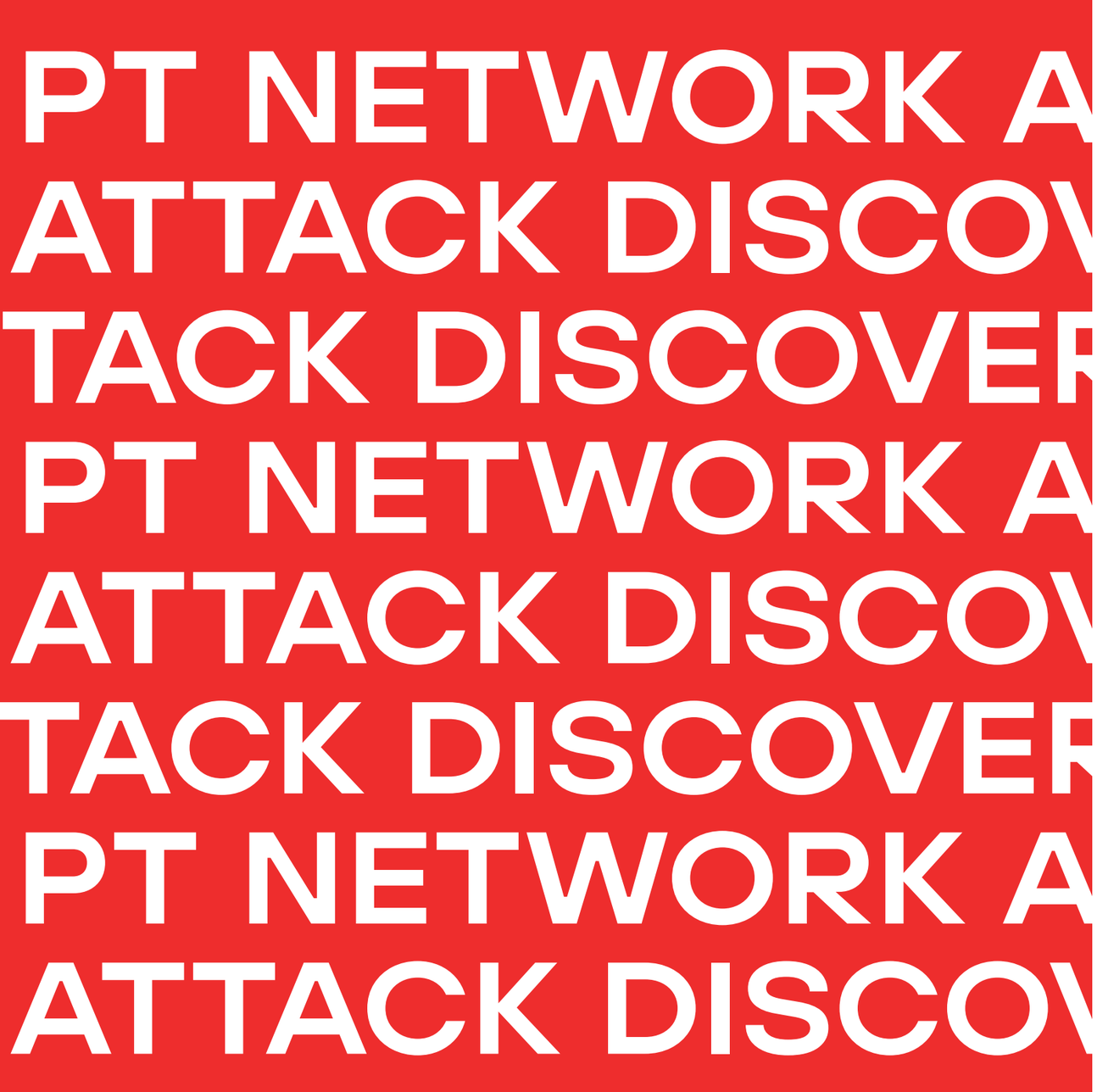
positive technologies

АНАЛИТИКА ПО ПИЛОТАМ PT NAD 2026



СОДЕРЖАНИЕ

РЕЗУЛЬТАТЫ АНАЛИЗА ПИЛОТНЫХ ПРОЕКТОВ

Мы изучили данные пилотных проектов PT NAD, проведенных во втором полугодии 2025 года и в первом полугодии 2026 года в компаниях России и СНГ. Несмотря на то что в ходе пилотных проектов не было зафиксировано признаков деятельности злоумышленников, анализ сетевого трафика позволил выявить многочисленные угрозы и потенциальные векторы компрометации. Мы определили те из них, которые встречаются чаще всего и напрямую влияют на уровень защищенности.

Рисунок 1. Компании — заказчики пилотных проектов

КАТЕГОРИИ ВЫЯВЛЕННЫХ ИНЦИДЕНТОВ

Все выявленные события и нарушения были разделены на три категории.

Рисунок 2. Категории выявленных инцидентов (доля компаний)

- Как и прежде, анализ отчетов по пилотным проектам подтверждает: сетевой периметр каждой компании подвергается постоянным попыткам эксплуатации уязвимостей и перебора паролей от доступных сервисов. О том, какие тенденции появились в области этих атак и какие технологии мы создаем для борьбы с ними на сетевом уровне, мы расскажем в конце аналитики.

- Потенциальные нарушения регламентов ИБ также встречались в каждой компании. Большую часть таких нарушений, как и в 2025 году, составляют передача паролей в незашифрованном виде и использование двух и более разных средств для удаленного управления. При этом в нашей статистике появились новые пункты.

- Согласно анализу, активность вредоносного ПО в этом году встречалась чаще (70%), чем в прошлом (46%), и в основном в эту категорию входят представители двух больших семейств ВПО — майнеры и резидентные прокси.

ПОТЕНЦИАЛЬНЫЕ НАРУШЕНИЯ РЕГЛАМЕНТОВ ИБ

Политика информационной безопасности компании — это свод правил, обеспечивающих комплексную защиту от ключевых киберугроз: несанкционированного доступа, утечки данных и внедрения вредоносного ПО. Эти правила регламентируют работу в сети, требования к паролям и действия в случае атаки. Нарушения из этого раздела называются потенциальными, потому что свод правил в каждой компании разный. Хотя в большинстве из них существуют требования к сложности паролей доменных учетных записей, сами правила немного различаются, расширяя или сужая рамки возможностей пользователей создавать слабые пароли.

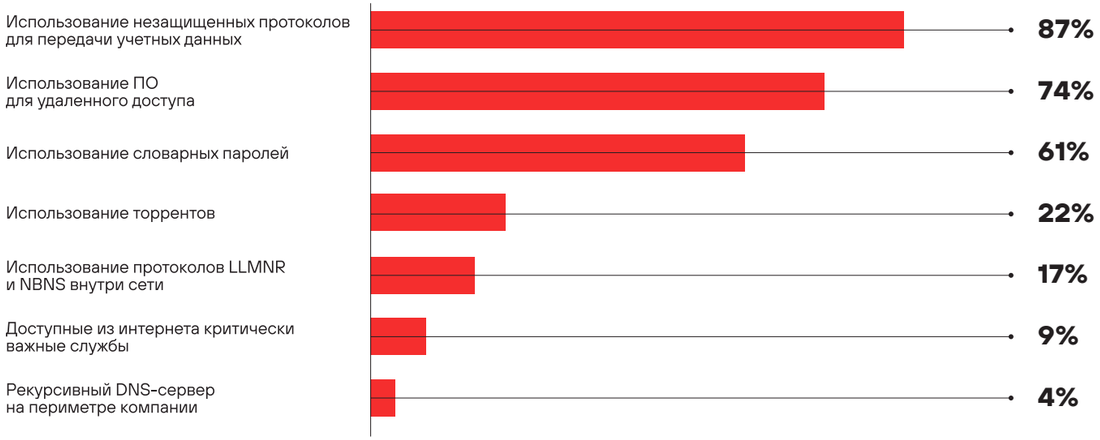


Рисунок 3. Нарушения регламентов ИБ (доля компаний)*

* Сумма долей может превышать 100%, если в одной компании одновременно присутствуют несколько указанных характеристик

Аутентификация по незащищенным протоколам — самое частое потенциальное нарушение регламентов. Сотрудники трех из четырех компаний аутентифицировались с корпоративными учетными данными без перехода на зашифрованный канал TLS или использования других механизмов защиты. И по сей день в большинстве компаний, где проводился пилот PT NAD, именно демонстрация паролей сотрудников в LDAP-трафике производила наибольшее впечатление: большинство российских компаний до внедрения средств классов NTA/NDR даже не догадывались о том, какой объем чувствительной информации передается в их сети в открытом виде. Передача аутентификационных данных в открытом виде по протоколу LDAP была обнаружена в 74% исследованных компаний, по протоколу HTTP — также в 74%

Несмотря на то что в большинстве случаев речь идет о тестовых или служебных системах, не хранящих данные компании или ее клиентов, на пилотных проектах встречались и веб-сервисы на сетевом периметре, в которых корпоративные пользователи аутентифицировались без перехода на защищенное соединение. А раз эти пароли в интерфейсе могут увидеть операторы PT NAD, то получить к ним доступ может и злоумышленник. К слову, разграничение ролей пользователей в PT NAD подразумевает и разграничение доступа операторов к данным учетных записей, которые извлек продукт. По нашему мнению, процент аутентификаций по протоколу HTTP без перехода на TLS в реальности еще выше и доходит до 100%. Однако во время пилотных проектов анализируется трафик лишь небольшого числа внутренних сетевых сегментов, поэтому мы видим далеко не все такие соединения.

С другой стороны, анализ содержимого незашифрованных сетевых сессий может принести массу полезных находок.

КЕЙС «SHADOW IT И АСУ ТП»

ВО ВРЕМЯ ПРОВЕДЕНИЯ ОДНОГО ИЗ ПИЛОТНЫХ ПРОЕКТОВ БЫЛО ЗАФИКСИРОВАНО, КАК ОДИН ИЗ ПРОМЫШЛЕННЫХ СТАНКОВ ИМПОРТНОГО ПРОИЗВОДСТВА РЕГУЛЯРНО ДЕЛАЛ СНИМКИ ЭКРАНА С ИНТЕРФЕЙСОМ ПРОГРАММЫ И КОММЕРЧЕСКИМИ СХЕМАМИ РЕЗКИ И ОТПРАВЛЯЛ ИХ НА СЕРВЕРЫ ПРОИЗВОДИТЕЛЯ. ТАКАЯ АКТИВНОСТЬ НЕ ТОЛЬКО ВЫЗОВЕТ ВОПРОСЫ У ОТДЕЛА ИБ, НО И УКАЖЕТ НА ПРОБЛЕМУ СЕТЕВОЙ СЕГМЕНТАЦИИ: УСТРОЙСТВА И СЕТИ АСУ ТП РЕКОМЕНДУЕТСЯ ВЫДЕЛЯТЬ В ОТДЕЛЬНЫЙ СЕТЕВОЙ СЕГМЕНТ С ВОЗДУШНЫМ ЗАЗОРОМ (AIR GAP).

Внизу списка расположились и другие протоколы — FTP, SMTP, POP3 и IMAP. Соединения по ним без перехода на шифрование устанавливались и вовне, с другими компаниями. Это говорит о том, что подобным проблемам подвержены и смежные организации большинства наших клиентов.

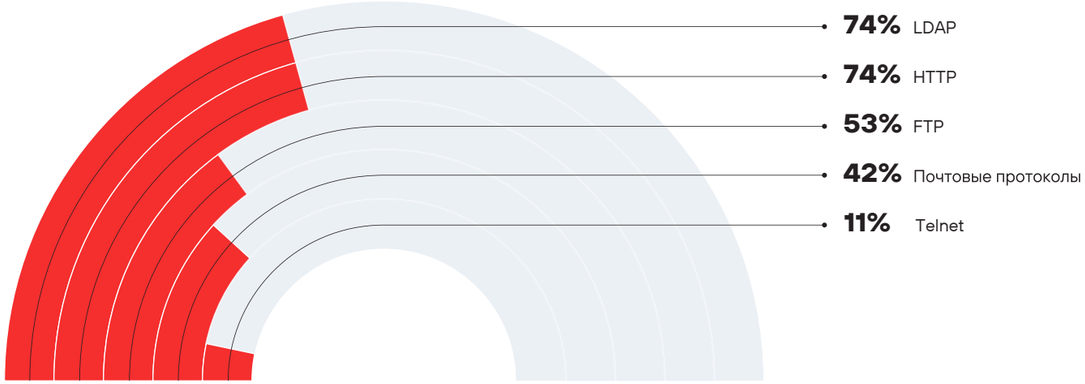


Рисунок 4. Незащищенные протоколы передачи данных (доля компаний)

Что касается средств удаленного управления, их использование стало нормой в российских организациях, и одним из наиболее популярных вариантов является AnyDesk: его мы обнаружили в 84% проанализированных компаний. Далеко не всегда его применение соответствует регламенту, ведь зачастую рекомендуется обращаться к отечественным решениям, например «Ассистенту» или RuDesktop — последний встречался в 82% российских компаний.

Статистика применения TeamViewer, напротив, пошла на спад — почти на треть. Если в прошлом году это средство для удаленного доступа применяли почти в 60% проанализированных компаний, то сейчас эта цифра составляет уже 42%. Возможно, виной тому стало ужесточение правил использования TeamViewer.

Важно понимать, что данные будут различаться для тех компаний, которые только проводят пилотный проект, и для тех, которые уже давно используют средства классов NTA/NDR.

> ПО НАШИМ НАБЛЮДЕНИЯМ, СРЕДНЯЯ СТАТИСТИКА ИСПОЛЬЗОВАНИЯ ANYDESK И TEAMVIEWER СРЕДИ ВСЕХ НАШИХ КЛИЕНТОВ СОСТАВЛЯЕТ 40% И 23% СООТВЕТСТВЕННО: ВСЕ ДЕЛО В ТОМ, ЧТО ПОСЛЕ ВНЕДРЕНИЯ РЕШЕНИЙ КЛАССОВ NTA/NDR СЛЕДИТЬ ЗА СОБЛЮДЕНИЕМ КОРПОРАТИВНЫХ ПОЛИТИК СТАНОВИТСЯ НАМНОГО ПРОЩЕ И ПРОЦЕНТ ИСПОЛЬЗОВАНИЯ ЗАПРЕЩЕННЫХ СРЕДСТВ СИЛЬНО ПАДАЕТ.

Это число будет еще ниже, если считать только регулярное использование этих средств удаленного управления, а не эпизодическое. Возможно, обе цифры портят сегменты Wi-Fi и VPN, к которым пользователи подключаются с личных устройств, не подчиняющихся корпоративным стандартам.

Заметно вырос процент использования средства RMS: главным образом за счет расширения покрытия этого инструмента правилами PT NAD. Несмотря на то что это средство удаленного управления было замечено в ряде атак APT-группировок и в связках с вредоносным ПО, пользователям оно нравится из-за возможности развернуть собственный сервер — аналогично RustDesk и GetScreen.

В итоговую статистику не попали другие средства удаленного управления, такие как GetScreen, LogMeIn, NoMachine, LiteManager и другие, чья доля использования среди исследованных компаний составляет менее 10%. Всего PT NAD способен обнаруживать более 35 различных средств и протоколов удаленного управления.

Кроме того, по сравнению с прошлым годом снизилось число инфраструктур, где используются протоколы локального разрешения имен LLMNR и NBNS: 17% против 54% в 2025 году. Такое значительное падение обусловлено тем, что теперь эти протоколы выключены в системах Windows по умолчанию, поскольку позволяют проводить poisoning-атаки в локальных сегментах.

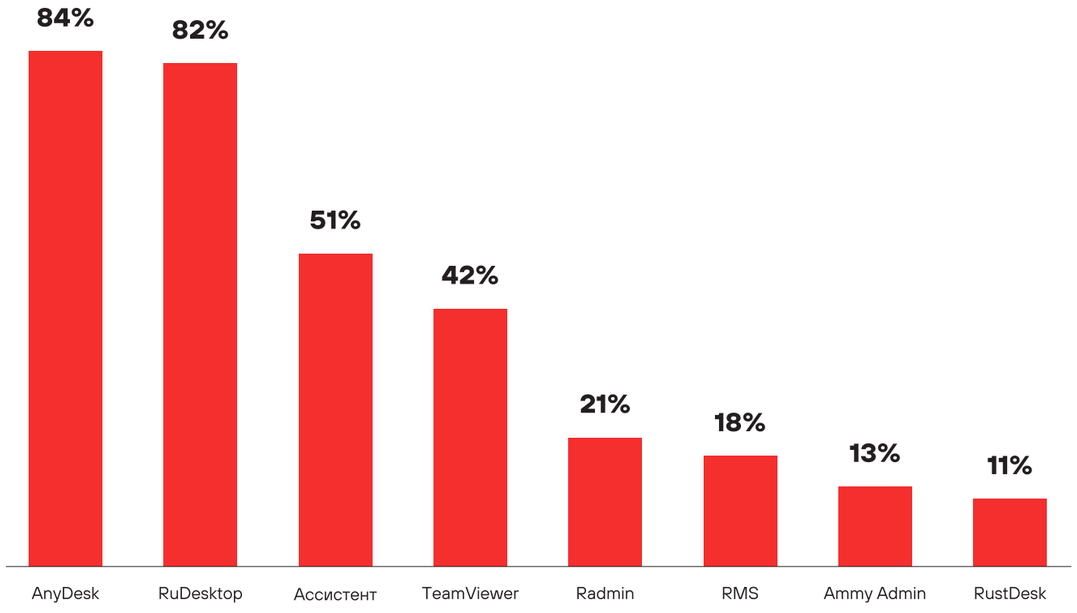


Рисунок 5. Выявленное ПО для удаленного доступа (доля компаний)

В аналитике по пилотам этого года появилось несколько новых пунктов. В первой половине 2026 года в PT NAD появились новые детекторы служб, доступных из интернета: речь идет о службе RDP, базах данных MySQL и Microsoft SQL Server и службе SMB, которые не рекомендуется «выставлять» в интернет. Процент компаний, у которых эти службы доступны на внешнем периметре, крайне мал, однако открытый для всех желающих доступ к ним из интернета может дорого обойтись. Среди служб, наиболее часто открытых на внешнем периметре, можно выделить RDP и Microsoft SQL Server. В одной компании был выявлен корпоративный сервис управления сертификатами Web Enrollment AD CS, доступный из интернета.

Кроме того, в 4% компаний локальные DNS-резолверы также были доступны из интернета и обрабатывали рекурсивные запросы для любых имен. Это ошибка конфигурации DNS-серверов: она может, например, сделать компанию участником DDoS-атаки или раскрыть злоумышленнику информацию о внутренних узлах. В пилотных отчетах следующего года мы ожидаем больше интересных нарушений, выявленных этим модулем.

АКТИВНОСТЬ И ТИПЫ ВРЕДОНОСНОГО ПО

Впервые о распространении такого вида вредоносных программ, как proxyware, или резидентные прокси, мы рассказали в прошлогодней аналитике. Резидентные прокси — это разновидность вредоносных программ, которые после заражения устройства не крадут пароли и не шифруют данные — вместо этого они пропускают через себя чужой сетевой трафик. Резидентными они называются потому, что заражают личные устройства обычных пользователей — телефоны и компьютеры, IP-адреса которых имеют чистую репутацию и высоко ценятся. Переданный через них трафик тарифицируется по гигабайтам и продается на специальных площадках. В 2025 году распространенность этого вида ВПО среди наших клиентов составила 46%, однако за последний год в арсенале PT ESC появились десятки детектов для новых разновидностей этих вредоносных программ, что увеличило процент обнаружений.

И несмотря на свою кажущуюся безобидность, они все равно считаются вредоносными: они попадают на устройства жертв скрытым образом и используют их ресурсы без ведома владельца — либо чистую репутацию IP-адреса, либо, в случае майнеров, вычислительные мощности CPU. Именно мнимая безобидность и привлекательность для авторов вредоносного ПО объясняют такой высокий процент распространения — 67% для proxyware и 54% для майнеров.

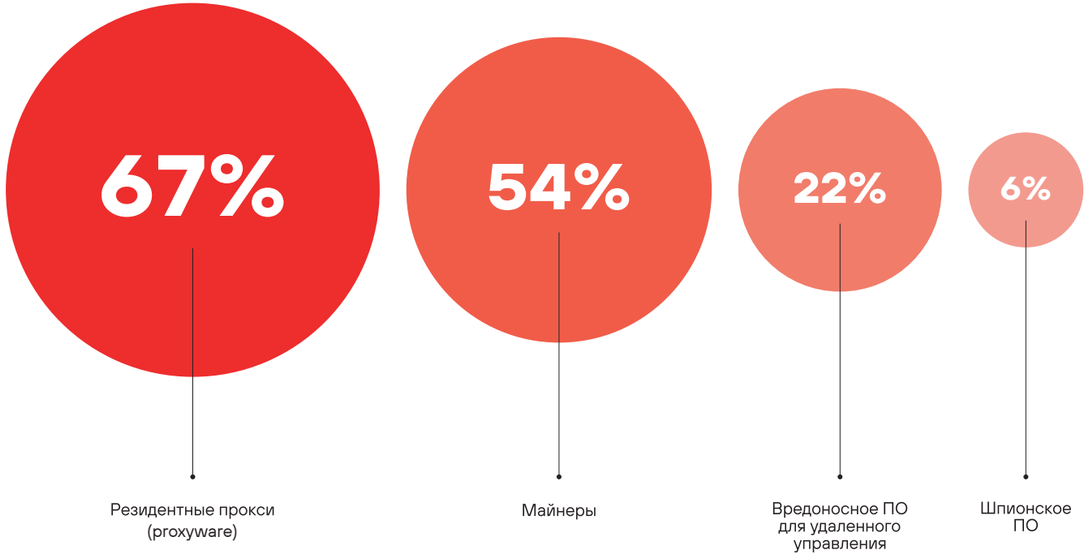


Рисунок 6. Категории выявленного вредоносного ПО (доля компаний)

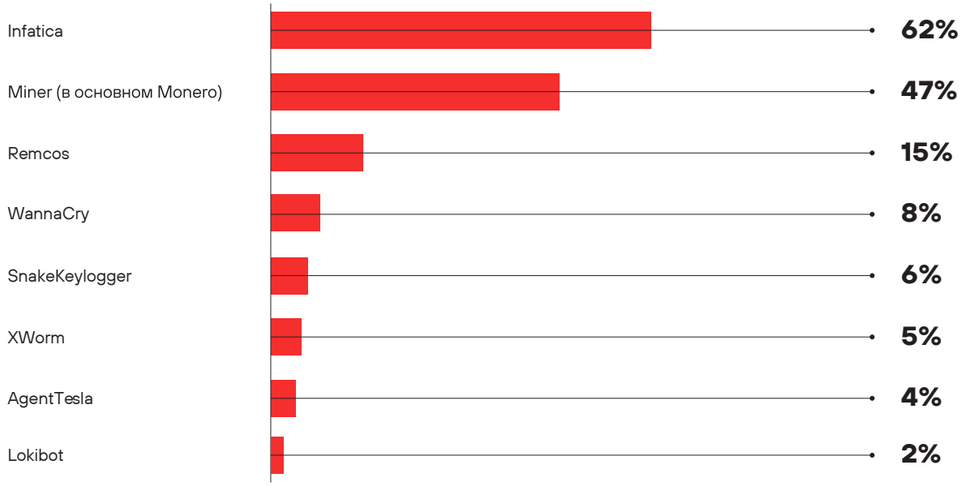


Рисунок 7. Семейства выявленного вредоносного ПО (доля компаний)

Если углубиться в детали, чаще всего встречаются майнеры криптовалюты Monero, добыча которой эффективно реализована на CPU. Самый распространенный сервис резидентных прокси — Infatica: мы встретили его в 62% исследованных компаний. Разумеется, не стоит расценивать эти цифры так, будто в 70% компаний существуют вредоносные программы: резидентные прокси часто заражают и мобильные устройства сотрудников, которые подключаются к корпоративному Wi-Fi, а криптомайнеры можно часто обнаружить на их личных ноутбуках, подключенных через корпоративный VPN.

Достаточно высокие места в нашей статистике заняли и по-настоящему опасные семейства — стилеры, средства скрытого удаленного управления и шифровальщики. Цифры выше лишний раз подчеркивают актуальность таких угроз — недооценивать их не стоит. Однако следует отметить, что значительная часть срабатываний сигнатур обусловлена запуском образцов в сетевой песочнице.

Указанные вредоносные программы преимущественно распространяются через почтовые вложения, а срабатывания на трафик песочниц редко подавляют правилами исключений в NTA- и NDR-системах.

В аналитике этого года мы не учитывали adware, но в большом числе компаний по-прежнему выявляется шифровальщик WannaCry. WannaCry — это дань памяти событиям 2017 года, когда весь мир стал жертвой глобальной кибер-пандемии[1]. В инфраструктурах российских компаний до сих пор попадаются отдельные узлы, зараженные этим червем, который уже не способен активно распространяться. К сожалению, без средств классов NTA/NDR заметить такие брошенные узлы крайне тяжело, поэтому процент компаний, которые уже долгое время используют такой класс решений и в которых остаются зараженные WannaCry узлы, стремится к нулю.

[1]

ПОПЫТКИ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ

Попытки эксплуатации уязвимостей — неотъемлемая часть интернета. Это своего рода норма: ботнеты пополняются именно за счет того, что уже зараженные боты постоянно сканируют случайные адреса. Именно этот факт подтолкнул экспертов PT NAD создать модуль для автоматической проверки успешности эксплуатации таких уязвимостей: он извлекает из сетевых запросов адреса вредоносных серверов и проверяет обращения к ним. И поскольку попыткам эксплуатации уязвимостей подвергается сетевой периметр буквально каждой организации, в этом году мы отошли от привычного формата статистики и теперь считаем популярность тех или иных уязвимостей в интернете относительно самой сканируемой уязвимости.

Поэтому верхние строки нашего перечня занимают те уязвимости, которые ботнеты сканируют по всему интернету. За точку отсчета мы выбрали уязвимость десятилетней давности — внедрение вредоносного кода в роутеры D-Link DIR-645 (CVE-2015-2051). Попытки ее эксплуатации были зафиксированы более чем с 30 тысячами разных IP-адресов, поэтому в топе самых сканируемых уязвимостей она будет составлять 100%. Важно понимать, что в наше исследование не попадают действия внутренних сканеров безопасности, поскольку мы анализировали только внешние попытки эксплуатации и ранжировали уязвимости относительно друг друга по количеству разных источников атак — на наш взгляд, это наиболее объективный показатель популярности.

Тренд этого раздела за минувший год не сильно изменился — топ по-прежнему возглавляют уязвимости в роутерах D-Link и GPON. Серьезно изменить рейтинг смогут только новые массовые уязвимости в IoT-устройствах, которые тяжело обновлять. Однако в этом году в топ-10 самых эксплуатируемых уязвимостей вошла новая RCE-уязвимость во фреймворке React — React2Shell. Она появилась на рубеже 2025 и 2026 годов и благодаря своей простоте и распространенности уязвимого ПО стала по-настоящему массовой.

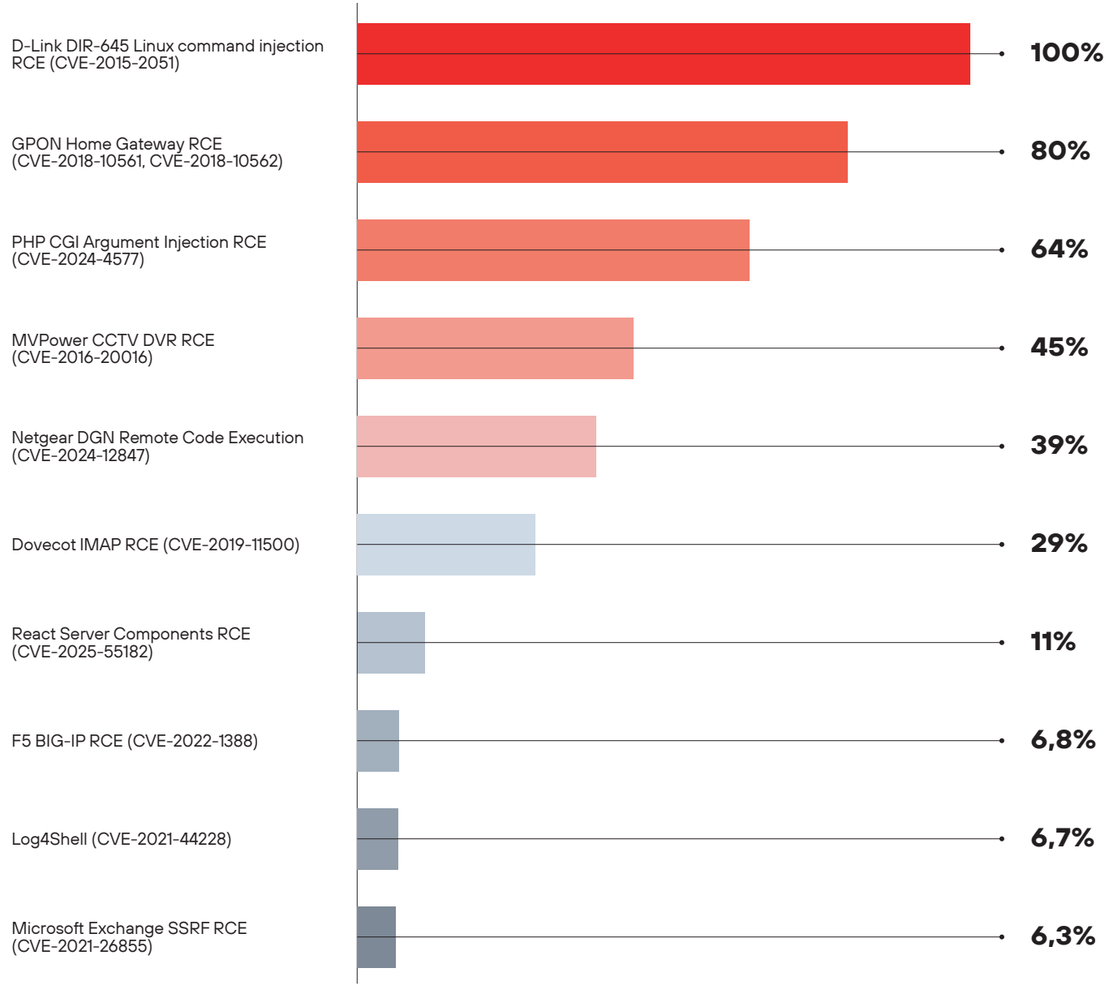


Рисунок 8. Популярность сканируемых уязвимостей в интернете (относительно наиболее популярной)

Идентификатор	Опасность по CVSS 3.1	Описание
Внедрение команд ОС D-Link DIR-645 Rev. Ax (CVE-2015-2051)	9,8 (критическая)	Маршрутизатор D-Link DIR-645 с прошивкой 1.04b12 и более ранними версиями позволяет злоумышленникам удаленно выполнять произвольные команды с помощью действия GetDeviceSettings в интерфейсе HNAP
Удаленное выполнение кода на Dasan GPON (CVE-2018-10561)	9,8 (критическая)	Уязвимость GPON-роутеров Dasan: добавление параметра ?images в URL позволяло обойти форму аутентификации админ-панели, то есть любой внешний пользователь мог попасть в веб-интерфейс и управлять устройством. На практике это означало получение полного контроля над роутерами
Внедрение аргументов PHP-CGI (CVE-2024-4577)	9,8 (критическая)	Уязвимость затрагивает PHP при работе в режиме CGI на платформах Windows. Проблема связана с функцией Best-Fit в Windows, которая некорректно обрабатывает символы в командной строке, позволяя злоумышленнику передавать аргументы двоичному файлу PHP, что в итоге может привести к получению полного контроля над системой или удаленному выполнению кода
Внедрение команд в MVPower CCTV DVR (CVE-2016-20016)	9,8 (критическая)	Уязвимость систем видеонаблюдения MVPower. В прошивке устройства был оставлен доступный без аутентификации веб-шелл по URI /shell. Атакующий отправлял HTTP-запрос по этому адресу с вредоносной командой в параметре, а веб-сервер JAWS выполнял ее на устройстве с правами root. На практике это позволяло без учетных данных получить полный контроль над устройством
Netgear DGN Remote Code Execution (CVE-2024-12847)	9,8 (критическая)	Уязвимость затрагивает маршрутизаторы NETGEAR DGN1000 с прошивкой ниже версии 1.1.00.48. Из-за отсутствия надлежащей проверки аутентификации злоумышленник удаленно мог отправить специально сформированный HTTP-запрос к обработчику setup.cgi и выполнить произвольные команды операционной системы с правами root. На практике это позволяло без учетных данных получить полный контроль над устройством
Dovecot IMAP RCE (CVE-2019-11500)	9,8 (критическая)	Уязвимость затрагивает Dovecot — популярный почтовый сервер. Проблема связана с некорректной обработкой нулевых байтов в строках, заключенных в кавычки, позволяя злоумышленнику удаленно отправить специально сформированный запрос, вызвать запись данных за пределами выделенной области памяти и в результате добиться выполнения произвольного кода на почтовом сервере без предварительной аутентификации
React Server Components RCE (CVE-2025-55182)	10,0 (критическая)	Уязвимость в React Server Components, связанная с небезопасной обработкой данных, отправляемых в React Server Functions. Злоумышленник мог отправить специально сформированный HTTP-запрос, который при десериализации позволял выполнить произвольный код на сервере
Удаленное выполнение кода в устройствах F5 BIG-IP (CVE-2022-1388)	9,8 (критическая)	Для эксплуатации злоумышленник сначала обходил аутентификацию в веб-интерфейсе, манипулируя HTTP-заголовками запроса. После обхода атакующий выполнял команды, обращаясь к REST API управления по URL /mgmt/tm/util/bash, где он мог передавать системные команды Linux.
Удаленное выполнение кода Log4j (CVE-2021-44228)	10,0 (критическая)	Уязвимость в Apache Log4j, популярной библиотеке журналирования для Java: позволяет выполнить произвольный код, отправив на журналирование специально сформированную строку
Microsoft Exchange SSRF RCE (CVE-2021-26855)	9,8 (критическая)	Уязвимость подделки серверных запросов в on-prem-версиях Microsoft Exchange, позволявшая неаутентифицированному злоумышленнику отправлять HTTP-запросы от имени почтового сервера. В составе цепочки ProxyLogon она применялась для обхода аутентификации и последующего удаленного выполнения команд на сервере

Таблица 1. Топ-10 наиболее часто эксплуатируемых уязвимостей на сетевом периметре

ВЫВОДЫ

По сравнению с пилотами в 2024–2025 годах картина недостатков ИБ и нарушений в 2025–2026 годах заметно изменилась

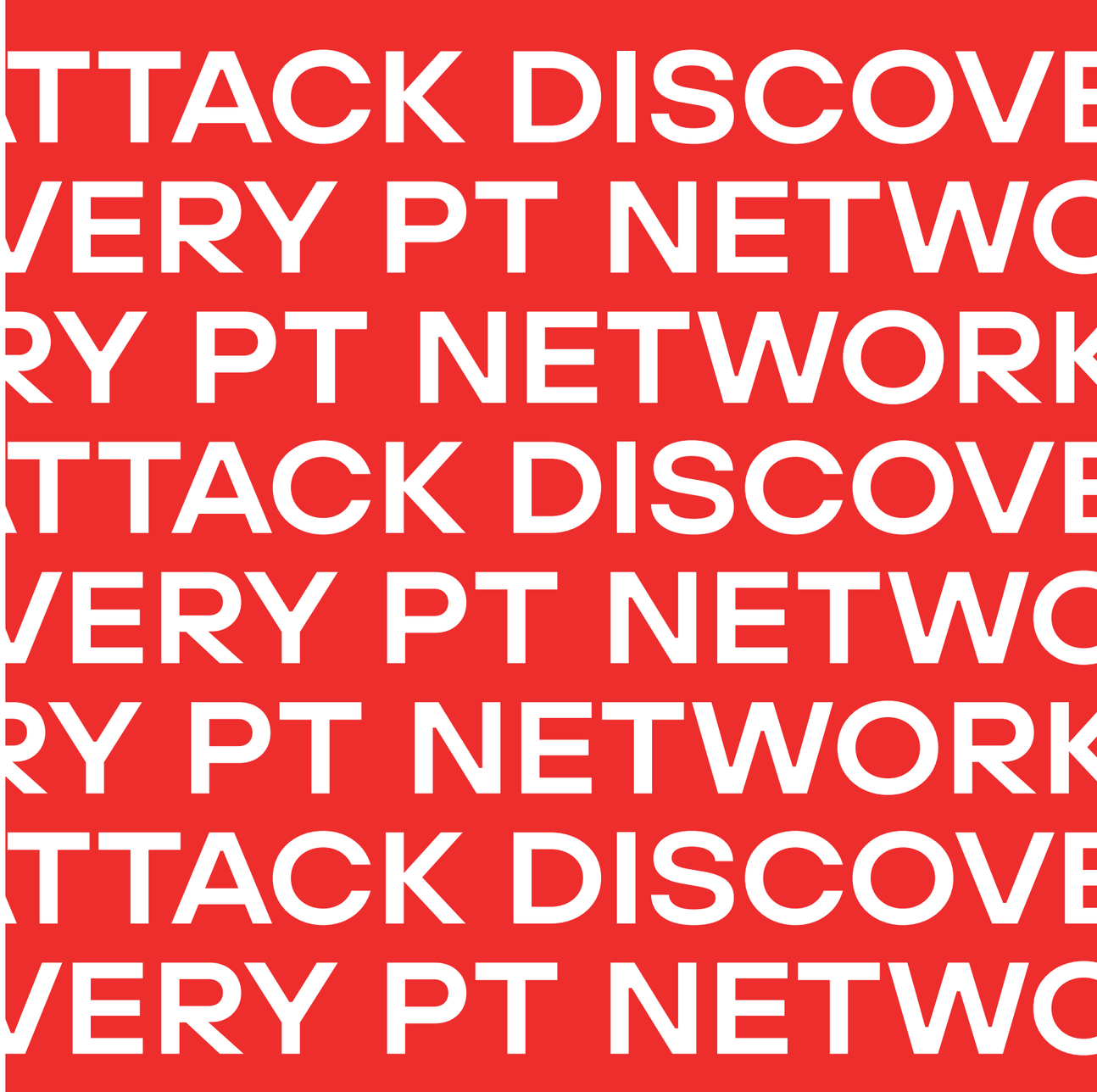
- Доля компаний, в которых выявлена активность вредоносного ПО, выросла с 46 до 70%. Основная причина роста — расширение покрытия правилами резидентных прокси (с 46 до 67%) и майнеров.
- Протоколы LLMNR и NBNS, которые в пилотах 2024–2025 годов были обнаружены в 54% инфраструктур, в пилотах 2025–2026 годов встречаются только в 17%. Это следствие того, что в новых версиях Windows эти протоколы по умолчанию выключены.
- Использование TeamViewer снизилось с 58 до 42%, а доля AnyDesk выросла с 69% в 2024–2025 годах до 84%. Изменения вызваны снижением популярности TeamViewer и улучшением покрытия AnyDesk.
- В топ-10 эксплуатируемых уязвимостей впервые вошла новая уязвимость RCE в React Server Components (CVE-2025-55182).
- Впервые в аналитике мы привели статистику небезопасных сетевых служб, доступных из интернета (RDP, SMB, баз данных).

ЧТО ЭТО ЗНАЧИТ ДЛЯ ПОЛЬЗОВАТЕЛЯ

Продукты классов NTA/NDR уже не стоит рассматривать исключительно как средства детектирования целевых атак. Одна из ключевых ценностей этого класса решений — непрерывный контроль соблюдения политик информационной безопасности и выявление shadow IT.

Аналитика пилотов PT NAD показывает, что после внедрения продукта доля несанкционированных средств удаленного доступа снижается.

При выборе и внедрении продукта для защиты сети важно не только обнаружение угроз, но и обеспечение сетевой видимости и контроль нарушений корпоративных политик.




pt