positive technologies

РЕЗУЛЬТАТЫ АНАЛИЗА ПИЛОТНЫХ ПРОЕКТОВ PT NETWORK ATTACK DISCOVERY (2024–2025 г.)

PT NETWORK A
ATTACK DISCO
TACK DISCOVER
PT NETWORK A
ATTACK DISCO
TACK DISCOVER
PT NETWORK A
ATTACK DISCO

СОДЕРЖАНИЕ

РЕЗУЛЬТАТЫ АНАЛИЗА ПИЛОТНЫХ ПРОЕКТОВ 4

КАТЕГОРИИ ВЫЯВЛЕННЫХ ИНЦИДЕНТОВ 5

Потенциальные нарушения регламентов ИБ 6

Активность и типы вредоносного ПО 9

Майнеры 10

Резидентные прокси (residential proxy) 11

Шпионское ПО и ВПО для удаленного доступа 11

Шифровальщик 12

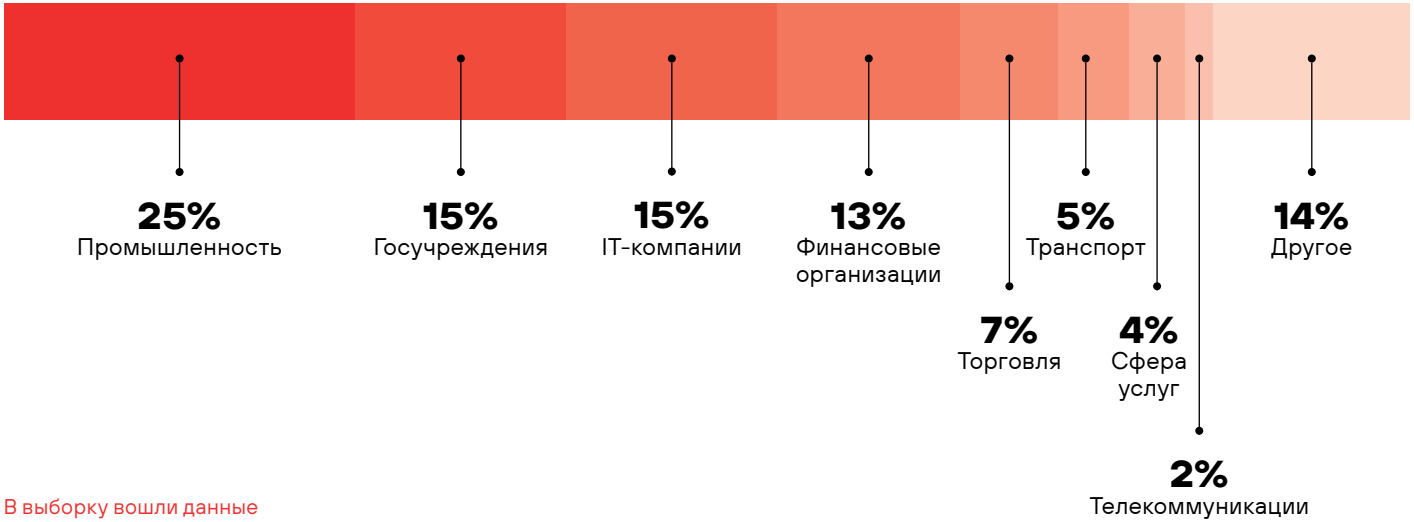
Попытки эксплуатации уязвимостей 13

ВЫВОДЫ 16

РЕКОМЕНДАЦИИ 17

РЕЗУЛЬТАТЫ АНАЛИЗА ПИЛОТНЫХ ПРОЕКТОВ

Мы изучили данные пилотных проектов PT NAD, проведенных за второе полугодие 2024 года и первое полугодие 2025 года в компаниях в России и СНГ, и определили угрозы ИБ, наиболее часто встречающиеся в корпоративных сетях.



В выборку вошли данные из проектов клиентов, которые дали свое согласие на анализ результатов мониторинга сетевой активности в их инфраструктуре. Все данные в исследовании обезличены

Рисунок 1. Компании — заказчики пилотных проектов

КАТЕГОРИИ ВЫЯВЛЕННЫХ ИНЦИДЕНТОВ

- Попытки эксплуатации уязвимостей на сетевом периметре были выявлены во всех компаниях.
- Потенциальные нарушения регламентов ИБ были обнаружены практически во всех компаниях, которые проводили пилотные проекты (96%); например, среди таких нарушений — использование незащищенных протоколов (HTTP, FTP, POP3, SMTP), программ для удаленного доступа.
- Активность вредоносного ПО была выявлена в 46% компаний. При анализе сетевого трафика чаще всего обнаруживалась активность майнеров, вредоносных программ типа residential proxy и вымогателя WannaCry.

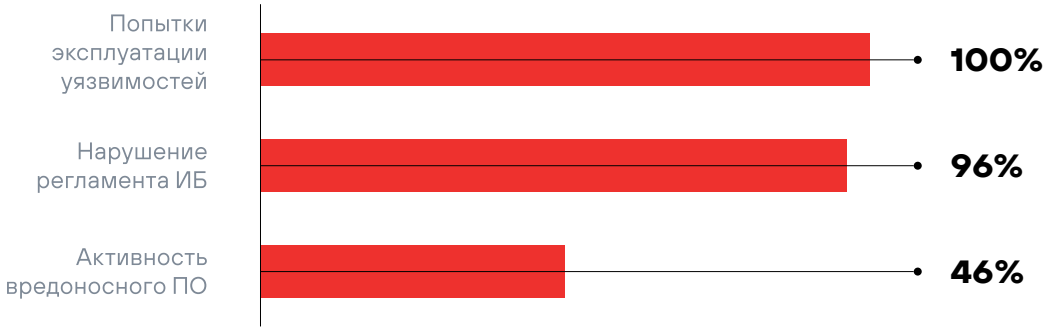


Рисунок 2. Категории выявленных инцидентов (доля компаний)

ПОТЕНЦИАЛЬНЫЕ НАРУШЕНИЯ РЕГЛАМЕНТОВ ИБ

Политика информационной безопасности — набор правил, обеспечивающих комплексную защиту от ключевых киберугроз: несанкционированного доступа, утечек данных и внедрения вредоносного ПО. Эти правила регламентируют работу в сети, требования к паролям и действия в случае атаки. Их соблюдение — гарантия стабильной работы компании, сохранности ее данных и инфраструктуры. Пренебрежение политикой ИБ повышает вариативность действий атакующих и повышает их шансы на реализацию недопустимых для бизнеса событий вследствие успешной кибератаки.

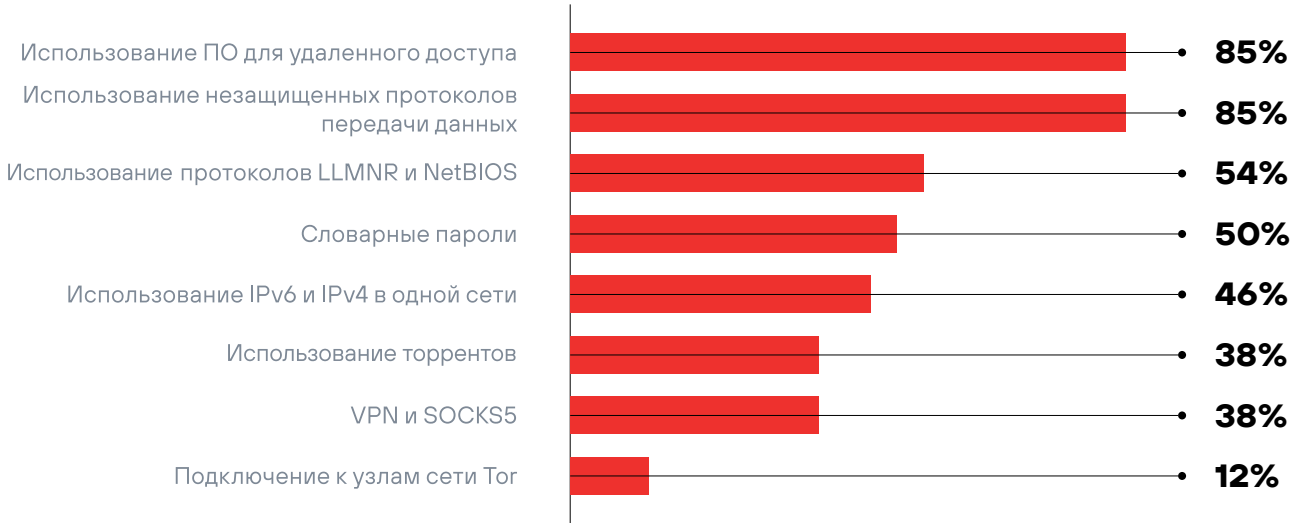


Рисунок 3. Нарушения регламентов ИБ (доля компаний)

Является ли та или иная активность нарушением внутренних политик ИБ — каждая организация решает самостоятельно

Например, почти в каждой организации разрешено лишь одно средство удаленного доступа (например, AnyDesk), а использование других является нарушением. Или использование слабых паролей, очевидно, является нарушением политики безопасности, однако требования к сложности доменных паролей каждая организация определяет сама. Именно поэтому перечисленные выше активности являются нарушениями лишь потенциально и требуют верификации клиентом.

В результате анализа отчетов пилотных проектов была выявлена частая сетевая активность ПО для удаленного доступа (AnyDesk, TeamViewer и др.) в корпоративных сетях (85% компаний). Несмотря на легитимные сценарии использования, неконтролируемое применение таких программ создает значительные риски, так как ПО для удаленного доступа — излюбленный инструмент злоумышленников для скрытого доступа к системам и данным.

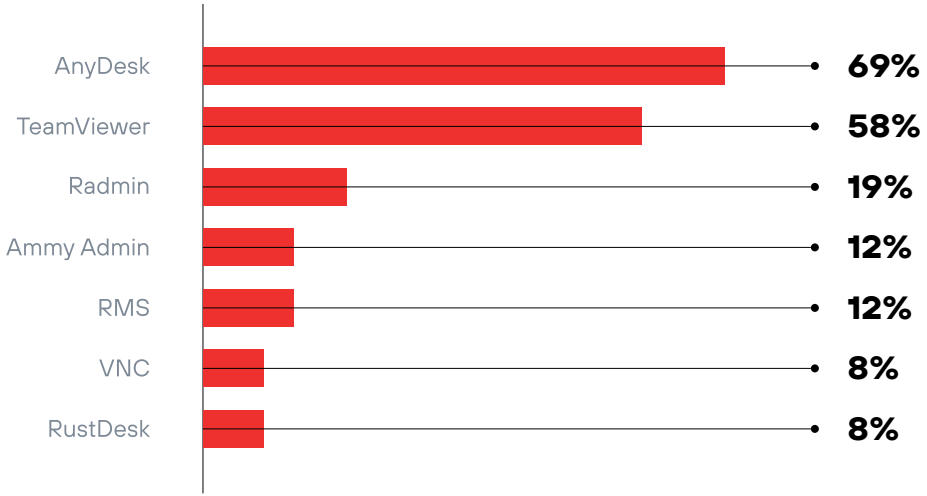


Рисунок 4. Выявленное ПО для удаленного доступа (доля компаний)

В каждой второй организации было выявлено использование словарных паролей, которое значительно облегчает задачу злоумышленников при реализации атак методом перебора: пароли легко подбираются с применением общедоступных словарей. Кроме того, слабые комбинации нередко используются при атаках типа «распыление пароля» (password spraying).

В 54% организаций зафиксировано использование протоколов LLMNR и NetBIOS, предназначенных для обнаружения сетевых ресурсов. Уязвимость такой конфигурации может быть использована злоумышленниками для перехвата значений Net-NTLMv2 challenge–response, передаваемых в сети, с последующим подбором учетных данных.

В 85% компаний был зафиксирован факт использования незащищенных протоколов передачи данных. Это создает серьезную угрозу: при получении доступа к сети злоумышленники могут перехватить и расшифровать передаваемую информацию. Содержание таких пакетов может варьироваться — от обычных данных до критически важных сведений (конфиденциальной информации, учетных записей пользователей). Последнее значительно облегчает развитие атаки и может привести к масштабным последствиям.

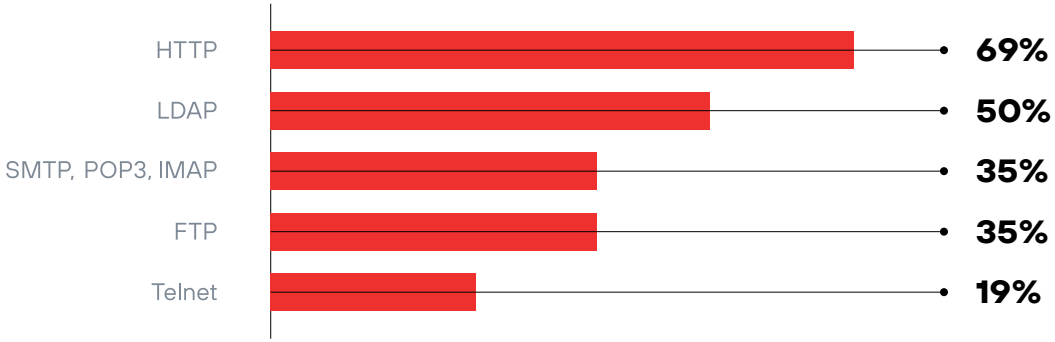


Рисунок 5. Незащищенные протоколы передачи данных (доля компаний)

В 69% компаний учетные данные для аутентификации передавались в открытом виде через небезопасный протокол HTTP, а в половине — через протокол LDAP. Оба протокола не обеспечивают шифрование передаваемой информации. LDAP активно используется в корпоративной среде, по нему часто передаются аутентификационные данные доменных пользователей. Перехват этих данных позволяет злоумышленнику получить несанкционированный доступ к ресурсам организации.

Не менее опасная угроза — использование протоколов SMTP, POP3 и IMAP (35%), применяемых для пересылки и получения электронной почты: в этих протоколах нет шифрования. В электронной переписке нередко содержится конфиденциальная информация, которая может быть раскрыта при прослушивании сетевого трафика.

АКТИВНОСТЬ И ТИПЫ ВРЕДОНОСНОГО ПО

В 46% компаний, которые проводили пилотные проекты PT NAD в 2024–2025 годах, была обнаружена активность вредоносного ПО. Чаще всего в сетевом трафике обнаруживались следы функционирования майнеров, вредоносных программ типа residential proxy, шпионского ПО, троянов удаленного доступа (RAT), а также известного вредоноса WannaCry.

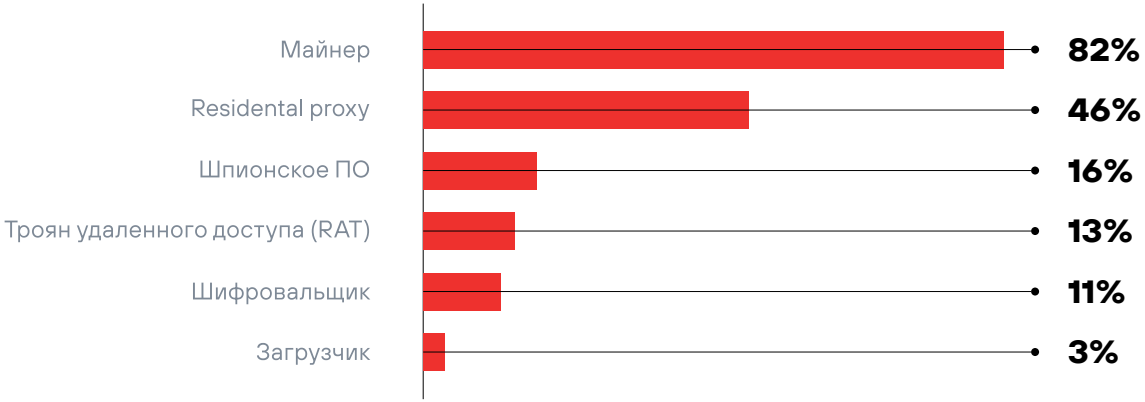


Рисунок 6. Вредоносное ПО, обнаруженное в ходе пилотных проектов (доля компаний)

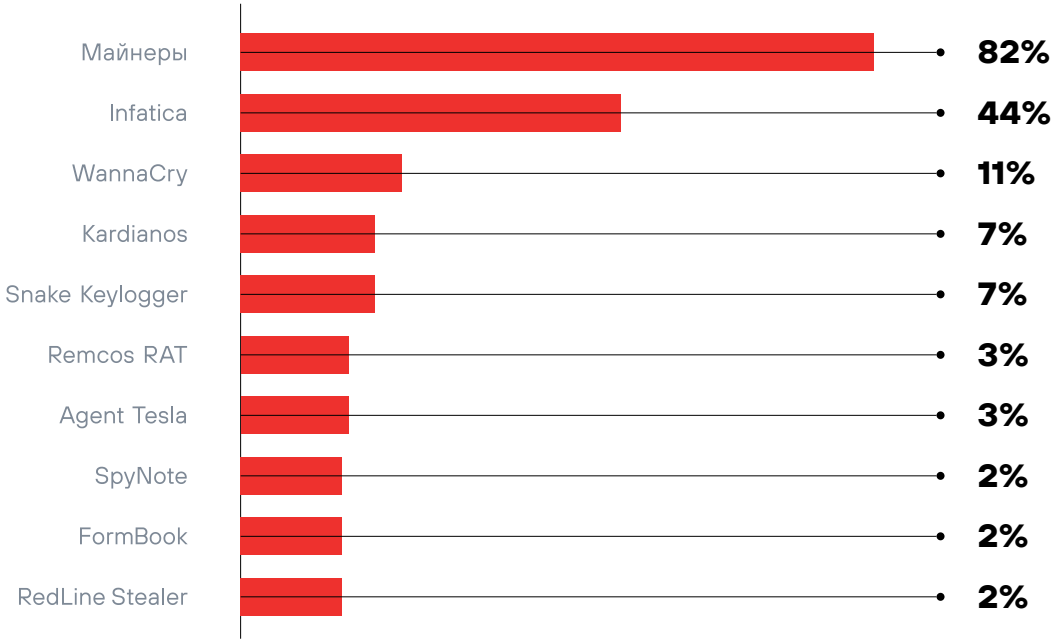


Рисунок 7. Топ-10 семейств ВПО, найденных на пилотных проектах (доля компаний)

Майнеры

Чаще всего в сетевом трафике организаций обнаруживались следы присутствия ПО для майнинга криптовалюты: в инфраструктуре 82% компаний были обнаружены индикаторы, сигнализирующие о наличии майнеров. Такие вредоносы работают скрытно, в них используются особые приемы для маскировки их деятельности и предотвращения обнаружения.

Майнеры попадают на устройства вместе с бесплатными программами, или через устройства других пользователей, уже зараженных майнерами, или в результате заражения в ходе массовой эксплуатации уязвимостей. Также в статистику могла попасть активность зараженных узлов из сегмента публичного Wi-Fi и активность личных устройств сотрудников компаний (BYOD, bring your own device).

Следы активности майнеров могут быть обнаружены в сетевом трафике практически любой организации.

Резидентные прокси (residential proxy)

Анализ показал, что в трафике 46% компаний есть следы активности вредоносных резидентных прокси. Такие программы не крадут данные и не дают прямого доступа злоумышленникам, а продают трафик зараженных устройств через сервисы-прокси. Пользователи этих сервисов маскируют свою активность под активность обычных домашних пользователей, что позволяет обходить системы защиты и затрудняет расследование.

Резидентные прокси интересуют как легитимные структуры (например, рекламные агентства), так и киберпреступников. Чаще всего фиксируется Infatica — proxyware, превращающее компьютер в узел сети прокси. Оно устанавливается вместе с бесплатными программами и незаметно запускает фоновую службу для перенаправления чужого трафика. Это приводит к росту нагрузки на устройство, снижению скорости интернета и может спровоцировать претензии к владельцу IP-адреса.

Шпионское ПО и ВПО для удаленного доступа

В 16% и 13% компаний были выявлены следы использования шпионского ПО и ВПО для удаленного доступа соответственно. RAT позволяют злоумышленникам красть, изменять или удалять информацию, а также использовать устройство как точку входа в сеть для дальнейшего развития атаки.

Одним из представителей троянов удаленного доступа к Windows-системам является Remcos RAT — вредоносное ПО, которое позволяет злоумышленникам полностью контролировать зараженный компьютер: вести запись экрана и звука, перехватывать нажатия клавиш, красть учетные данные и загружать дополнительную вредоносную нагрузку, при этом активно сопротивляясь обнаружению антивирусной защитой.

Изначально Remcos был разработан как легальный инструмент для удаленного администрирования систем Windows. Однако некоторое время спустя атакующие изучили функциональность инструмента и приспособились использовать его в злонамеренных целях.

Кроме того, в рамках исследования был выявлен троян удаленного доступа SpyNote, специально разработанный для Android-устройств. Вредонос проникает в систему под видом различных легитимных приложений и предоставляет злоумышленникам обширный набор возможностей для слежения и контроля:

- перехват SMS-сообщений, банковских кодов;
- запись аудио, фото- и видеосъемка;
- отслеживание геолокации;
- удаленное управление смартфоном;
- обход встроенных средств защиты.

Распространение вредоноса происходит преимущественно через SMS-фишинг (смишинг), когда пользователям рассылаются сообщения с вредоносными ссылками или файлами, маскирующимися под безобидные приложения; это особенно опасно для неопытных пользователей.

Важно отметить, что большинство троянов удаленного доступа имеют функции шпионского ПО — могут скрытно записывать экран пользователя, определять его местоположение и регистрировать ввод данных с клавиатуры, что представляет серьезную угрозу для безопасности информации и конфиденциальности пользователей.

В ходе исследования обнаружены следы Snake Keylogger, Agent Tesla, FormBook и RedLine — многофункционального вредоносного ПО для кражи данных, перехвата клавиш, скриншотов и сбора системной информации. Обычно они распространяются через фишинговые письма и вредоносные PDF; стоит отметить, что FormBook и RedLine распространяются также по модели malware as a service, что делает их доступными даже для малоопытных киберпреступников и объясняет их популярность.

Шифровальщик

В 11% компаний была выявлена активность шифровальщиков — программ для блокировки доступа пользователей к данным путем шифрования отдельных файлов или файловой системы в целом, — а именно активность достаточно старого вымогателя WannaCry.

Несмотря на то что эпидемия WannaCry произошла весной 2017 года и с момента выпуска исправлений прошло уже более восьми лет, у довольно большого числа организаций внутри все еще остались зараженные вредоносом узлы. Кроме того, часть срабатываний приходится на трафик с принесенных сотрудниками с собой личных устройств (BYOD).

ПОПЫТКИ ЭКСПЛУАТАЦИИ УЯЗВИМОСТЕЙ

Дополнительно мы изучили данные по выявленным попыткам эксплуатации уязвимостей в сетевом трафике. По результатам анализа мы составили список из десяти уязвимостей, которые чаще всего пытались эксплуатировать на периметре российских компаний и компаний в странах СНГ.

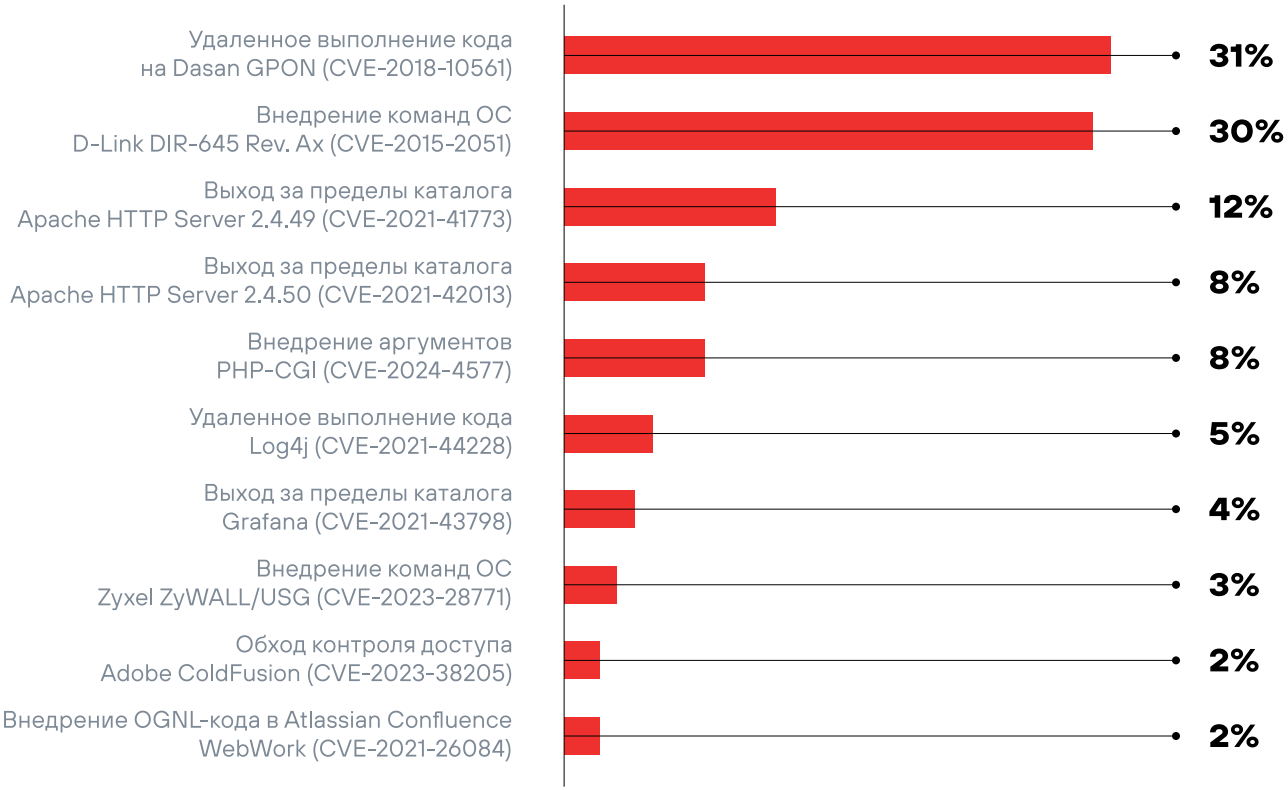


Рисунок 8. Топ-10 наиболее часто эксплуатируемых уязвимостей на сетевом периметре

Несмотря на то что обо всех вышеперечисленных уязвимостях известно несколько лет и они имеют способы устранения, атакующие продолжают активно эксплуатировать их. Наиболее показательные примеры — уязвимости роутеров Dasan GPON и D-Link DIR-645, о которых стало известно еще семь и десять лет назад соответственно, а попытки эксплуатации этих уязвимостей не прекращаются по сей день.

Это подчеркивает и еще одну проблему — широкое распространение устаревшего оборудования и ПО, в частности EOL-продуктов (end of life), когда вендоры не выпускают обновлений, в том числе обновлений безопасности. В результате миллионы устройств остаются подключенными к интернету, представляя собой при этом идеальные цели для автоматизированных атак, получения несанкционированного доступа и формирования ботнетов.

Идентификатор	Опасность по CVSS 3.1	Описание
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 удаленного контроля над роутерами
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 удаленным злоумышленникам выполнять произвольные команды с помощью действия GetDeviceSettings в интерфейсе HNAP
Выход за пределы каталога Apache HTTP Server 2.4.49 (CVE-2021-41773)	7,5 — Высокая	Уязвимость в Apache HTTP Web Server версии 2.4.49, которая существует из-за ошибки в том, как сервер Apache выполняет преобразование между разными схемами пути URL. Эта уязвимость позволяет получить доступ к файлам из областей вне корневого каталога сайта. При ее успешной эксплуатации появляется возможность загрузить произвольные системные файлы и исходные тексты веб-скриптов, доступные для чтения пользователю, под которым запущен HTTP-сервер
Выход за пределы каталога Apache HTTP Server 2.4.50 (CVE-2021-42013)	9,8 — Критическая	Уязвимость CVE-2021-42013 является прямым следствием неполноценного исправления CVE-2021-41773 в Apache HTTP Server 2.4.50. По своей сути это та же проблема обхода каталога, позволяющая получать несанкционированный доступ к файлам за пределами разрешенных каталогов и, при наличии CGI-скриптов, добиться удаленного выполнения кода

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

Идентификатор	Опасность по CVSS 3.1	Описание
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
Удаленное выполнение кода Log4j (CVE-2021-44228)	10,0 — Критическая	Уязвимость в Apache Log4j, популярной среде ведения журналов Java, связанная с выполнением произвольного кода путем отправки команды на журналирование определенной строки
Выход за пределы каталога Grafana (CVE-2021-43798)	7,5 — Высокая	Уязвимость обхода каталога, позволяющая неаутентифицированным злоумышленникам читать локальные файлы с сервера, используя пути, связанные с плагинами
Внедрение команд ОС Zyxel ZyWALL/USG (CVE-2023-28771)	9,8 — Критическая	Неправильная обработка сообщений об ошибках в устройствах Zyxel ZyWALL/USG позволяла неаутентифицированному атакующему выполнять команды на устройстве. Ранее уязвимость эксплуатировалась операторами ботнетов: файрвол мог быть использован для проведения DDoS-атак
Обход контроля доступа Adobe ColdFusion (CVE-2023-38205)	7,5 — Высокая	Уязвимость некорректного контроля доступа, которая позволяет обойти меры безопасности и получить доступ к административным интерфейсам CFM и CFC
Внедрение OGNL-кода в Atlassian Confluence WebWork (CVE-2021-26084)	9,8 — Критическая	Уязвимость в Atlassian Confluence, возникшая из-за использования языка Object-Graph Navigation Language (OGNL) в системе тегов. Позволяет произвести внедрение кода на OGNL и таким образом исполнить произвольный код на устройствах, где развернут Confluence Server или Confluence Data Center. Причем в некоторых случаях эксплуатировать ее может даже неаутентифицированный пользователь (если в Confluence включена опция Allow people to sign up to create their account)

ВЫВОДЫ

Средства защиты периметра, такие как IDS, IPS и NGFW, постоянно совершенствуются — но и злоумышленники продолжают развивать свои инструменты и методы атак. Хотя оператор SOC может своевременно обнаруживать и останавливать некоторые кибератаки, все чаще злоумышленники получают доступ к внутренней сети организации. В таких условиях периметровых средств защиты становится недостаточно, и возникает необходимость в дополнительном мониторинге и анализе сетевого трафика внутри IT-инфраструктуры. При правильно настроенном мониторинге внутреннего трафика злоумышленники не могут эффективно скрывать свои действия от специалистов по безопасности.

Системы поведенческого анализа трафика (NTA/NDR) позволяют получать полную картину сетевой активности и выявлять даже сложные угрозы: использование туннелей, перемещение внутри сети, активность вредоносного ПО. Внедрение глубокого анализа трафика обеспечивает организациям детальное понимание состояния сети, позволяет выявлять уязвимые места и оперативно реагировать на инциденты. Использование подобных решений сокращает время обнаружения и нейтрализации угроз, повышает эффективность работы службы ИБ и снижает общие затраты на обеспечение кибербезопасности.

РЕКОМЕНДАЦИИ

1. Для минимизации рисков мы рекомендуем отказаться **от средств удаленного доступа**. Если такой возможности нет, следует использовать только один такой инструмент; обеспечить использование только актуальных версий ПО с последними обновлениями безопасности; строго ограничить круг пользователей, имеющих право на удаленный доступ; использовать двухфакторную аутентификацию для входящих подключений, а также установить строгий контроль и мониторинг использования таких средств; вести журналы действий пользователей и оперативно реагировать на подозрительную активность.

2. Для снижения рисков атак, связанных **с использованием уязвимых протоколов передачи данных**, рекомендуется переходить на защищенные протоколы — HTTPS, SLDAP, Kerberos, SFTP, FTPS и SSH. Для почтовых клиентов и серверов необходимо обеспечить использование TLS. Пароли должны формироваться и контролироваться в соответствии с установленной политикой безопасности, включающей требования к их надежности. Следует полностью отказаться от использования словарных и стандартных паролей (паролей по умолчанию).

3. Для эффективной защиты организации необходимо наладить процесс управления уязвимостями (например, с использованием специализированных решений класса vulnerability management) и управления активами (asset management). Полное устранение всех недостатков сразу, как правило, невозможно, поэтому важно правильно расставлять приоритеты.

На приоритет при устранении уязвимостей влияют:

- значимость актива, на котором обнаружена уязвимость;
- доступность актива для потенциального злоумышленника;
- степень опасности уязвимости;
- популярность уязвимости среди атакующих;
- наличие готовых эксплойтов.

Кроме того, необходимо регулярно сканировать сеть и системы на наличие новых уязвимостей. Обнаруженные уязвимости следует оперативно устранять, применяя актуальные обновления и патчи, а также следить за сообщениями вендоров об этапах жизненного цикла используемых в инфраструктуре устройств.

4. Для защиты корпоративной инфраструктуры от вредоносного ПО необходимо применять комплекс организационных и технических мер.

   С организационной стороны ключевым является соблюдение сотрудниками базовых правил кибербезопасности: избегать перехода по подозрительным ссылкам, не скачивать и не открывать неизвестные вложения, использовать надежные пароли и включать двухфакторную аутентификацию. Дополнительно рекомендуется разработать и внедрить политику ИБ, включающую меры по предотвращению заражений, план реагирования на инциденты и процедуры восстановления IT-инфраструктуры.

   В части технических мер организациям следует внедрять специализированные решения для защиты от вредоносного кода, такие как песочницы. Подобные системы позволяют анализировать объекты как при ручной загрузке, так и автоматически — например, проверяя вложения электронной почты или файлы, передаваемые в сетевом трафике.

PT NETWORK A
ATTACK DISCO
TTACK DISCOVE
PT NETWORK A
ATTACK DISCO
TTACK DISCOVE
PT NETWORK A
ATTACK DISCO