



PT



Топ угроз ИБ в корпоративных сетях

Результаты мониторинга
сетевого трафика в 2020 году

ptsecurity.com

Об исследовании

Чем дольше злоумышленникам удастся скрываться от службы безопасности компании, тем глубже они могут проникнуть в инфраструктуру, украсть больше данных и стать богаче. Атакующим успешно удастся скрыть от антивирусного ПО применение своих инструментов, но спрятать активность в сетевом трафике уже гораздо сложнее, потому что для этого им придется вносить изменения в протоколы передачи данных. Для анализа трафика используются решения класса систем анализа трафика ([network traffic analysis, NTA](#)).



ЭТО ВТОРОЕ ПОДОБНОЕ ИССЛЕДОВАНИЕ

Результаты пилотных внедрений PT NAD за 2019 год смотрите на сайте [Positive Technologies](#).

Что мы сделали?

Мы проанализировали результаты мониторинга сетевой активности в 41 компании, где проводились пилотные проекты по внедрению

01 | **PT Network Attack Discovery** – система анализа трафика

02 | **PT Anti-APT** – комплекс для раннего выявления сложных угроз, состоящего из

- + PT NAD
- + [PT Sandbox](#)¹ (песочница)

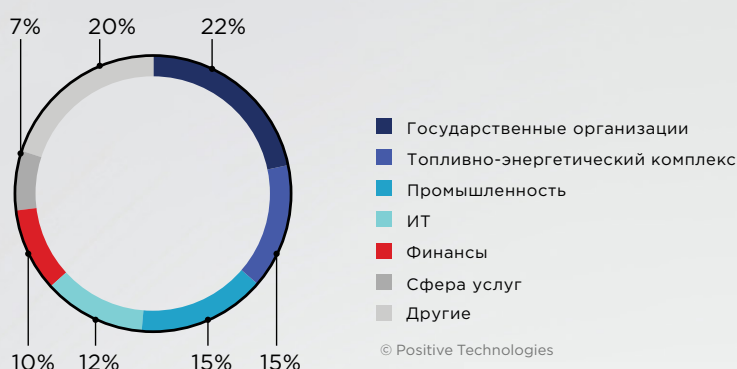


Рисунок 1. Портрет участников исследования

¹ В выборке представлены только те проекты, заказчики которых дали согласие на анализ результатов мониторинга сетевой активности и публикацию в обезличенном виде.

Категории угроз ИБ



PT NAD позволяет **выявлять** угрозы как во внутренних сетях, так и на периметре

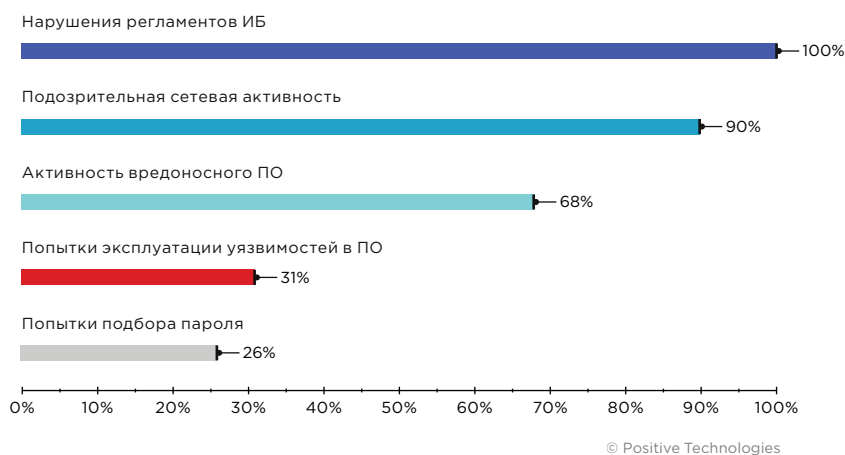


Рисунок 2. Категории выявленных угроз (доли компаний)

В 100% компаний были обнаружены угрозы в инфраструктуре

01 | **Нарушения регламентов ИБ** выявлены абсолютно в каждой организации (100%). Среди них — использование ПО для удаленного доступа и использование незащищенных протоколов.

В 24% компаний — на периметре сети

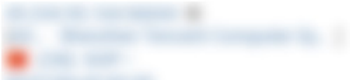

02 | **Подозрительная сетевая активность**, как и в прошлом году, была выявлена в большинстве компаний (90%). К ней относятся сокрытие трафика, запуск инструментов сканирования сети, попытки удаленного запуска процессов.

03 | **Активность вредоносного ПО** — еще одна популярная угроза. Она выявлена в 68% организаций.

04 | **Попытки эксплуатации уязвимостей** в ПО были замечены в каждой третьей компании. Это и попытки атак внутри сети, так и успешные атаки для систем, расположенных на периметре. Больше половины случаев связано с уязвимостью CVE-2017-0144 в реализации протокола SMBv1. Она эксплуатировалась известным шифровальщиком WannaCry, и была устранена еще в 2017 году. Однако злоумышленники продолжают ее активно использовать, выискивая в сети компьютеры, на которых за 3,5 года так и не было установлено обновление. В 2019 году попытки эксплуатации уязвимости CVE-2017-0144 встречались также часто и были выявлены в каждой пятой компании.

05 | **Попытки подбора паролей** (26%) также обнаружены с помощью систем анализа трафика. Так, например, в одной компании злоумышленники пытались подобрать пароль к системе управления базой данных, веб-интерфейс которой был доступен через интернет. В случае успеха атакующие смогли бы получить доступ к базе данных веб-сайта, в том числе к учетным данным пользователей.

Общие сведения

Протоколы [http, tcp](#)
 Начало 11 декабря 2020, 02:21:11
 Конец 11 декабря 2020, 02:23:46
 Длительность 2 минуты 34 секунды
 Отправлено 106 КБ, 982 пакета
 Получено 2 МБ, 1 515 пакетов
 Отправитель 
 Получатель 

Атаки

■ LOGIN [PTsecurity] PHPMYADMIN Login Bruteforce (60 attempts in 10 mins) ⋮
 Exploitation Attributes was Detected

Файлы

TXT index.php 65 Б ⋮
 ↑ /phpmyadmin/

HTML index.php 15.24 КБ ⋮
 ↓ /phpmyadmin/

TXT index.php 68 Б ⋮
 ↑ /phpmyadmin/

[Еще 35 файлов](#) ▾

Учетные записи

!	root	123
!	root	1234
!	root	12345
!	root	123456
!	root	1234567
!	root	12345678
!	root	123456789
!	root	1234567890
!	root	321root
!	root	football
!	root	mysql
!	root	mysql1
!	root	mysql123
!	root	mysql123456
!	root	mysql123456789
!	root	mysql2
!	root	mysqlmysql
!	root	password

Рисунок 3. Подбор аутентификационных данных

Рассмотрим подробнее самые распространенные категории угроз: **нарушения регламентов ИБ, подозрительная сетевая активность, активность вредоносного ПО.**

01 | Регламенты ИБ нарушены в 100% компаний

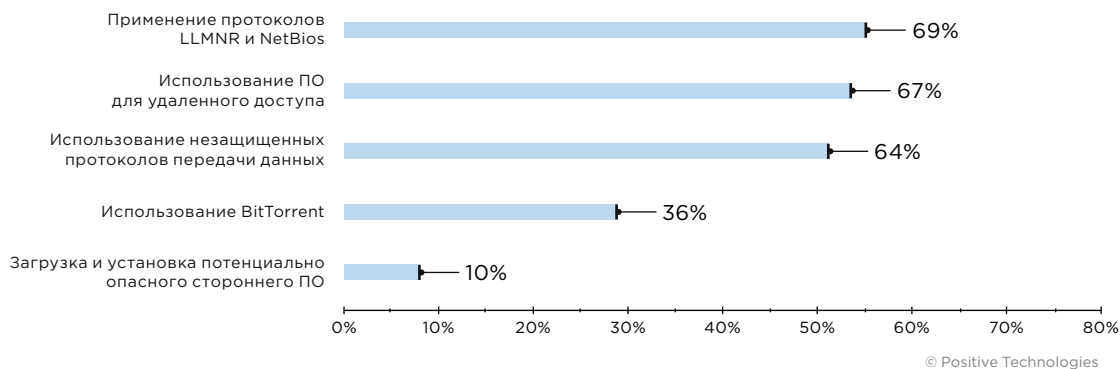


Рисунок 4. Топ-5 нарушений регламентов ИБ (доли компаний)

Одно из наиболее часто выявляемых нарушений регламентов ИБ — использование ПО для удаленного доступа. В большинстве компаний (59%) применяется TeamViewer, в 21% компаний — Ammyu Admin. Также были замечены LightManager, Remote Manipulator System (RMS), Dameware Remote Control (DWRC), AnyDesk и другие.



Почти в половине компаний,

которые используют ПО для удаленного доступа, установлено одновременно несколько таких программ. Так, например, в одной государственной организации было выявлено сразу пять: Ammy Admin, RMS, AeroAdmin, LiteManager, TeamViewer.

В 6 из 7

промышленных организаций применяется ПО для удаленного доступа в нарушение регламентов ИБ

В исследовании [«Как организована удаленная работа в компаниях в России и странах СНГ»](#) мы отмечали, что в популярном ПО для удаленного доступа могут содержаться критически опасные уязвимости. Например, CVE-2019-11769, которая позволяет перехватывать учетные данные TeamViewer в открытом виде из памяти процессов. Кроме того, с помощью ПО для удаленного доступа злоумышленники могут незаметно подключаться к узлам инфраструктуры компании. Поэтому если нет возможности полностью отказаться от использования ПО для удаленного доступа, то рекомендуем ограничиться только одним инструментом и обязательно установить актуальные обновления.

69% компаний используют устаревшие протоколы LLMNR и NetBios. Этот недостаток конфигурации злоумышленники могут использовать для перехвата значений NetNTLMv2 challenge-response, передаваемых по сети, и дальнейшего подбора учетных данных.

02 Число подключений по RDP растет, насколько они легитимны?

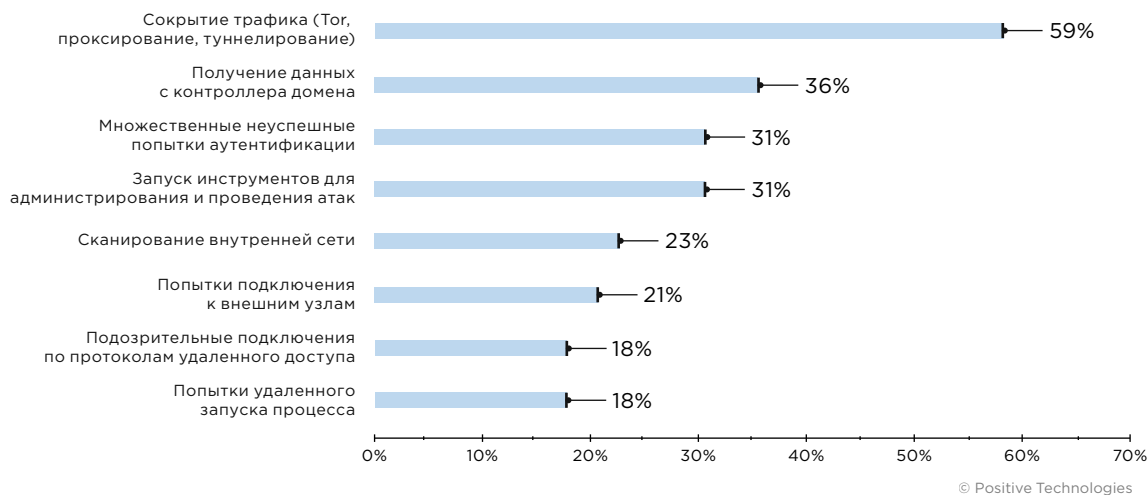


Рисунок 5. Подозрительная сетевая активность (доля компаний)

в 4 из 5

компаний ИТ-отрасли применялись инструменты для сокрытия трафика: Tor, проксирование, туннелирование

Переход компаний на удаленную работу повлиял и на сетевую активность — выросла доля подключений во внешнюю сеть по протоколу удаленного доступа RDP: в 2019 году составляла 3%, в 2020 году достигла 18%. Очевидно, что такие подключения должны тщательно контролироваться.

Так, например, в одной промышленной организации PT NAD зафиксировал подключение по RDP на внешний ресурс, содержащий облачное хранилище. В его адрес по протоколам RDP и HTTPS в общей сложности было передано 23 ГБ данных. Злоумышленники могли применить технику T1071 — использование протоколов прикладного уровня по классификации MITRE ATT&CK. Ее суть заключается в том,

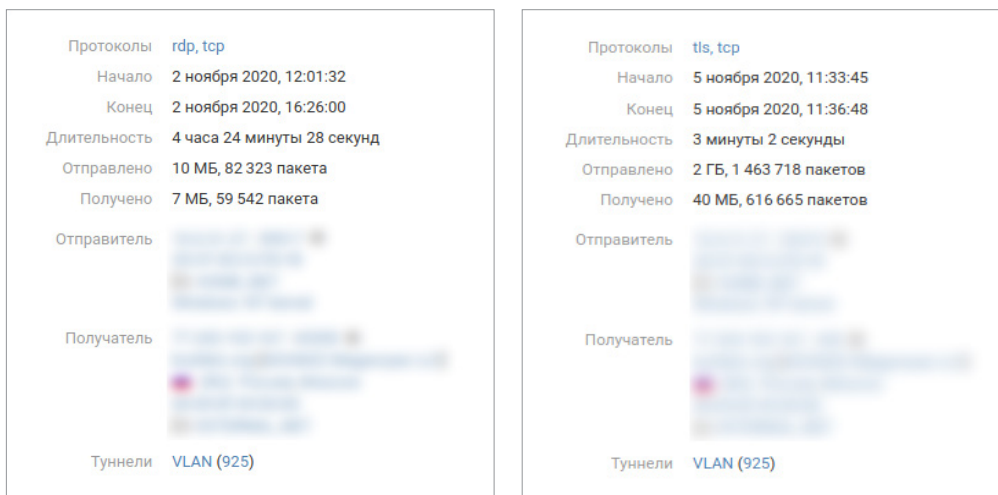


Рисунок 6. Подозрительные подключения по RDP и HTTPS

что нарушители или вредоносное ПО осуществляют скрытную передачу украденных данных на подконтрольные серверы, используя распространенные протоколы прикладного уровня.

В половине промышленных компаний было зафиксировано получение данных с контроллера домена. Сама по себе эта активность легитимная, однако выгрузка состава доменных групп или списка администраторов может говорить об активности злоумышленников в инфраструктуре компании и быть частью разведки.

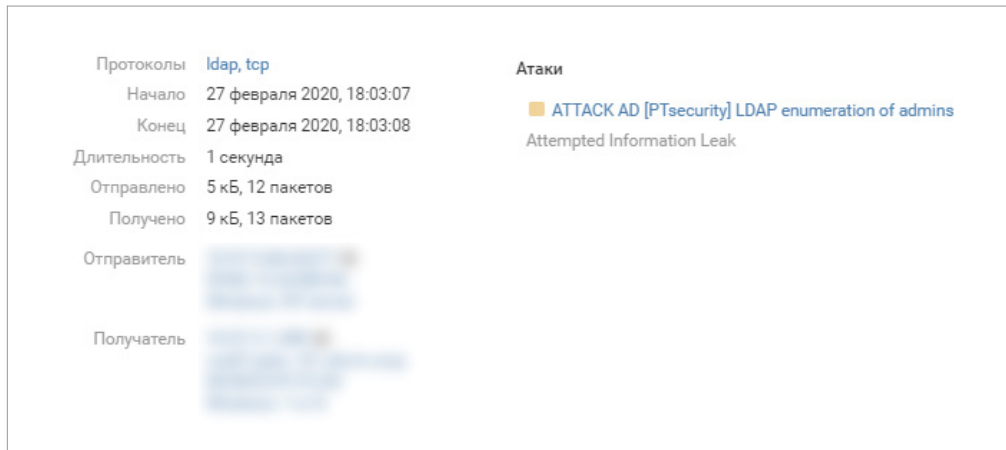


Рисунок 7. Получение информации об административных учётных записях по протоколу LDAP

03 ВПО обнаружено в каждой государственной и промышленной организации

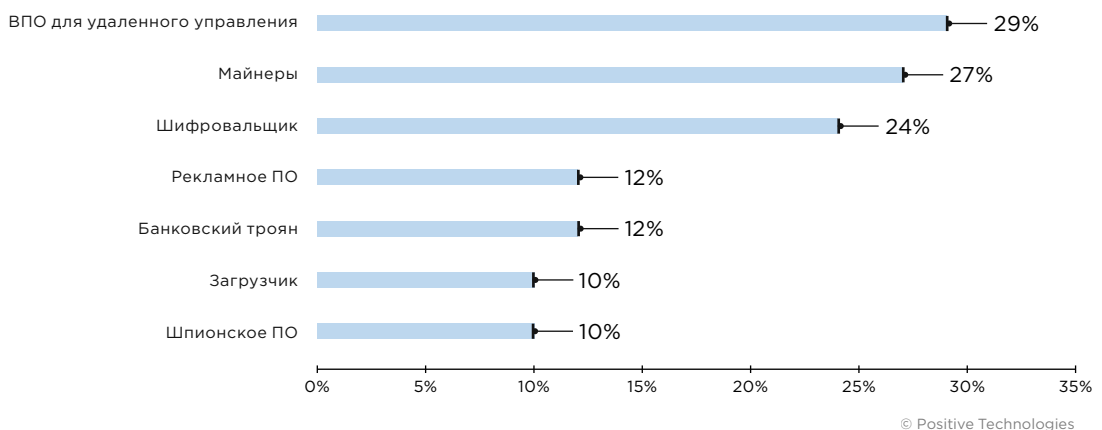


Рисунок 8. ТОП-5 типов активного вредоносного ПО (доля компаний)

В каждой четвертой организации выявлены попытки подключения к засинкхололенным доменам (доменным адресам, которые были ранее замечены во вредоносных кампаниях, а теперь обращения к ним перенаправляются на специальные sinkhole-серверы для недопущения

связи ВПО с командными серверами). В каждой пятой компании отмечены попытки удаленного запуска процесса. Такая сетевая активность может свидетельствовать о действиях вредоносного ПО.

В ходе пилотных проектов по мониторингу сетевой активности и выявлению сложных угроз в 2020 году мы столкнулись с активностью 36 семейств вредоносного ПО. Среди них были и такие как шифровальщик WannaCry, банковские трояны RTM, Ursnif и Dridex.

Шпионское ПО AgentTesla было выявлено в трех организациях. Весной 2020 года ВПО Agent Tesla встречался в фишинговых кампаниях, связанных с COVID-19. ВПО было изменено для кражи учетных данных электронной почты из клиента Outlook, а также паролей от Wi-Fi.

В 68%

анализируемых компаний выявлена активность вредоносного ПО

В каждой четвертой компании выявлена активность криптомайнеров. Как правило, PT NAD обнаруживал запросы на разрешение доменных имен, относящихся к известным майнинг-пулам, таким как antpool.com, supportxmr.com, minexmr.com, nanopool.org, xmrpool.eu, monerohash.com, io.litecoinpool.org. Злоумышленники могут устанавливать майнеры в нагрузку к основному ВПО или после выполнения своей цели, например, кражи данных. Кроме того, майнеры могут использовать до 80% свободной мощности компьютера, что грозит компаниям существенным снижением их производительности.

Обнаружение любого ВПО в инфраструктуре — это повод для проведения тщательного расследования. Наличие ВПО может свидетельствовать о серьезных недостатках в системе безопасности компании.

Протоколы: dns, udp
 Начало: 3 сентября 2020, 13:19:41
 Конец: 3 сентября 2020, 13:19:41
 Длительность: 0 секунд
 Отправлено: 76 Б, 1 пакет
 Получено: 160 Б, 1 пакет
 Отправитель: [blurred]
 Получатель: [blurred]

DNS			
Query	eth.nanopool.org	AAAA	
	mine... HOST		
	mine... HOST		
	NOERROR	flags: RA, RD	
Non-authori...	eth.nanopool.org	AAAA	TTL: 300
	eth.nanopool.org	AAAA	TTL: 300
	eth.nanopool.org	AAAA	TTL: 300

Рисунок 9. Разрешение доменного имени известного майнинг-пула



Системы мониторинга сетевой активности стали чаще устанавливать внутри инфраструктуры компании, а не для выявления внешних атак.

Заключение

Компании теперь более осознанно подходят к выбору, пилотированию и внедрению технических средств. По нашим наблюдениям, системы мониторинга сетевой активности стали чаще устанавливать внутри инфраструктуры компании, а не для выявления внешних атак. Это решение хоть и требует хорошего понимания внутренней инфраструктуры и топологии сети, зато дает возможность выявить подозрительные действия во внутренней сети компании.

Результаты мониторинга сетевой активности, полученные в 2020 году, в целом близки к прошлогодним:

- В каждой компании встречаются нарушения регламентов ИБ: используется ПО для удаленного доступа, устаревшие и незащищенные протоколы передачи данных.
- Вместе с переходом на удаленную работу ожидаемо выросла и доля подключений по RDP. Они обязательно должны контролироваться, ведь в 2020 году количество атак на протоколы для удаленного доступа выросло более чем в три раза.
- Практически в каждой организации замечена подозрительная сетевая активность: применяются инструменты для сокрытия трафика, выявлены подозрительные подключения на внешние узлы.

Использование NTA-систем позволяет не только вовремя обнаружить подозрительные подключения, но и обратиться к истории сетевой активности узла и проверить, не было ли других подобных попыток.

Может случиться так, что в момент проведения атаки еще не существовало правил обнаружения угроз и индикаторов компрометации, которые доступны сегодня. Поэтому необходимо проверять трафик не только в режиме реального времени, но и проводить ретроспективный анализ с учетом новой информации. Сохранение копий трафика и повторный его анализ позволяют провести детальное расследование и обнаружить действия злоумышленника даже для тех событий, которые произошли раньше.

А как атакуют вашу компанию?

Проверьте сеть и периметр — закажите бесплатный пилот PT NAD на ptsecurity.com:

ЗАКАЗАТЬ ПИЛОТ 

О компании

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга «Эксперт-400».

Следите за нами в соцсетях ([Facebook](#), [ВКонтакте](#), [Twitter](#)), а также в разделе «[Новости](#)» на сайте ptsecurity.com.