



От email до сети — комплексная защита вашего бизнеса:

защищаем электронную переписку, сетевую
инфраструктуру и критические данные

Виктор Еременко
Константин Рудаков
Ника Ларина

Время обнаружения – ключевая метрика



55%

Нарушение бизнеса

Доля инцидентов,
остановивших работу
компании

9

дней до обнаружения

Медиана детектирования,
годом ранее — 17

3,5 года

**Самый долгий
инцидент**

Столько активность
оставалась незамеченной

Четыре двери в инфраструктуру



36%



Веб-приложения
на периметре

Exchange, Bitrix,
SharePoint, NetScaler

28%



Компрометация
подрядчика

Доступ через
доверенного партнёра

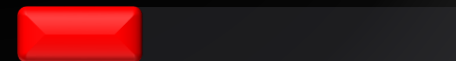
17%



Фишинговые
письма

Вложения, ссылки,
обращения в сервисы

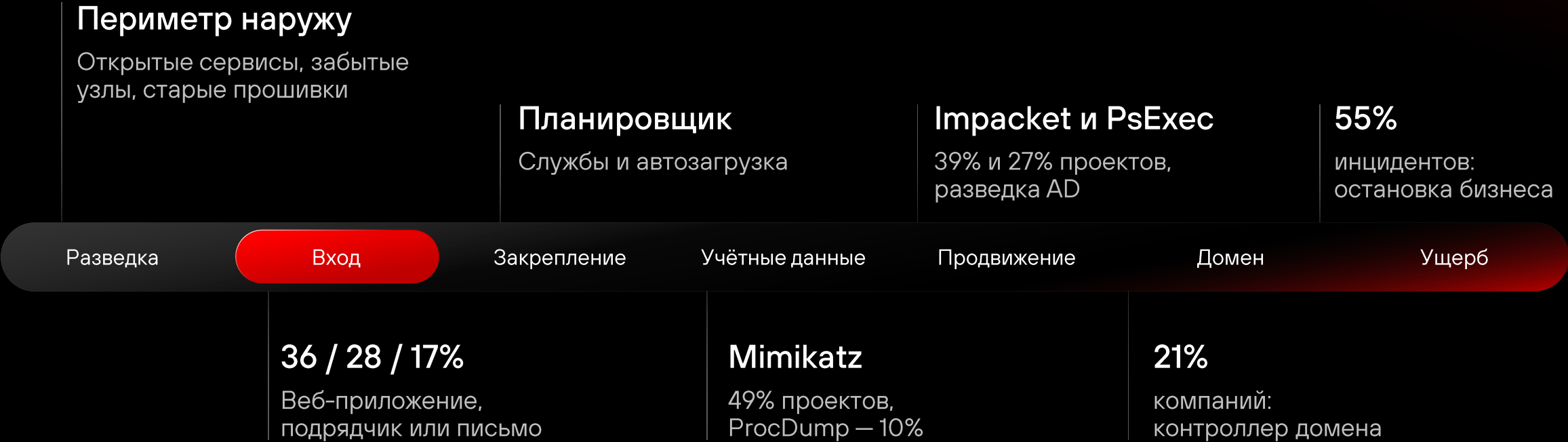
11%



Публичные
сервисы

VPN, RDP, SSH на периметре

От входа до остановки бизнеса



Почему это срывает



Сегментация сети

Один вход открывает
доступ ко всей сети



Устаревшее ПО

Непатченные системы и снятые
с поддержки ОС



Нет 2FA

Украденный пароль
даёт полный доступ



Антивирус

Отсутствует или настроен
некорректно

Ни один из этих пробелов не закрывается одним продуктом: нужны контроль периметра и границ сегментов, видимость внутреннего трафика и проверка файлов. Об этом — дальше.

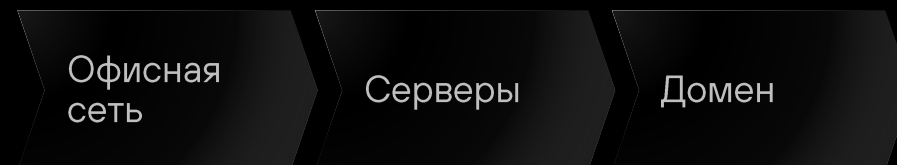
Цель — сервисы, сеть лишь маршрут



Точка входа

- Веб-приложение на периметре
- Учётные данные подрядчика
- Письмо, VPN, RDP

Сетевая инфраструктура — транзит



Атакующий не «ломает сеть» — он ищет в ней путь до целевого сервиса.

Целевые сервисы

1С, ERP, АБС

Базы данных

Почта и CRM

Резервные копии

АСУ ТП и биллинг

Защищать только вход бессмысленно: маршрутов до сервиса десятки, и часть из них лежит внутри уже доверенной зоны.

Контроль нужен на всём маршруте — на границе, между сегментами и на подступах к самим сервисам.

Первая линия обороны

тризтех[^]

pt

L4 Firewall

Быстрый, но «слепой» привратник: он проверяет только обложку пакета (паспорт и номер комнаты).

Но не знает, какое приложение отправляет данные и что находится внутри самого пакета.



Полный контроль

тризтех[^]

pt

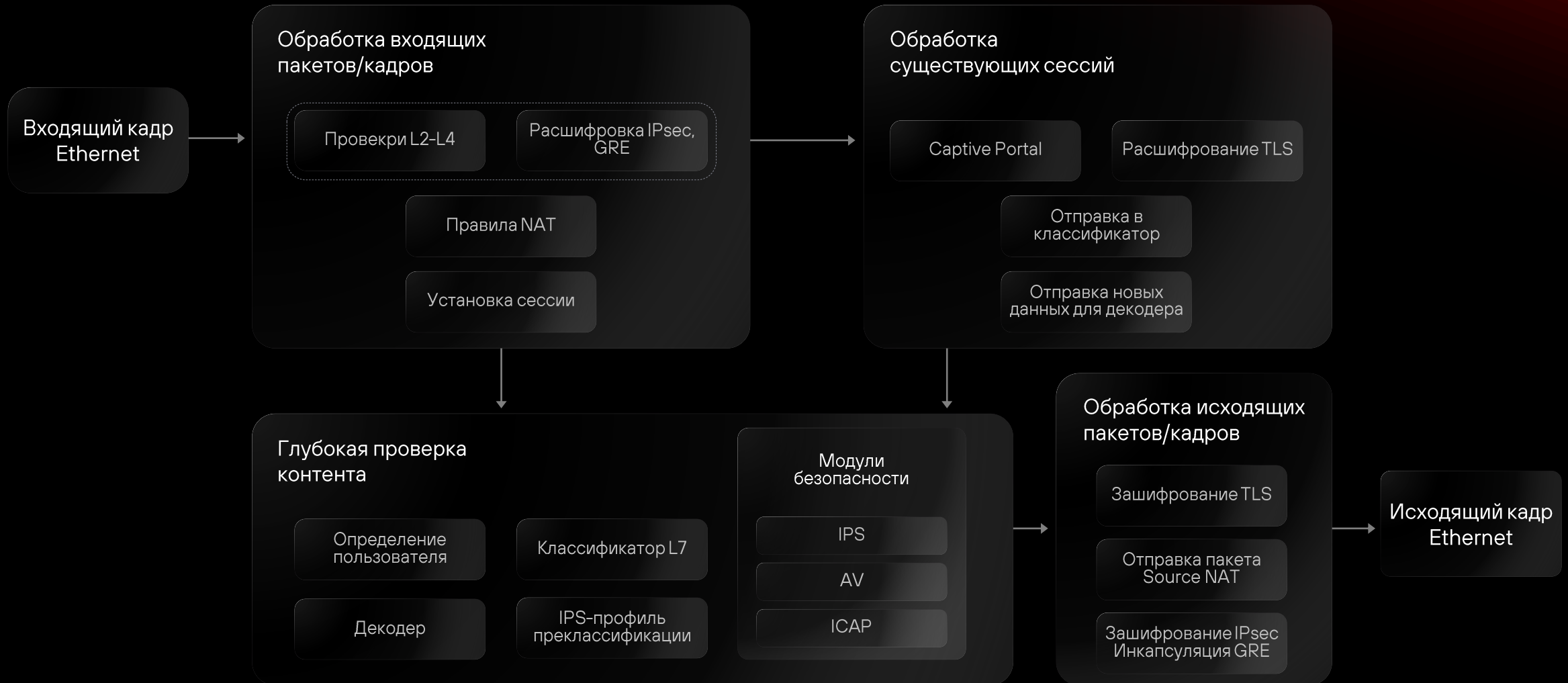
NGFW

- Работает на всех уровнях OSI
- Фильтрация
- Предотвращение вторжений
- Контроль приложений
- Инспекция шифрованного трафика
- Управление на основе идентификации пользователей



Как работает PT NGFW

тризтех⁺



Функции РТ NGFW

тризтех[^]



ИТ

Routing
static, OSPF, BGP, PBR

VPN
Site-to-site, GRE
Remote Access

NAT
Source, Destination, PAT

Кластеризация
Active-Standby

ИБ

IPS/IDS

Application control

AntiVirus

ICAP

URL-filtering

User Identity

GeoIP

SSL-inspection

Инспекция TLS 1.2 и 1.3



Точная идентификация приложений, передающих данные по HTTPS

Реализация по классической схеме методом man-in-the-middle (MITM)

Возможность исключения трафика из расшифровки

Более 99% интернет-трафика передаётся по протоколу **tls***

PT NGFW

Политики

Объекты

Устройства

Журналы

Параметры

Межсетевые экраны

Трафик

Расшифрование

IPS

Антивирус

Политика аутентификации

ICAP

IPsec

Удаленный доступ

Система управления

Аудит

Аутентификация

Журнал расшифрования

Сборщик журналов: Default-LC

2 авг. 2026 г., 15:43 – 3 авг. 2026 г., 15:43

Откл

Скрыть фильтры · 0

Добавить фильтр

Экспорт в формате CSV

Обновить

Время...	Действие	Зона источника	Адрес источника
03.08,...	Расшифровывать	Trusted	192.168.1.16
03.08,...	Расшифровывать	Trusted	192.168.1.16
03.08,...	Не расшифровывать	Trusted	192.168.1.16
03.08,...	Расшифровывать	Trusted	192.168.1.16

Журнал расшифрования

Общая информация

Действие

Расшифровывать

Время создания записи

03.08, 12:36:54

Запись получена

03.08, 12:36:54

Протокол IP

TCP (6)

Приложение

tls/rambler

Категории URL

Search Engines, Internet Portals

Название устройства

PT NGFW2

Модель устройства

pt-ngfw-1010

Серийный номер устройства

PT002

Идентификатор правила

019a3f11-85ac-71f1-9...

Правило расшифрования

decrypt any SalesGroup

Правило NAT

svc SNAT all

Rule sections/groups

Pre-rules

Global Pre-rules

service rules Pre-rules

Central Office Pre-rules

Post-rules

Central Office Post-rules

No.	Name	State	Source Zone	Ad...	User	Destination Zone	Add	URL category	Service	Action	Decryption mode	Logging
Global · Pre-rules +												
4	decrypt.19	Enabled	* Any	h-	* Any	* Any	*	* Any	* Any	Decrypt	TLS forward proxy	At rule hit
5	DND DC	Enabled	* Any	* Ar	* Any	* Any	h	* Any	* Any	Do not decrypt	TLS forward proxy	Do not log
6	decrypt .55	Enabled	* Any	h-	* Any	* Any	*	* Any	* Any	Decrypt	TLS forward proxy	Any TLS han
7	decrypt win srv	Enabled	* Any	* Ar	* Any	* Any	h	* Any	* Any	Decrypt	TLS forward proxy	Any TLS han
8	decrypt 100rage	Enabled	* Any	* Ar	* Any	* Any	h	* Any	* Any	Decrypt	TLS forward proxy	Any TLS han
9	skip WL	Enabled	* Any	* Ar	* Any	* Any	*	custom_white_list	* Any	Do not decrypt	TLS forward proxy	At rule hit

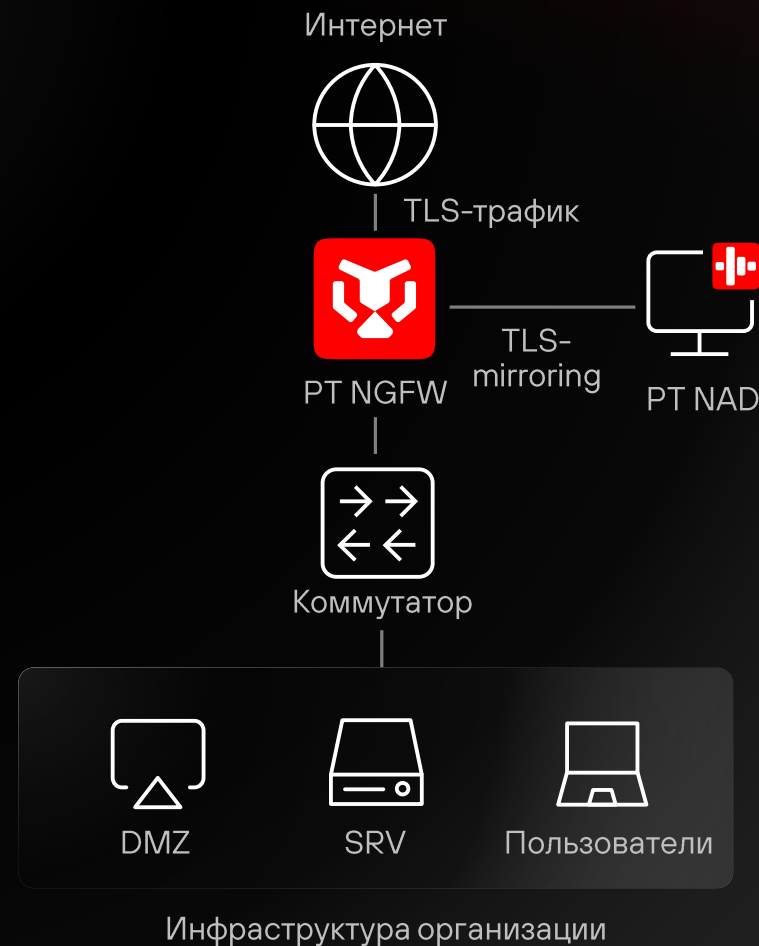
Источник: HTTP архив. Статистика по веб-протоколам

PT NGFW + PT NAD

тризтех[^]

pt

- > Расшифровка TLS-трафика PT NGFW
- > Анализ расшифрованного трафика остальными политиками PT NGFW
- > Параллельное зеркалирование со специального интерфейса PT NGFW
- > Получение зеркалированного трафика PT NAD. Дополнительный анализ



PT NGFW + PT NAD. Настройка

тризтех[^]



- 1 Настроить профиль зеркалирования
- 2 Указать в правиле Расшифрования профиль зеркалирования



Подробная инструкция

PT NGFW Policies Objects Devices Logs Settings

2

Security

NAT

Decryption

Authentication

Global

service rules

Branch

Central Of..

Editing decryption rule

Rule properties Match conditions Action on match

Action

Decryption mode

Logging

Decryption profiles · 1

+ Add

PT NGFW Policies Objects Devices Logs Settings

1

Users

Services

Addresses

Zones

IPS

URL categ

Auth profil

Decryption mirroring

Editing the mirroring profile

Name

Device group

Destination MAC address

Description

Mirror interfaces

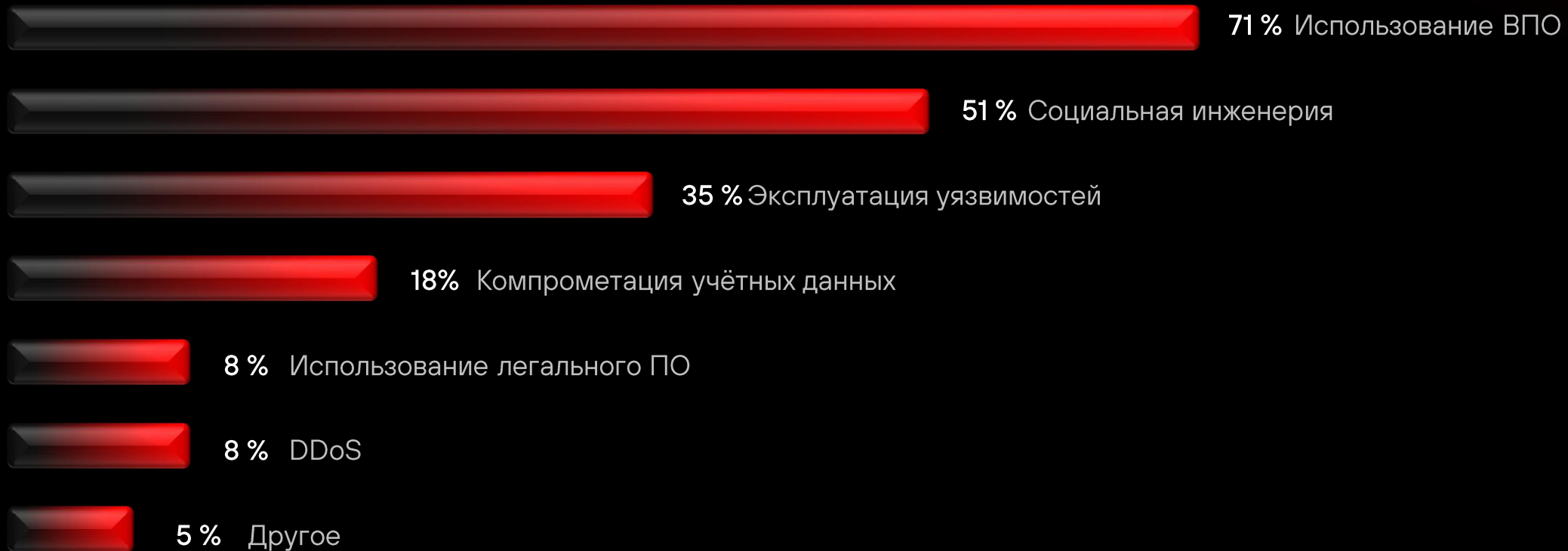
+ Add

Name	VLAN ID	Virtual context	Device name	Device
eth1-3.0	0	Default	sh-presales-cluster	Centra

Как можно усилить защиту?

тризтех[^]

pt



Тренды атак в 2026 году

Модули безопасности. IPS



 Сигнатуры от PT Expert Security Center

 Быстрое обновление сигнатур и защита от эксплойтов, ориентированная на российский рынок

PT NGFW

Policies

Objects

Devices

Logs

Settings

Applications

Users

Services

Addresses

Zones

IPS

URL categories

Auth profiles

Decryption mirroring profiles

Global

service rules

Branch

Central Of...

IPS

Global

service rules

Central Office

Profiles

Groups

Signatures

Threat name	Default action	Threat ca...	Severity
Vopak	Allow	Adware	Low
WDJiang	Allow	Adware	Low
Wajam	Allow	Adware	Low
Wajam	Allow	Adware	Low
Wajam	Allow	Adware	Low
Wajam/Soctuseer	Allow	Adware	Low
WanNeng	Allow	Adware	Low
Wapron	Allow	Adware	Low
Wapron	Allow	Adware	Low
Wapron	Allow	Adware	Low

PT NGFW

Policies

Objects

Devices

Logs

Settings

Firewalls

Traffic

Decryption

IPS

Antivirus

Authentication policy

ICAP

IPsec

Remote access

Management System

Audit

Authentication

IPS logs

Log collector: Default-LC

Aug 8, 2026, 17:35 – Sep 8, 2026, 17:35

Off

Hide filters · 0

Add filter

Export to CSV

Refresh

Entry generation time	Action	Threat name
09/08, 4:49:51 PM	Drop	SharePoi
09/08, 4:49:38 PM	Drop	Langflow
09/08, 4:49:27 PM	Drop	Langflow
09/08, 4:49:23 PM	Drop	Possible
09/08, 4:49:12 PM	Drop	Possible
09/08, 4:49:02 PM	Drop	XFLTRea
09/08, 4:48:53 PM	Drop	Nmap TL
09/08, 4:48:36 PM	Drop	log4j RCt

IPS log

General information

Entry generation time
09/08, 4:49:27 PM

Entry received
09/08, 4:49:08 PM

IP protocol
TCP (6)

Application
http

Device name
PT NGFW1

Device model
pt-ngfw-1010

Device serial

Rule ID
019a3b27-611d-71fe-a

Security rule
content.ips.av.icap

Session ID
30010460505951800

Virtual context name
Default

Threat category
Attack

Threat name
Langflow AI Unauthentic...

Severity
medium

CVE
CVE-2025-3248

File name

Action
Drop

SID
10014265

X-Forwarded-For IP

URL

★ Поддержка профилей IPS

Модули безопасности. Антивирус

тризтех[▲]

pt

PT Protect

Группа содержит
все сигнатуры антивируса
Action = Drop
Журналирование при срабатывании

PT Detect

Группа содержит
все сигнатуры антивируса
Action = Allow
Журналирование при срабатывании

The screenshot displays the PT NGFW management interface. On the left, a sidebar lists various security modules: Traffic, Decryption, IPS, Antivirus (selected), Authentication policy, ICAP, IPsec, Remote access, Management System, Audit, and Authentication. The main panel is divided into two sections. The top section, titled 'Security', shows a list of modules including NAT, Decryption, Authentication, Global, and service rules. The bottom section, titled 'Antivirus logs', shows a log collector for 'Default-LC' with a date range from August 8, 2026, to September 8, 2026. The logs are currently set to 'Off'. A table of logs is displayed, showing entry generation times and actions. A detailed view of a log entry for 'Shadowsocks.exe' is shown on the right, including general information such as entry generation time, IP protocol, threat name, device name, and device serial.

Security

- NAT
- Decryption
- Authentication
- Global
- service rules

Rule properties **Match conditions** **Action on match**

Action
Allow

Logging
At session start and end

Security profiles - 1

- PT-Detect Antivirus

PT NGFW Policies Objects Devices **Logs** Settings

Antivirus logs Log collector: Default-LC

Aug 8, 2026, 17:35 – Sep 8, 2026, 17:35

Off

Hide filters - 0
Add filter

Export to CSV Refresh

Entry generation time	Action	Malware ID
08/24, 9:36:55 AM	Reset both	997216
08/24, 7:36:19 AM	Reset both	2058169
08/24, 7:36:17 AM	Reset both	997216
08/24, 5:36:25 AM	Reset both	2058169
08/24, 5:36:23 AM	Reset both	997216

Shadowsocks.exe

General information

Entry generation time 08/24, 9:36:55 AM	Entry received 08/24, 9:36:56 AM
IP protocol TCP (6)	File name Shadowsocks.exe
Threat name Malicious.Generic	Application http/github
Device name PT NGFW1	Device model pt-ngfw-1010
Device serial	Virtual context name Default
Rule ID 019a3b88-5841-7619-...	Security rule content.av
Antivirus version hash	URL /github-production-re...
Algorithm hash SHA256	Hash AED3ADA5F8FE7C73...

PT NGFW + многое 😊

тризтех[^]



Интеграция с SIEM



Remote Access VPN



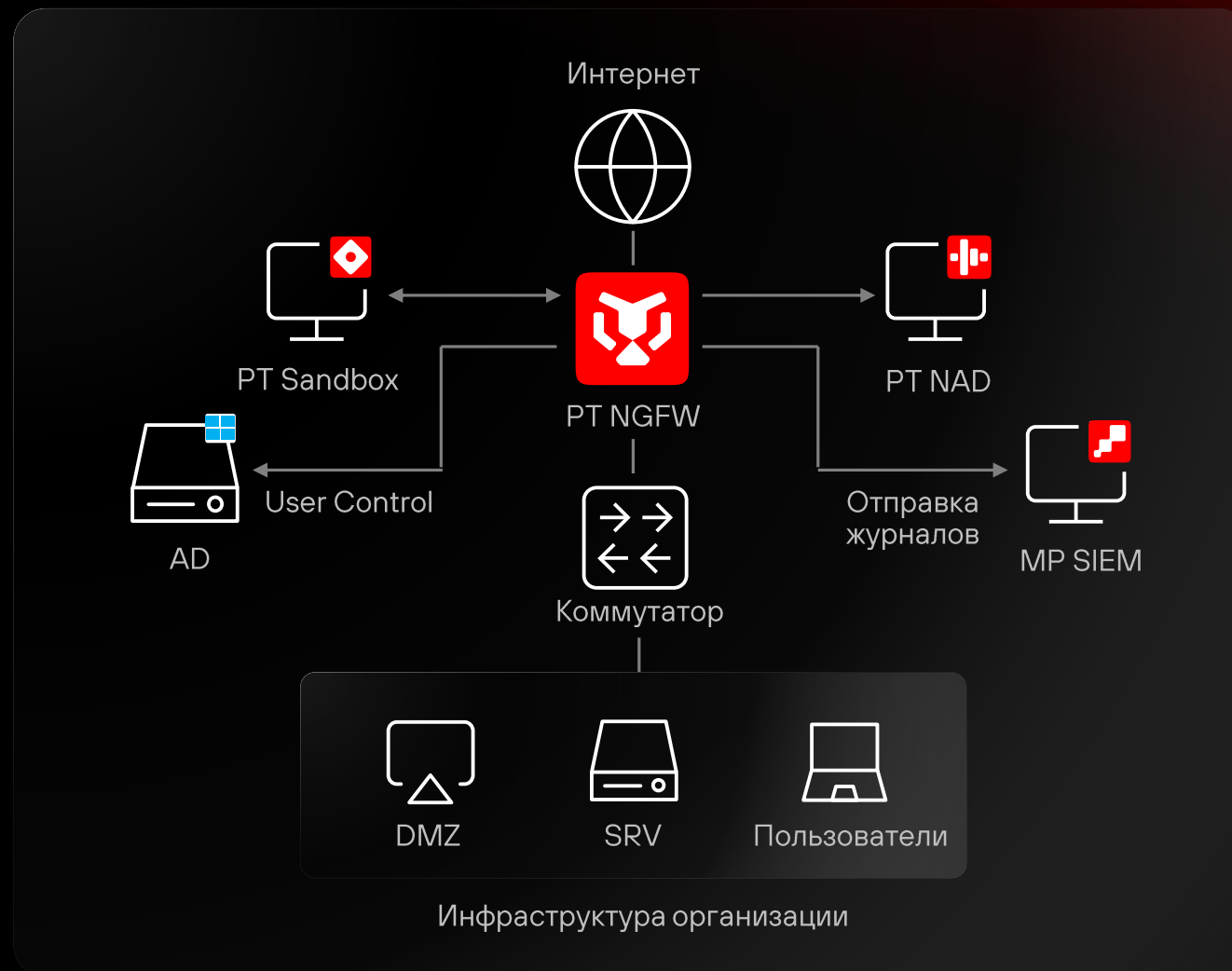
Интеграция
с Active Directory



URL-фильтрация

API

Captive Portal



PT NGFW + PT Sandbox

тризтех[^]

pt

Антивирусное сканирование:

- Межсетевой экран отправляет файлы из HTTP-ответов на ICAP-сервер.
- ICAP-сервер сканирует файлы на наличие вирусов и возвращает результат.

Фильтрация контента:

- Межсетевой экран отправляет HTTP-запрос на ICAP-сервер.
- ICAP-сервер анализирует запрос и блокирует доступ к запрещенным ресурсам.



PT NGFW + PT Sandbox. Настройка

тризтех[▲]

pt

1 Создать объект Сервис ICAP

2 Создать профиль ICAP



Подробная инструкция

PT NGFW Policies Objects Devices Logs Settings

1

New ICAP server

Address type
☒ IP address ☐ FQDN

IP address
For example, 192.168.100.50

Port
1344
From 1 to 65535

Max connections
100

Max tries
1
From 1 to 5

Verdict timeout, s
30
From 1 to 900 seconds

2

New ICAP profile

General Request modification Response modification

State
☒ Enabled

ICAP Server
sb

☒ Logging

☐ Monitoring mode ⓘ

Fallback action
☒ Bypass ☐ Block

Content type
* Any

- > ☐ Archives · 16
- > ☐ Documents · 34
- > ☐ Encrypted · 1
- > ☐ Executables · 18
- > ☐ Images · 10
- > ☐ Media · 24
- > ☐ Other · 1
- > ☐ Scripts · 8

PT NGFW + PT Sandbox. Настройка

тризтех[▲]

pt

- 3 Указать в правиле Безопасности профиль ICAP
- 4 События в отдельном журнале



Подробная инструкция

PT NGFW Policies Objects Devices Logs Settings

3

Security

NAT

Decryption

Authentication

Global

service rules

Editing security rule

Rule properties Match conditions Action on match

Action

Drop

Logging

At rule hit

Security profiles · 1

SandboxRespM

ICAP

Push to devices

4

PT NGFW Policies Objects Devices Logs Settings

Firewalls

Traffic

Decryption

IPS

Antivirus

Authentication policy

ICAP

IPsec

Remote access

Management System

Audit

Authentication

ICAP logs

Log collector: Default-LC

Aug 8, 2026, 17:35 – Sep 8, 2026, 17:35

Off

Hide filters · 1

Action is block

Clear filters

Export to CSV

Refresh

Entry generation time	Action	Content ca
09/08, 9:55:58 AM	Block	Executab
09/08, 9:25:58 AM	Block	Executab
09/07, 7:53:27 PM	Block	Executab
09/07, 10:10:39 AM	Block	

ICAP logs

General information

Action	Block	Entry generation time	09/07, 7:53:27 PM
Entry received	09/07, 7:53:09 PM	IP protocol	TCP (6)
Application	http/windows.defender.u...	Content category	Executables
Content type	exe	File name	mpam-fe_bd_1.1.26070.71...
ICAP Server URI	icap://10.0.105.22:1344/s...	Error	export server connection ...
URL	definitionupdates.micros...	URL categories	Content Delivery Networks
Device name	PT NGFW1	Device model	pt-ngfw-1010



PT Sandbox



Вредоносные файлы и ссылки: как они к нам попадают



Три основных канала
распространения ВПО:



Электронная почта



Узлы



Веб-ресурсы



В вашем почтовом ящике — новое письмо!



Электронная почта
является традиционным
вектором кибератак
на организации

Но одной электронной
почтой злоумышленник
не ограничивается



Не менее важные векторы доставки ВПО



Граница сети, которую, как правило защищают СЗИ типа NGFW и WAF, но без акцента проверки передаваемых файлов



Внутренние сетевые взаимодействия



Рабочие станции пользователей



Системы документооборота и конвейеры разработки



Корпоративные файловые хранилища



Обновления программного обеспечения у ИТ-служб

Основа для фундамента безопасности



Песочницы позволяют обезопасить внутреннюю сеть организации от еще неизвестных вредоносных программ, а также выявить целевые атаки на инфраструктуру

1

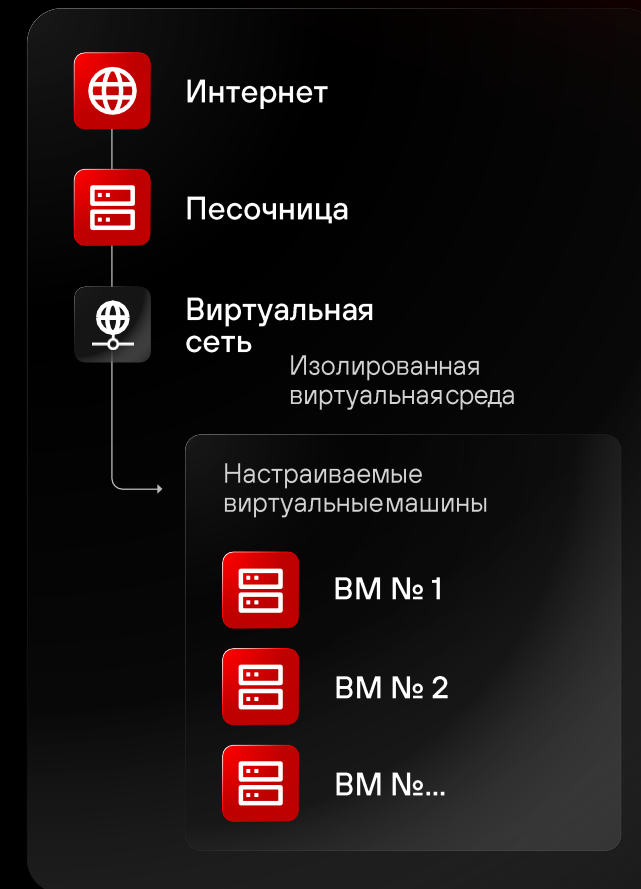
Запускают файлы в изолированной среде, не связанной напрямую с инфраструктурой

2

Можно запустить файл в этой среде, посмотреть, как он себя ведет, какие процессы запускает, что откуда скачивает

3

После проверки **принимается решение о том**, безопасен ли файл и можно ли пропустить его в инфраструктуру



Защита традиционного вектора — почты



	Поведенческий анализ	Антифишинг, антиспам	Secure email gateway (почтовый шлюз безопасности)
PT Sandbox	✓	✗	✗
PT Email Gateway	✗	✓	✓
PT Email Security	✓	✓	✓

Функции:

- контролирует входящий поток
- анализирует поведение
- выявляет атаки до стадии получения вредоносной нагрузки
- дает контекст для SOC

Единая консоль управления

Контроль доставки почты

Глубокий поведенческий анализ



Как работает PT Email Security



Система получает письма от внешних почтовых серверов через почтовый шлюз или через транспорт с почтовых серверов организации, затем передает их средствам проверки



Что под защитой PT Email Security и PT Sandbox



Контроль основных каналов передачи файлов и ссылок в компании за счет легкой интеграции с любыми системами ИТ и ИБ — источниками объектов для анализа



Электронная почта

Интеграция с почтовыми серверами организации. PT Email Security проверяет тело письма и ссылки в нем, а также почтовые вложения (в том числе архивированные, разделенные на части и защищенные паролями)



API-коннектор

Благодаря асинхронному API-коннектору поддерживается интеграция с любыми системами ИТ и ИБ как источниками по HTTP и HTTPS



Объекты из сетевого трафика

Интеграция по ICAP с IDS, IPS, NDR- и NTA-системами, прокси-серверами, межсетевыми экранами (NGFW) и системами защиты веб-приложений (WAF)



Файловые хранилища

PT Sandbox проверяет на наличие угроз файлы в корпоративных системах обмена данными, в том числе в S3-совместимых



Ручная загрузка файлов

Можно вручную отправить любой файл, вызывающий сомнения, на проверку через веб-интерфейс и получить вердикт о его безопасности



Средства для работы с электронной почтой



Почтовый шлюз



Для обеспечения безопасности приема электронных писем с фильтрацией подключений

Встроенный почтовый транспортный агент



Для управления транспортом электронных писем в инфраструктуре

Обезвреживание писем с угрозами



Настраиваемая правилами доставка письма с удаленным активным содержимым

Обработка писем в зависимости от отправителя и получателей



Конфигурируемые правила обработки писем

Антифишинг- и антиспам-проверка писем (APAS)



Средства для анализа фишинга и спама (разработка PT ESC)

Проверка адресов в письмах по спискам DNS-блокировок



Подключение внешних репутационных списков для проверки IP-адресов и доменных имен, найденных в заголовках и ссылках

Статический анализ файлов и ссылок



Для защиты от известных угроз
и проверки легитимности
ссылок используется
комбинация методов анализа

Собственные YARA-правила



Правила экспертного центра PT ESC,
создаваемые в ходе расследования
инцидентов и анализа деятельности
хакерских группировок

Категоризация веб-ресурсов



Классификация интернет-ресурсов
по их назначению и типу контента
для предотвращения инцидентов ИБ

Репутационный анализ



Репутационный анализ файлов
и ссылок по базе индикаторов
компрометации (PT IoC) для
точечного выявления угроз

Антивирусный анализ



Собственная антивирусная
лаборатория PT AV
и дополнительные средства

Анализ содержимого ссылок



Поиск и скачивание контента
по ссылкам с проверкой
его легитимности

Политики предварительной фильтрации при анализе файлов



Для снижения нагрузки на систему поведенческого анализа можно управлять правилами проверки объектов



Пользовательские правила определения объектов с угрозами

Персональные параметры, по которым система будет относить файлы и ссылки к опасным или потенциально опасным объектам



Правила для проверки офисных документов

Настройка параметров проверки файлов OpenDocument и Microsoft Office методом поведенческого анализа



Правила для проверки PDF-файлов

Настройка параметров проверки файлов PDF методом поведенческого анализа



Фильтрация извлеченных ссылок

PT Email Security и PT Sandbox скачивают и проверяют контент только по тем ссылкам, которые удовлетворяют указанным пользователем параметрам

Параметры проверки источников



Возможностей настройки
пользовательских правил много
и на этот случай есть
методические материалы



Параметры источника

Параметры проверки

Правила обработки писем

Задания

Пользовательские правила определения опасных и потенциально опасных файлов

Вы можете настроить, какие еще файлы, кроме определяемых системой, необходимо относить к опасным и потенциально опасным.

+ Добавить

Вставить правило

apk.tampered apk.tampered	Назначаемый уровень оп... Опасный	Считать опасными Только файлы со всеми указанными признаками	Типы файлов APK	Метки Формат подделан	
office.encrypted	Назначаемый уровень оп... Потенциально опасный	Считать опасными Только файлы со всеми указанными признаками	Типы файлов IQY, Документы, Презентации, Таблицы, SLK	Метки Зашифрованный	
office.hasAction	Назначаемый уровень оп... Потенциально опасный	Считать опасными Только файлы со всеми указанными признаками	Типы файлов IQY, Документы, Презентации, Таблицы, SLK	Метки Содержит Action	
office.hasActiveX	Назначаемый уровень оп... Потенциально опасный	Считать опасными Только файлы со всеми указанными признаками	Типы файлов IQY, Документы, Презентации, Таблицы, SLK	Метки С элементами ActiveX	

ML-средство для статического анализа



PT Email Security и PT Sandbox
теперь также проводят первичную
проверку исполняемых файлов
с помощью ML-технологии
на основе модели ByteDog



PT ML

Positive Technologies Machine Learning

Версия 5.35.0.149817

Версия базы
знаний 4.0.0.67 от 27 июля, 13:32

Проверяются Сетевой трафик при поведенческом
анализе, исполняемые файлы при
статическом анализе **Бета**

 [Параметры](#)

Поведенческий анализ



Для защиты от неизвестных угроз, нового вредоносного ПО и целевых атак песочница использует многоуровневую проверку в сочетании с инструментами PT Expert Security Center (PT ESC)

Многоуровневая проверка файлов



Анализ сетевого трафика и подключений



Анализ дампов памяти и процессов



ML-технологии для выявления аномального поведения в системных событиях и сетевом трафике

Изолированная среда PT Email Security

Поддерживает виртуальные среды с Windows, Linux



Экспертные инструменты



Кастомизация виртуальных машин в соответствии с реальными рабочими станциями



Уникальные приманки, имитирующие настоящие файлы, процессы или данные, характерные для разных отраслей



Anti-evasion-защита от популярных техник обхода виртуальных сред

Поведенческий анализ: виртуальные среды

pt

В виртуальных средах
PT Email Security
поддерживаются
образы ОС:



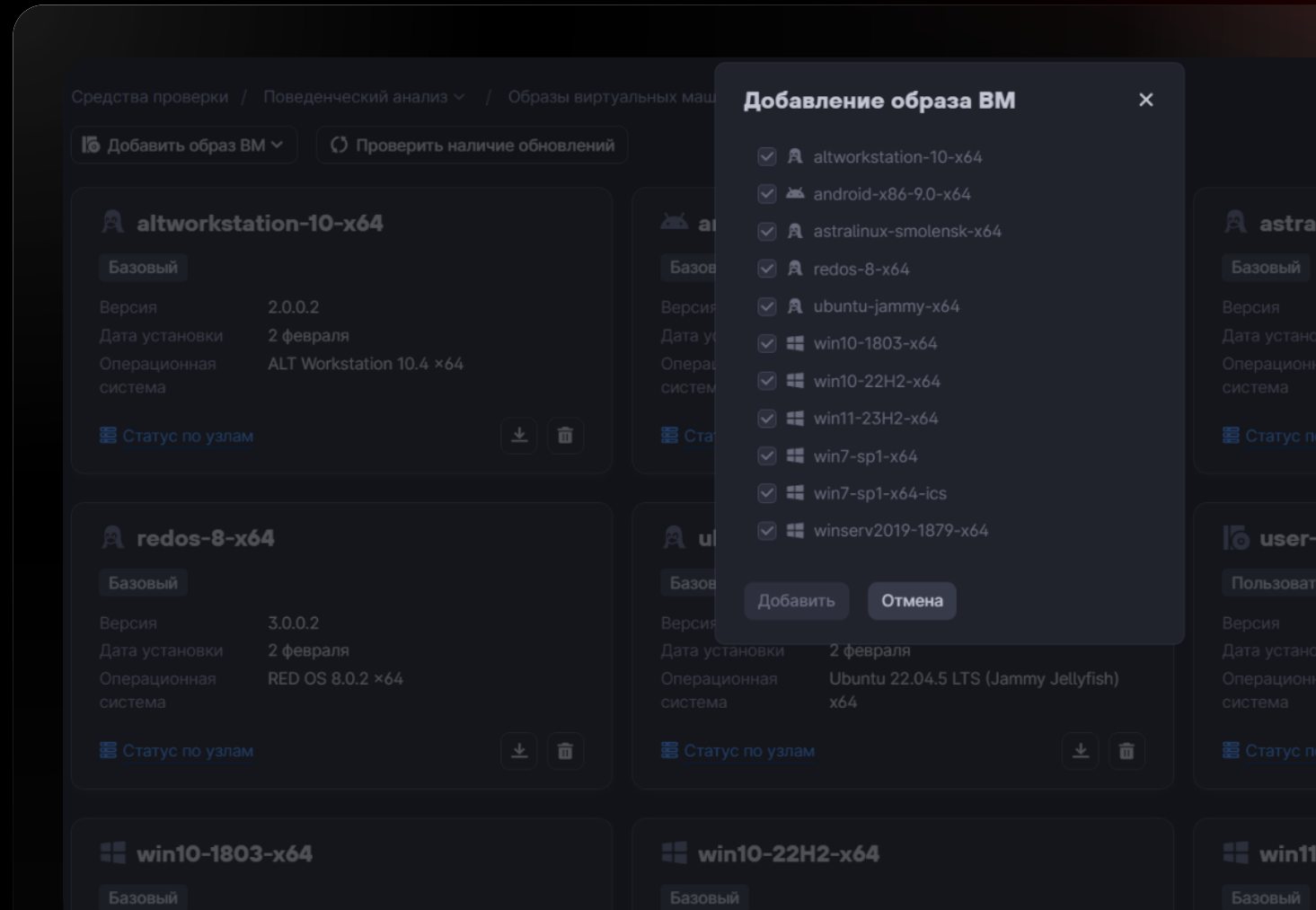
Windows

Windows версий 7–11,
Windows Server 2016 и 2019



Linux

Astra Linux SE 1.7 и 1.8, «РЕД ОС»
версий 7–8, Ubuntu Linux, Alt Linux



Анализ в Android



sensor.classifier.manager.apk

Вердикт: **Бэкдор** | Образ VM: android-x86-90-x64 | Формат файла: APK | Продолжительность: 1 мин 6 с | Версия правил ПА: 2.10.1347 | Версия сетевых правил: 2.0.0.7002 | Версия PT DPI: 12.4.9514

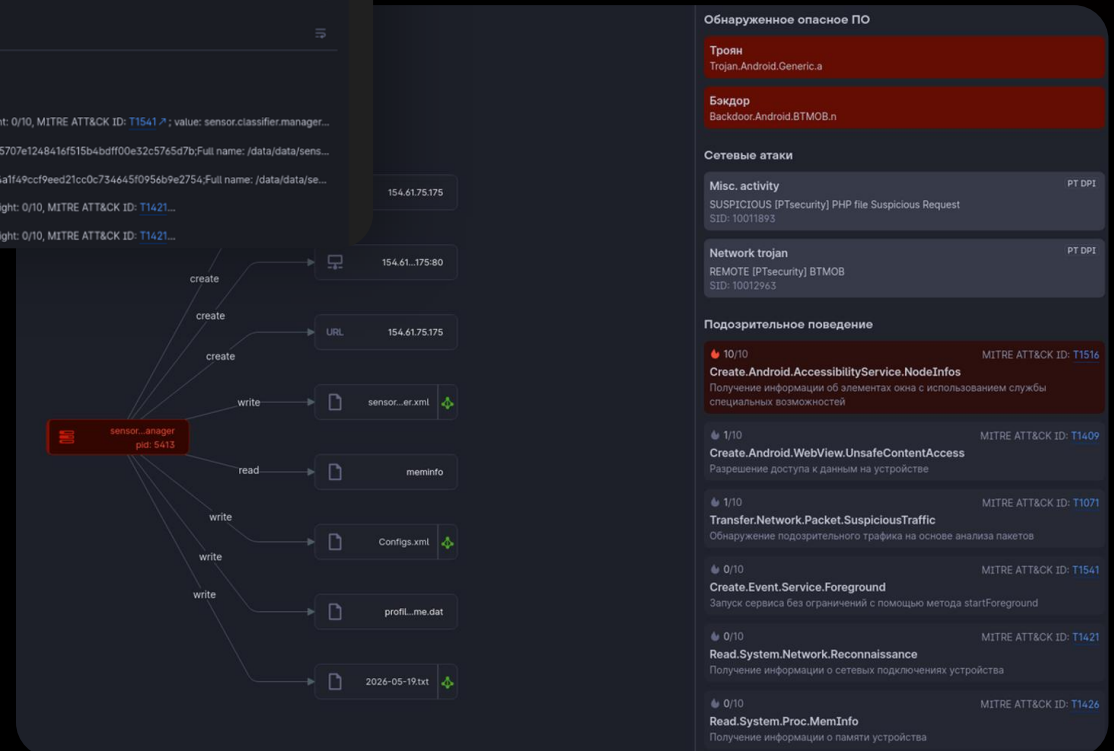
Диаграмма ПА | Диаграмма ПА **5413** | Угрозы **Бета** | События

* По умолчанию | ↺ | ● Режим QL-запросов

Время рег...	PID	Процесс	Действие	Тип объекта	Объект	Вердикт	Дополнительная информация
0:00,000	1376	sensor.classifier.manager	INIT	INIT	5413 sensor.classifier.manager		Status: Success
0:00,000	1376	sensor.classifier.manager	CREATE	PROCESS	5413 sensor.classifier.manager		
0:00,409	5413	sensor.classifier.manager	SUSPICIOUS_BEHAVIOUR	Не определен	—		Create.Event.Service.Foreground; Weight: 0/10, MITRE ATT&CK ID: T1541.1; value: sensor.classifier.manager...
0:01,207	5413	sensor.classifier.manager	REVEALED	DROP	/data/data/sensor.classifier.manager/shared_prefs/s..._er.xml	Угроза не обнаружено	Sha-256: 87bcff122f4bb1de95cbfd87d5365707e124841ef515b4bdf00e32c5765d7b; Full name: /data/data/se...
0:01,282	5413	sensor.classifier.manager	REVEALED	DROP	/data/data/sensor.classifier.manager/shared_prefs/s..._er.xml	Угроза не обнаружено	Sha-256: bfbdb5870c0a3712d37a580f324a1f49ccf9eed21cc0c734645f0956b9e2754; Full name: /data/data/se...
0:04,973	5413	sensor.classifier.manager	SUSPICIOUS_BEHAVIOUR	Не определен	—		Read.System.Network.Reconnaissance; Weight: 0/10, MITRE ATT&CK ID: T1421...
0:04,975	5413	sensor.classifier.manager	SUSPICIOUS_BEHAVIOUR	Не определен	—		Read.System.Network.Reconnaissance; Weight: 0/10, MITRE ATT&CK ID: T1421...



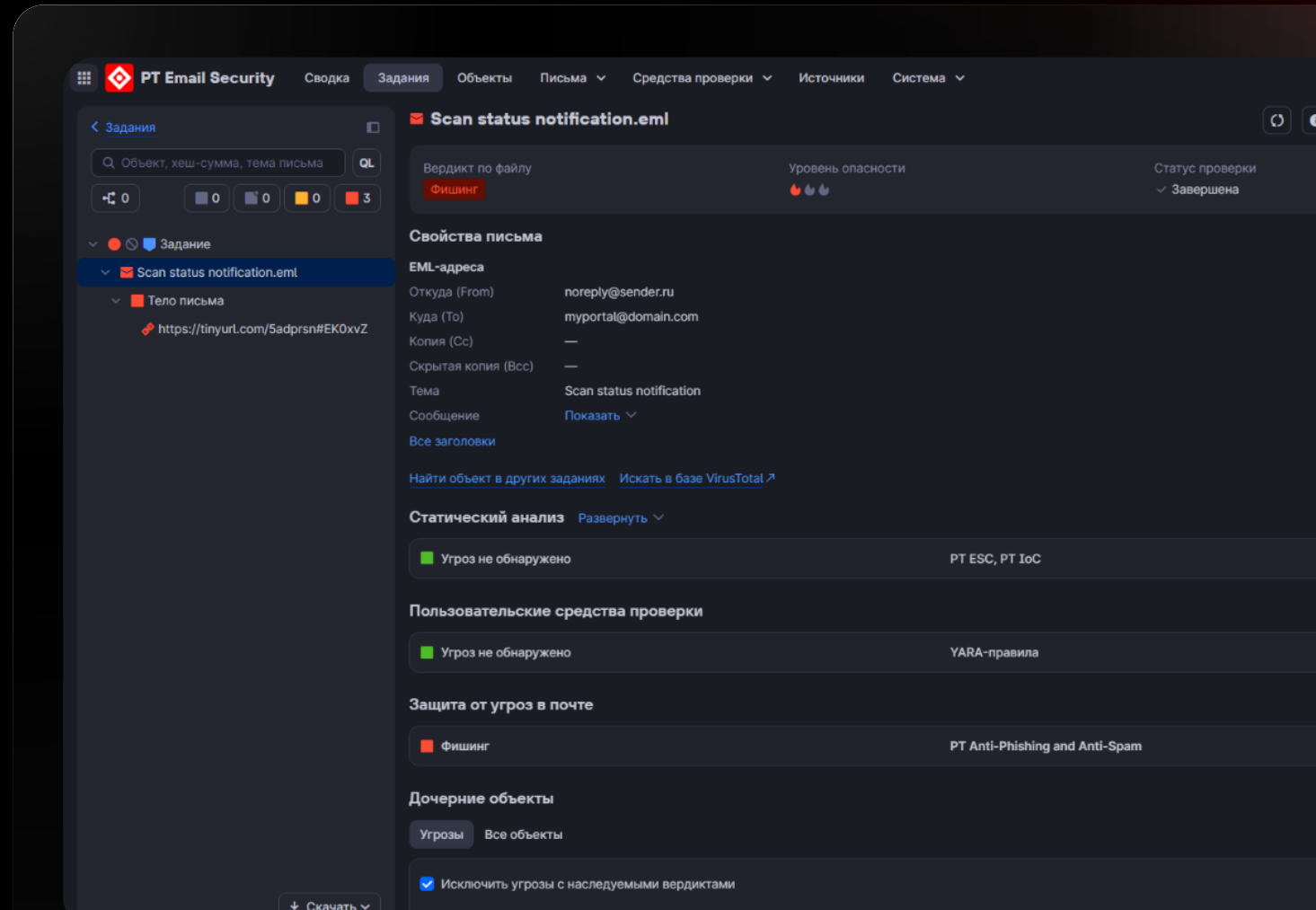
Поведенческий анализ
Android-приложений на образе ОС Android
PT Sandbox извлекает из памяти данные
Android-приложений и сохраняет их в виде
DEX-дампов. Такие данные могут содержать
скрытый или загружаемый во время выполнения код



Защита от адресного фишинга



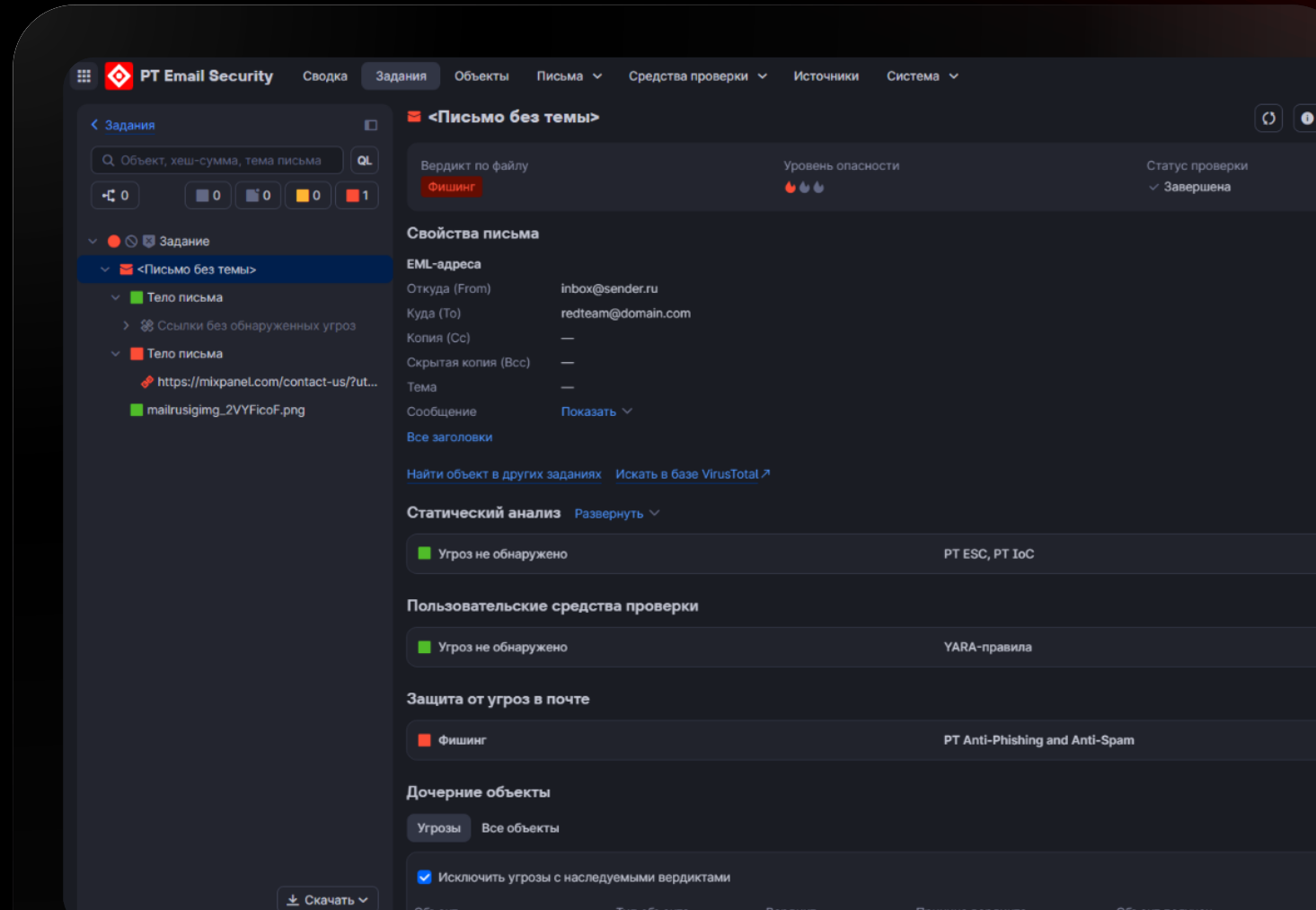
- 1 Движок AntiPhishing/AntiSpam заточен на поиск признаков фишинга в почтовых сообщениях. В данном случае в письме присутствовала сокращенная фишинговая ссылка



Фишинг с применением QR-кодов



- 1 В этом случае анализ письма не показал ничего необычного. Однако помимо явно прописанных ссылок в письме содержался QR-код, скрывающий фишинговый URL



Случай из практики работы PT Sandbox



Запуск вредоносного ПО
в обход антивирусных средств

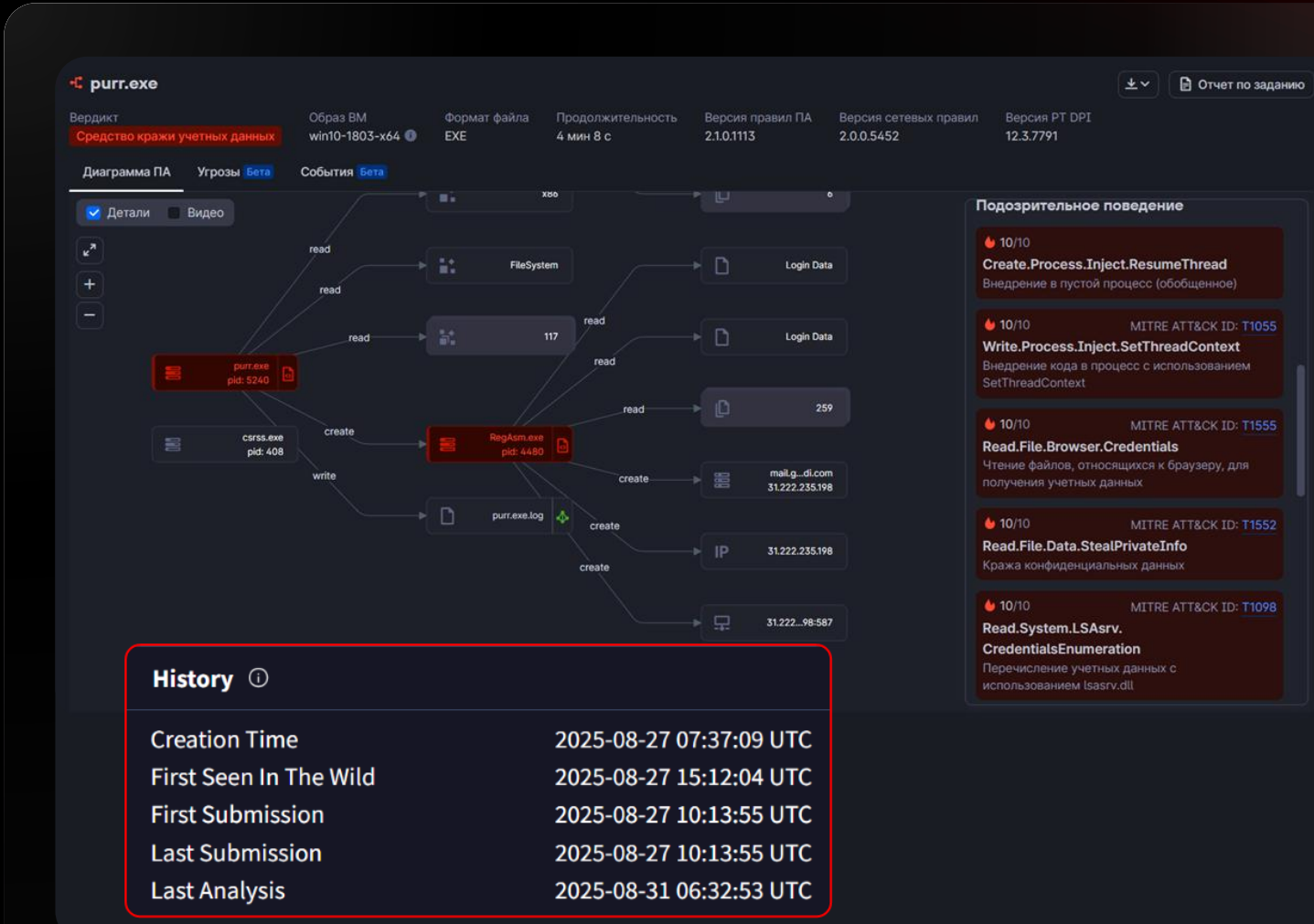
Agent Tesla

Дата выявления: 2025-08-27

10:07:20.080

Одно из самых популярных семейств.
Уже более 10 лет с момента
обнаружения, но каждый день
появляются его новые модификации

На момент выявления в песочнице
образец еще не встречался публично



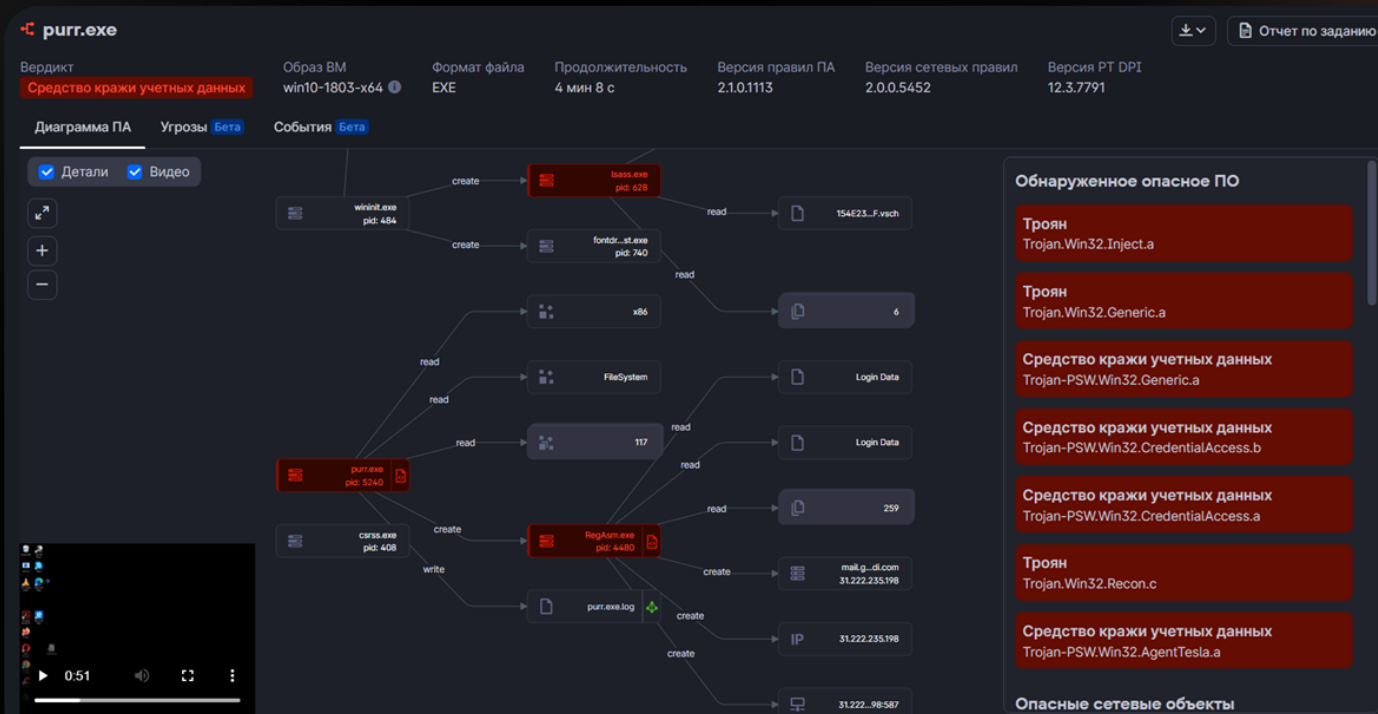
Запуск ВПО в обход антивирусных средств



1 Обнаруженное опасное поведение программы уже известно для результата проверки в песочнице и подкрепляется информацией о сетевых подключениях, которые подсвечены связанными индикаторами

2 Для сокрытия от антивирусов происходит инъекция в процесс. Легитимный services.exe запускается в приостановленном состоянии, вместо его легитимного кода в памяти загружается вредоносный код. Процесс возобновляется, но выполняет уже вредоносный код

3 После происходят этапы кражи учетных записей в LSASS и последующее применение штатного RegAsm.exe для отправки украденных данных



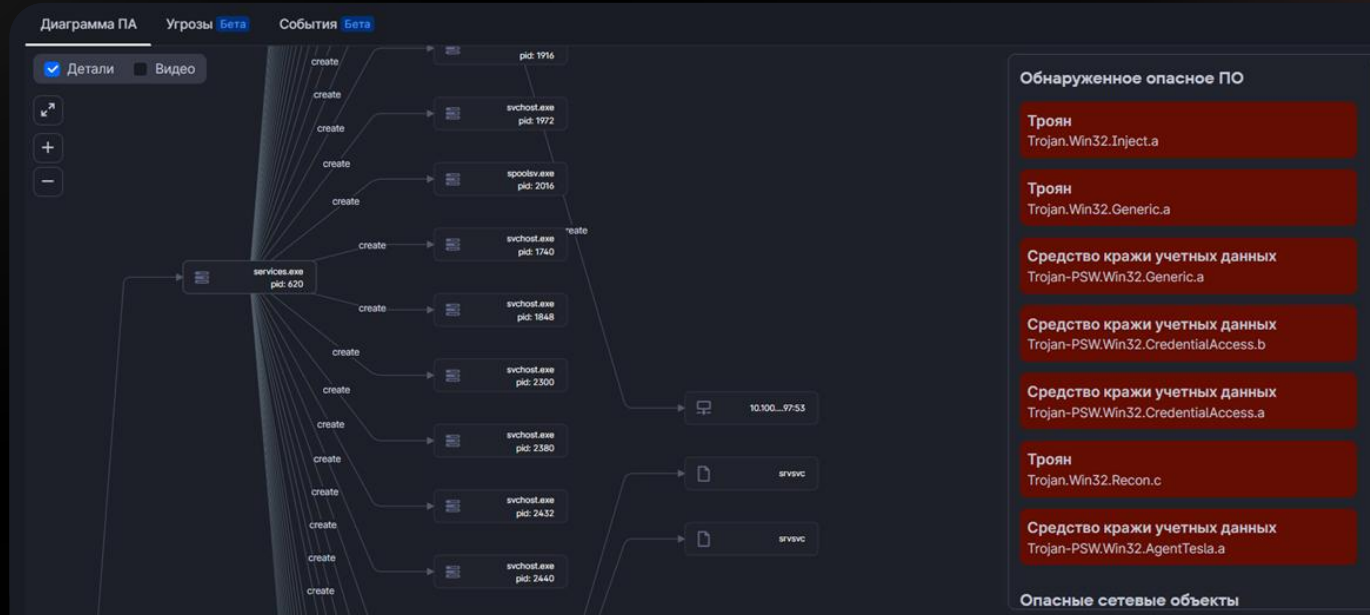
Запуск ВПО в обход антивирусных средств



1 Обнаруженное опасное поведение программы уже известно для результата проверки в песочнице и подкрепляется информацией о сетевых подключениях, которые подсвечены связанными индикаторами

2 Для скрытия от антивирусов происходит инъекция в процесс. Легитимный services.exe запускается в приостановленном состоянии, вместо легитимного кода в памяти загружается вредоносный код. Процесс возобновляется, но выполняет уже вредоносный код

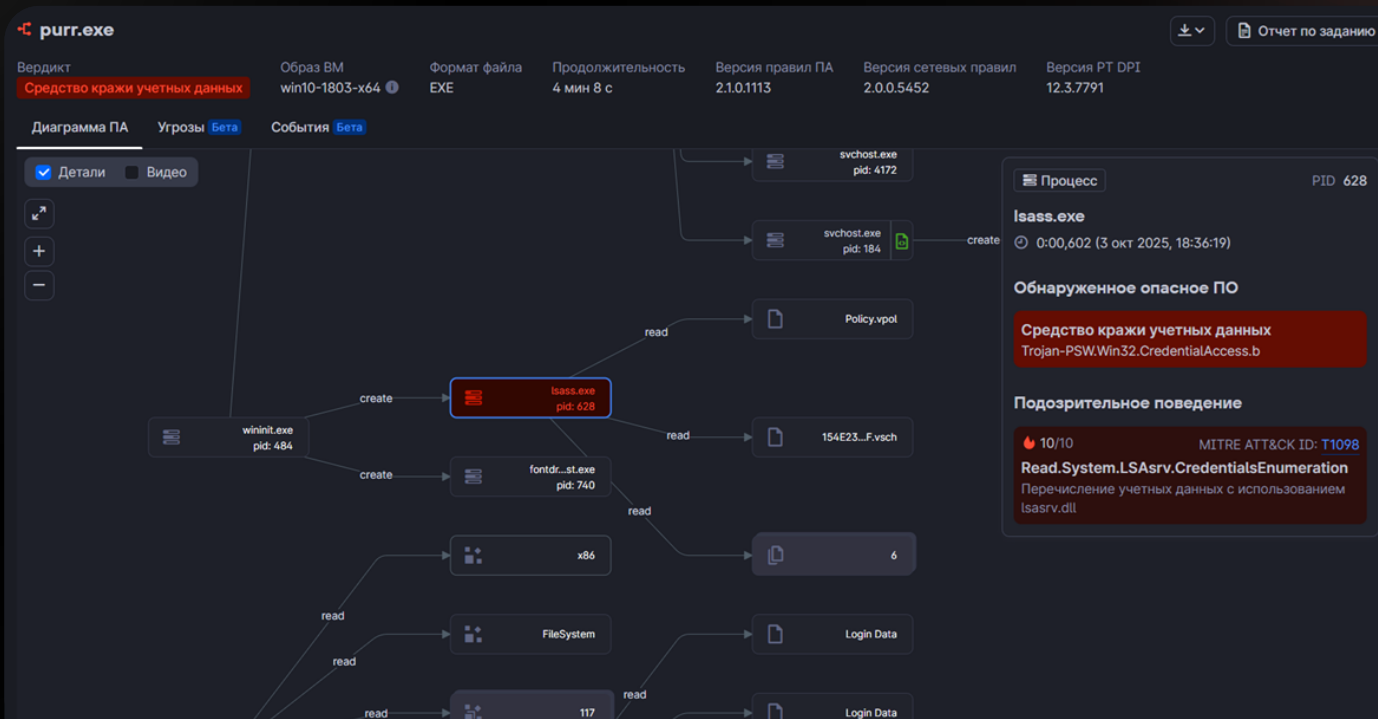
3 После происходят этапы кражи учетных записей в LSASS и последующее применение штатного RegAsm.exe для отправки украденных данных



Запуск ВПО в обход антивирусных средств



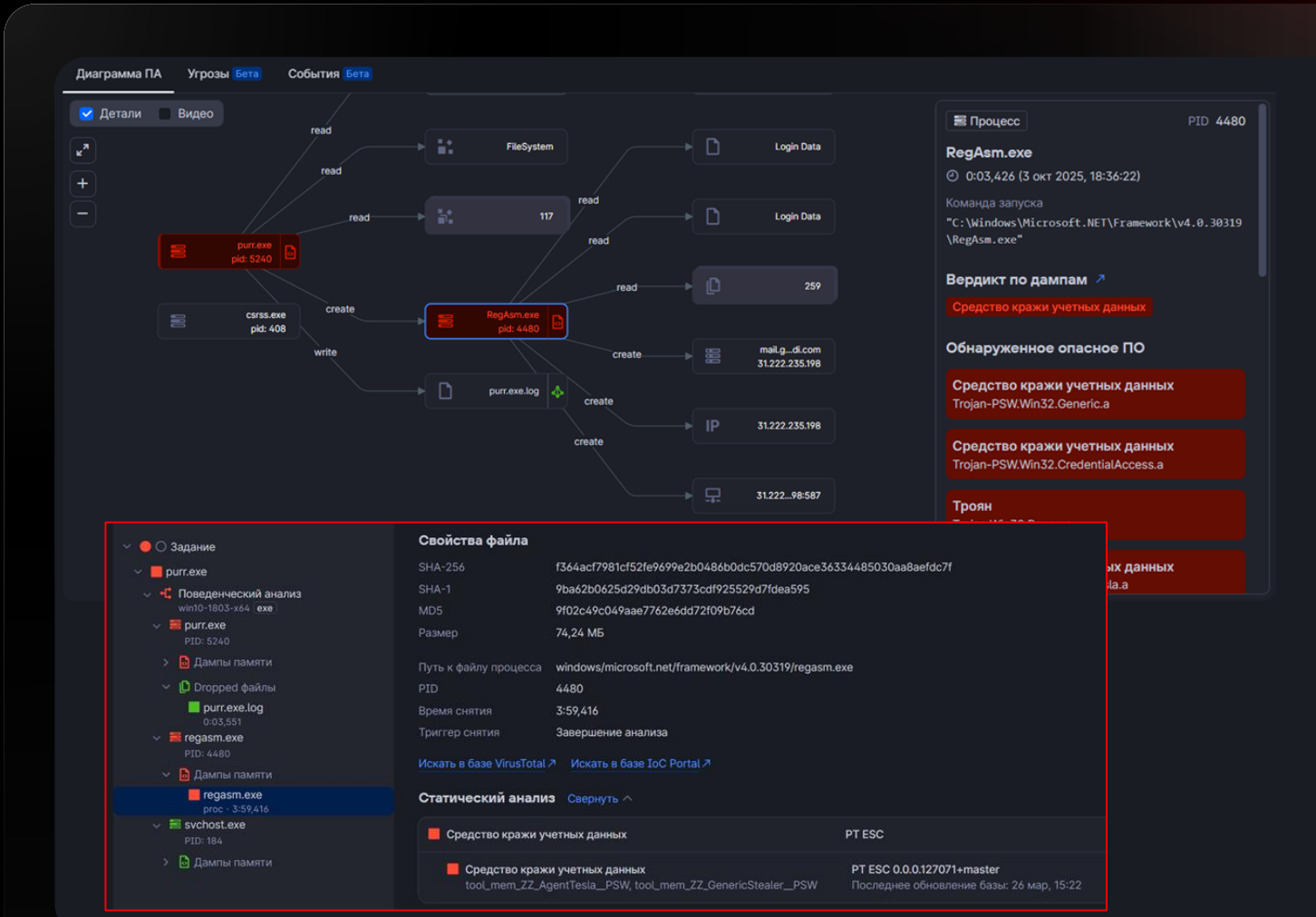
- 1 Обнаруженное опасное поведение программы уже известно для результата проверки в песочнице и подкрепляется информацией о сетевых подключениях, которые подсвечены связанными индикаторами
- 2 Для сокрытия от антивирусов происходит инъекция в процесс. Легитимный services.exe запускается в приостановленном состоянии, вместо его легитимного кода в памяти загружается вредоносный код. Процесс возобновляется, но выполняет уже вредоносный код
- 3 После происходят этапы кражи учетных записей в LSASS и последующее применение штатного RegAsm.exe для отправки украденных данных



Запуск ВПО в обход антивирусных средств



3 После происходят этапы кражи учетных записей в LSASS и последующее применение штатного RegAsm.exe для отправки украденных данных



Подробнее про PT Sandbox и PT Email Security можно узнать на стендах и по ссылкам

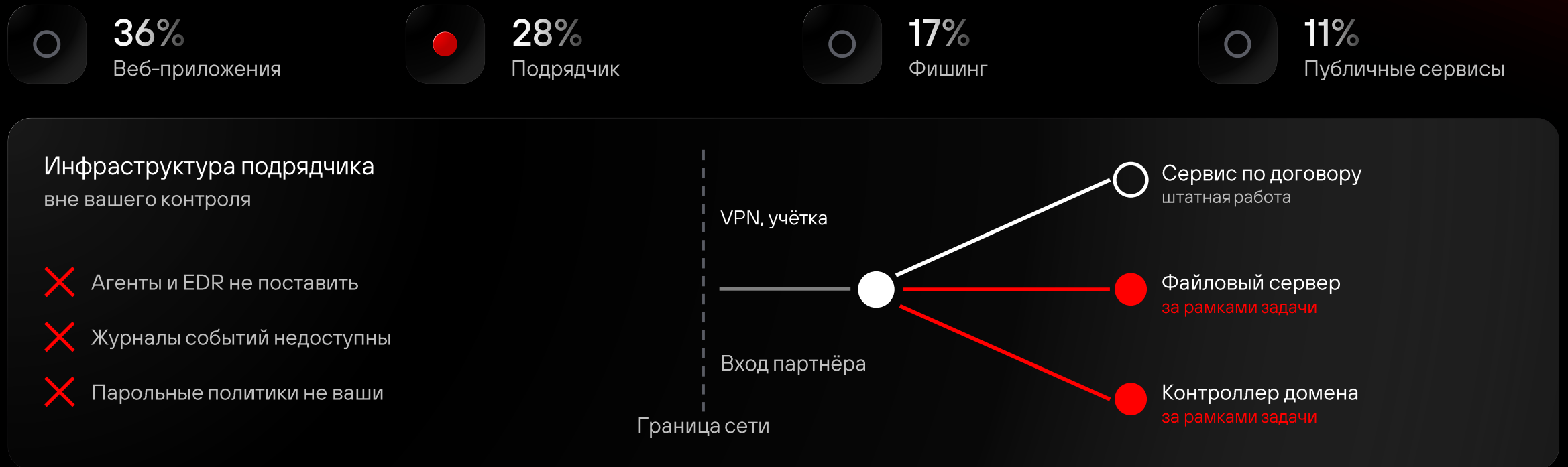


Про PT Sandbox



Про PT Email Security

Четыре двери в инфраструктуру



Единственная точка контроля — анализ трафика внутри вашей сети

Как работает PT NAD



Захватывает,
разбирает сетевой трафик
на периметре
и в инфраструктуре
с помощью технологии DPI

Исходная копия
сетевых трафика

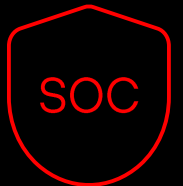


Видимость сети

Обнаружение хакера в сети

Аномалии

Контроль регламентов ИБ



С помощью статистических и поведенческих модулей обнаруживает активность злоумышленника **на самых ранних этапах проникновения в сеть**, а также во время попыток закрепиться в ней и развить атаку

Что закрывает PT NAD



Эксплуатация уязвимостей

Попытки пробить сервисы на периметре и внутри сети



Доступы подрядчиков

Куда ходит партнёр после подключения к сети



Горизонтальное перемещение

Разведка, удалённый запуск команд, атаки на AD



Каналы управления и утечки

Туннели в DNS и TLS, DGA-домены, вынос данных



Расследование инцидентов

Кто, куда и когда ходил — по сохранённым сессиям



Анализ поверхности атаки

Что открыто наружу и между сегментами



Инвентаризация

Реальная карта узлов, сервисов и связей

Методы анализа трафика



Классический

Глубокая
экспертиза

ML

PT ExpertCloud

Сигнатурный
анализ

Обнаружение новых
активов

Пользовательские
правила
профилирования

Сведения
об индикаторах

Репутационные
списки

Экспертные модули

Анализ зашифрованного
трафика

Проверка обнаружений

Интеграция
с Sandbox

Детектирование
приложений

Поиск DGA-доменов

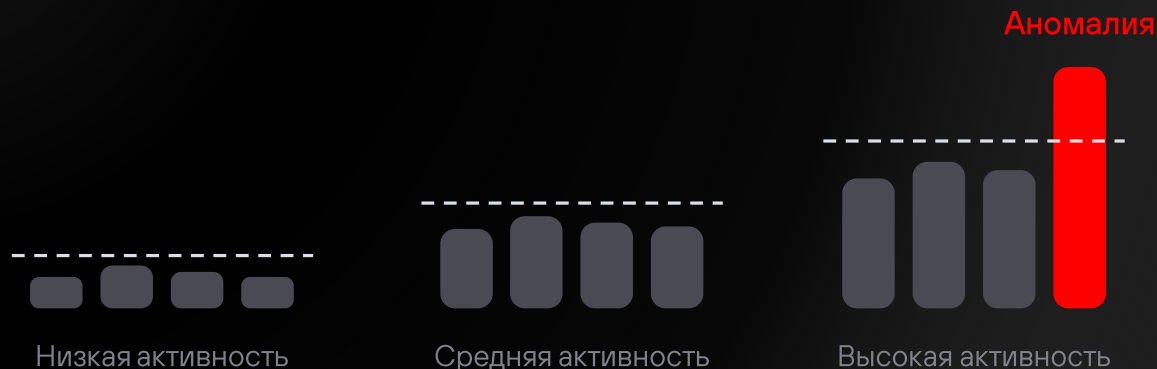
Облачные обнаружения

ML внутри PT NAD



Модель не знает, как «должно быть» вообще — она учится на вашей сети

Узлы группируются по профилю активности



Профилирование узлов

Новый узел попадает в кластер с низкой активностью — всплеск сразу заметен

Поведенческие детекты

Kerberoasting, DNS-туннели, удалённое выполнение команд, спреинг паролей

Домены, созданные машиной

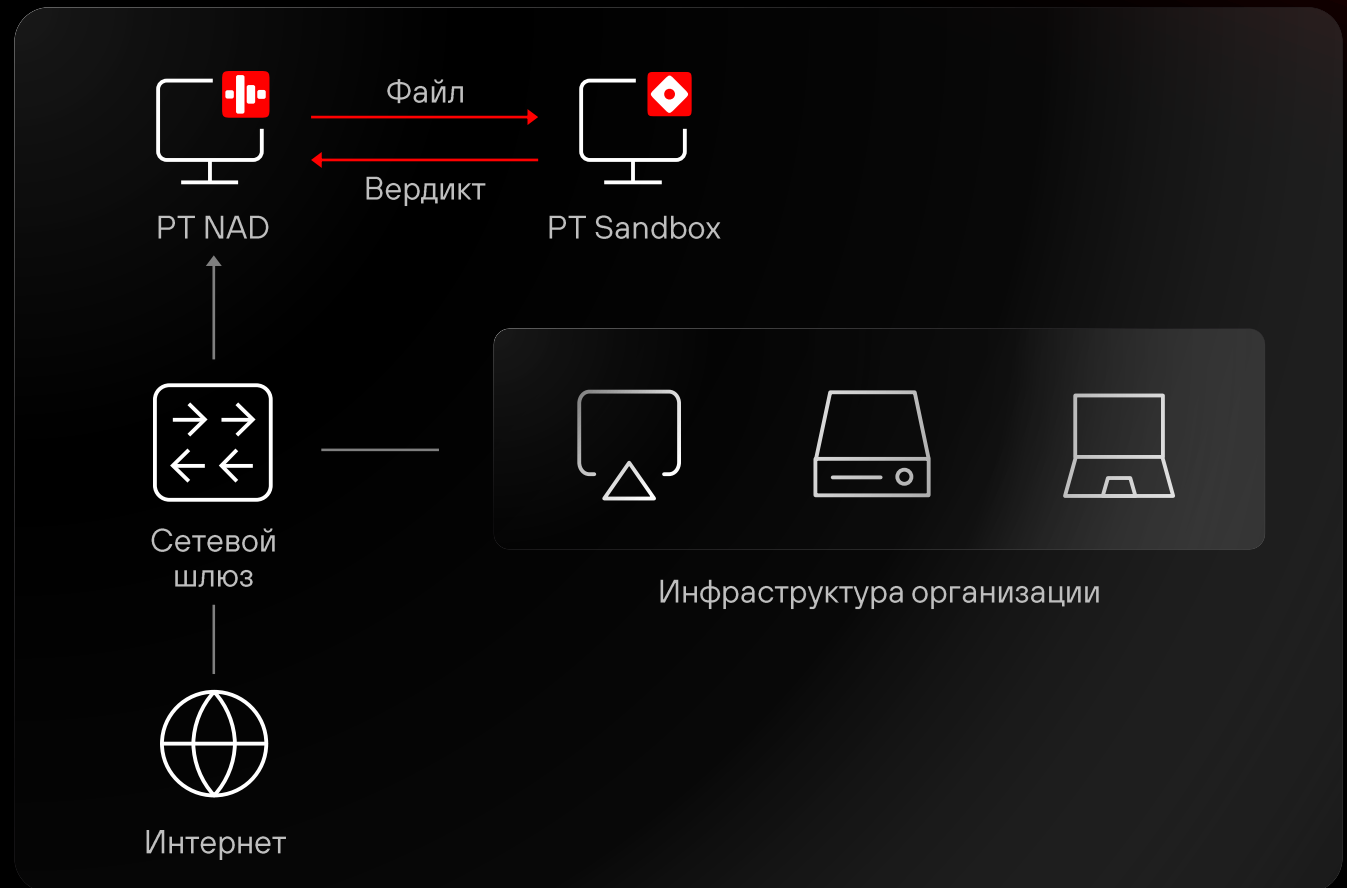
Распознавание DGA-имён для связи вредоноса с командным сервером

Пунктир — норма кластера:
аномалия считается от неё, а не от среднего по сети

PT NAD + PT Sandbox



- Обнаружение угроз
- Поиск следов компрометации
- Хранение контекста атаки
- Выявление ВПО
- Локализация угроз
- Защита актуальных каналов
- Выявление скрытых и новых угроз



Экспертиза внутри PT NAD



Основана на знании о реальных атаках

Ландшафт угроз и расследования
PT Expert Security Center, а не абстрактные правила

Приоритизирована

Уровни опасности отделяют критичное
от фонового шума

Объясняет себя

К каждому срабатыванию — описание,
чем это опасно, и рекомендации, что предпринять

ГЛАВНОЕ

Плейбук к срабатыванию

пошаговая инструкция оператора по верификации алерта

- 1 Что именно сработало и на каком узле
- 2 Какие поля сессии подтверждают атаку
- 3 Чем отличить легитимную активность администратора
- 4 Что проверить на стороне хоста и в смежных системах
- 5 Какие действия предпринять и когда эскалировать

Аналитик первой линии разбирает срабатывание сам:
экспертиза приходит вместе с алертом, а не хранится в голове у одного человека

Атака через подрядчика



Подрядчик приходит с легитимным доступом — атаку выдают только действия внутри сети

Доступ в неразрешенный сегмент сети



TA0001 — Initial Access

pt

NAD

PT NAD.1

Дашборды

Сессии

Атаки

Сетевые связи

Лента активности

Узлы

🔒 Доступ подрядчика в неразрешенный сегмент сети

Общие сведения

Пользовательский фильтр

Дополнительные данные

Общие сведения

Сессий больше 1 за 10 минут по фильтру Integrator Danger Traffic Flow.

Опасность

Высокая

Первая сессия

5 ноября, 12:10

Последняя сессия

6 ноября, 10:27

Длительность

22 ч 17 мин 5 с

Отслеживание

Включено

Обнаружена

5 ноября, 12:20

Данные дополнены

6 ноября, 10:30

Комментарий

Пользовательский фильтр

src.groups == "INTEGRATOR_SUBNET" && dst.groups != "SERVICE_SUBNET"

Дополнительные данные

TOP('src.ip', 10)	TOP('app_proto')	TOP('dst.ip')	TOP('credentials.login')
10.125.124.26 ⓘ	http	10.158.3.2 ⓘ	—

Сканирование локальной сети



TA0007 — Discovery

Общие сведения

Протоколы
[tcp](#) → [unknown](#)

Начало
21 августа 2026, 11:49:49

Конец
21 августа 2026, 11:49:57

Длительность
[7 секунд, 815 миллисекунд](#)

Отправлено
234.48 КБ, 3 908 пакетов

Получено
234.48 КБ, 3 908 пакетов

Сессии
3908 (500 в секунду)

Хранилище
[public-release](#)

Отправитель

[H13102](#) ⓘ
[192.168.88.237:2616](#)
📁 [HOME_NET](#)



Получатель

[H7533](#) ⓘ
[192.168.88.235](#)
📁 [HOME_NET](#)
3 908 портов:
[1093 — 5000](#)

Атаки

■ [\[ANOMALY\] \[PTsecurity\] TCP SYN scan](#)

Все атаки (1) ▾

Атаки (1)

■ [\[ANOMALY\] \[PTsecurity\] TCP SYN scan](#)

Обнаружена 21 августа 2026, 11:49:50

SID [13000014](#) Ревизия 1

Класс [Unknown Traffic](#)

[Показать еще](#) ▾

Разведка домена



TA0007 – Discovery

Общие сведения

Обнаружена	21 августа 2026, 10:38:10	Тактики и техники АТТ&СК
Название	ATTACK AD [PTsecurity] LDAP enum user group membership	Discovery
Опасность	■ Средняя	Account Discovery
SID	10005705	
Ревизия	2	
Класс	Information leak attempt	

Атакующий узел
H846
10.0.52.130
HOME_NET



Атакуемый узел
H2
10.0.52.101
dc1-dc-01.ptsecurity.ru
HOME_NET

Описание и рекомендации

Описание	Попытка получения информации о членстве пользователя в группах домена от контроллера домена с помощью протокола LDAP, позволяющего получать доступ к информационным службам распределенных каталогов. Данная информация может использоваться злоумышленниками при выборе цели для атаки.
Рекомендации	Проверьте список доменных служб и выясните, какие из них могут отправлять подобные LDAP-запросы. Если такие службы не обнаружены или владелец узла не является администратором, то данная активность может означать этап сбора данных злоумышленниками.
Плейбук	Посмотреть

Использование утилит администрирования



TA0008 — Lateral Movement

Общие сведения

Обнаружена 21 августа 2026, 09:37:20
Название [ATTACK AD \[PTsecurity\] PSEXEC tool usage](#)
Опасность ■ Высокая
SID [10002263](#)
Ревизия 4
Класс [Active Directory exploitation attributes](#)

Тактики и техники ATT&CK

[Lateral Movement](#)
[Lateral Tool Transfer](#)

Атакующий узел
[H4231](#) ⓘ
[10.0.177.160](#)
 [HOME_NET](#)



Атакуемый узел
[H3768](#) ⓘ
[10.0.176.67](#)
 [HOME_NET](#)

Описание и рекомендации

Описание Использование средства администрирования PSEXEC, позволяющего удаленно выполнять команды. Данный инструмент активно используется как администраторами, так и злоумышленниками.
Рекомендации Проверьте список выполненных команд и легитимность удаленного выполнения команд данным узлом.

Туннелирование трафика



TA0011 — Command and Control

Общие сведения

Обнаружена	21 августа 2026, 05:17:22	Тактики и техники ATT&CK
Название	TOOLS [PTsecurity] Chisel HTTP Tunnel Tool Connection Attempt	Command and Control
Опасность	■ Высокая	Web Protocols
SID	10014678	
Ревизия	1	
Класс	Exploitation attributes	
Вредоносное ПО	Chisel	

Атакующий узел
H47 ⓘ
192.168.235.100
🔗 HOME_NET



Атакуемый узел
H16 ⓘ
192.168.235.101
🔗 HOME_NET

Описание и рекомендации

Описание	Обнаружен HTTP-заголовок, специфичный для Chisel. Chisel — это инструмент, с помощью которого можно создавать туннели для передачи данных различных протоколов внутри SSH-соединения поверх сообщений HTTP и WebSocket. Данный инструмент может использоваться в сети как легитимно, так и злоумышленниками (его применение было отмечено во время расследования нескольких инцидентов).
Рекомендации	Проверьте легитимность использования Chisel в вашей сети. Проверьте сетевую активность, срабатывание других правил для рассматриваемых узлов, а также наличие обращений к вредоносным ресурсам (IP-адресам или доменам).
Плейбук	Посмотреть
См. также	github.com/jpillora/chisel

Управление скомпрометированной машиной



TA0002 — Execution

Общие сведения

Протоколы
[tcp](#) → [smb](#)

Начало
21 августа 2026, 00:57:37

Конец
21 августа 2026, 00:57:37

Длительность
[224 миллисекунды](#)

Отправлено
13.28 КБ, 85 пакетов

Получено
156.84 КБ, 139 пакетов

Хранилище
[public-release](#)

Отправитель

[H53](#) ⓘ
[172.16.164.1:52628](#)
[00:50:56:C0:00:01](#)
📁 [HOME_NET](#)
🐧 [Linux](#)



Получатель

[H172](#) ⓘ
[172.16.164.130:445](#)
[00:0C:29:36:6E:DD](#)
📁 [HOME_NET](#)
🖥️ [Microsoft Windows NT 6 or newer](#)

Атаки

- [ATTACK AD \[PTsecurity\] SMB Remote task start via xml](#)
- [SHELL \[PTsecurity\] Windows DIR tool output](#) 📄
- [ATTACK AD \[PTsecurity\] DCERPC Remote job add via TaskSche...](#)

Все атаки (4) ▾

Файлы

📄 [ChXORspT.tmp](#) ↓ 📄 143,35 КБ
[\\172.16.164.130\ADMIN\\$\Temp\](#)

Все файлы (1) ▾

Именованные каналы

[atsvc](#) ↑ 3,7 КБ ↓ 484 Б
[\\172.16.164.130\IPC\](#)

Учетные записи

Логин
🟢 [CONTOSO\user02](#)

Внедрение в инфраструктуру



TA0003 – Persistence

T0 + 85mc	DCE_RPC_REQUEST	ExecMethod	DCE_RPC_RESPONSE
	cmd	cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN\$_1593447672.03 2>&1	result success
	method	Create	
	object_path	Win32_Process	
	path	C:\	
T0 + 110mc	DCE_RPC_REQUEST	ExecMethod	DCE_RPC_RESPONSE
	cmd	cmd.exe /Q /c ipconfig 1> \\127.0.0.1\ADMIN\$_1593447672.03 2>&1	result success
	method	Create	
	object_path	Win32_Process	
	path	C:\	
T0 + 170mc	DCE_RPC_REQUEST	ExecMethod	DCE_RPC_RESPONSE
	cmd	cmd.exe /Q /c net localgroup administrators yev /add 1>	result success
	method	Create	
	object_path	Win32_Process	
	path	C:\	

Вынос данных из инфраструктуры



TA0040 — Impact

ППП Аномальная выгрузка данных на облачные сервисы

Общие сведения

Пользовательский фильтр

Информация о клиенте

Превышение порога
срабатывания правила

Дополнительные данные

Общие сведения

Обнаружено превышение объема исходящего трафика в сессиях с клиентом 10.8.15.212 по фильтру Cloud Storage Services.

Опасность ■ Средняя

Первая сессия 26 июля, 14:54

Последняя сессия 26 июля, 15:26

Длительность 31 мин 57 с

Обнаружена 26 июля, 15:31

Чувствительность
правила Средняя

Комментарий



Пользовательский фильтр

```
app_service in ["Yandex.disk", "DropBox", "GoogleDrive", "MS_OneDrive"]
```





Точно выявляет сложные сетевые атаки и сокращает время обнаружения хакеров **до одного часа**



Упрощает расследование инцидентов и показывает слабые точки в сети



Сокращает время реагирования на приоритетные угрозы

Результат

Сокращает время присутствия злоумышленника в сети **до считанных минут**



День ТризТех Звезда родилась

тризтех⁺

pt

Первое мероприятие ТризТех
о новом сетевом вендоре,
больших планах, реальных
проектах и том, что происходит
с сетевой безопасностью
в России прямо сейчас

24 сентября в 10:30
Бесплатная онлайн-трансляция



Ещё больше о
PT NGFW здесь:



Канал ТризТех



Марафон PT NGFW



Задай
вопрос
спикеру





Спасибо!