



Результаты анализа трафика в 41 компании и новые возможности PT NAD



Ольга Зиненко
Старший аналитик ИБ



Кирилл Черкинский
Менеджер по продвижению продуктов



Алексей Леднёв
Заместитель руководителя отдела экспертных
сервисов и развития SOC

ptsecurity.com

t.me/PTNADChat



Почему важно

мониторить внутренний трафик

ptsecurity.com

Защиты периметра недостаточно



В **93%** проектов

по тестированию на проникновение, проведенных в 2019 году, наши специалисты смогли преодолеть сетевой периметр и получить доступ к ресурсам ЛВС*

30 минут

минимум требовалось на проникновение в локальную сеть. В среднем – 4 дня*

206 дней

среднее время незаметного присутствия злоумышленников в инфраструктуре**

В любую корпоративную сеть, даже хорошо защищенную на периметре, можно проникнуть.

Когда злоумышленник попадает во внутреннюю сеть, его действия остаются незамеченными для периметровых средств защиты.



**Нужно контролировать
и внешний, и внутренний трафик**

* [Итоги внешних пентестов — 2020](#), Positive Technologies

** 2019 Cost of a Data Breach Report, Ponemon institute

Какие решения подходят?

NTA (Network Traffic Analysis) — системы анализа трафика:

- Анализируют трафик как на периметре, так и в инфраструктуре
- Выявляют атаки с помощью комбинации способов детекта
- Предоставляют информацию, необходимую для расследования инцидентов

Многие клиенты Gartner рассказали, что NTA инструменты выявили подозрительную активность в трафике, которую пропустили периметровые решения

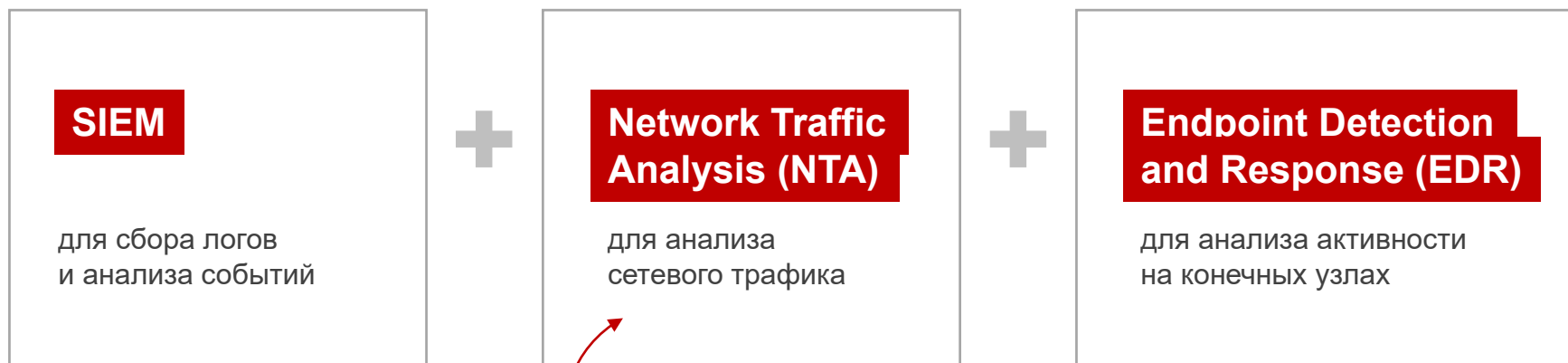
Market Guide Network Detection and Response, Gartner, 2020

NTA входит в топ технологий для выявления угроз, работой которых довольны в SOC

Common and Best Practices for Security Operations Centers:
Results of the 2019 SOC Survey, SANS Institute 2019

NTA — обязательный компонент SOC

SOC — это не только про SIEM. Основа SOC, по мнению Gartner:



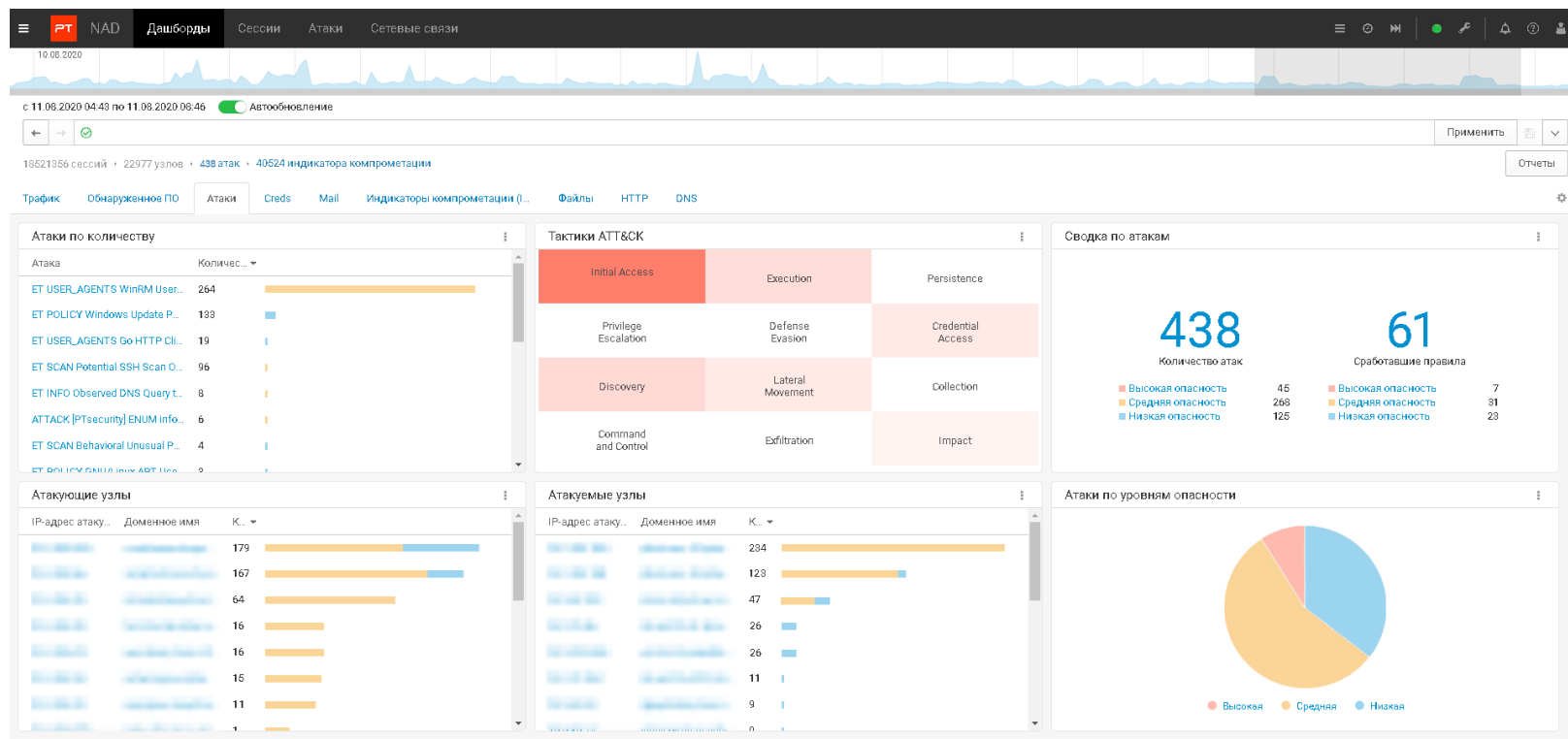
**Без этого компонента SOC
упускает события на уровне сети,
а значит у злоумышленников есть больше
возможностей остаться незамеченными**

PT Network Attack Discovery



PT NAD — система глубокого анализа сетевого трафика (NTA) для выявления атак на периметре и внутри сети.

Система знает, что происходит в сети, обнаруживает активность злоумышленников даже в зашифрованном трафике и помогает в расследованиях.



NTA — решения класса Network Traffic Analysis



Топ угроз ИБ в корпоративных сетях, 2021

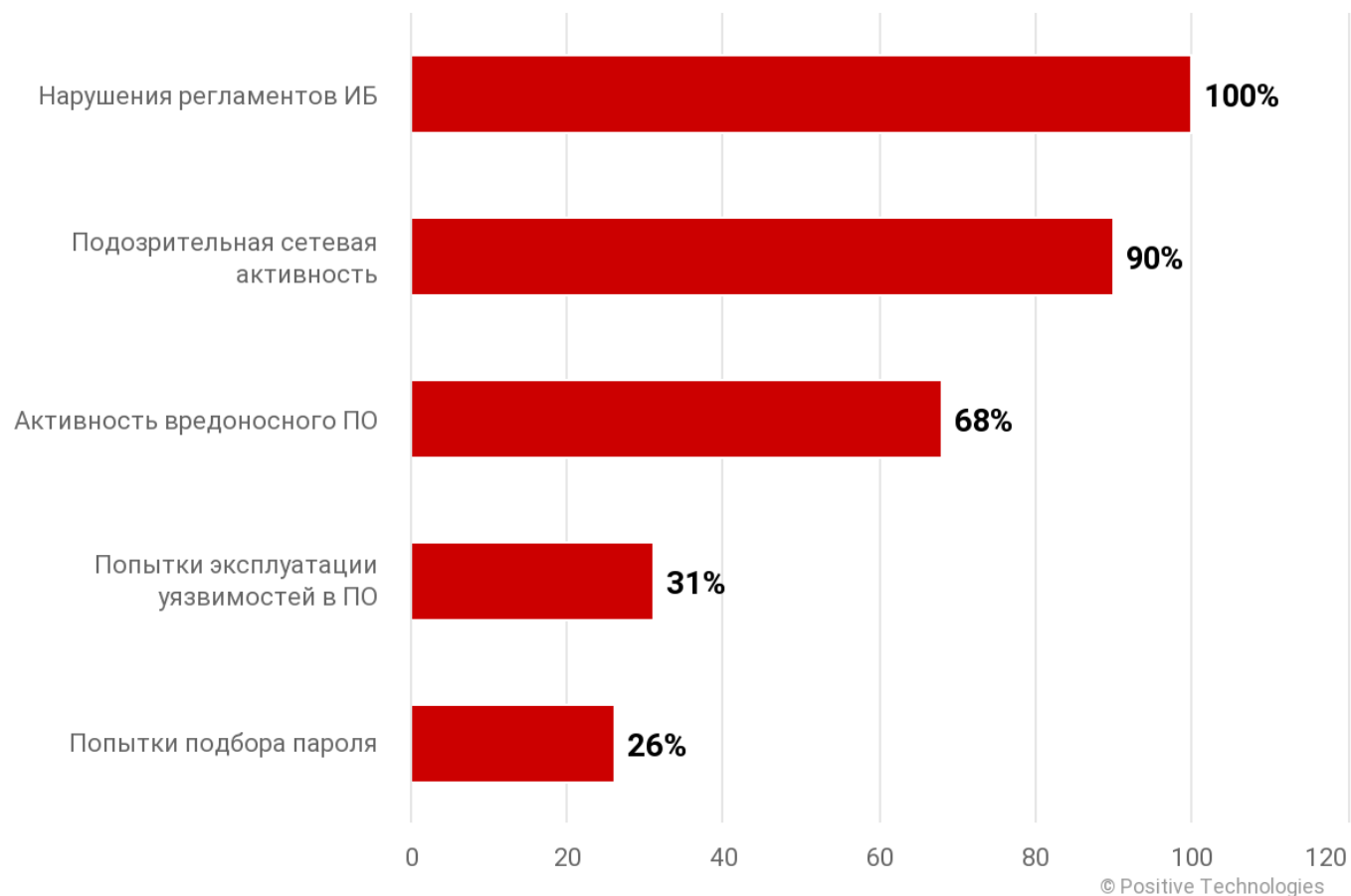


Об исследовании

Более **650**
выявленных угроз ИБ
в корпоративных сетях

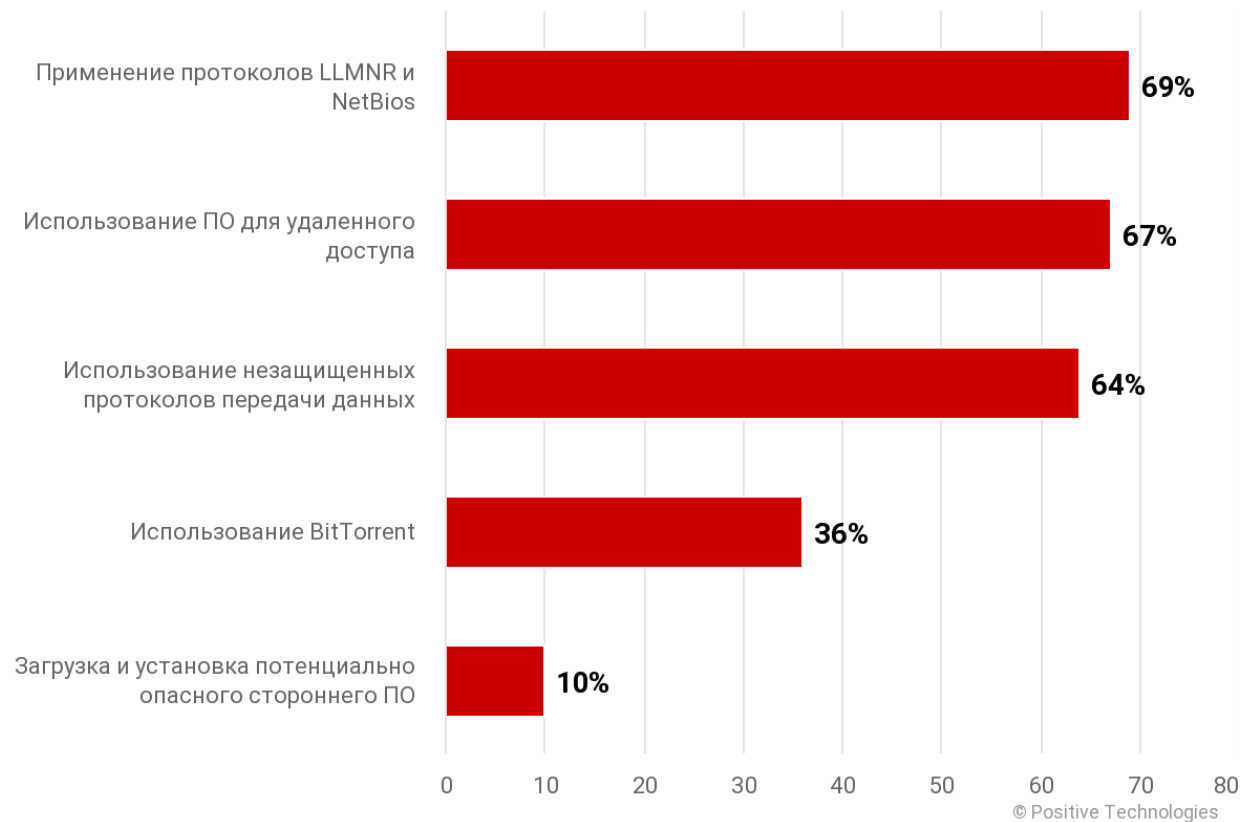


Категории угроз ИБ



Категории выявленных угроз (доли компаний)

Нарушения регламентов ИБ





В **67%** компаний используется ПО для удаленного доступа в обход политик безопасности

В **64%** компаний используются незащищенные протоколы передачи данных

Топ-5 нарушений регламентов ИБ (доли компаний)

Нарушения регламентов ИБ

РТ

Название	Класс	 	Обнаружена	IOC	IP-адрес атакующего
REMOTE [PTsecurity] TeamViewer	Potential Corporate Privacy Violation		27.07.2020 11:26:41		
REMOTE [PTsecurity] TeamViewer	Potential Corporate Privacy Violation		27.07.2020 11:26:41		
REMOTE [PTsecurity] TeamViewer	Potential Corporate Privacy Violation		27.07.2020 11:26:04		
REMOTE [PTsecurity] TeamViewer	Potential Corporate Privacy Violation		27.07.2020 11:26:04		

Протоколы **teamviewer, tcp**

Начало 27 июля 2020, 11:26:41

Конец 27 июля 2020, 11:37:18

Длительность 10 минут 37 секунд

Отправлено 5 МБ, 12 578 пакетов

Получено 975 КБ, 9 236 пакетов

Отправитель

Получатель

Все атаки сессии

-  REMOTE [PTsecurity] TeamViewer
Potential Corporate Privacy Violation
-  REMOTE [PTsecurity] TeamViewer
Potential Corporate Privacy Violation

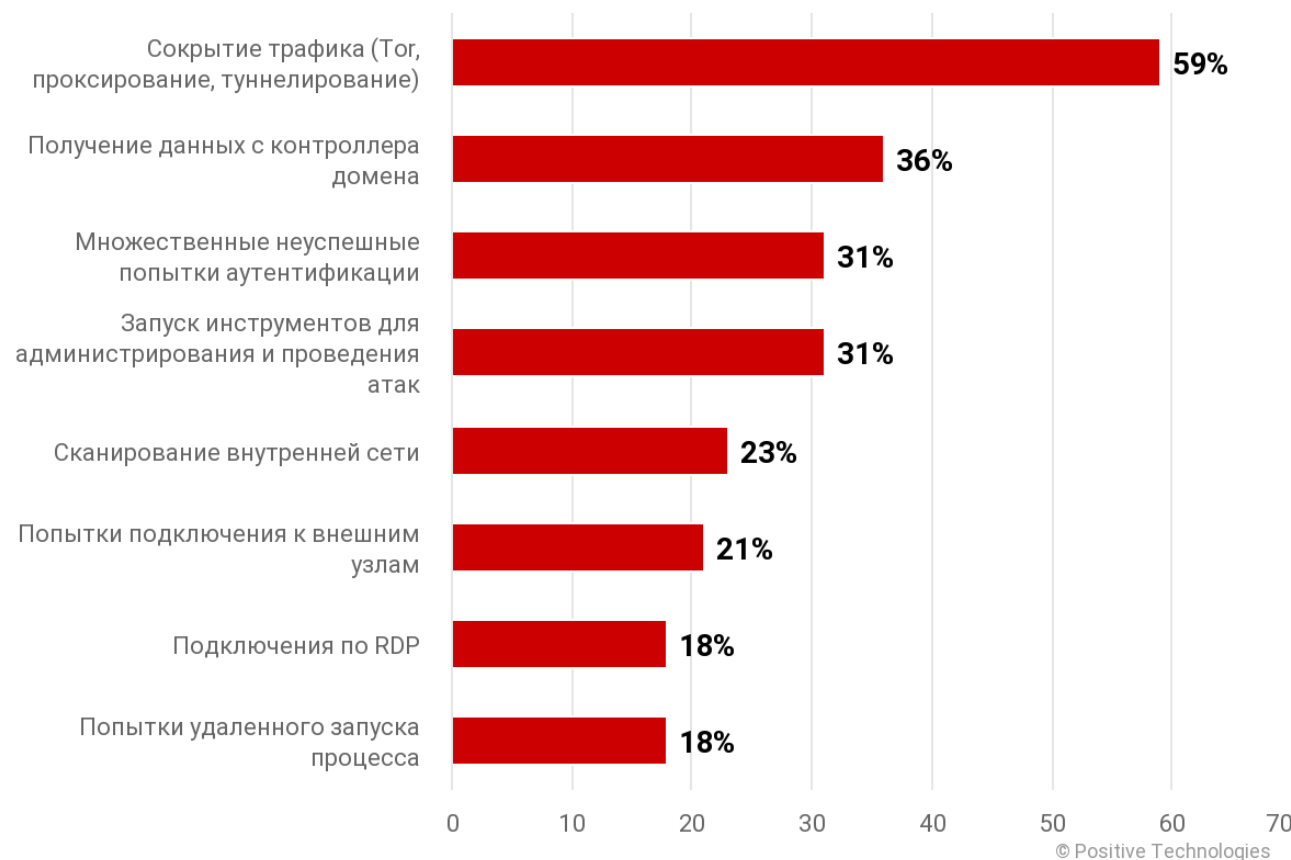
Примеры использования средств удаленного администрирования

Нарушения регламентов ИБ

Протоколы	ftp, tcp	Учетные записи	
Начало	28 июля 2020, 15:00:41	✓	
Конец	28 июля 2020, 19:09:23		
Длительность	4 часа 8 минут 42 секунды		
Отправлено	68 кБ, 1 122 пакета		
Получено	73 кБ, 796 пакетов		
Отправитель			
Получатель			

Пример подключения к файловым серверам с раскрытием учетных данных

Подозрительная сетевая активность



Подозрительная сетевая активность



Сессия

Протоколы [ldap, tcp](#)

Начало 11 августа 2020, 03:45:30

Конец 11 августа 2020, 03:45:32

Длительность 2 секунды

Отправлено 143 кБ, 372 пакета

Получено 520 кБ, 478 пакетов

Отправитель

Получатель

Все атаки сессии

- ATTACK AD [PTsecurity] Domain accounts enumeration via LDAP query
Attempted Information Leak

Общие сведения

Протоколы [ldap, tcp](#)

Начало 27 февраля 2020, 18:03:07

Конец 27 февраля 2020, 18:03:08

Длительность 1 секунда

Отправлено 5 кБ, 12 пакетов

Получено 9 кБ, 13 пакетов

Отправитель

Получатель

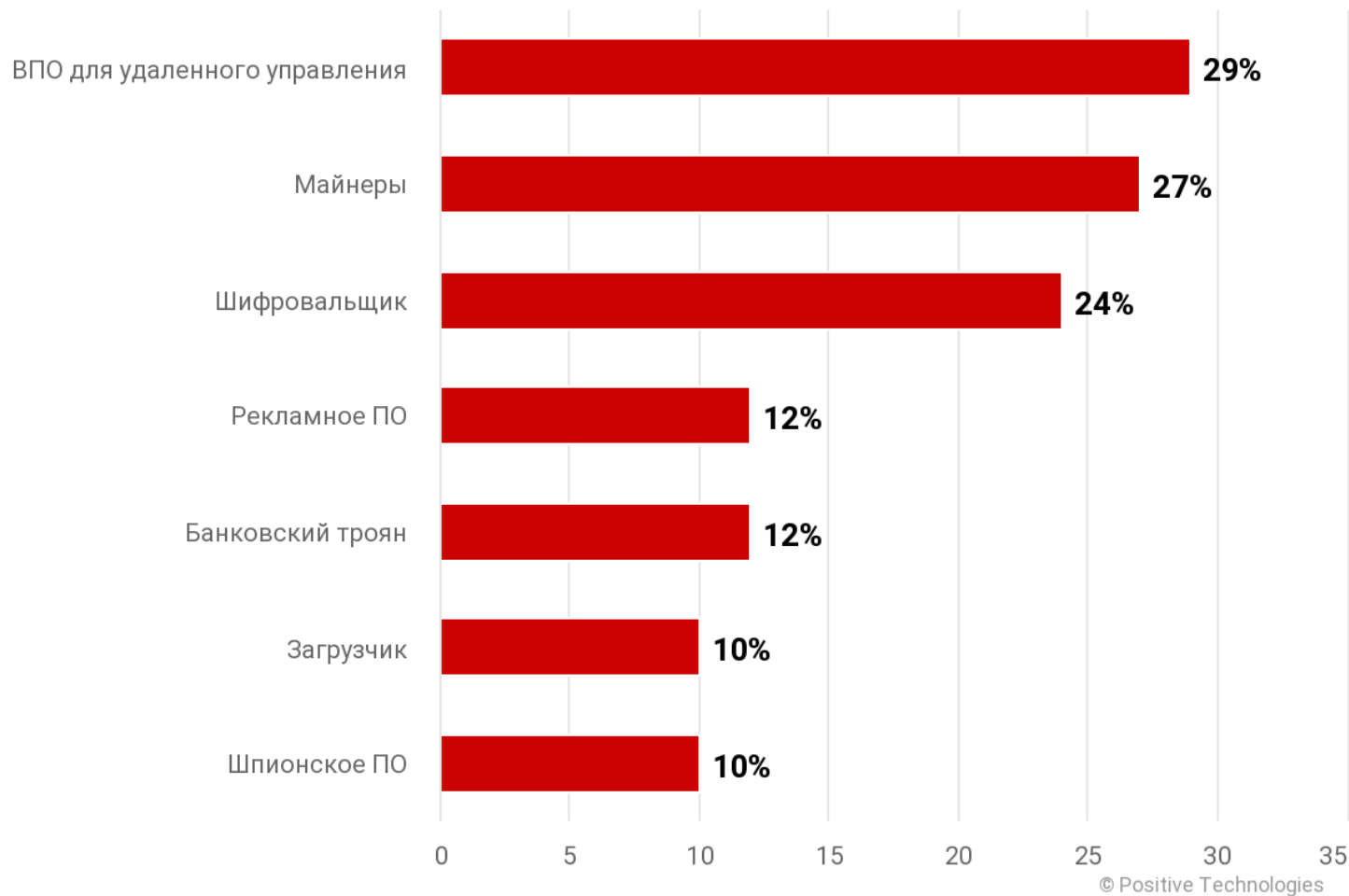
Атаки

- ATTACK AD [PTsecurity] LDAP enumeration of admins
Attempted Information Leak

Сбор информации о доменных учетных записях

Активность ВПО

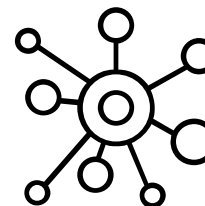
PT



Выявлено

36 семейств вредоносного ПО

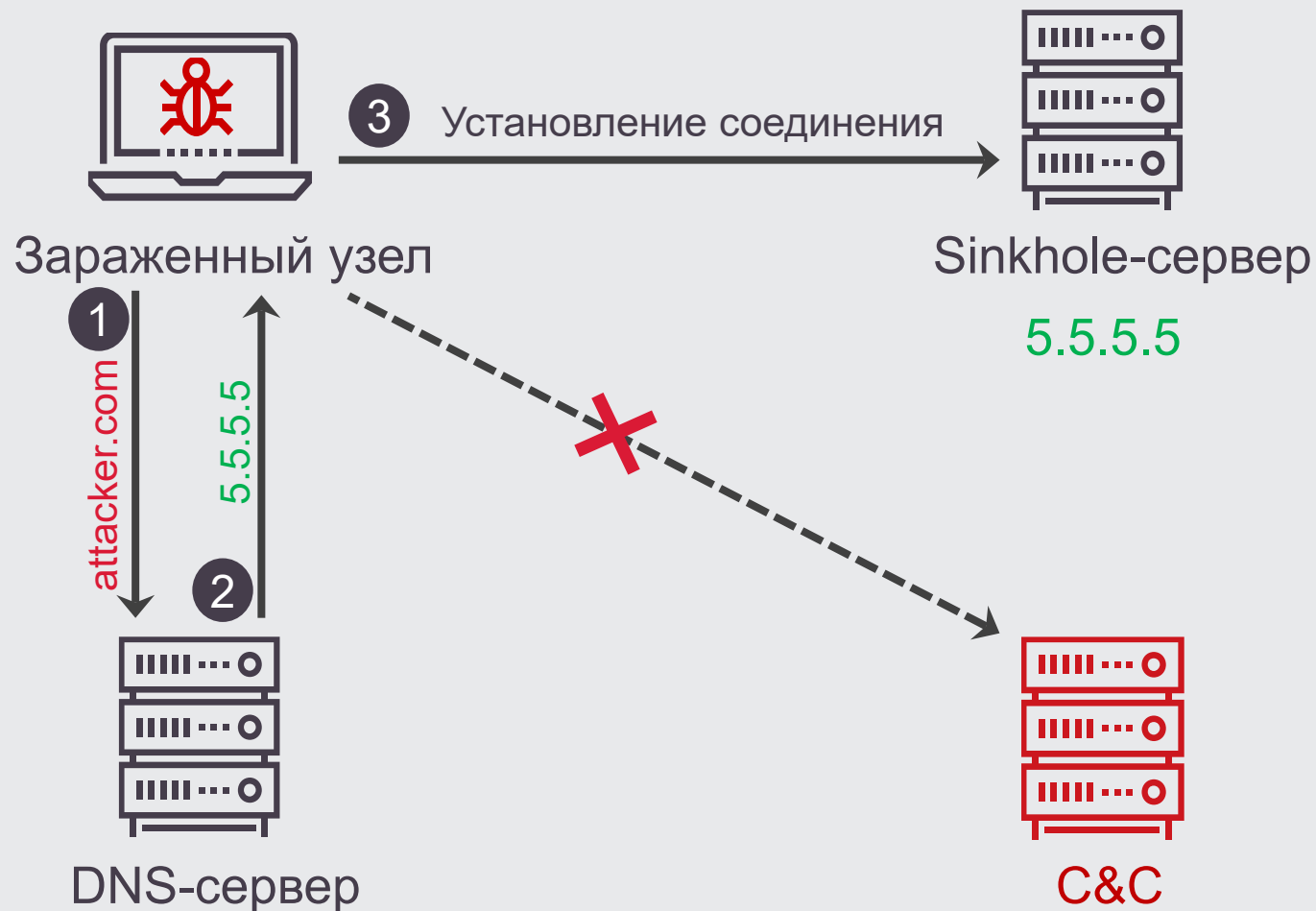
Среди них:



WannaCry
RTM
Ursnif
Dridex
Mirai

Активность ВПО

В каждой четвертой компании
были выявлены попытки
подключения к «засинкхолонным»
доменам



Активность ВПО

PT

Общие сведения

Протоколы [http, tcp](#)

Начало 23 июля 2020, 08:32:18

Конец 23 июля 2020, 08:32:20

Длительность 1 секунда

Отправлено 1 кБ, 6 пакетов

Получено 1 кБ, 6 пакетов

Отправитель

Получатель

Атаки

ET TROJAN Possible Compromised Host AnubisNetworks Sinkhole Cookie Value Snkz
A Network Trojan was Detected

SINKHOLE [PTsecurity] snkz HTTP cookie set
Exploitation Attributes was Detected

Файлы

set_app_list.jsp 630 Б

↑ /galaxy/xml/

HTTP

23.07.20 08:32:19	POST	630 Б UNKNOWN	OK 200	text/html	0 Б HTML	^	
connection	Keep-Alive	content-length	630	content-type	application/x-www-form-urlencoded	host	Apache-HttpClient/UNAVAILABLE (java 1.4)
connection	close	content-type	text/html	date	Thu, 23 Jul 2020 05:32:19 GMT	server	nginx
set-cookie	btst=; path=/; domain=.web1-main.ssuggest.com; Max-Age=1; Expires=Thu, 01 Jan 1970 00:00:01 GMT; HttpOnly; SameSite=Lax; btst=; path=/; domain=.web1-main.ssuggest.com; Max-Age=1; Expires=Thu, 01 Jan 1970 00:00:01 GMT; HttpOnly; SameSite=Lax; btst=77ac198dd8216b61d926164fc3d88bef 195.239.81.66 1595482339 1595482339 0 1 0; path=/; domain=.web1-main.ssuggest.com; Expires=Thu, 15 Aug 2020 00:00:00 GMT; HttpOnly;						

Пример обнаружения попыток подключения к синкхолу

Активность ВПО



🏠

🔍

🔒 https://

⏪

Задания

📄

Поделиться

🖨

Печать

📁

В черный или белый список...

Структура задания

📁 /elite/smtpd.arm4

ОПАСНЫЕ И ПОТЕНЦИАЛЬНО ОПАСНЫЕ ФАЙЛЫ ^

📁 /elite/smtpd.arm4

/elite/smtpd.arm4

Свойства файла

Подробнее

SHA-256

20BD5AB3C6E94E2446358CDE53B73C1EA5EE0839961A76D32758BB660C22B379

Показать SHA-1, MD5

Размер

89,00 КБ

MIME-тип

application/x-executable

Итоговый результат проверки

📁

Обнаружено опасное ПО (Компьютерный червь)

Тип самого опасного вредоносного ПО, обнаруженного в результате проверки разными методами

Антивирусное сканирование

📁

Компьютерный червь

Avira

Антивирус	База обновлена	Вредоносное ПО
Avira, 8.3.60.46	21 июня, 03:00	LINUX/Mirai.rqhgu

📁

Троян

Bitdefender

Антивирус	База обновлена	Вредоносное ПО
Bitdefender, 11.0.1.19	21 июня, 23:33	Trojan.Linux.Mirai.1

📁

Установщик ВПО

ClamAV

Антивирус	База обновлена	Вредоносное ПО
ClamAV, 0.101.4	21 июня, 16:07	Unix.Dropper.Mirai-7135892-0

Пример детектирования трояна Mirai в PT Sandbox

Полный отчет

PT



ptsecurity.com/ru-ru/premium/top-ugroz-ib-v-korporativnyh-setyah-2021/



PT NAD 10.1

Обзор новых возможностей



Что нового в РТ NAD



- Данные об угрозах в ленте активностей
- Новые модули аналитики для выявления сложных угроз
- Контроль сетевых узлов
- Еще более прозрачная сеть: определение и разбор новых протоколов
- Работа с трафиком для незавершенных сессий
- Другие приятные улучшения

Лента активностей



PT

NAD

Дашборды

Сессии

Атаки

Сетевые связи

Узлы

Лента активностей

☰

🔄

⏮

⏭

🟢

🔑

❓

👤

Решение

Опасность

Тип

Отслеживание

Адрес узла, группа

×

5 активностей • 4 высокой опасности • 0 средней опасности • 1 низкой опасности

2 марта

Сортировка по времени обнаружения

08:41

Неизвестный DHCP-сервер

Проблема устранена

Активность была 1 марта, 16:41 – 2 марта, 8:38 (15 часов 57 минут 31 секунда)

Обнаружен неизвестный DHCP-сервер по адресу [REDACTED]

Больше не актуально.

08:41

Неизвестный DHCP-сервер

Активность была 1 марта, 15:39 – 2 марта, 8:40 (17 часов 1 минута 12 секунд)

Обнаружен неизвестный DHCP-сервер по адресу [REDACTED]

Что-то странное, Иван, разберитесь.

1 марта

17:48

Сессий больше 0 за 10 минут

Неинтересно

Активность была 1 марта, 16:28 – 17:48 (1 час 20 минут 0 секунд)

Сессий больше 0 за 10 минут по фильтру HTTP-трафик.

17:01

Использование словарных паролей

Активность была 1 марта, 16:54 (0 секунд)

На узле [REDACTED] были найдены учетные записи со словарными паролями.

17:01

Использование словарных паролей

Ложное срабатывание

Активность была 1 марта, 16:54 (0 секунд)

На узле [REDACTED] были найдены учетные записи со словарными паролями.

Словарные пароли

PT

Общие сведения

На узле 10.20.68.204 были найдены учетные записи со словарными паролями.

Опасность	Высокая
Первая сессия	25 февраля 2021, 12:51
Последняя сессия	15 марта 2021, 12:37
Длительность	17 дней 23 часа 46 минут 51 секунда
Отслеживание	Включено
Обнаружена	25 февраля 2021, 14:24
Данные дополнены	15 марта 2021, 12:40

30% - доля успешных атак методом подбора учетных данных*

* [Итоги внешних пентестов — 2020](#), Positive Technologies

Информация об узле

Узел	H2989
IP-адрес	10.20.68.204
Группы	SERVERS, HOME_NET

Учетные записи

Логин	Пароль	Протокол	Была активна ▼
administrator	P@ssw0rd	http	15 Мар 2021, 12:37

Описание и рекомендации

Описание	Обнаружено использование словарных паролей для аутентификации. Такие пароли легко подобрать, используя общедоступные словари. Это может стать точкой проникновения в инфраструктуру или использоваться для
----------	--

Неизвестный DHCP-сервер



Общие сведения

Обнаружен неизвестный DHCP-сервер по адресу 192.168.23.150.

Опасность	Высокая
Первая сессия	15 марта 2021, 19:12
Последняя сессия	15 марта 2021, 19:25
Длительность	13 минут 8 секунд
Отслеживание	Включено
Обнаружена	15 марта 2021, 19:27

Комментарий

Информация об узле

Узел	H7
IP-адрес	192.168.23.150
Группы	HOME_NET, Root, Unmanaged hosts

Описание и рекомендации

Описание	Обнаружен новый DHCP-сервер. Этот сервер может оказаться ранее незамеченным и легитимным или вредоносным и контролируемым злоумышленниками. Во втором случае с его помощью атакующие могут проводить атаки mitm, позволяющие перехватывать трафик с целью получения учетных данных пользователей.
Рекомендации	Убедитесь, что обнаруженный DHCP-сервер принадлежит вашей инфраструктуре и является

Аномальные LDAP-запросы



Общие сведения

Обнаружена 15.03.2021 14:33:52

Название [ANOMALY] [PTsecurity] Unseen before ldap search query

Опасность ■ Низкая

SID 12000001 Ревизия 1

Класс Unknown Traffic

Тактики и техники ATT&CK

[Discovery](#)

[Account Discovery](#)

[Password Policy Discovery](#)

[Permission Groups Discovery](#)

Атакующий узел 10.10.8.13 ⓘ
jdoe.example.local
📁 HOME_NET, USERS

→

Атакуемый узел 10.20.9.19 ⓘ
dc.example.local
📁 DC_SERVERS, HOME_NET, SERVERS_INFR

Описание и рекомендации

Описание Обнаружен подозрительный LDAP-запрос типа search. Подобные запросы используются для получения информации из Active Directory. Оповещение выводится, если узел запросил нетипичную информацию, такую как информация о доменных учетных записях, группах или политиках. Данная активность может указывать на компрометацию сети и проведение разведки злоумышленниками.

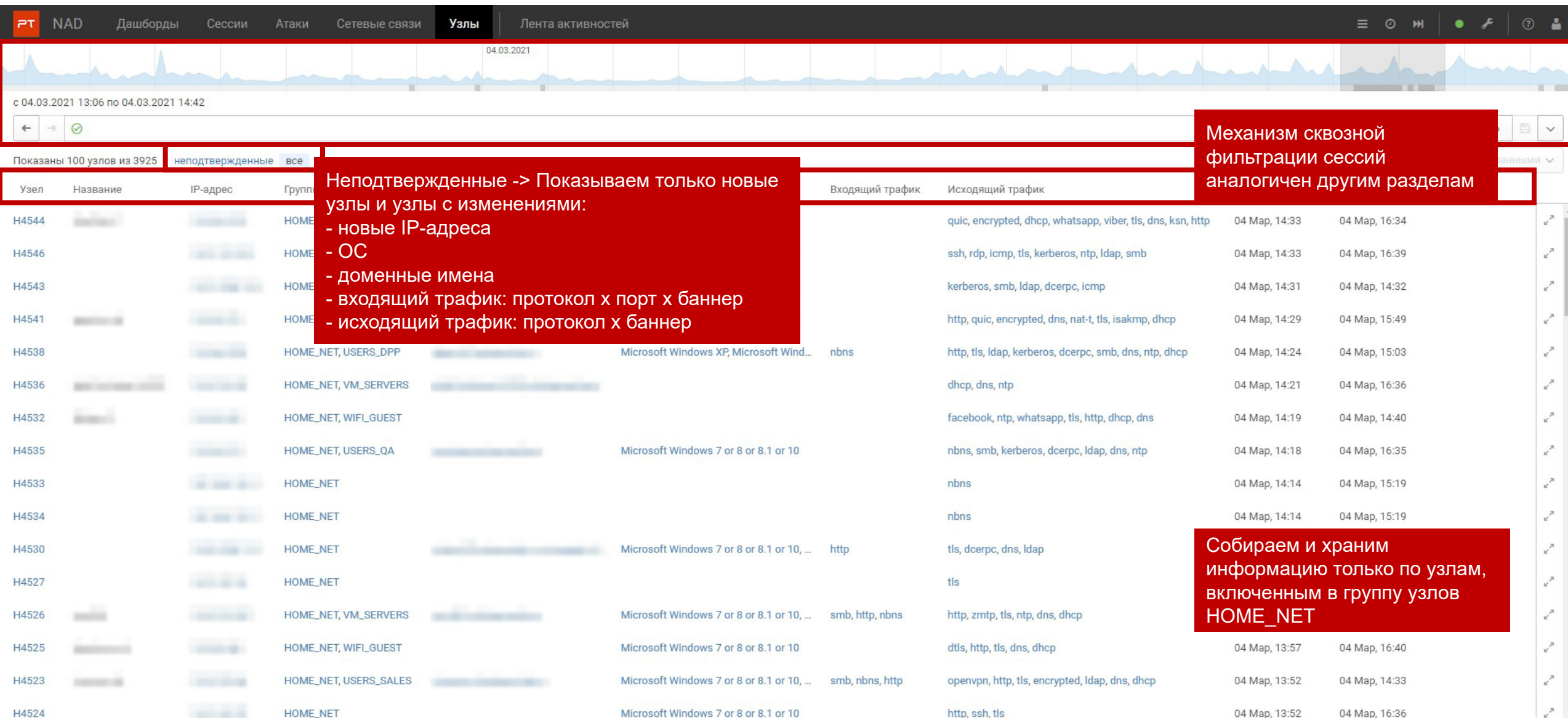
Рекомендации Выясните причину отправки запроса и проанализируйте данные, полученные в ответе узлом. На основе этой информации сделайте вывод о легитимности запроса.

Причина срабатывания

```
{
  "filter": "(samaccountname=rroy$)",
  "attributes": [],
  "hash": "samaccountname|"
}
```

Контроль сетевых узлов

РТ



Контроль сетевых узлов

PT



с 17.03.2021 17:58 по 17.03.2021 18:58

← 1 из 36 → x

Общие сведения

IP-адреса

Домены

Операционные системы

Входящий трафик

Исходящий трафик

Общие сведения

Узел 14714
Название 14714-01
IP-адрес 192.168.25.147
MAC 08:00:27:00:00:00
Группы HOME_NET, Root, PT Demo Root, VLAN 22/23
Обнаружен 12 марта 2021, 15:22:07
Был активен 18 марта 2021, 10:54:02

Комментарий

Text area for comments.

✓ Подтвердить изменения

IP-адреса

IP-адрес	Первая сессия ▼	Последняя сессия
192.168.25.147	15 Мар 2021, 19:15	18 Мар 2021, 10:54
192.168.25.148	12 Мар 2021, 15:22	15 Мар 2021, 19:12

Если IP адресов несколько, они сводятся в таблицу

Домены

Домен	Первая сессия ▼	Последняя сессия
14714-01.demo.net	15 Мар 2021, 14:02	18 Мар 2021, 10:54

Контроль сетевых узлов



PT

NAD

Дашборды

Сессии

Атаки

Сетевые связи

Узлы

Лента активностей

10.03.2021

с 13.03.2021 18:17 по 16.03.2021 18:17

← → ✓

Применить

1 из 60

Общие сведения

IP-адреса

Домены

Операционные системы

Входящий трафик

Исходящий трафик

Операционные системы

ОС	Первая сессия	Последняя сессия
Microsoft Windows	15 Мар 2021, 18:54	15 Мар 2021, 19:04
Microsoft Windows 7 or 8 or 8.1	15 Мар 2021, 18:03	15 Мар 2021, 19:12
Microsoft Windows 7 or 8 or 8.1 or 10	12 Мар 2021, 15:32	17 Мар 2021, 08:13

✓ Подтвердить изменения

Входящий трафик

Протокол	Порт	Баннер	Первая сессия	Последняя сессия
nbns	137/udp	—	15 Мар 2021, 19:15	15 Мар 2021, 19:15
rdp	3389/udp	—	15 Мар 2021, 18:55	15 Мар 2021, 19:04
rdp	3389/tcp	—	15 Мар 2021, 18:54	15 Мар 2021, 19:04
dcercp	135/tcp	—	15 Мар 2021, 18:03	15 Мар 2021, 19:03
dcercp	49665/tcp	—	15 Мар 2021, 18:03	15 Мар 2021, 19:12

Исходящий трафик

Протокол	Баннер	Первая сессия	Последняя сессия
ftp	—	15 Мар 2021, 19:32	15 Мар 2021, 19:32
telnet	—	15 Мар 2021, 19:12	15 Мар 2021, 19:12

Уникальные комбинации
протокол-порт-баннер

Уникальные комбинации
протокол-баннер

Новые протоколы

Определение протоколов:

- DB2 DRDA
- DHCPv6
- Canon-BJNP
- Guardant
- SMB-mailslot
- Encrypted

Разбор протоколов:

- QUIC
- RDP
- MC-NMF
- Сервисы ATSVС и SVCCTL (over DCE RPC)
- WMI ExecMethod и ExecMethodAsync

Разбор ATSV, SVCCTL (over DCERPC)

PT

DCERPC

Versions 5.0

25.01.2006 23:19:28.129 (T0)	DCE_RPC_BIND	SRVSVC v.3.0 (NDR32bit v.2.0)	DCE_RPC_BIND_ACK
T0 + 9mc	DCE_RPC_REQUEST	NetShareEnumAll	DCE_RPC_RESPONSE
T0 + 6426mc	DCE_RPC_BIND	ATSVC v.1.0 (NDR32bit v.2.0)	DCE_RPC_BIND_ACK
T0 + 6446mc	DCE_RPC_BIND	ATSVC v.1.0 (NDR32bit v.2.0)	DCE_RPC_BIND_ACK
T0 + 6530mc	DCE_RPC_REQUEST	JobAdd	DCE_RPC_RESPONSE
	cmd \\BLACKWORM-VICTI\Admin\$\WINZIP_TMP.exe		result success
	server_name \\BLACKWORM-VICTI		
T0 + 6541mc	DCE_RPC_REQUEST	JobAdd	DCE_RPC_RESPONSE
	cmd \\BLACKWORM-VICTI\c\$\WINZIP_TMP.exe		result success
	server_name \\BLACKWORM-VICTI		

Разбор WMI ExecMethod и ExecMethodAsync

DCE_RPC_REQUEST	name ExecMethod pa... cmd cmd.exe /Q /c cd 1> \\127.0.0.1\ADMIN\$\ method Create object_path Win32_Process path C:\ProgramData\VMware	DCE_RPC_RESPONSE
DCE_RPC_REQUEST	name ExecMethod pa... cmd cmd.exe /Q /c dir 1> \\127.0.0.1\ADMIN\$\ method Create object_path Win32_Process path C:\ProgramData\VMware	DCE_RPC_RESPONSE
DCE_RPC_REQUEST	name ExecMethod p. cmd cmd.exe /Q /c SHTASKS /RU SYSTEM /CRE/ method Create object_path Win32_Process path C:\ProgramData\VMware	<div>name ExecMethod params cmd cmd.exe /Q /c SHTASKS /RU SYSTEM /CREATE /SC DAILY /ST 00:00 /TN "Microsoft Windows WSUS" /TR "C:\ProgramData\VMWare\svchost.exe -L socks5://127.0.0.1:8080" 1> \\127.0.0.1\ADMIN\$_1605483226.0161984 2>&1 method Create object_path Win32_Process path C:\ProgramData\VMware</div>
DCE_RPC_REQUEST	name ExecMethod p cmd cmd.exe /Q /c SHTASKS /RU SYSTEM /CRE/ method Create object_path Win32_Process path C:\ProgramData\VMware	DCE_RPC_RESPONSE

Определение шифрованных протоколов

Общие сведения

Протоколы	<u>encrypted, tcp</u>
Начало	15 марта 2021, 22:43:45
Конец	15 марта 2021, 22:44:00
Длительность	15 секунд
Отправлено	2 КБ, 11 пакетов
Получено	15 КБ, 18 пакетов
Отправитель	10.10.8.3:1656 ⓘ jdoe.example.local 1C:1B:3A:3A:35:5B 📁 HOME_NET, USERS Microsoft Windows 7 or 8 or 8.1 or 10
Получатель	104.222.181.255:443 ⓘ proxy.digitalre... [AS... TELECOM ITALIA ...] 🇺🇸 (US) США— 00:1C:7F:6C:8F:6F 📁 EXTERNAL_NET Linux Ubuntu 14.04-16.10

Операции с трафиком незавершенной сессии

10.0.176.248:51927 → 10.0.176.95:5985 (Сессия не завершена) ← 19 из 5000 →

Общие сведения

HTTP

KERBEROS

Общие сведения

Протоколы	http, tcp
Начало	24 февраля 2021, 13:13:18
Конец	24 февраля 2021, 13:15:40
Длительность	2 минуты 22 секунды
Отправлено	254 КБ, 177 пакетов
Получено	9 КБ, 44 пакета
Отправитель	10.0.176.248:51927 windows-ci-medium-06.build.pt... 00:50:56:A6:42:8F DEV_SERVERS, HOME_NET Microsoft Windows 7 or 8 or 8.1 or 10
Получатель	10.0.176.95:5985 dc2-bwec-01.build.ptsecurity.ru 00:50:56:99:C6:F0 DEV_SERVERS, HOME_NET Microsoft Windows 7 or 8 or 8.1
Хранилище	ptdpi-52

Атаки

ET USER_AGENTS WinRM User Agent Detected - Possible Lateral Movement
Potentially Bad Traffic

Файлы

BIN 15 1.73 КБ
↓ /wsman/subscriptions/95E2153A-ADDE-4A50-91C7-CB465A77D7C2/

Учетные записи

✓ BUILD.PTSECURITY.RU
\\WIN-MED-06\$

Зарегистрировать инцидент

Отправить в хранилище

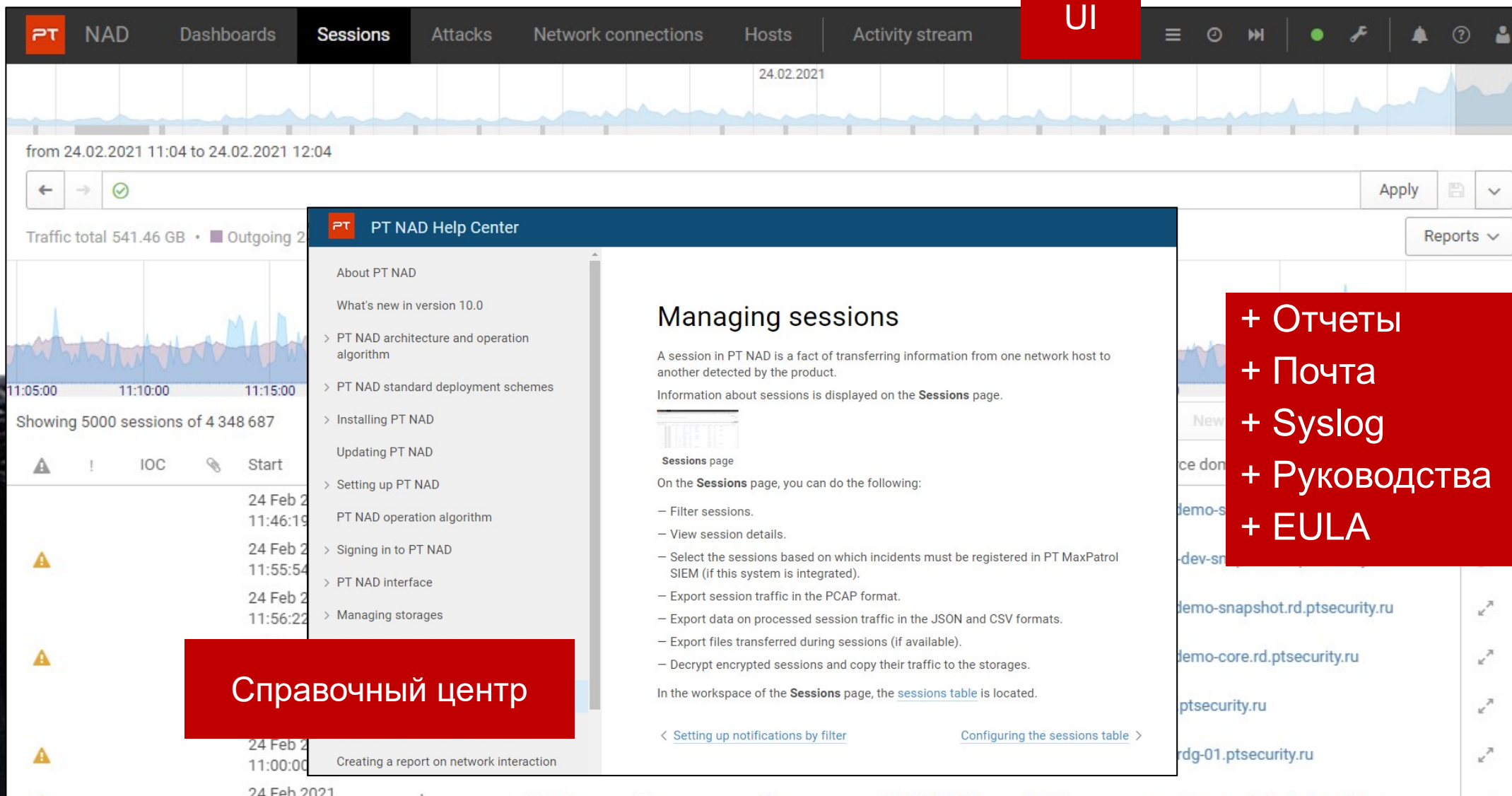
Скачать дамп

Скачать файлы

English! Do you speak it?

PT

UI



The screenshot displays the PT NAD interface. The top navigation bar includes tabs for NAD, Dashboards, Sessions (active), Attacks, Network connections, Hosts, and Activity stream. A red box with the text 'UI' is positioned over the Sessions tab. Below the navigation bar, a timeline shows traffic data from 24.02.2021 11:04 to 24.02.2021 12:04. The main content area shows a traffic total of 541.46 GB and a list of sessions. A red box with the text 'Справочный центр' (Help Center) is positioned over the bottom left of the interface. A PT NAD Help Center overlay is visible, showing the 'Managing sessions' page. The overlay includes a table of contents with links to various sections, including 'About PT NAD', 'What's new in version 10.0', 'PT NAD architecture and operation algorithm', 'PT NAD standard deployment schemes', 'Installing PT NAD', 'Updating PT NAD', 'Setting up PT NAD', 'PT NAD operation algorithm', 'Signing in to PT NAD', 'PT NAD interface', and 'Managing storages'. The 'Managing sessions' page text states: 'A session in PT NAD is a fact of transferring information from one network host to another detected by the product. Information about sessions is displayed on the Sessions page. On the Sessions page, you can do the following: Filter sessions. View session details. Select the sessions based on which incidents must be registered in PT MaxPatrol SIEM (if this system is integrated). Export session traffic in the PCAP format. Export data on processed session traffic in the JSON and CSV formats. Export files transferred during sessions (if available). Decrypt encrypted sessions and copy their traffic to the storages. In the workspace of the Sessions page, the sessions table is located.' The bottom of the overlay shows links for 'Setting up notifications by filter' and 'Configuring the sessions table'.

PT NAD Help Center

About PT NAD

What's new in version 10.0

- > PT NAD architecture and operation algorithm
- > PT NAD standard deployment schemes
- > Installing PT NAD
- > Updating PT NAD
- > Setting up PT NAD
- > PT NAD operation algorithm
- > Signing in to PT NAD
- > PT NAD interface
- > Managing storages

Managing sessions

A session in PT NAD is a fact of transferring information from one network host to another detected by the product.

Information about sessions is displayed on the **Sessions** page.

On the **Sessions** page, you can do the following:

- Filter sessions.
- View session details.
- Select the sessions based on which incidents must be registered in PT MaxPatrol SIEM (if this system is integrated).
- Export session traffic in the PCAP format.
- Export data on processed session traffic in the JSON and CSV formats.
- Export files transferred during sessions (if available).
- Decrypt encrypted sessions and copy their traffic to the storages.

In the workspace of the **Sessions** page, the [sessions table](#) is located.

< [Setting up notifications by filter](#) [Configuring the sessions table](#) >

+ Отчеты
+ Почта
+ Syslog
+ Руководства
+ EULA

Пользовательские настройки

РТ

Личный кабинет

Личные данные

Смена пароля

Настройка интерфейса

Настройка уведомлений

Настройка отчетов

Настройка интерфейса

Язык

Русский

Часовой пояс

UTC +03 Moscow, Kirov, Simferopol

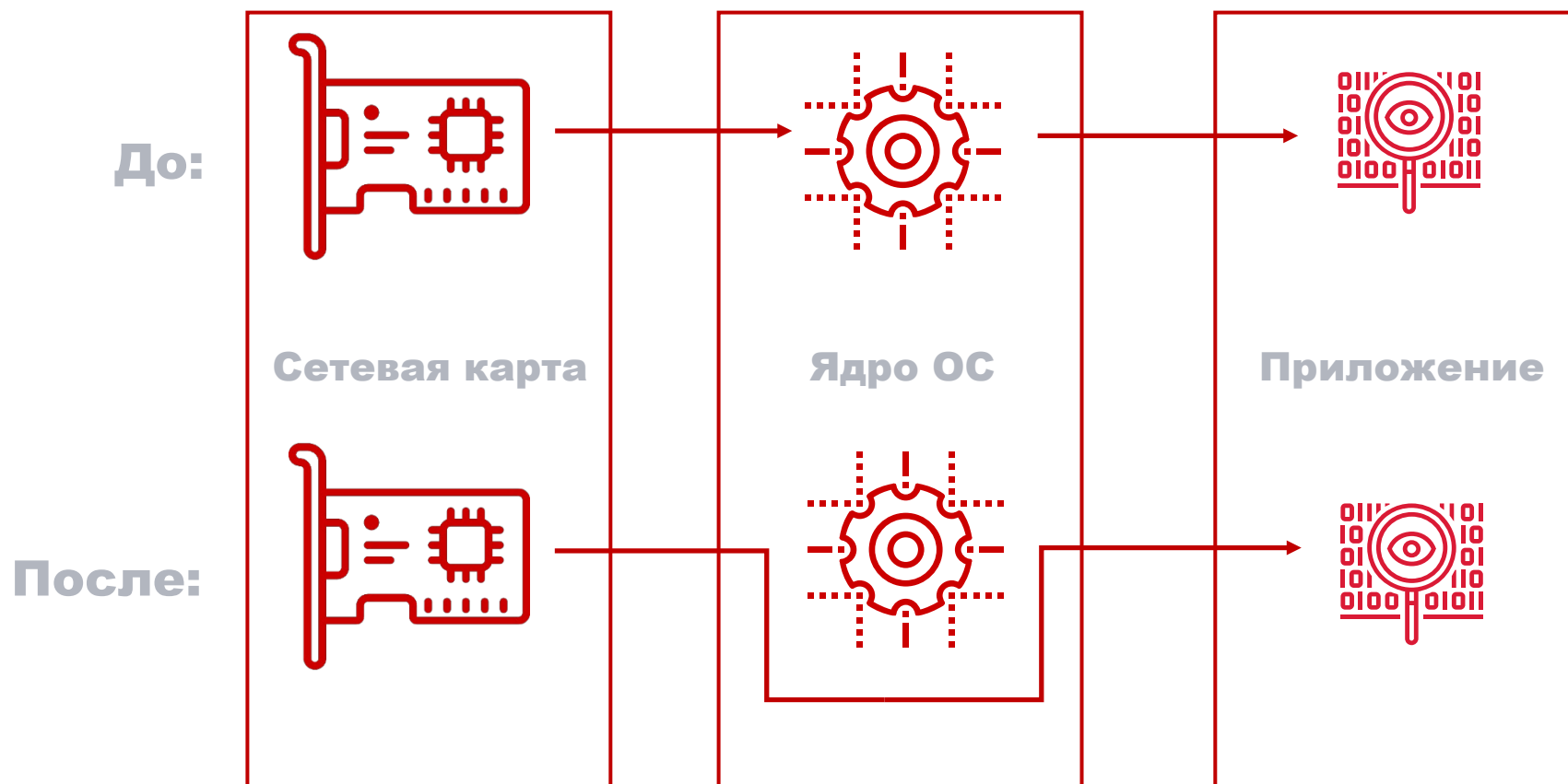
☐

Показывать расширенную информацию в карточках сессий и атак

Сохранить

Отмена

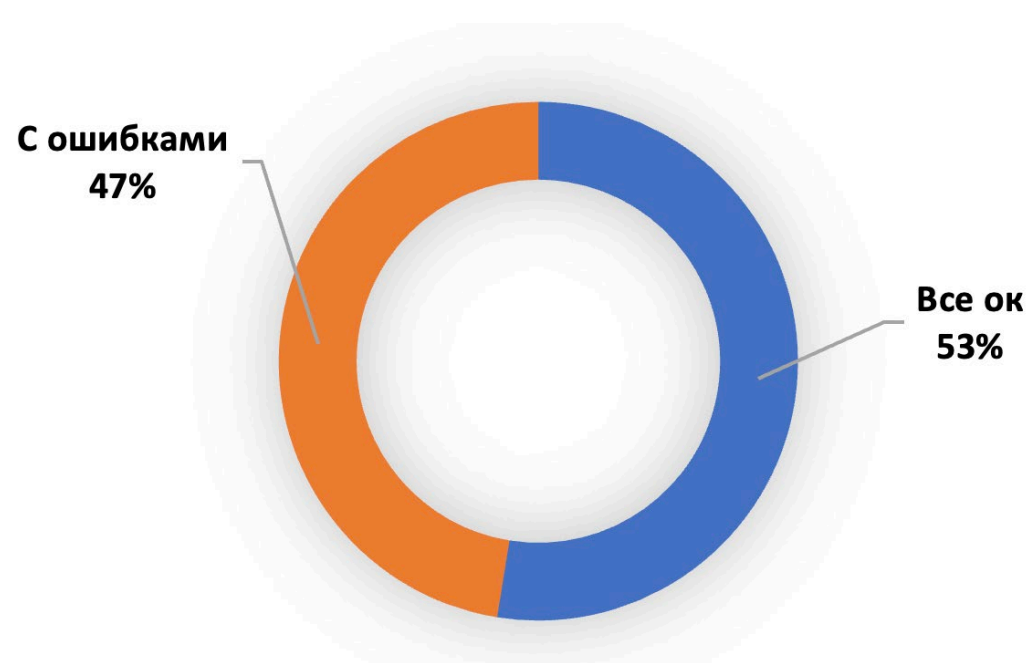
Переход на DPDK



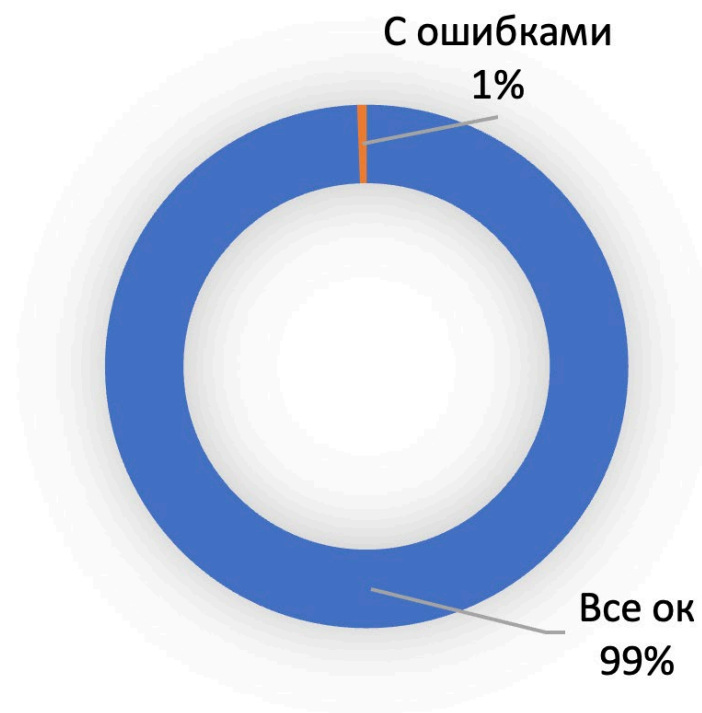
Чтение трафика с **0** потерями на скоростях **10** Гбит/с, **1-7** Млн пкт/с с одного интерфейса

Поддержка правил suricata 5.x

PT

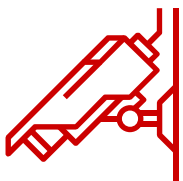


PT NAD 10.0



PT NAD 10.1

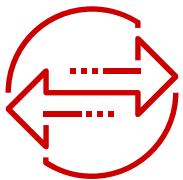
И другие улучшения:



Определение ОС через PT
OsDetectLib (вместо p0f)



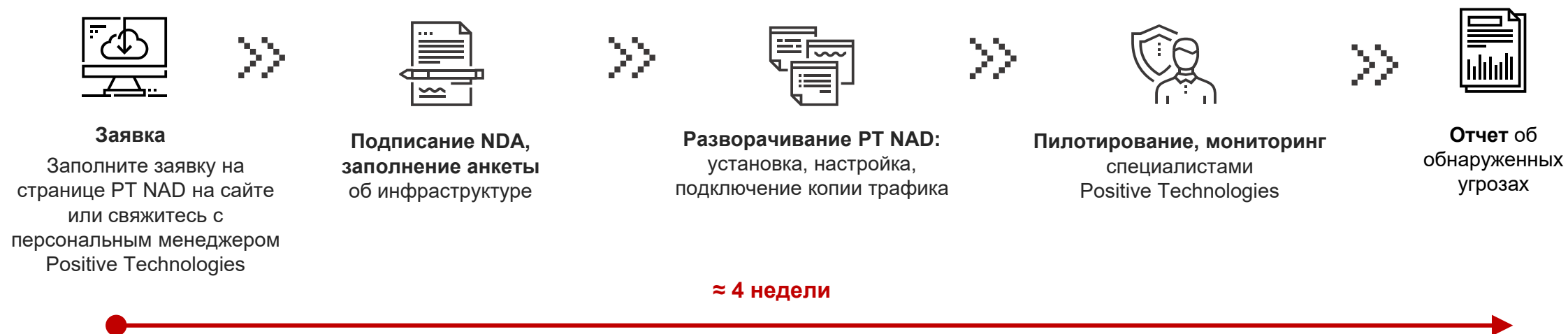
Обновление базы данных геолокации IP
(GeoLite2 от MaxMind)



Улучшенная интеграция с PT Sandbox



Как провести пилот PT NAD



Что дальше

PT

Задать вопрос:
t.me/PTNADChat

Обновить версию:
support.ptsecurity.com

Пройти обучение:
Partners@ptsecurity.com

ПИЛОТ:

ptsecurity.com/ru-ru/products/network-attack-discovery/#free-demo



Ольга Зиненко
Старший аналитик ИБ



Алексей Леднёв
Заместитель руководителя отдела
экспертных
сервисов и развития SOC



Кирилл Черкинский
Менеджер по продвижению продуктов
Kcherkinskiy@ptsecurity.com