kaspersky



Обзор 2026

Киберпульс. ИТ / Телеком.

Россия.

Ключевая статистика киберугроз для ИТ-организаций и телекоммуникационного сектора в России

135 минут

Средняя продолжительность DDoS-атаки на операторов связи в I полугодии 2026 года — самый высокий показатель среди всех отраслей[1]

Распределение инцидентов высокой критичности по отраслевым секторам. Глобальная статистика.[2]



Данные по основным типам угроз для ИТ и телекома в России в 2026 году

+20,2%
рост количества атак с помощью стилеров[3]

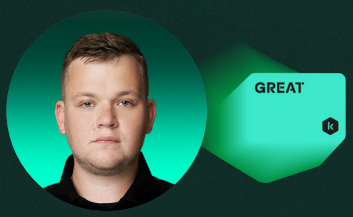
-9,6%
снижение количества атак с помощью эксплойтов[3]

+19,7%
рост количества атак с применением бэкдоров[3]

+61%
рост количества DDoS-атак на российские ИТ-компании, H1 2026 vs H1 2025[1]

ИТ и телеком всё чаще подвергаются атакам программ-вымогателей. Дело в том, что эти отрасли наиболее чувствительны к данному типу угроз — крупные инфраструктуры, дорогие данные, большой ущерб от простоев. К тому же стоимость проведения атак вымогателей заметно снизилась за счет использования злоумышленниками инструментов ИИ.

x2,6
рост атак с помощью программ-вымогателей[3]



Дмитрий Галов
Руководитель Kaspersky GReAT в России и СНГ

Телекоммуникационная инфраструктура остаётся одной из важных целей для злоумышленников: атаки могут быть направлены как на сами операторские сети и сервисы, так и на доступные через них системы. Интерес к отрасли проявляют кибершпионские и финансово мотивированные группировки, а также хактивисты. При этом компрометация телеком-инфраструктуры потенциально затрагивает не только операторов, но и организации и пользователей, которые зависят от их услуг. В таких условиях особенно важны постоянный мониторинг инфраструктуры, своевременное выявление уязвимостей и аномальной активности, а также проактивная защита от целевых атак.

1 По данным Kaspersky DDoS Protection
2 По данным отчёта « Анатомия ландшафта киберугроз: глобальная аналитика и практические выводы»
3 По данным Kaspersky Global Research and Analysis Team (GReAT) за 9 первых месяцев 2026 года по сравнению с 9 первыми месяцами 2025 года

Ландшафт киберугроз для ИТ и телекома: главные истории 2026

Что скрывает BO Team: бэкдор ZeronetKit изнутри и связь с Head Mare

Подробнее

В начале 2026 года группировка BO Team заявила о взломе нескольких интернет-провайдеров и провела фишинговую кампанию против сервисных компаний нефтегазовой отрасли. Для получения первичного доступа злоумышленники рассылают письма с вложениями, маскируемыми под офисные документы: «акт проверки» и «форму письменных пояснений». При открытии PDF-приманки на устройство незаметно от пользователя устанавливается бэкдор, который подключается к серверу управления (C2), закрепляется, собирает данные и выполняет команды атакующих.

Исследователи описали задействованный в атаках новый бэкдор ZeronetKit. Он обеспечивает устойчивый доступ, разведку и удалённое выполнение, работает в связке с загрузчиками и другими бэкдорами, включая небезызвестный BrockenDoor, для доставки и контроля. Ещё одна заметная особенность кампании — инфраструктурное и инструментальное пересечение с другой известной группой Head Mare —вплоть до работы C2 на одном скомпрометированном хосте.

CPU-Z / HWMonitor: атака типа watering hole — метод копипаста

Подробнее

В начале 2026 выявлены атаки типа watering hole* на посетителей ресурсов cpuid.com, на котором размещались установщики популярного программного обеспечения для системного администрирования CPU-Z, HWMonitor и PerfMonitor.

Сайт был скомпрометирован, и вместо нужных установщиков жертвы скачивали модифицированный вредоносный дистрибутив, который открывал легитимное приложение, но параллельно запускал вредоносную DLL, использующую технику подгрузки DLL (DLL Sideloading). В момент загрузки пользователь видел ожидаемую установку, в то время как загрузчик обращался к C2 и закреплялся в инфраструктуре для дальнейшего продвижения.

Особенность кампании — её избирательность: в код загрузчика вшит массив из большого числа MAC-адресов, по которому выполнялась фильтрация целей; полезная нагрузка доставлялась только «разрешённым» системам, что снижало шум и усложняло анализ. Атака затронула организации, в том числе из российской телекоммуникационной отрасли.

Arra Ghouls: пир во время киберчумы

Подробнее

В ходе мониторинга киберугроз эксперты «Лаборатории Касперского» выявили новую фишинговую кампанию неизвестной группы Arra Ghouls, затронувшую почти два десятка российских организаций, в том числе ИТ и телеком. Злоумышленники рассылают таргетированные письма с архивами и «документами», которые при открытии запускают многоступенчатую цепочку: после запуска вложений подтягиваются дропперы и загрузчики, устанавливающие удалённый доступ и обеспечивающие закрепление в среде. При этом для пользователя всё выглядит как обычное открытие документа.

В кампании применяется сочетание инструментов удалённого администрирования и шпионских средств (NetSupport RAT, Remcos), доставляемых через скрипты и DLL-подмену, что упрощает обход детектирования за счёт легитимного внешнего вида компонентов. Отмечаются техники закрепления через планировщик задач и автозагрузку. Операторы избирательно фильтруют цели и быстро ротируют C2, снижая шум и усложняя анализ, в результате чего получают устойчивый удалённый доступ и возможность дальнейшего продвижения по сети.



Захватывающие истории мирового кибербеза — в новом подкасте от Kaspersky GReAT

Слушать

* Watering hole (водопой — англ.) — стратегия таргетированных атак, в рамках которой злоумышленники размещают вредоносное ПО на сайтах, где, по их мнению, часто бывают потенциальные жертвы, и ожидают, когда зловред попадет на их компьютеры. Название watering hole взято из мира дикой природы: хищники нередко выслеживают свою добычу у рек и озер.

Сетевая безопасность — в фокусе для ИТ и телекома



Анна Кулашова
Вице-президент «Лаборатории Касперского» по развитию бизнеса в России и странах СНГ

В 2026 году ИТ и телеком — ключевая инфраструктура цифровой экономики. Любые сетевые сбои мгновенно затрагивают широкий круг организаций, их клиентов, сервисы и влияют на выручку. Угроза сместилась «в сеть»: рост зашифрованного трафика, массовые DDoS-атаки и манипуляции маршрутизацией усиливают риски. Быстрое масштабирование технологий 5G, FTTx, edge, IoT, развитие гибридных облаков помогают решать бизнес-задачи, но вместе с этим расширяют поверхность потенциальной атаки и усложняют контроль трафика. На этом фоне видимость в сети, управляемая сегментация и устойчивость к перегрузкам становятся приоритетом и ключом к снижению операционных и регуляторных рисков.

1 Zero Trust-сегментация критичных систем и трафика

- Карта критичных сервисов и доверенных связей; всё иное — по умолчанию запрещено.
- Разделение прод/офис/партнёры/админ; админ-доступы — только JIT и по MFA.
- Единая политика в ЦОД, облаках и филиалах; быстрый карантин сегмента при инциденте.
- Постоянное управление рисками ИИ: мониторинг, оценка угроз и контроль соответствия требованиям.

Специализированные решения для защиты и сегментации сети

Защита и контроль сети	Kaspersky NGFW
Безопасный доступ к корпоративной сети	Kaspersky ZTNA
Построение корпоративной сети	Kaspersky SD-WAN

2 Раннее выявление скрытых операций (включая зашифрованный трафик)

- Профиль «нормы» сети и поиск аномалий: редкие домены, долгие сессии, нестандартные регионы.
- Контроль egress: интернет — только тем, кому нужен; TLS-расшифровка — где можно, поведенческий анализ — где нельзя.
- Автоответ: блокировка C2 на NGFW и изоляция хоста/сегмента через SD-WAN.

3 Сокращение интернет-экспозиции и контроль «теневых» подключений

- Инвентаризация публичных IP/портов/доменов и регулярный отчёт; отключение лишнего.
- Запрет прямых RDP/SSH с интернета; админ-доступы — через шлюзы и окна времени.
- Блокировка несанкционированных туннелей (VPN, TOR, DoH/QUIC); публикации — в DMZ с IPS и строгими allow-правилами.

4 Устойчивость к DDoS и непрерывность ключевых сервисов

- Многоуровневая защита: провайдерский скраббинг + профили rate limiting/антифлудна периметре.
- Приоритизация DNS, SIP/IMS, биллинга и порталов; отдельные пороги и плейбуки реагирования.
- Двойная связность и auto-failover по метрикам качества; изолированная плоскость управления.

5 Защита сетевой инфраструктуры и обеспечение её отказоустойчивости

- Администрирование из выделенной зоны с MFA и полным журналированием; запрет из пользовательских сетей.
- Резервирование и автоматическое переключение. Многоканальные подключения, дублирование туннелей и хабов, выбор пути по задержке/потерям/джиттеру, механизмы сглаживания потерь, аварийный внеполосный канал для управления с помощью SD-WAN.
- Мониторинг DNS/NTP/BGP и алерты на утечки маршрутов и неожиданные изменения.



www.kaspersky.ru

© 2026 АО «Лаборатория Касперского».
Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

#kaspersky
#активируйбудущее