



# Распространенные угрозы ИБ **в корпоративных сетях**

---

Результаты анализа сетевого трафика  
в различных компаниях в России и СНГ



[ptsecurity.com](http://ptsecurity.com)

## Содержание

Что такое network traffic analysis	3
Об исследовании	4
Что скрывает сеть	4
Подозрительная сетевая активность	5
Активность вредоносного ПО	7
Нарушения регламентов ИБ	9
Незащищенные протоколы внутри сети: опасно или нет	9
Средства удаленного доступа: удобство или риск	11
Торренты: блокировать или разрешать	12
Выводы	12
PT Network Attack Discovery	13

## Что такое network traffic analysis

В IT-инфраструктуре современной компании ежедневно генерируются большие объемы сетевого трафика. Отслеживать уязвимые места в сетевых взаимодействиях между устройствами по мере разрастания инфраструктуры и внедрения новых технологий становится сложнее. В свою очередь, киберпреступники владеют целым арсеналом техник для сокрытия своего присутствия в скомпрометированной инфраструктуре и маскировки генерируемого вредоносного трафика под легитимный. Информации о сетевых адресах, портах и протоколах, по которым устанавливаются соединения, уже недостаточно для своевременного выявления угроз и реагирования на них. Необходим глубокий анализ трафика — с разбором протоколов до уровня приложений (L7). С этой задачей успешно справляются решения класса network traffic analysis (NTA).

В NTA-системах применяются алгоритмы машинного обучения, поведенческий анализ, правила детектирования, а также есть возможность ретроспективного анализа. Это позволяет выявлять подозрительную сетевую активность, активность вредоносного ПО, попытки эксплуатации уязвимостей как на периметре, так и внутри сети, нарушения регламентов ИБ и другие угрозы. Аналитическое агентство Gartner отмечает, что ряд организаций используют NTA-решения в составе центров мониторинга и реагирования на угрозы информационной безопасности (security operations centers, SOC) наряду с решениями для защиты конечных пользователей и SIEM-системами.

## Об исследовании

В 2018 году компания Positive Technologies выпустила новое решение класса NTA — PT Network Attack Discovery (PT NAD). В этом отчете мы представляем результаты мониторинга сетевой активности в инфраструктуре 36 компаний, где проводились пилотные проекты по внедрению PT NAD и комплекса для раннего выявления сложных угроз (PT Anti-APT), в состав которого входит PT NAD. Средний срок пилотного проекта — месяц. В выборку вошли проекты за 2019 год, выполненные в крупных компаниях из ключевых отраслей экономики (штат более 1000 человек) в России и СНГ. В выборке представлены только те проекты, заказчики которых дали согласие на исследование результатов мониторинга сетевой активности и их публикацию в обезличенном виде.

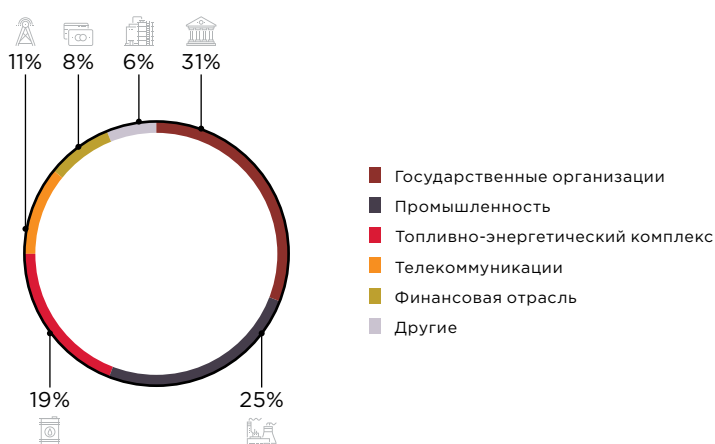


Рисунок 1. Портрет участников

## Что скрывает сеть

Для наглядности мы разделили все выявленные в корпоративной сети угрозы по категориям. В инфраструктуре 97% компаний обнаружена подозрительная сетевая активность. В 94% организаций глубокий анализ сетевого трафика выявил нарушения регламентов ИБ, а в 81% компаний — активность вредоносного ПО. Рассмотрим подробнее наиболее распространенные угрозы из этих категорий и постараемся разобраться, в чем их опасность.

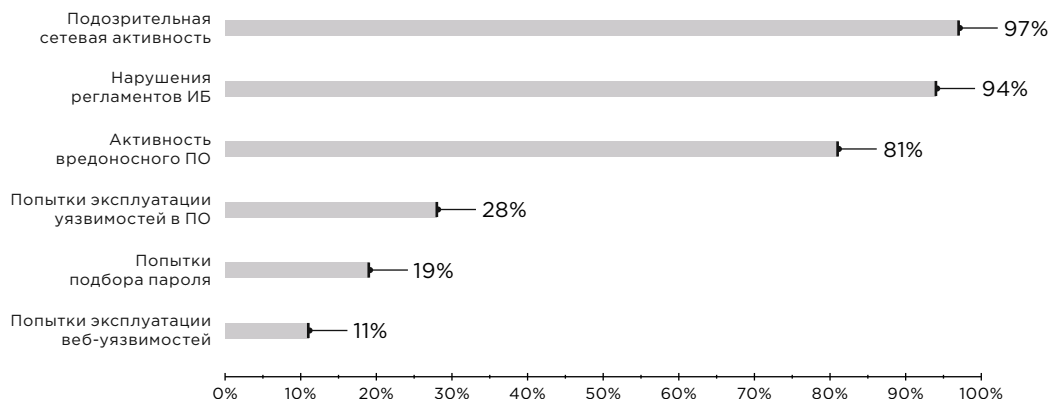


Рисунок 2. Категории выявленных угроз (доли компаний)



## Подозрительная сетевая активность

Какой трафик считать подозрительным? Например, VPN-туннели, проксирование запросов и подключения к анонимной сети Tor. Они были выявлены в 64% компаний.

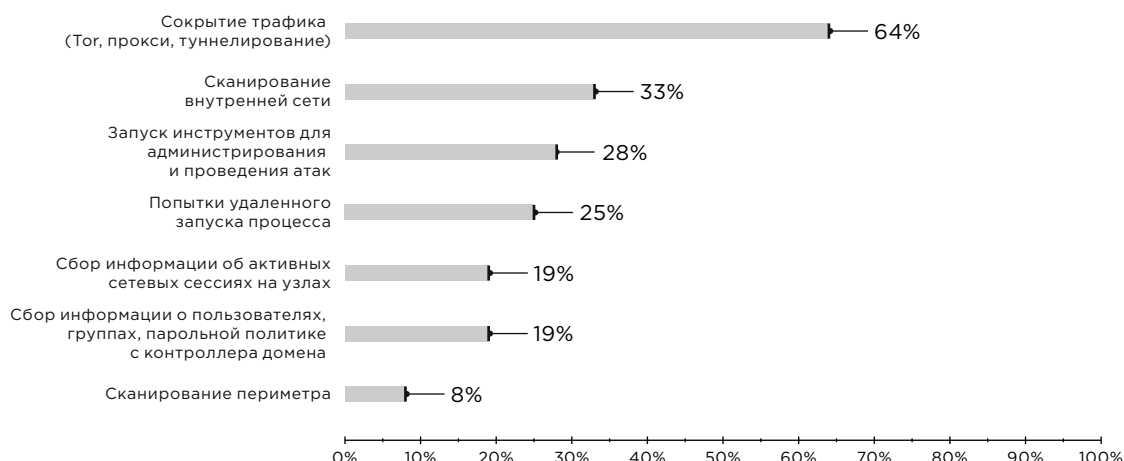


Рисунок 3. Подозрительная сетевая активность (доли компаний)



### Чем опасны Tor, VPN и прокси

В то время как сотрудники подключаются к анонимной сети Tor, поднимают прокси-серверы и настраивают VPN для обхода блокировки веб-ресурсов, злоумышленники могут использовать те же технологии для связи с управляющими серверами (C2-серверами). Например, бэкдор ZxShell группировки АРТ41 умеет устанавливать прокси-соединения по протоколам SOCKS и HTTP. Кроме того, профессиональные взломщики шифруют трафик, которым вредоносное ПО обменивается с C2-серверами. Решения класса NTA умеют выявлять аномалии в зашифрованном трафике.

К подозрительной сетевой активности мы относим также действия, свидетельствующие о разведке и перемещениях потенциального злоумышленника внутри сети. Например, в эту категорию вошли сканирования сети, множественные неуспешные попытки подключения к узлам, следы сбора информации об активных сетевых сессиях на конкретном узле или во всем домене.

**В 22%**  
компаний выявлено  
использование PsExec

В 28% компаний выявлена активность ряда утилит и инструментов, которая может свидетельствовать о компрометации. Почему мы говорим «может» и как проверить эту гипотезу? Сегодня наблюдается тенденция к атакам типа living off the land. При таких атаках для удаленного выполнения команд на узлах используются встроенные в ОС механизмы и доверенные программы. В Windows-инфраструктуре это могут быть PowerShell, WMI, утилиты из набора Sysinternals. Например, утилита PsExec хорошо зарекомендовала себя как среди IT-администраторов, так и среди злоумышленников.

Отличить в режиме реального времени действия злоумышленников, выполняемые посредством легитимных инструментов, от действий системных администраторов сложно. Ни одно средство защиты не сделает этого со стопроцентной достоверностью, поэтому злоумышленники, используя легитимные инструменты, могут долго оставаться незамеченными.

Один из способов выявления атак класса living off the land — хранение и анализ сетевого трафика. В нем содержится информация о тех действиях, которые на первый взгляд не вызывают подозрений. Он играет важную роль в ретроспективном анализе — при расследовании инцидентов, когда специалисту необходимо построить timeline событий в сети и раскрыть цепочку атаки. Это, как правило, остается за рамками пилотного проекта, поэтому в случае выявления подозрительной сетевой активности мы говорим лишь о *возможной* компрометации. Но бывают и исключения. В одной из компаний, где во время «пилота» были обнаружены следы присутствия APT-группировки, анализ сетевого трафика выявил следы использования злоумышленниками легитимных инструментов из состава Sysinternals — PsExec и ProcDump. Своевременное выявление злонамеренной активности позволило заблокировать действия злоумышленников.

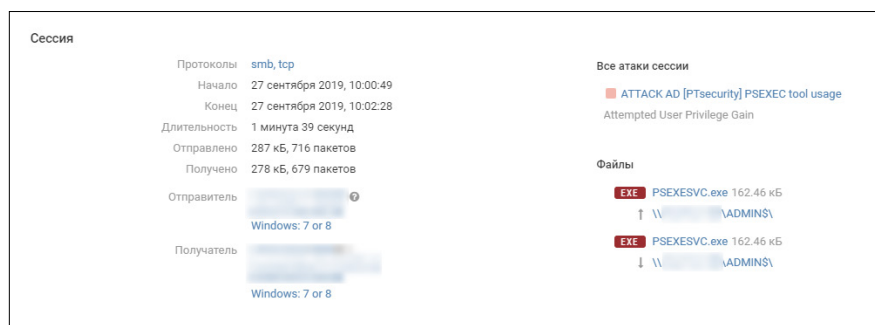


Рисунок 4. Удаленное выполнение команд с помощью утилиты PsExec

## Активность вредоносного ПО

По некоторым аномалиям в трафике можно с большой уверенностью судить о фактах заражения вредоносным ПО. Рассмотрим их подробнее. В 39% компаний мы выявили попытки подключения серверов и рабочих компьютеров к засинкхолонным доменам.



### Что такое засинкхолонный домен (sinkholed domain)

Это доменное имя, которое было замечено во вредоносных кампаниях. Обращения по таким адресам перенаправляются на специальные sinkhole-серверы, препятствуя связи вредоносного ПО с C2-серверами. Попытки подключения к засинкхолонным доменам — верный признак заражения вредоносным ПО.

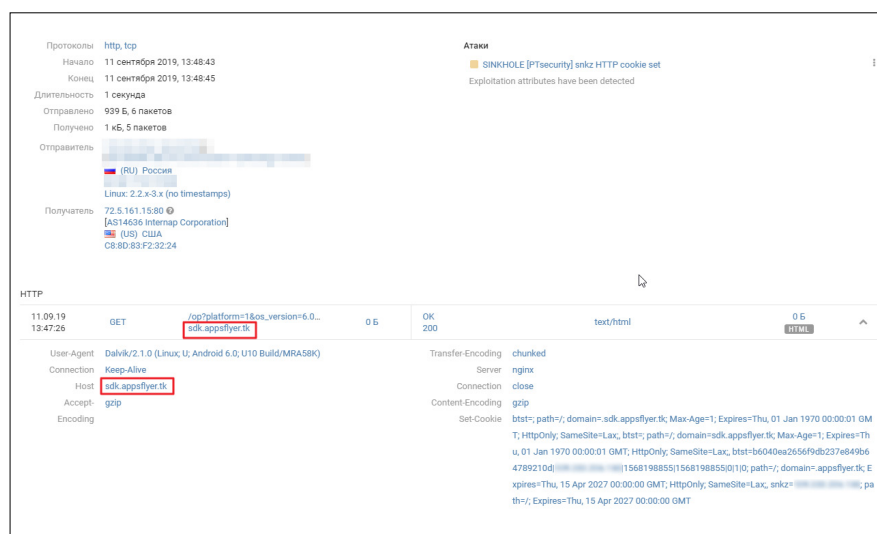


Рисунок 5. Попытки разрешения засинкхолонного доменного имени

Запросы на засинкхолонные домены могут быть показателем угрозы разной степени риска — от ботов для рассылки спама до сложной целенаправленной атаки. Так, во время одного из пилотных проектов мы обнаружили в корпоративной сети заказчика попытки подключения сразу к трем засинкхолонным доменам, два из которых были замечены в APT-атаках группы Sofacy (APT28).

Существуют репутационные списки — базы данных адресов, замеченных во вредоносных кампаниях. Эти базы данных регулярно обновляются и импортируются в средства защиты для блокирования вредоносной активности. Но злоумышленники научились обходить системы защиты, которые полагаются на репутационные списки. Продвинутые зловерды сегодня генерируют доменные имена C2-серверов динамически при помощи специальных алгоритмов ([domain generation algorithms](#), DGA). В нескольких компаниях в ходе пилотных проектов нам удалось выявить запросы на автоматически сгенерированные адреса. О методе, который мы используем для выявления таких запросов, мы [подробно рассказывали ранее](#).



Рисунок 6. Примеры DGA-доменов

Множественные попытки подключения к внешним серверам по порту 445/TCP (SMB) — еще один пример подозрительной сетевой активности, свидетельствующий о заражении вредоносным ПО. Это индикатор шифровальщика WannaCry или схожего с ним по методу распространения зловеда. Есть и другие индикаторы — например, запросы на так называемые адреса killswitch, относящиеся к кампании WannaCry. Но чаще других зловердов в инфраструктуре встречаются майнеры и рекламное ПО — они обнаружены в 55% и 28% зараженных компаний соответственно. В 47% организаций выявлено вредоносное ПО нескольких типов.

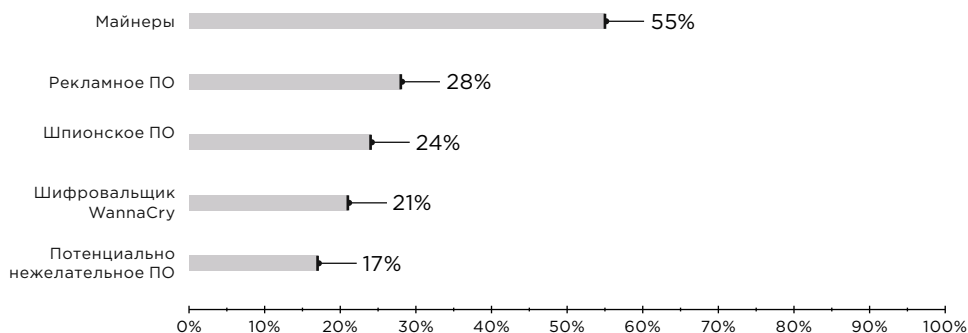


Рисунок 7. Топ-5 вредоносного ПО (доли зараженных компаний)

Ошибочно полагать, что майнеры грозят только большими счетами за электроэнергию, а рекламное ПО — навязчивыми всплывающими окнами. Если вас заразили любым видом вредоносного ПО, необходимо выявить источник угрозы как можно раньше. Инфицирование могло произойти из-за брешей в инфраструктуре, через которые взломщик может причинить более значительный ущерб, чем кажется на первый взгляд. Например, в одной из компаний на периметре был обнаружен узел с открытым портом 445/TCP (SMB) и множественные попытки эксплуатации уязвимости MS17-010 на этом узле.



## Нарушения регламентов ИБ

Политики безопасности многих организаций запрещают сотрудникам посещать сомнительные ресурсы, скачивать торренты, устанавливать мессенджеры, использовать утилиты для удаленного доступа. Эти меры призваны поддерживать безопасность на приемлемом уровне, однако сотрудники могут ими пренебрегать. Причин, по которым это происходит, множество, мы не будем заострять на них внимание. Достаточно отметить, что нарушения регламентов информационной безопасности наблюдаются в 94% компаний, и это повод рассказать, чем грозит несоблюдение сетевой гигиены.

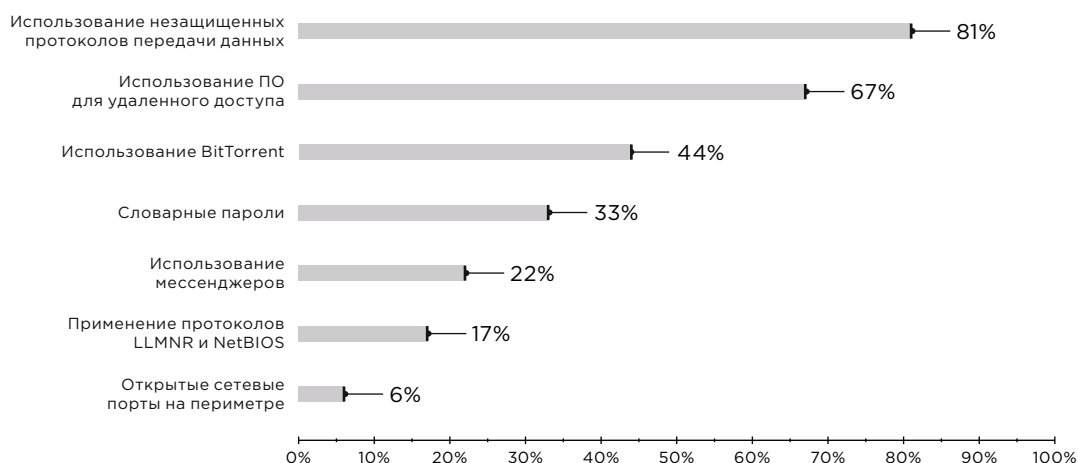


Рисунок 8. Топ-7 нарушений регламентов ИБ (доли компаний)

### Незащищенные протоколы внутри сети: опасно или нет

В инфраструктуре 81% компаний чувствительные данные передаются в открытом виде. А значит, кто угодно в корпоративной сети, в том числе потенциальный злоумышленник, может перехватывать трафик и искать в нем чувствительную информацию, например логины и пароли. Наряду с открытыми протоколами нередко выявляется и другая проблема — словарные пароли.

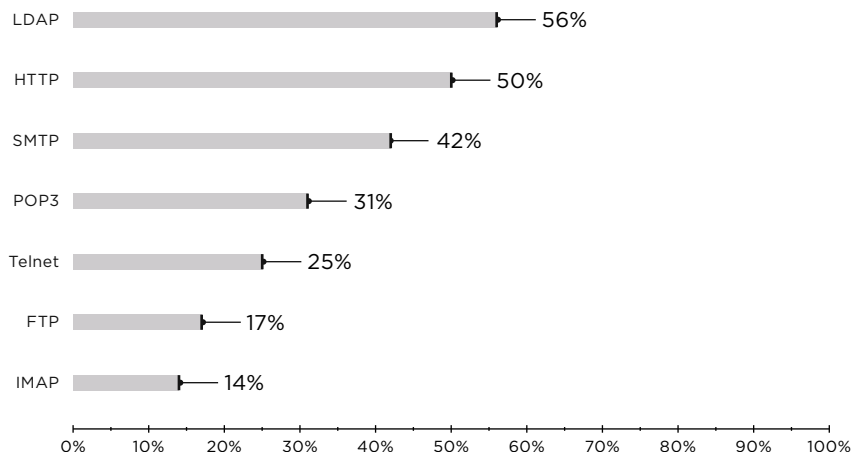


Рисунок 9. Использование незащищенных протоколов передачи данных (доли компаний)

В 56% компаний выявлена передача учетных данных по протоколу LDAP без шифрования. По этому протоколу работают службы каталогов. Администраторы используют их для централизованного администрирования и управления доступом к сетевым ресурсам. Если в открытом LDAP-трафике злоумышленнику удастся перехватить доменные учетные записи, он сможет использовать их для дальнейшего перемещения по сети.

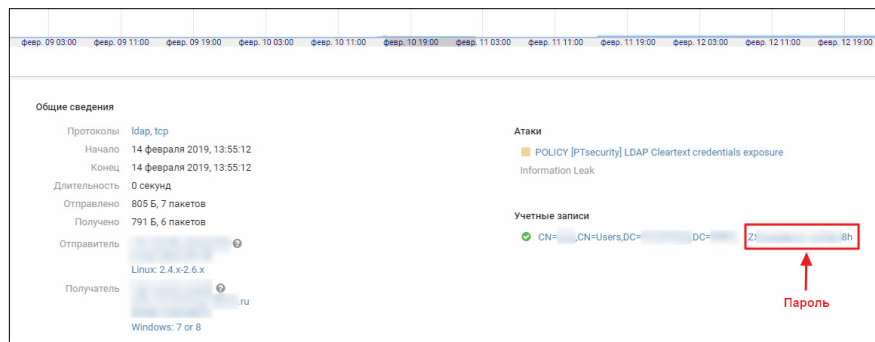


Рисунок 10. Передача учетных данных в открытом виде по LDAP

В каждой второй компании используют незащищенный протокол HTTP для доступа к веб-интерфейсам внутренних сервисов. Например, в двух компаниях логины и пароли для доступа к системе мониторинга Zabbix передавались в открытом виде в теле запроса. Какие угрозы подстерегают при таком варианте аутентификации? Во-первых, компрометация учетных данных может привести к утечке информации о моделях и версиях используемого в инфраструктуре ПО и оборудования, что облегчит хакеру разведку внутри сети. Во-вторых, перехватив учетную запись администратора Zabbix, злоумышленник сможет выполнять команды ОС на сервере и использовать этот сервер для дальнейших атак.

Еще один пример небезопасной передачи данных по HTTP — это аутентификация по схеме Basic. При Basic-аутентификации учетные данные передаются в заголовке запроса в кодировке Base64. Перехватив пакеты с запросами на аутентификацию, злоумышленник найдет в них нужный заголовок и декодирует из него пароль. Угроза актуальная для 33% компаний.

Отдельно остановимся на угрозе при передаче незашифрованного почтового трафика. В 42% компаний не настроен переход на защищенные соединения (TLS) при отправке электронной почты. Если злоумышленник получит доступ к внешнему сетевому трафику компании, он сможет читать письма, которые сотрудники отправляют через интернет. Доступ к внешнему трафику компании есть у интернет-провайдера. Он, в свою очередь, сам может стать жертвой кибератаки, или незашифрованная переписка может попасть в руки злоумышленников с оборудования провайдера по вине инсайдеров.

## Рекомендации

Используйте защищенные протоколы: HTTPS, SLDAP, Kerberos, SFTP, FTPS, SSH. Настройте почтовые клиенты и серверы на использование TLS. Исключите словарные пароли и пароли по умолчанию. Пересмотрите парольную политику — убедитесь, что ее правила отвечают требованиям к стойкости, контролируйте их выполнение.



в **58%**

компаний  
используется  
TeamViewer

## Средства удаленного доступа: удобство или риск

Еще одну угрозу создают средства для удаленного доступа. В 67% компаний используются RAdmin, TeamViewer, Ammyu Admin и другие аналогичные инструменты. Это удобно, например, для сотрудников, которые работают из дома. В чем заключается риск? Домашний компьютер сотрудника может быть взломан, и тогда злоумышленник сможет подключаться к корпоративной сети через настроенную программу для удаленного доступа.

Еще один сценарий использования подобных программ — удаленный доступ для подрядчиков IT-услуг. Мы советуем избегать этого. Сегодня 14% APT-группировок, атакующих российские компании, пользуются доверительными отношениями (*trusted relationship*) своих жертв с компаниями-партнерами, контрагентами или подрядчиками. Помните, что необычно длительные соединения и подключения в нерабочее время могут быть признаками компрометации.

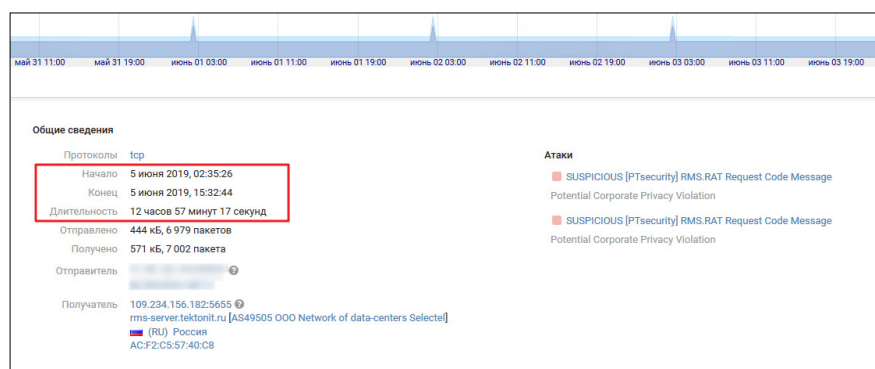


Рисунок 11. Подозрительное подключение с использованием программы RMS

По большому счету неважно, для каких целей в компании используются средства удаленного администрирования. Важно, что если злоумышленник проникнет в инфраструктуру, он сможет использовать их для перемещения по сети, оставаясь незамеченным для средств защиты, ведь его действия будут выполняться от имени доверенного лица и по санкционированному каналу связи.



## Рекомендации

Если отказаться от средств удаленного доступа не представляется возможным, ограничьтесь использованием только одного такого средства. Разграничьте права локальных пользователей и настройте политику белых списков ПО с помощью AppLocker.

## Торренты: блокировать или разрешать

Как показывают результаты наших пилотных проектов, в 44% компаний сотрудники используют пиринговые сети для передачи данных, например скачивают торренты. Это создает дополнительную нагрузку на канал связи и снижает его пропускную способность. Но есть и другой риск. Под видом различного ПО, фильмов и других файлов на торрент-трекерах скрывается множество вредоносных: можно стать жертвой массовой атаки шифровальщика, а можно наткнуться и на вредоносное ПО APT-групп. Например, через торренты распространяется шифровальщик [STOP](#), а группировка APT37 под видом загрузчика видео с YouTube размещала на торрент-ресурсах бэкдор [KARAE](#).



### Рекомендации

Установите в организации запрет на ПО, использующее протокол BitTorrent для передачи данных. Введите политику белых списков с помощью AppLocker.

## Выводы

Обеспечение кибербезопасности не должно ограничиваться периметром и традиционными средствами защиты. Как показали результаты нашего исследования, 92% угроз выявляются тогда, когда враг уже внутри.

Кибергруппировки преодолевают защиту на периметре интересующих их организаций, и об этом [свидетельствует](#) тенденция к росту доли успешных целевых атак. Это повод сместить фокус внимания с предотвращения атак на периметре на своевременное выявление компрометации и реагирование внутри сети. Однако выявить тщательно спланированную, порой разнесенную во времени кибератаку сложно. Злоумышленников больше не останавливают антивирусы: они регулярно модифицируют исходные коды вредоносного ПО, применяют бестелесные техники, эксплуатируют уязвимости нулевого дня. Динамический анализ тоже не панацея: злоумышленники [научились выявлять](#) технологии виртуализации, которые обычно применяют в песочницах. В конце концов, нельзя исключать, что злоумышленник сможет обойтись внутри сети вообще без вредоносного ПО, ограничиваясь теми инструментами, использование которых разрешено политиками безопасности.

Тем не менее действия взломщиков оставляют следы в сетевом трафике, а значит, задача специалиста по кибербезопасности — обнаружить эти следы. Результаты наших пилотных проектов показали, что решения класса NTA позволяют эффективно выявлять угрозы разной степени риска — от нарушений регламентов ИБ до сложных целенаправленных атак.

# PT Network Attack Discovery

PT Network Attack Discovery (PT NAD) — система глубокого анализа сетевого трафика (network traffic analysis, NTA) для выявления атак на периметре и внутри сети.

## Основные преимущества PT NAD



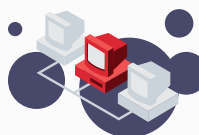
### 01

**Повышает прозрачность взаимодействий внутри сети.** PT NAD определяет более 50 протоколов и разбирает до уровня L7 модели OSI наиболее распространенные из них. Это позволяет получить полную картину активности в инфраструктуре и выявить проблемы ИБ, которые снижают эффективность системы защиты и способствуют развитию атак.



### 02

**Выявляет угрозы на периметре и внутри.** PT NAD использует репутационные сервисы, правила обнаружения, машинное обучение и ретроспективный анализ. Набор правил и репутационные списки PT NAD ежедневно пополняются экспертизой команды PT Expert Security Center. Специалисты PT ESC непосредственно участвуют в разборе актуальных методов и средств проведения кибератак, анализируют вредоносное ПО и расследуют инциденты ИБ в крупнейших компаниях из различных отраслей.



### 03

**Помогает выявлять сложные целенаправленные атаки.** PT NAD использует эвристические методы, поведенческий анализ, умеет выявлять аномалии в зашифрованном трафике. Как только база знаний получает обновление, можно выполнить повторный анализ трафика. Это помогает обнаружить новые виды угроз в инфраструктуре, которые не были обнаружены ранее.



### 04

**Эффективен в расследованиях.** PT NAD хранит записи трафика и 1200 параметров сетевых взаимодействий. Поэтому оператор системы может быстро узнать, что предшествовало подозрительному событию ИБ, с кем взаимодействовал скомпрометированный узел и как началась атака.

PT NAD соответствует требованиям регулирующих организаций по защите критической информационной инфраструктуры (приказы ФСТЭК № 239 и 235), персональных данных (приказ ФСТЭК № 21), а также информации в ГИС, в АСУ ТП и в информационных системах общего пользования (приказы ФСТЭК № 19, 31 и 489).

## О компании

[ptsecurity.com](http://ptsecurity.com)  
[pt@ptsecurity.com](mailto:pt@ptsecurity.com)  
[facebook.com/PositiveTechnologies](https://facebook.com/PositiveTechnologies)  
[facebook.com/PHDays](https://facebook.com/PHDays)

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.