месяца фигурировали open-source зависимости и AI-агенты, сторонние сервисы, публичные Wi-Fi-сети, корпоративные платформы и компоненты критической инфраструктуры.

Последствия тоже различались: от кражи учетных данных и интеллектуальной собственности до шифрования систем и вмешательства в работу OT.

Вредоносный код через доверенный npm-пакет

11 июля злоумышленник опубликовал несколько вредоносных версий npm-пакета jscrambler, используемого вместе с продуктом Code Integrity.

Такой сценарий позволяет вредоносному коду попасть в инфраструктуру через доверенную зависимость и потенциально выполняться уже в процессе сборки или установки приложения. Для команд ИБ это еще один повод контролировать не только готовые приложения, но и зависимости, package manager, токены публикации и CI/CD.

Clop атакует PLM-системы

В июле группировка Clop атаковала интернет-доступные инстансы PTC Windchill и FlexPLM, эксплуатируя CVE-2026-12569.

Такие платформы могут содержать проектную документацию, сведения о продуктах, разработке и цепочках поставок. Поэтому их компрометация особенно чувствительна для производственных, инженерных и retail-компаний.

Утечка через систему поддержки Ernst & Young

Инцидент Ernst & Young был связан с компрометацией сторонней тикет-системы, используемой IT-персоналом. В заявках могли находиться документы с налоговой и клиентской информацией.

Случай показывает риск вспомогательных сервисов: даже если система поддержки не относится к основным бизнес-приложениям, через нее могут проходить чувствительные данные, вложения и внутренние ссылки.

DNS poisoning в публичных Wi-Fi-сетях

В кампании Hospitality Wi-Fi Poisoning злоумышленники компрометировали Wi-Fi gateway и captive portal в гостиничных сетях, меняли DNS-настройки и перенаправляли пользователей через свою инфраструктуру.

Атакующему не нужно заражать устройство или отправлять фишинговое письмо: достаточно контролировать сетевой шлюз. Пользователь может попасть на поддельную страницу и передать корпоративные учетные данные или OAuth-токены. Особенно актуален такой риск для сотрудников в командировках, аэропортах, отелях, на конференциях и в коворкингах.

Кража данных через стороннюю инфраструктуру

В июле сразу несколько инцидентов показали, что для давления на компанию злоумышленникам необязательно останавливать ее работу.

Amgen сообщила о краже данных из облачных хранилищ сторонних провайдеров. Потенциально могли быть затронуты пациентские данные, интеллектуальная собственность и R&D-материалы.

Analog Devices раскрыла несанкционированный доступ и эксфильтрацию отдельных файлов, при этом операционная деятельность компании не была нарушена.

В случае Stadler Rail технические данные были получены через file-sharing-платформу поставщика, после чего злоумышленники потребовали выкуп.

Эти случаи показывают, что облачные хранилища, сервисы обмена файлами и инфраструктура подрядчиков становятся полноценной частью поверхности атаки.

Атака на национальную кадастровую систему Румынии

14 июля кибератака нарушила работу IT-инфраструктуры румынского агентства ANCPI, включая национальную кадастровую систему e-Terra и почтовые сервисы.

Расследование подтвердило атаку вымогателей, в ходе которой была зашифрована и удалена часть инфраструктуры виртуализации.

Здесь последствия вышли за пределы утечки данных и напрямую повлияли на доступность государственного цифрового сервиса.

Атаки на системы водоснабжения США

26–27 июля скоординированные атаки затронули операционные технологии более чем 30 муниципальных систем водоснабжения в Миннесоте.

В отдельных случаях злоумышленники меняли настройки, IP-адреса и пароли на подключенных к интернету OT- и PLC-устройствах. Такие инциденты показывают, что целью атак может становиться уже не только информация, но и системы, связанные с реальными технологическими процессами. Для OT-сред особенно важны сегментация, ограничение удаленного доступа и контроль публичной экспозиции.

Эксплуатация корпоративных платформ и систем управления

В июле продолжалась эксплуатация уязвимостей в Microsoft SharePoint Server, ServiceNow AI Platform, Arista VeloCloud Orchestrator и Cisco Secure Firewall Management Center.

Такие системы привлекательны для атакующих, поскольку дают доступ к административным функциям, документам, интеграциям и другим частям инфраструктуры.Особенно чувствительны on-prem платформы и management-интерфейсы, доступные напрямую из интернета.

Что объединяет инциденты июля

У многих атак месяца есть общий паттерн: злоумышленники используют инфраструктуру, которой организация уже доверяет.

Это могут быть зависимости, AI-агенты, системы поддержки, облачные сервисы, платформы поставщиков, публичный Wi-Fi или корпоративные management-системы.Поэтому поверхность атаки сегодня включает не только собственные серверы и рабочие станции, но и весь набор сервисов, интеграций и инфраструктурных компонентов, через которые проходят корпоративные данные и учетные записи.

Что важно учитывать

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

Интенсивность важнее одной цифры

Количество запросов и количество доменов могут двигаться в противоположных направлениях.Рост DGA и ransomware-related обращений при сокращении доменного пула показывает, что небольшое число элементов инфраструктуры может создавать высокую интенсивность активности.

Поэтому объем события всегда необходимо оценивать вместе с его контекстом.

Работа с DNS-сигналами дает измеримый результат

Резкое снижение числа уникальных Botnets & C2-доменов после устранения источников заражения показывает, что DNS-телеметрия может быть не только источником наблюдения.

Она помогает найти подозрительную активность внутри инфраструктуры, связать ее с конкретным источником и проверить результат реагирования.

Доверенная инфраструктура сама становится каналом атаки

Open-source зависимости, GitHub workflow, AI-агенты, cloud storage, file-sharing, support-платформы, публичные Wi-Fi, SharePoint и management-системы объединяет один принцип: пользователь или организация изначально доверяют этой инфраструктуре. Именно поэтому атакующим необязательно пробивать защиту напрямую. Иногда эффективнее использовать уже существующий доверенный канал.

Для ИБ-команд это означает, что контроль должен охватывать не только классический периметр, но и DNS-трафик, облачные сервисы, зависимости, сторонние интеграции и административную инфраструктуру.Поэтому вопрос заключается не только в том, блокируются ли опасные домены. Важно понимать, насколько управляем DNS-слой: видит ли команда запросы из разных сегментов инфраструктуры, может ли связать событие с конкретным устройством, обнаружить повторяющийся паттерн и передать DNS-сигнал в общий процесс мониторинга и расследования.

Чем быстрее команда проходит путь от подозрительного обращения до источника и контекста события, тем больше практической ценности дает DNS-телеметрия.

SkyDNS

О SkyDNS

SkyDNS — российский разработчик решений для защиты на уровне DNS. Мы помогаем компаниям выявлять и блокировать угрозы еще на этапе обращения к домену — до установления соединения с вредоносной инфраструктурой.

Совместимость с существующим стеком

SkyDNS работает параллельно с другими средствами защиты и дополняет их без конфликтов

Непрерывная адаптация к новым угрозам

Центр аналитики SkyDNS постоянно обновляет индикаторы, списки вредоносных ресурсов и правила выявления аномалий

Снижение нагрузки на ИБ-команду

SkyDNS блокирует вредоносные DNS-запросы до соединения, снижая число инцидентов и объем ручной работы

Защита при больших нагрузках

SkyDNS обрабатывает более 2 млрд DNS-запросов в сутки и блокирует около 3 млн угроз, сохраняя стабильность при пиковых нагрузках

Хотите понять, что происходит в DNS-трафике вашей инфраструктуры?

Оставьте заявку, и специалисты SkyDNS помогут определить, какие DNS-сигналы требуют проверки, найти источники подозрительной активности и встроить DNS-телеметрию в процессы мониторинга, защиты и расследования.

Оставить заявку

skydns.ru sales@skydns.ru 8 (800) 333-33-72