



## Константин Рудаков

Руководитель направления  
по развитию продуктов для защиты  
от целевых атак



## Владимир Клепче

Архитектор продуктов  
для информационной безопасности

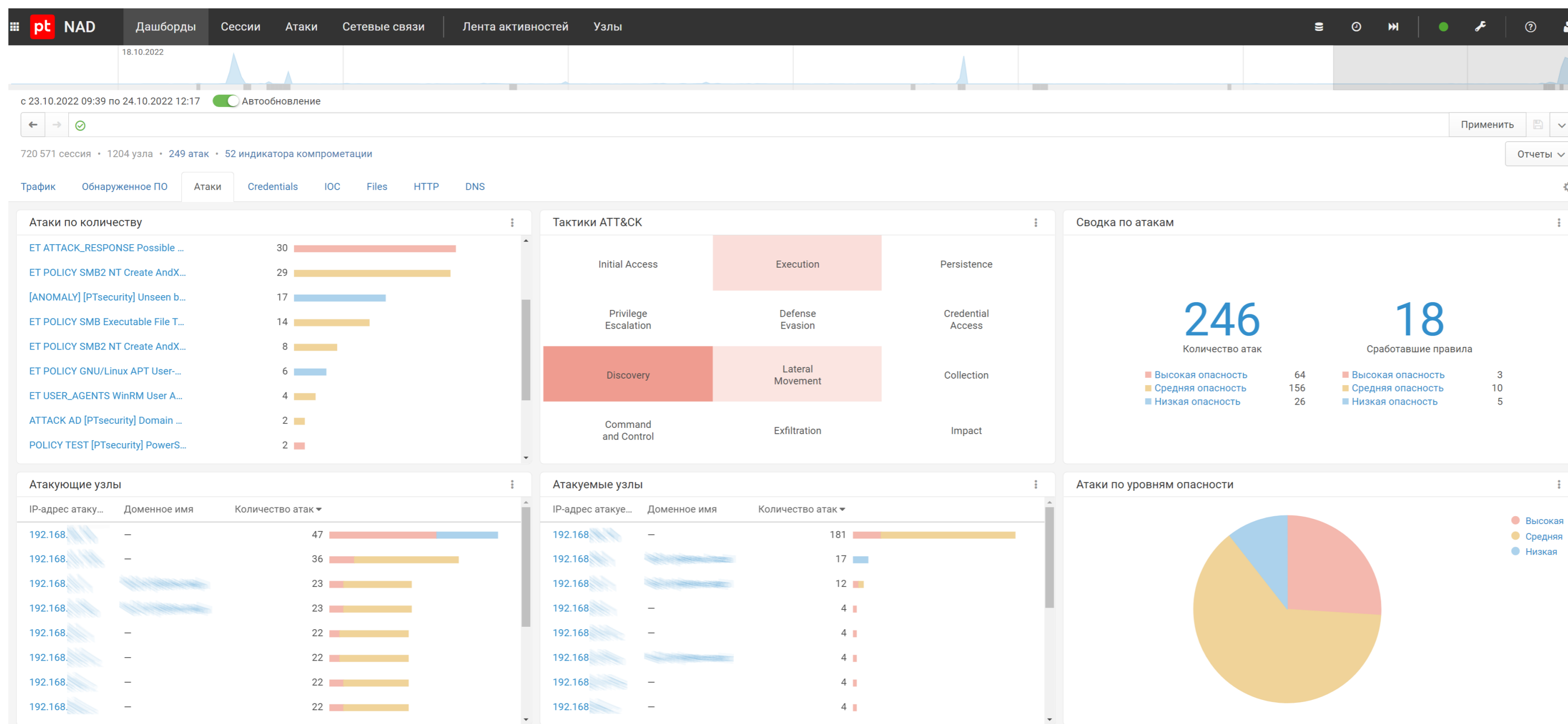


# PT Network Attack Discovery 11.1

# PT Network Attack Discovery



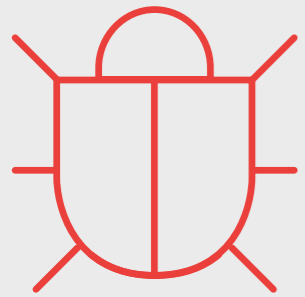
Система поведенческого анализа сетевого трафика для выявления атак на периметре и внутри сети



Дашборды  
PT NAD



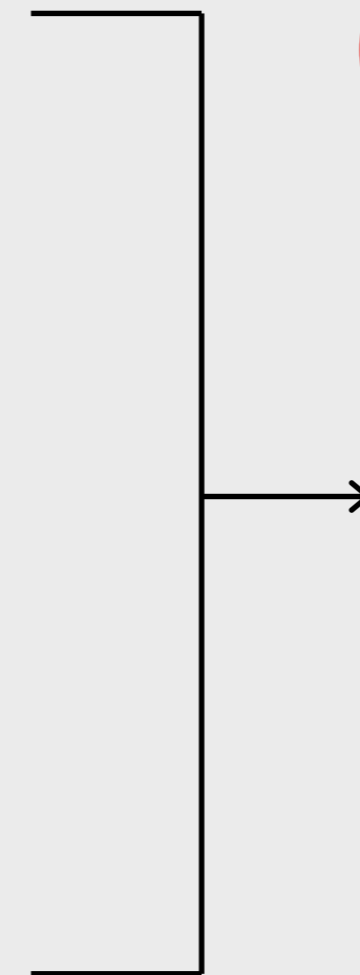
Выявляет целевые атаки  
на периметре и внутри сети



Обнаруживает  
скрытые угрозы



Проверяет сетевую  
активность узлов



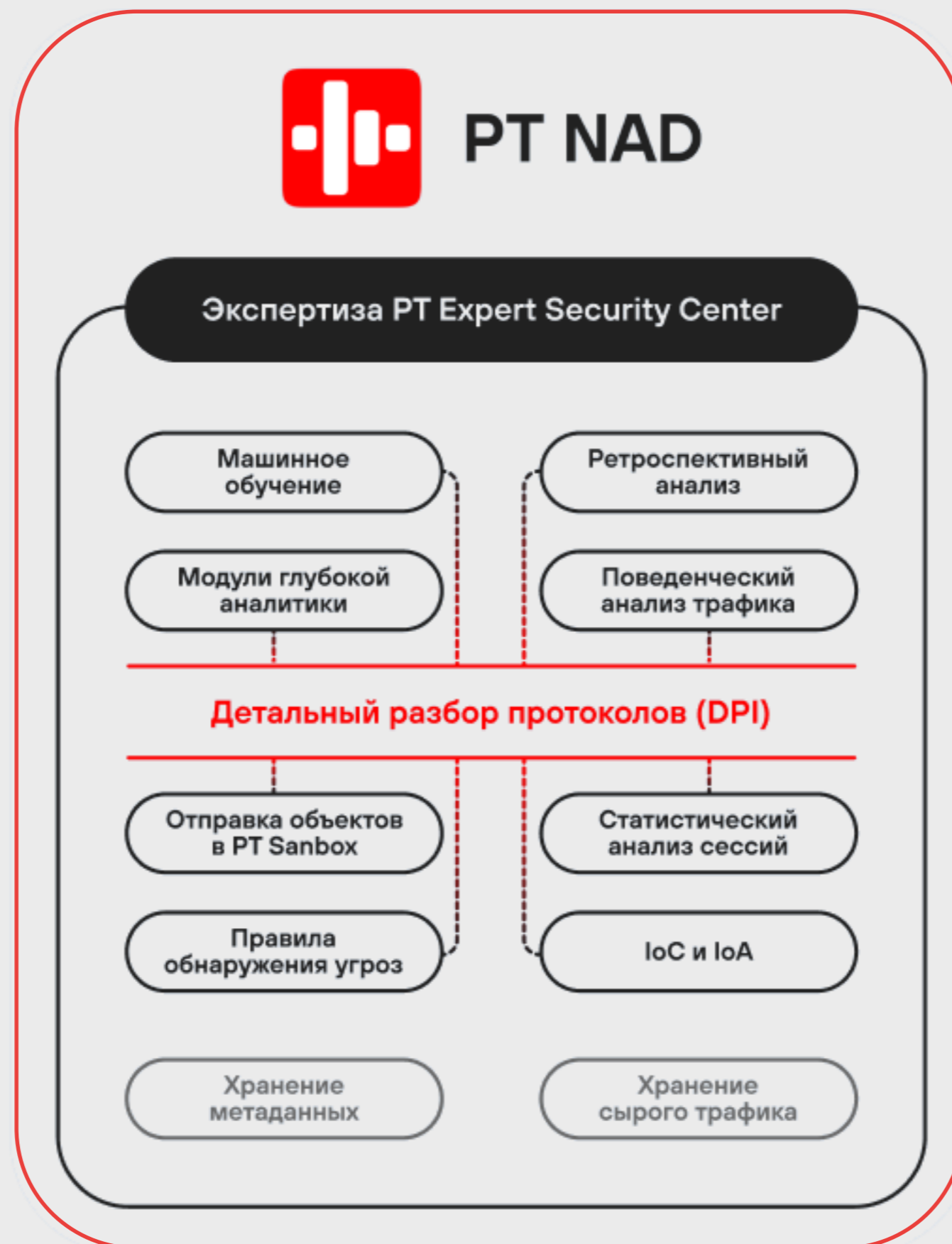
**Результат**

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

# Как работает PT NAD



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



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





# PT NAD 11.1. Новые способы обнаружения атак



Обнаружение  
ICMP-туннелей

Обнаружение  
подозрительной активности  
в трафике SMB



PT NAD

Обнаружение  
использования  
фреймворков Cobalt Strike  
и Brute Ratel C4

Обнаружение успешной  
эксплуатации  
уязвимостей

Обнаружение новых  
оповещений



# PT NAD 11.1. Новые способы обнаружения атак



## Обнаружение ICMP-туннелей

Протоколы [icmp, icmp](#)

Начало 18 мая 2023, 15:15:50

Конец 18 мая 2023, 15:15:54

Длительность 4 секунды

Отправлено 3 КБ, 28 пакетов

Получено 6 КБ, 56 пакетов

Отправитель [H350613](#) ⓘ

[HOME\\_NET](#)

Получатель [H78875](#) ⓘ

[HOME\\_NET, WIFI\\_GUEST](#)

Хранилище [ptdpi](#)

**Атаки**

- ATTACK [PTsecurity] An ICMP tunnel was found
- Tunneling Traffic was Detected

---

**ICMP**

0	echo	data_len	56	echoreply	data_len	56
		ttl	65			
0	—			echoreply	data_len	56
0	echo	data_len	57	echoreply	data_len	57
		ttl	65			
0	—			echoreply	data_len	57
0	echo	data_len	58	echoreply	data_len	58
		ttl	65			



# PT NAD 11.1. Новые способы обнаружения атак



**PT NAD** обнаруживает  
установление ICMP-туннелей  
по накопленным  
статистическим данным  
пакетов ICMP

**Модуль позволяет** выявлять  
любые хакерские  
инструменты

## < Обнаружен туннель ICMP

### Общие сведения

Информация об узле

Клиенты

Описание и рекомендации

### Общие сведения

Обнаружен ICMP туннель по адресу [REDACTED].

Опасность ■ Высокая

Первая сессия 18 мая, 15:15

Последняя сессия 18 мая, 15:15

Длительность 5 с

Отслеживание Включено

Обнаружена 18 мая, 16:14

### Информация об узле

Узел [H78875](#) ⓘ

IP-адрес [REDACTED] ⓘ

Группы HOME\_NET, WIFI\_GUEST



# PT NAD 11.1. Новые способы обнаружения атак



Обнаружение  
ICMP-туннелей

**Обнаружение  
подозрительной активности  
в трафике SMB**



**PT NAD**

Обнаружение  
использования  
фреймворков Cobalt Strike  
и Brute Ratel C4

Обнаружение успешной  
эксплуатации  
уязвимостей

Обнаружение новых  
оповещений





# PT NAD 11.1. Новые способы обнаружения атак



Выявление зашифрованного SMB-трафика



Обнаружение неизвестных пайпов SMB

Злоумышленники могут скрывать свою активность внутри зашифрованных SMB-пакетов

Если узел неожиданно начнет использовать зашифрованную версию протокола SMB, **PT NAD ЭТО ВЫЯВИТ**



# PT NAD 11.1. Новые способы обнаружения атак



## Выявление зашифрованного SMB-трафика

src.host\_id == H331508 && smb.rqs.command == ENCRYPTED

Общий трафик 44,00 КБ · Отправлено 23,19 КБ · Получено 20,81 КБ · Средняя скорость трафика 12 Б/с

20:25:00 20:30:00 20:35:00 20:40:00 20:45:00 20:50:00 20:55:00 21:00:00 21:05:00 21

10.31.48.29:56824 → 10.0.180.142:445

Общие сведения		NTLM 0.12, SMB 2.002, SMB 2.???	DFS, LEASING, LARGE_MTU
NTLM		]	]
SMB			dialect 2.1.???
Расширенные сведения			security_mode SIGN_ENABLED
			server_guid 56BE0D04-ADFB-4F22-A9F6-4218B3F0F369
			server_start_time 2023-05-22T23:55:08.964121
			server_time 2023-05-23T00:21:46.084522
Tree_id	0x0000		
Negotiate_protocol		success	
Encrypted		-	



## Выявление зашифрованного SMB-трафика

< Зашифрованный SMB-трафик

<b>Общие сведения</b>	<b>Общие сведения</b>	
Информация об узле	Зафиксирован аномальный зашифрованный SMB-трафик с узла <a href="#">10.31.48.29</a> .	
Серверы	Опасность <span style="color: red;">■</span> Высокая	Комментарий
Описание и рекомендации	Первая сессия 22 мая, 20:21	<div style="border: 1px solid #ccc; height: 100px;"></div>
	Последняя сессия 22 мая, 20:22	
	Длительность 15 с	
	Отслеживание Включено	
	Обнаружена 22 мая, 20:24	
	<b>Информация об узле</b>	
	Узел <a href="#">H331508</a> ⓘ	
	IP-адрес 10.31.48.29 ⓘ	
	Группы HOME_NET, TEST	



# PT NAD 11.1. Новые способы обнаружения атак



Выявление зашифрованного SMB-трафика



Обнаружение неизвестных пайпов SMB

Именованные каналы SMB (пайпы) могут использоваться инструментами атакующих и вредоносным ПО для коммуникации с агентами  
PT NAD определяет новые пайпы SMB в сети



# PT NAD 11.1. Новые способы обнаружения атак



## Обнаружение неизвестных пайпов SMB

The screenshot displays the PT NAD interface for a detected SMB pipe. At the top, a search bar contains the filter `pipes.name == "vgauth-service"`. Below it, a traffic summary shows: "Общий трафик 3,98 КБ · Отправлено 2,06 КБ · Получено 1,92 КБ · Средняя скорость трафика 1 Б/с". A timeline graph shows traffic starting at 20:15:00 and ending at 20:15:00. The connection details are: `10.31.48.29:56482 → 10.0.180.142:445`.

The interface is divided into two main sections: "Общие сведения" (General information) and "Расширенные сведения" (Advanced information). The "Общие сведения" section includes:

- Протоколы: smb, tcp
- Начало: 22 мая 2023, 20:11:35
- Конец: 22 мая 2023, 20:11:35
- Длительность: 0 секунд
- Отправлено: 2 КБ, 12 пакетов
- Получено: 2 КБ, 13 пакетов
- Отправитель: H331508 (10.31.48.29:56482, 54:7F:EE:65:2F:BC, HOME\_NET, TEST, Microsoft Windows NT 6 or newer)
- Получатель: H96487 (10.0.180.142:445, 00:50:56:AF:4D:FC)

The "Расширенные сведения" section includes:

- Именованные каналы: `vgauth-service` (↑ 72 Б ↓ 0 Б), `\\10.0.180.142\IPC$`
- Учетные записи: Administrator (checked)



# PT NAD 11.1. Новые способы обнаружения атак



## Обнаружение неизвестных пайпов SMB

< Неизвестный именованный канал SMB

Общие сведения

Соединения

Описание и рекомендации

**Общие сведения**

Обнаружено SMB-соединение с обращением к именованному каналу **vgauth-service**.

Опасность ■ Средняя

Первая сессия 22 мая, 20:11

Последняя сессия 22 мая, 20:11

Длительность 1 с

Отслеживание Включено

Обнаружена 22 мая, 20:15

Данные дополнены 22 мая, 20:38

Комментарий

**Соединения**

Клиент	IP-адрес кл...	Домен кли...	Группы кли...	Сервер	IP-адрес се...	Домен сер...	Учетные за...	Первая сес...	Последн...
H331508...	10.31.48...	—	HOME_NE...	H96487 ⓘ	10.0.180...	—	Administr...	22 мая, 2...	22 мая, 2...



# PT NAD 11.1. Новые способы обнаружения атак



Обнаружение  
ICMP-туннелей

Обнаружение  
подозрительной активности  
в трафике SMB



PT NAD

Обнаружение  
использования  
фреймворков Cobalt Strike  
и Brute Ratel C4

Обнаружение успешной  
эксплуатации  
уязвимостей

Обнаружение новых  
оповещений



# PT NAD 11.1. Новые способы обнаружения атак



## Обнаружение использования Cobalt Strike и Brute Ratel C4\*

PT NAD обнаруживает маяки и агенты по периодическим HTTP-запросам к управляющему серверу (C2), которые используются для взаимодействия, получения команд и предоставления отчета о результатах их выполнения



[Ищем иголку вредоносных запросов в стоге трафика: PT NAD vs. Cobalt Strike и Brute Ratel C4](#)

\* Cobalt Strike и Brute Ratel C4 — фреймворки для постэксплуатации зараженных систем





## Обнаружение использования Cobalt Strike и Brute Ratel C4

### < Использование Cobalt Strike

#### Общие сведения

Сервер

Клиенты

Описание и рекомендации

#### Общие сведения

Обнаружена активность Cobalt Strike при обращении к серверу 

Опасность ■ Высокая

Первая сессия 29 марта, 16:05

Последняя сессия 6 апреля, 19:40

Длительность 8 д 3 ч 34 мин 59 с

Отслеживание Включено

Обнаружена 29 марта, 16:08

Данные дополнены 6 апреля, 19:40

Комментарий

#### Сервер

Узел [H96487](#) ⓘ

IP-адрес  ⓘ



# PT NAD 11.1. Новые способы обнаружения атак



## Обнаружение использования Cobalt Strike и Brute Ratel C4

**Общие сведения**

Протоколы http, tcp  
 Начало 29 марта 2023, 16:54:43  
 Конец 29 марта 2023, 16:55:14  
 Длительность 30 секунд  
 Отправлено 907 Б, 8 пакетов  
 Получено 4 КБ, 8 пакетов  
 Отправитель H331508  
 10.31.48.29:53804  
 54:7F:EE:5B:F0:C1  
 HOME\_NET, ...  
 Microsoft Windows NT 6 or newer  
 Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2...  
 Получатель H96487  
 10.0.180.142:80  
 00:50:56:AF:4D:FC  
 HOME\_NET  
 Linux  
 Apache/2.2.22 (Ubuntu)  
 Хранилище ptdpi-52

**Атаки**

- TOOLS [PTsecurity] Cobalt Strike HTTP activity  
 Exploitation Attributes was Detected

**Файлы**

- manual.cfg.bat 3.06 КБ

---

**HTTP**

29.03.23 16:54:43	GET	/manual.cfg.bat example.com	0 Б	OK 200	application/x-msdos-program	3.06 КБ EXE
----------------------	-----	--------------------------------	-----	-----------	-----------------------------	----------------

```

accept */*
cache-control no-cache
connection Keep-Alive
cookie SESSIONID=LZ92X7OzyjXNPIuk8JKLYuNAfykphsgAk7W-VjJAWwMOHYTeczi6nuV7LJ0x_HVJiVoQyr4oqVfLsMfLc858kCktw_pRL-uYsigbl6hejoFyMR7SookaZzGihJTEZ222KxbWY4mZa4AfeGSybhJyrscq_TkgdXqHC11IKfTrgc
host example.com
user-agent Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729
accept-ranges bytes
connection Keep-Alive
content-length 3061
content-type application/x-msdos-program
date Wed, 29 Mar 2023 13:54:43 GMT
etag 41fc-e159-5a011b5f258c0
last-modified Thu, 05 Mar 2020 01:46:51 GMT
server Apache/2.2.22 (Ubuntu)
keep-alive timeout=5, max=100
  
```



# PT NAD 11.1. Новые способы обнаружения атак



Обнаружение  
ICMP-туннелей

Обнаружение  
подозрительной активности  
в трафике SMB



PT NAD

Обнаружение  
использования  
фреймворков Cobalt Strike  
и Brute Ratel C4

**Обнаружение успешной  
эксплуатации  
уязвимостей**

Обнаружение новых  
оповещений



## Обнаружение успешной эксплуатации уязвимостей

PT NAD автоматически извлекает индикаторы компрометации из сетевых запросов и проверяет факты обращения к ним

### < Успешная эксплуатация уязвимости

#### Общие сведения

Атакующий узел

Атакуемый узел

Сработавшие правила

Обнаруженные команды

Обращения к IOC

Описание и рекомендации

#### Общие сведения

Нарушитель, используя узел [10.31.48.29](#), успешно проэксплуатировал уязвимость на узле [10.0.180.142](#) с использованием индикатора компрометации [5.6.7.8:1389](#).

Опасность ■ Высокая

Первая сессия 22 мая, 18:39

Последняя сессия 22 мая, 18:44

Длительность 5 мин 1 с

Отслеживание Включено

Обнаружена 22 мая, 19:03

Комментарий



# PT NAD 11.1. Новые способы обнаружения атак



## Обнаружение успешной эксплуатации уязвимостей

dst.ip == '5.6.7.8' && dst.port == 1389 || (src.host\_id == 'H331508' && dst.host\_id == 'H96487' && alert.sid in [2034647, 2034649, 2034700, 2034757, 2034759, 2034800, 10006902, 2034661, 2034783, ...])

Общий трафик 4,71 КБ · Отправлено 608 Б · Получено 4,11 КБ · Средняя скорость трафика 648 Б/с

10.31.48.29:58620 → 10.0.180.142:80

Категория	Содержимое
Общие сведения	<p>Протоколы: http, tcp</p> <p>Начало: 22 мая 2023, 18:39:36</p> <p>Конец: 22 мая 2023, 18:39:36</p> <p>Длительность: 0 секунд</p> <p>Отправлено: 608 Б, 8 пакетов</p> <p>Получено: 4 КБ, 8 пакетов</p> <p>Отправитель: H331508 (10.31.48.29:58620, 54:7F:EE:65:2F:BC) - HOME_NET, TEST, Microsoft Windows NT 6 or newer, curl/7.68.0</p> <p>Получатель: H96487 (10.0.180.142:80, 00:50:56:AF:4D:FC) - HOME_NET, QA, Linux, SimpleHTTP/0.6 Python/3.11.1</p> <p>Хранилище: ptdpi-52</p>
Атаки	<ul style="list-style-type: none"> <li>ET EXPLOIT Apache log4j RCE Attempt (http ldap) (CVE-2021-44228) - Attempted Administrator Privilege Gain</li> <li>ET EXPLOIT Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228) - Attempted Administrator Privilege Gain</li> <li>ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (CVE-2021-44228) - Attempted Administrator Privilege Gain</li> <li>ET EXPLOIT Apache log4j RCE Attempt (http ldap) (Outbound) (CVE-2021-44228) - Attempted Administrator Privilege Gain</li> <li>ET EXPLOIT Apache log4j RCE Attempt (tcp ldap) (Outbound) (CVE-2021-44228) - Attempted Administrator Privilege Gain</li> <li>ET EXPLOIT Apache log4j RCE Attempt - lower/upper TCP Bypass M2 (Outbound) (CVE-2021-44228) - Attempted Administrator Privilege Gain</li> <li>ATTACK [PTsecurity] log4j RCE aka Log4Shell TCP attempt (CVE-2021-44228) - Attempted Administrator Privilege Gain</li> <li>ET INFO Possible Apache log4j RCE Attempt - Any Protocol TCP (CVE-2021-44228) - Misc Activity</li> </ul>



# PT NAD 11.1. Новые способы обнаружения атак



## Обнаружение успешной эксплуатации уязвимостей

### < Успешная эксплуатация уязвимости

Общие сведения

Атакующий узел

Атакуемый узел

Сработавшие правила

Обнаруженные команды

Обращения к IOC

Описание и рекомендации

#### Атакуемый узел

Узел [H96487](#) ⓘ  
IP-адрес 10.0.180.142 ⓘ  
Группы HOME\_NET, QA

#### Сработавшие правила

Опасность	Название ▲	Класс
■	ATTACK [PTsecurity] log4j RCE aka Log4Sh...	Attempted Administrator Privilege Gain
■	ET EXPLOIT Apache log4j RCE Attempt - lo...	Attempted Administrator Privilege Gain
■	ET EXPLOIT Apache log4j RCE Attempt - lo...	Attempted Administrator Privilege Gain



# PT NAD 11.1. Новые способы обнаружения атак



Обнаружение  
ICMP-туннелей

Обнаружение  
подозрительной активности  
в трафике SMB



PT NAD

Обнаружение  
использования  
фреймворков Cobalt Strike  
и Brute Ratel C4

Обнаружение успешной  
эксплуатации  
уязвимостей

**Обнаружение новых  
оповещений**



Оповещение о срабатывании потенциально важных новых правил

PT NAD подсвечивает срабатывания, которые не регистрировались до этого и могли остаться незамеченными

< Новые оповещения

Общие сведения  
Сработавшие правила  
Клиенты  
Серверы  
Описание и рекомендации

**Общие сведения**

Некоторые правила впервые сработали.

Опасность ■ Высокая

Первая сессия 21 мая, 15:15

Последняя сессия 23 мая, 08:33

Длительность 1 д 17 ч 17 мин 53 с

Отслеживание Включено

Обнаружена 21 мая, 15:15

Данные дополнены 23 мая, 00:50

Комментарий

**Сработавшие правила**

Опасность	SID	Название	Срабатываний	Класс	Обновлено	Сработало
■	<a href="#">12000004</a>	ATTACK AD [PTsecurity] Kerberoasting attack	1	Attempted ...	—	23 мая, 08:33
■	<a href="#">12000006</a>	TOOLS [PTsecurity] Cobalt Strike HTTP activ...	1	Exploitatio...	—	22 мая, 18:26
■	<a href="#">13100000</a>	ATTACK [PTsecurity] An ICMP tunnel was fo...	1	Tunneling ...	—	21 мая, 15:15





# PT NAD 11.1. Фильтры



Добавление  
личных  
и общих  
фильтров

Поиск сохраненных фильтров

Личные 3

- 20 декабря 2021, 13:55  
33333  
proto == "tcp" && app\_proto == "ldap"
- 20 декабря 2022, 10:48  
SIP  
app\_proto == sip
- 27 апреля, 16:24 [Настройка уведомлений](#) [Настройка отчетов](#) [Скопировать в общие](#) [Удалить фильтр](#)  
testfilter  
alert

Общие

Фильтров нет

testfilter  
alert

Общие 1

- 22 мая, 16:42, Константин Рудаков [Скопировать в личные](#) [Удалить фильтр](#)  
testfilter->shared  
alert

## Управление исключениями из ленты активностей

16:44

- Перейти к дашбордам
- ✓ Выбрать решение
- Перейти к правилу
- + Добавить исключение
- Не отслеживать

11:12

Какое исключение нужно добавить?

- Не регистрировать срабатывания правила [Аномалия] Установленные соединения на новый внешний порт
- Не регистрировать срабатывания всех правил

Исключения хранятся в справочнике [Исключения](#)

Отмена



## Расширение механизма исключений для атак

В PT NAD 11.1 появились новые параметры исключения для правил обнаружения атак:

- идентификаторы узлов
- группы узлов
- доменные имена

### Добавление исключения ×

Правило  
(10006397) SHELL [PTsecurity] Metasploit Mettle TCP session... ▾

Клиенты	Серверы
192.168.22.131 H700 HOME_NET example.com	192.168.22.168 H700 HOME_NET example.com

Комментарий  
Пример с новыми параметрами исключений

Сохранить Отмена



## Исключения для флуд-атак и сканирований

В PT NAD 11.1 можно добавить в исключения сетевой флуд и сканирование сети, которые определяются несигнатурными механизмами

### Общие сведения

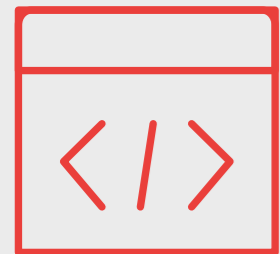
Обнаружена флуд-атака TCP SYN на узел [10.0.52.141](#), в рамках которой было открыто 1 347 сессий (65 сессий в секунду).

Опасность ■ Средняя

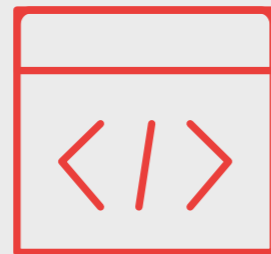
Первая сессия 22 мая, 09:51

Комментарий

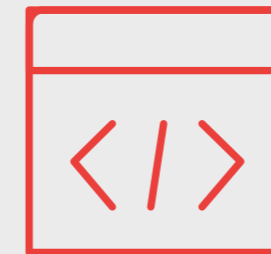
- Перейти к дашбордам
- Выбрать решение
- Перейти к правилу
- Добавить исключение**
- Не отслеживать



Мастер  
настройки



Переход от  
механизма захвата  
трафика PF\_RING  
к DPDK



Добавление инструмента  
для определения  
проблем с захватом  
и обработкой трафика

PT NAD 11

**Инсталлятор**



Устанавливает PT NAD

PT NAD 11.1

**Конфигуратор**

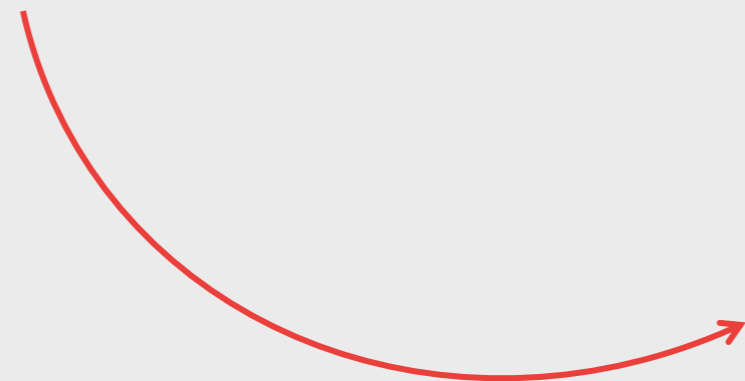


Настраивает базовые  
параметры PT NAD

**Поддерживает**



**Односерверную  
и многосерверную  
конфигурации**



**PT NAD,  
установленный  
и обновленный  
через инсталлятор**



Настраивает

GRUB

Параметры  
захвата трафика

Сроки хранения  
файлов PCAP и ES

Сетевые интерфейсы  
(порты):

- управления
- межкомпонентного взаимодействия
- захвата





# PT NAD 11.1. Конфигуратор



| PT NAD configuration wizard |

Welcome to PT NAD configuration wizard.

PT NAD version: 11.1.272  
Server role: Custom server  
Server components: Core, Sensor

Press <Continue> to start the basic PT NAD configuration.

Press <Main menu> to go to the main menu and change only a few specific parameters.

<Continue>

<Main menu>

| PT NAD configurator main menu |

Choose one of the settings sections below:

Network settings

Sensor settings

Pcap storage settings

Elasticsearch settings

<Exit>

<Save and exit>



# PT NAD 11.1. Конфигуратор



## Basic sensor settings

Choose one or more network interfaces for traffic capture:

- pci-04-00-0 VMware VMXNET3 Ethernet Controller (rev 01) [PTDPI DPDK]
- pci-0b-00-0 VMware VMXNET3 Ethernet Controller (rev 01) ens192 00:50:56:b6:c3:d9 192.168.54.1/24 [MANAGEMENT INTERCONNECT SYSTEM DPDK]
- pci-0c-00-0 VMware VMXNET3 Ethernet Controller (rev 01) [PTDPI DPDK]
- pci-13-00-0 VMware VMXNET3 Ethernet Controller (rev 01) [PTDPI DPDK]
- pci-14-00-0 VMware VMXNET3 Ethernet Controller (rev 01) [PTDPI DPDK]
- pci-1b-00-0 VMware VMXNET3 Ethernet Controller (rev 01) [PTDPI DPDK]

<Back>

<Next>

## Capture speed

Choose the expected capture traffic speed. The number of the ptdpi threads will be configured depending on this value.

- up to 200 Mbps
- up to 1 Gbps
- up to 2 Gbps
- up to 5 Gbps
- up to 10 Gbps
- more than 10 Gbps

<Cancel>

<Ok>



**DPDK** —  
рекомендуется  
для всех  
физических карт



**AF-PACKET** —  
остается только  
для совместимости  
с существующими  
внедрениями



**PF-RING** —  
не поддерживается  
PT NAD версии 11.1  
и выше



**DPDK** — рекомендуется для всех физических карт



**AF-PACKET** — остается только для совместимости с существующими внедрениями

Унифицированная конфигурация: для новых инсталляций всегда указывается DPDK

На одном сенсоре могут одновременно работать карты с поддержкой нативного DPDK и без нее

```
nadadmin@localhost:~$ sudo ptdpci devlist
```

```
ptdpci devlist...
```

```
pci-02-00-0 Ethernet controller: Intel Corporation  
82599ES 10-Gigabit SFI/SFP+ Network Connection  
(rev 01)
```

```
Driver: ixgbe
```

```
Drivers available: ixgbe
```

```
Local cpu: 0,4, 1,5, 2,6, 3,7
```

```
Usage: [ DPDK_NATIVE ]
```

```
pci-05-00-1 Ethernet controller: Broadcom Limited  
NetXtreme BCM5720 Gigabit Ethernet PCIe
```

```
Driver: tg3
```

```
Drivers available: tg3
```

```
Local cpu: 0,4, 1,5, 2,6, 3,7
```

В параметрах указываются идентификаторы PCI

Например:

- capture\_type: **dpdk**
- capture\_if: **pci-02-00-0 pci-05-00-1**



# PT NAD 11.1. Инструмент для определения проблем с захватом и обработкой трафика



```
ptuser@ptnad-01:/tmp/11.1$ ptdpictl traf
ptdpictl traf... 2023-05-22 15:24:24,379 - INFO - run:20 - NAD traffic analyzer
2023-05-22 15:24:24,516 - INFO - run:37 - Host 127.0.0.1; Start 22/05/2023, 11:24; End 22/05/2023, 12:24
-2023-05-22 15:24:24,994 - INFO - run:67 - Source level
```

metric	total	%	bytes.total	bytes.recv	bytes.sent
TCP	4610		267 MB	133 MB	134 MB
BAD_CHECKSUM	0	0.00	0 B	0 B	0 B
Errors	569	12.34	20 MB	11 MB	9 MB
ASYNC	1	0.02	64 kB	0 B	64 kB
Errors & !ASYNC	568	12.32	20 MB	11 MB	9 MB
GAP_DETECT	1	0.02	705 kB	505 kB	199 kB
OUT_OF_WINDOW	0	0.00	0 B	0 B	0 B
GAP_DETECT & OUT_OF_WINDOW & !ASYNC	0	0.00	0 B	0 B	0 B
TUNNELS	0	0.00	0 B	0 B	0 B
TUNNELS_VLAN	0	0.00	0 B	0 B	0 B
TUNNELS_GRE	0	0.00	0 B	0 B	0 B
TUNNELS_TEREDO	0	0.00	0 B	0 B	0 B
TUNNELS_VLAN & ASYNC	0	0.00	0 B	0 B	0 B



# PT NAD 11.1. Инструмент для определения проблем с захватом и обработкой трафика



```
+-----+-----+
| Sensor name      |          |
| Stat time       | 2023-05-22T12:24:35.008535 (UTC) |
| Up time        | 0d 02h 39m 38s |
+-----+-----+
| Interface name   | pci-04-00-0    |
| Speed          | 3.96 MB/sec    (31.64 Mb/sec) |
| Packets        | 4582 pkt/sec   |
| Kernel drops   | 0 pkt/sec (0 abs) |
| Other drops    | 0 pkt/sec (0 abs) |
| Invalid checksums | 0 pkt/sec (0 abs) |
| Packet size max | 1514 bytes     |
+-----+-----+
| Interface name   | pci-0c-00-0    |
| Speed          | 194.0 B/sec    (1.55 kb/sec) |
| Packets        | 2 pkt/sec     |
| Kernel drops   | 0 pkt/sec (0 abs) |
| Other drops    | 0 pkt/sec (0 abs) |
| Invalid checksums | 0 pkt/sec (0 abs) |
| Packet size max | 98 bytes      |
+-----+-----+
```



# PT NAD 11.1. Прочие улучшения



Добавление команд  
в интерфейс командной  
строки

nad-status



Улучшение отображения  
репутационных списков  
в транзакциях DNS



Разбор протокола DTLS



# Полезные ссылки



Телеграм-чат  
о PT NAD  
[t.me/PTNADChat](https://t.me/PTNADChat)



Дополнительные  
материалы о PT NAD  
[clck.ru/33f7PP](https://clck.ru/33f7PP)



[pt@ptsecurity.com](mailto:pt@ptsecurity.com)



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