# НОВОСТИ ИЗ МИРА APT

# ЧТО НОВОГО ПРЕДЛАГАЮТ РАЗРАБОТЧИКИ ANTI-APT РЕШЕНИЙ?

Владимир Соловьев
Старший специалист АО «ДиалогНаука»
24 ноября 2020 года

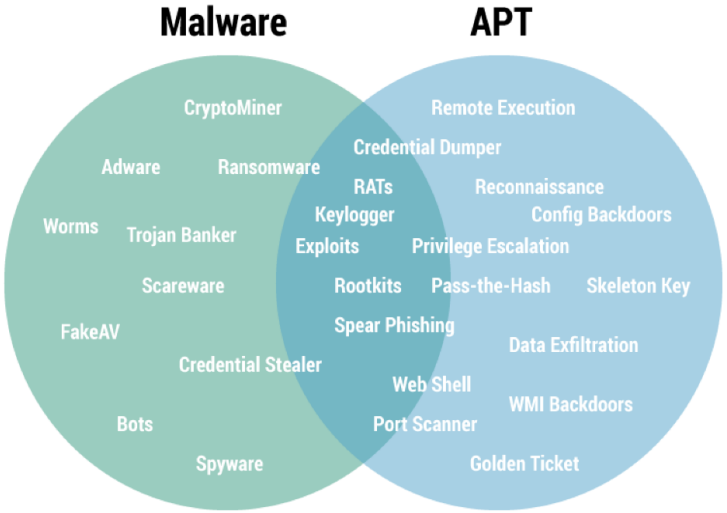
# О КОМПАНИИ

- Создана в 1992 году СП «Диалог» и Вычислительным центром РАН
- Первые продукты – ревизор ADinf, антивирусы Aidstest и Dr. WEB
- На сегодняшний день «ДиалогНаука» является одной из ведущих российских компаний, специализирующихся в области информационной безопасности

# Ключевые клиенты

# Введение

- APT (Advanced Persistent Threat):
  - ✓ Advanced (Продвинутая) – «Злоумышленник чаще умнее»
  - ✓ Persistent (Непрерывная) – «Злоумышленник достигает успеха»
  - ✓ Threat (Угроза) – «Атака может быть в любой момент»

# Этапы APT-атак

**Сбор данных о жертве**

- Выявление цели
- Сбор информации
- Разработка стратегии
- Разработка инструментов

**Первичное заражение**

- Доставка боевой нагрузки
- Эксплуатация уязвимостей в обход СЗИ
- Социальная инженерия
- Инвентаризация сети

**Активная фаза/ закрепление**

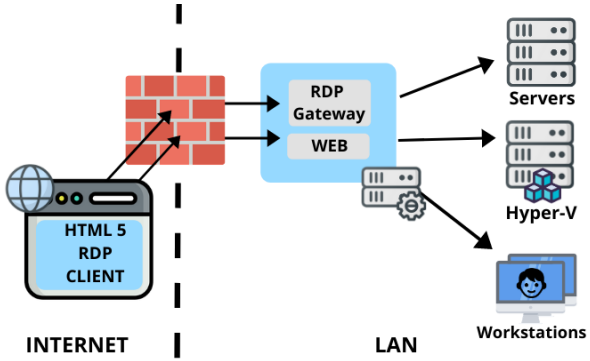
- Распространение в сети
- Поиск ключевой информации
- Повышение привилегий
- Получение удаленного контроля

**Достижение цели**

- Хищение данных
- Изменение данных
- Связь с управляющими серверами
- Сокрытие следов
- Ботнет сеть

# Общая статистика по APT-атакам*

- 2019: открытые военные операции в киберпространстве, тема кибербезопасности вышла на первый план в политике
- 2020: “remote”-атаки через/на протоколы удаленного доступа





*Согласно данным из открытых источников

# Топ паролей | 2020

| Position | Password | Number of users | Time to crack it | Times exposed |
|---|---|---|---|---|
| 1. ↑ (2) | 123456 | 2,543,285 | Less than a second | 23,597,311 |
| 2. ↑ (3) | 123456789 | 961,435 | Less than a second | 7,870,694 |
| 3. (new) | picture1 | 371,612 | 3 Hours | 11,190 |
| 4. ↑ (5) | password | 360,467 | Less than a second | 3,759,315 |
| 5. ↑ (6) | 12345678 | 322,187 | Less than a second | 2,944,615 |
| 6. ↑ (17) | 111111 | 230,507 | Less than a second | 3,124,368 |
| 7. ↑ (18) | 123123 | 189,327 | Less than a second | 2,238,694 |
| 8. ↓ (1) | 12345 | 188,268 | Less than a second | 2,389,787 |
| 9. ↑ (11) | 1234567890 | 171,724 | Less than a second | 2,264,884 |
| 10. (new) | senha | 167,728 | 10 Seconds | 8,213 |

# Общая статистика по APT-атакам*

- 2019: открытые военные операции в киберпространстве, тема кибербезопасности вышла на первый план в политике
- 2020: “remote”-атаки через/на протоколы удаленного доступа
  - ✓ **Июль:** Garmin был атакован шифровальщиком WastedLocker
  - ✓ **Август:** Обнародована информация о взломах группировки RedCurl
  - ✓ **Сентябрь:** Fancy Bear (APT28) атаки на правительство Азербайджана

*Согласно данным из открытых источников

# Общая статистика по APT-атакам*

- 2019: открытые военные операции в киберпространстве, тема кибербезопасности вышла на первый план в политике
- 2020: “remote”-атаки через/на протоколы удаленного доступа
  - ✓ **Июль:** Garmin был атакован шифровальщиком WastedLocker
  - ✓ **Август:** Обнародована информация о взломах группировки RedCurl
  - ✓ **Сентябрь:** Fancy Bear (APT28) атаки на правительство Азербайджана

Большинство атак можно было избежать при использовании Anti-APT и EDR решений

*Согласно данным из открытых источников



## НОВОСТИ ИЗ МИРА APT

ЧТО НОВОГО ПРЕДЛАГАЮТ РАЗРАБОТЧИКИ ANTI-APT РЕШЕНИЙ?

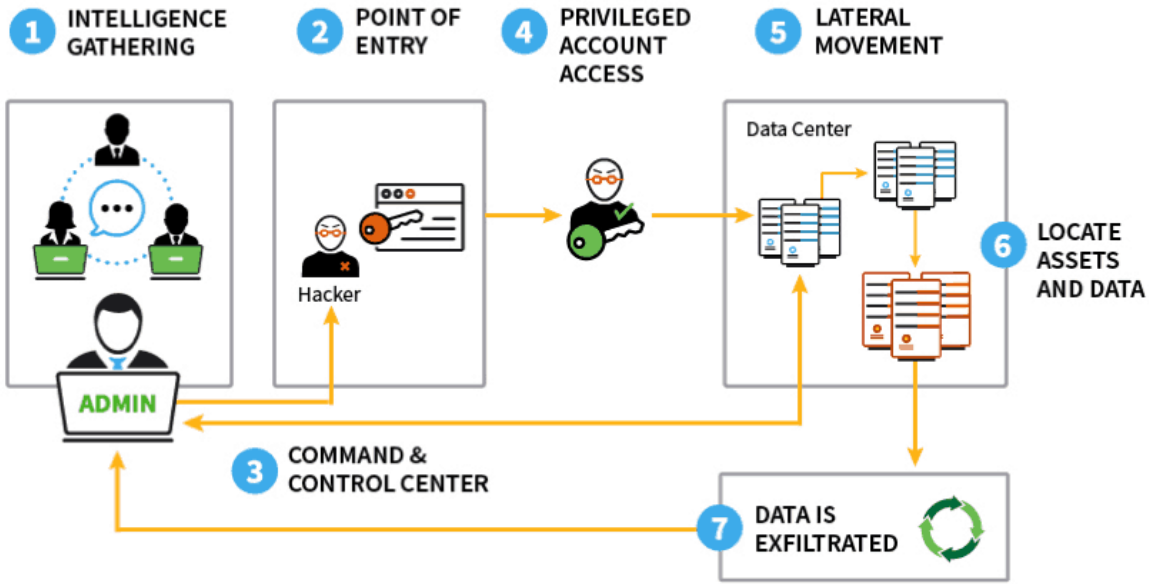

FireEye – американская компания, выпускающая средства защиты информации от атак нового поколения (APT). Основные решения:

- FireEye EX – система защиты электронной почты
- FireEye NX – система веб-защиты от вредоносных программ
- FireEye CM – система централизованного управления
- FireEye HX – система защиты конечных устройств

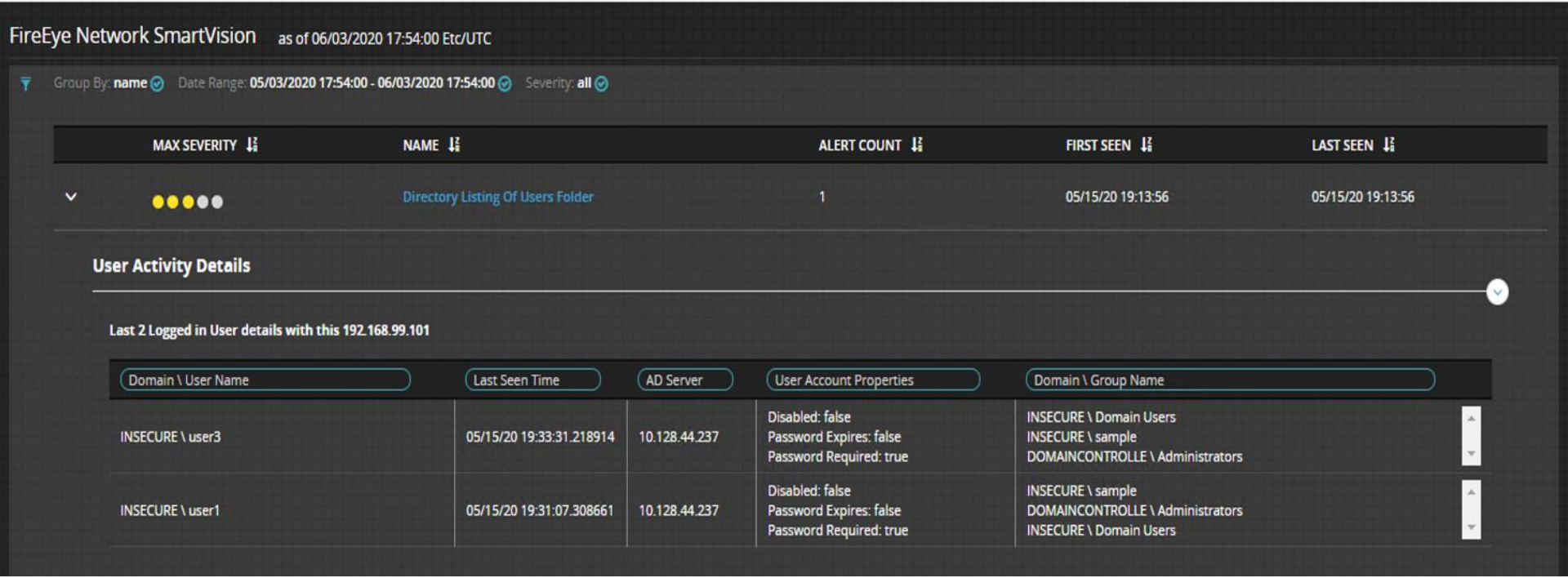
- FireEye FX, PX, AX …

# Синхронизация Active Directory для SmartVision

- SmartVision – функционал FireEye NX по противодействию атакам типа «lateral movements»



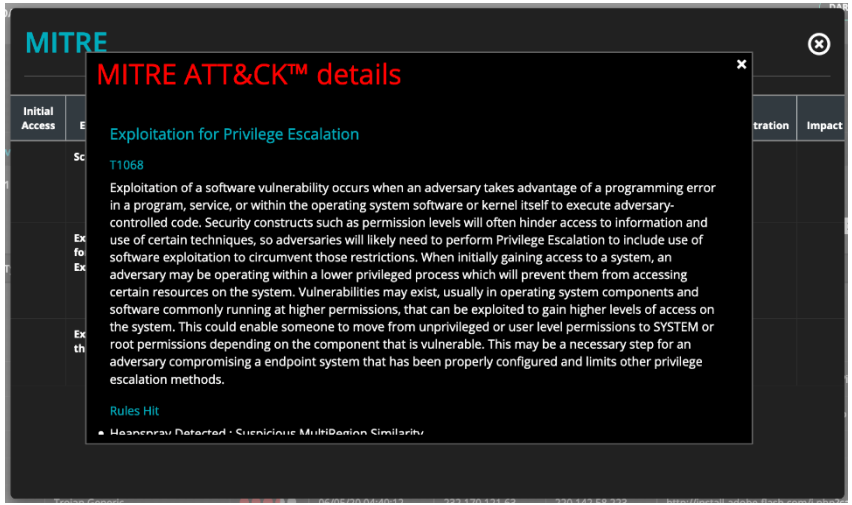
# Синхронизация Active Directory для SmartVision



# FireEye | NX

## Соответствие атаки по модели MITRE ATT&CK

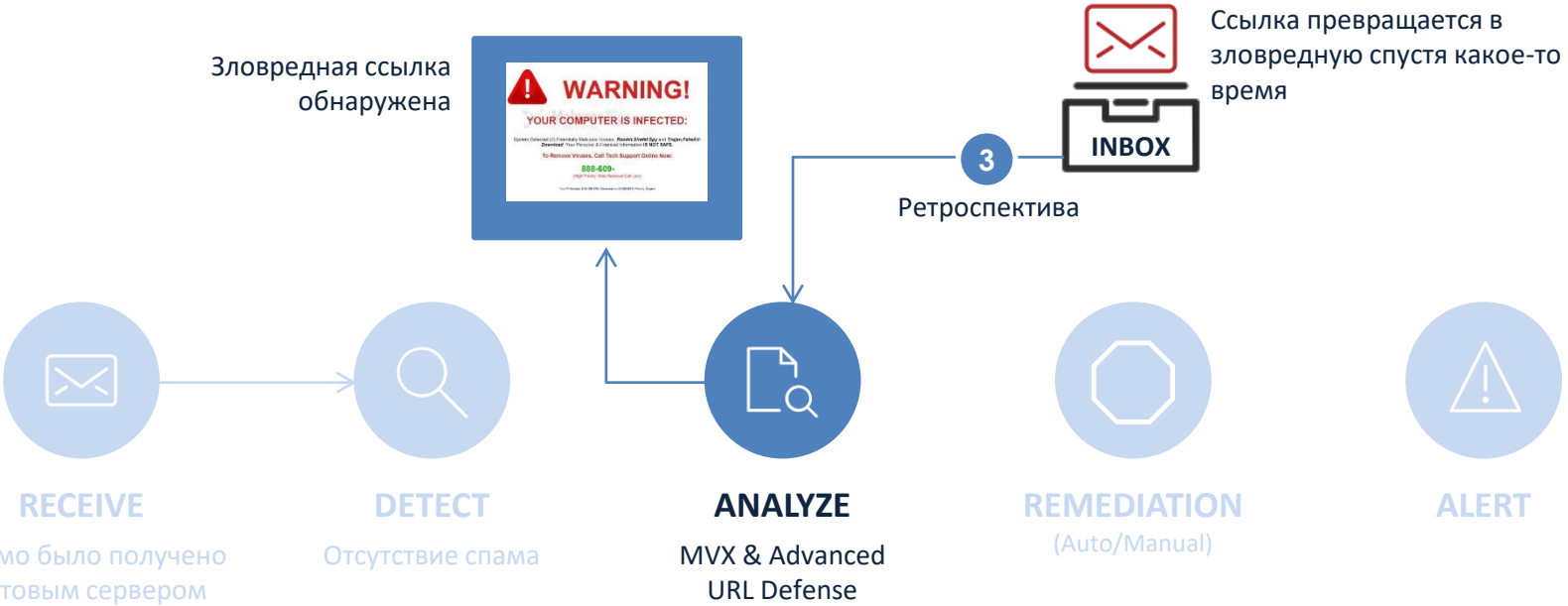
| | Alert Type | ID | File Type | Malware | Severity | Time (UTC) | Source IP | Destination IP | URL | Artifacts |
|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | Web Infection | 474 | | Malware.Binary.url | | 06/05/20 04:47:54 | 2011::1:74ec:56c5 | 2011::1:5f4d:ea6d | rogkadej.cn/nuc/index.php | |
| ☐ | Malware Object | 248 | pdf | Malware.Binary.pdf | | 06/05/20 04:45:48 | 2011::1:74ec:56c5 | 2011::1:5f4d:ea6d | rogkadej.cn/nuc/spl/pdf.pdf | HEX |
| ☐ | Malware Callback | 2542 | | Bot.Grum | | 06/05/20 04:44:22 | 2011::1:74ec:56c5 | 2011::1:77f6:cec7 | http://195.190.13.130/spm/page.php?id=1977&... | |




### Artifacts Description

| | | |
|---|---|---|
| ⚠ | Malicious Alerts | List of malicious alerts triggered during analysis |
| | OS Change Graph | Graphical view of OS change events |
| | OS Change Table | Table view of os change events. First column shows the type of event, second column shows mode of event along with the number of times it is seen, and third column shows all values for the event |
| | Macro | Extracts Macro (if exists) in doc/docx/docm samples |
| | Floss | The FireEye Labs Obfuscated String Solver (FLOSS) is an open source tool that automatically detects, extracts, and decodes obfuscated strings in Windows Portable Executable (PE) files. |
| | Screenshots | Screenshots of important events of submission |
| | Faude Screenshot | Faude screenshot |
| | PE Parser | PE Parser |
| | Gen Obj Hash | Hash of file |
| Hex | Hex | Hexadecimal view of file |
| | MITRE | Mitre Att&ck Mapping |

# Ретроспективное устранение угрозы



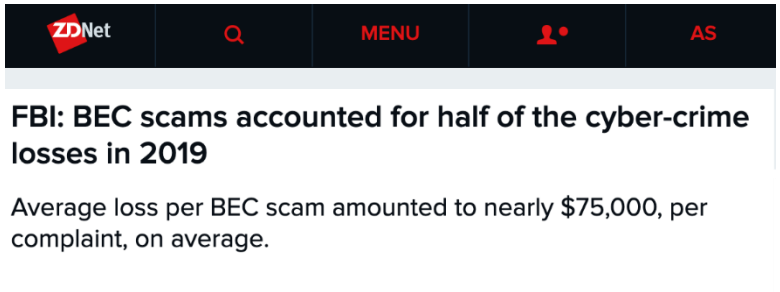
# Синхронизация с Active Directory для Anti-BEC

**True Sender :**

Steve Jobs
<steve.jobs@apple.com>

**False Sender :**

Steve Jobs
<steve.jobs@lemon.com>



# Malware Protection для MacOS

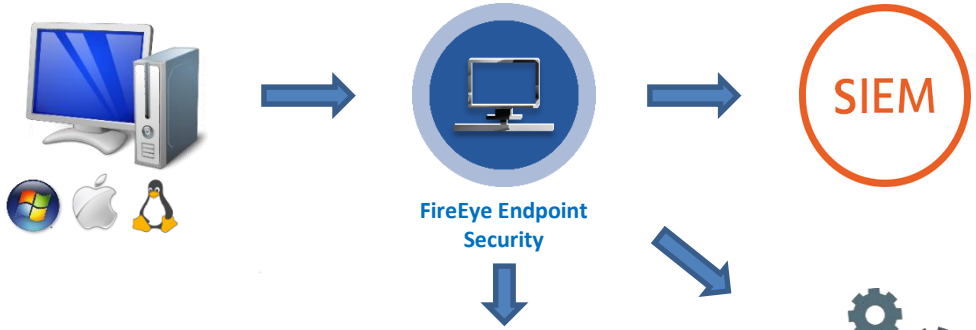

- Добавлена возможность обнаружения и блокировки ВПО с помощью машинного обучения на MacOS

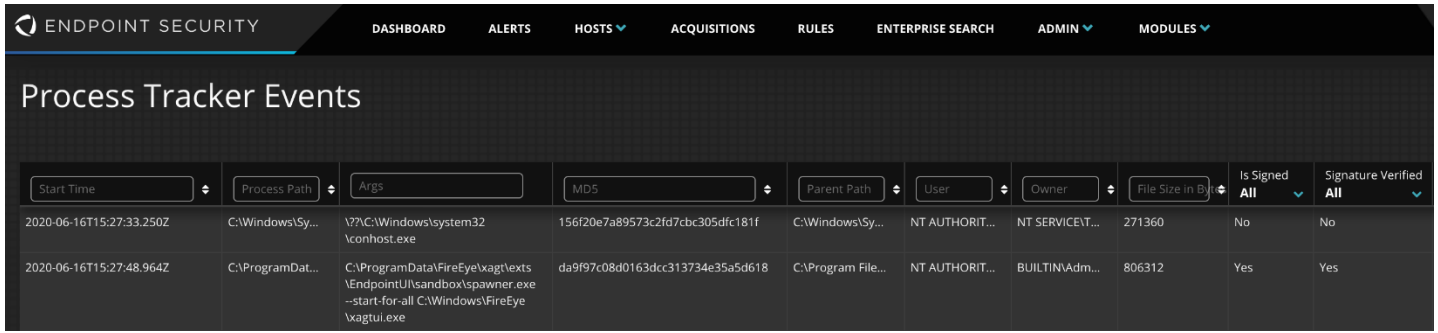
# Дополнительные модули

- В FireEye HX появилась возможность добавления дополнительных функциональных модулей. На текущий момент представлены следующие модули:
  - ✓ Process Tracker
  - ✓ Enricher
  - ✓ UAC Protect
  - ✓ Host Management
  - ✓ Event Streamer
  - ✓ Process Guard
  - ✓ Logon Tracker
  - ✓ Host Remediation
  - ✓ Agent Console
  - ✓ Triage Trigger

# Модуль Process Tracker

- Сбор и отправка журналов :
  - ✓ Path
  - ✓ Arguments
  - ✓ MD5
  - ✓ User
  - ✓ … и т д.

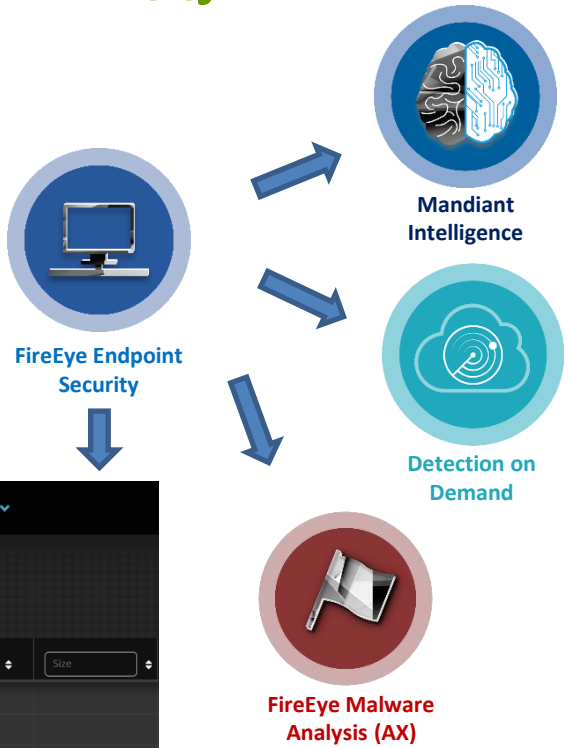


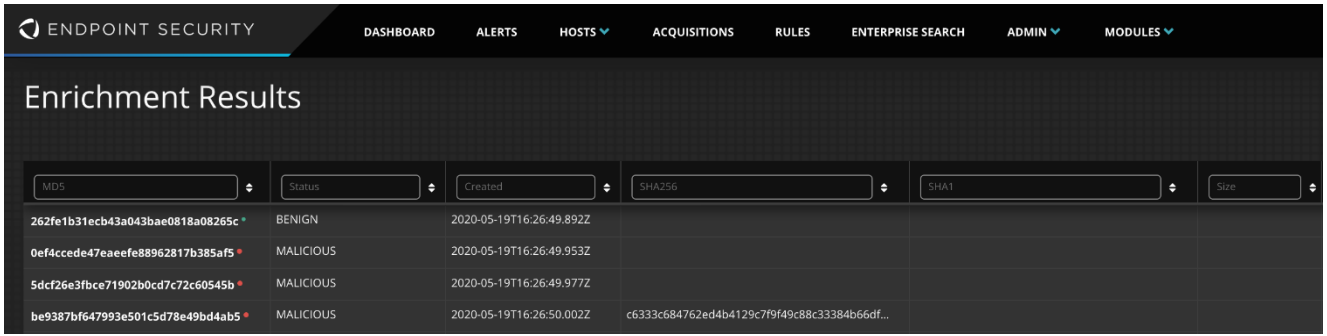



# FireEye | HX

## Модуль Enricher

- Используется с Process Tracker
- Обогащение расширенной информацией:
  - ✓ Intelligence lookup
  - ✓ Sandbox Analysis
  - ✓ Alert if Malicious



# Модуль UAC Protect

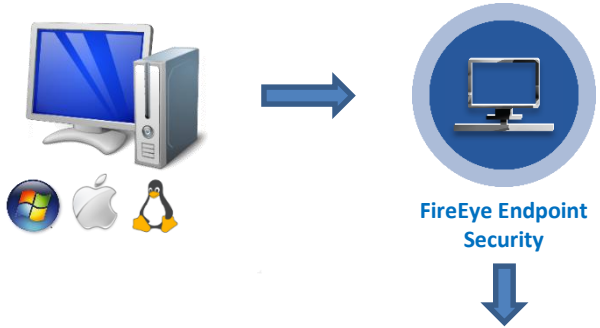
- UAC Protect предотвращает множественные UAC Bypass техники.
  - ✓ Token manipulation
  - ✓ Process Masquerading
  - ✓ Environmental Variable Hijacking
  - ✓ Shell Command Hijacking
  - ✓ COM handler Hijacking
  - ✓ Program Output Abuse

MITRE ATT&CK™

**T1036 : Masquerading**
**T1088 : Bypass User Account Control**
**T1134 : Access Token Manipulation**

# Модуль Host Management

- Поиск по:
  - ✓ Online/Offline
  - ✓ OS
  - ✓ User Logged in
  - ✓ Agent Version
  - ✓ … и т д.




ENDPOINT SECURITY

DASHBOARD | ALERTS | HOSTS | ACQUISITIONS | RULES | ENTERPRISE SEARCH | ADMIN | MODULES

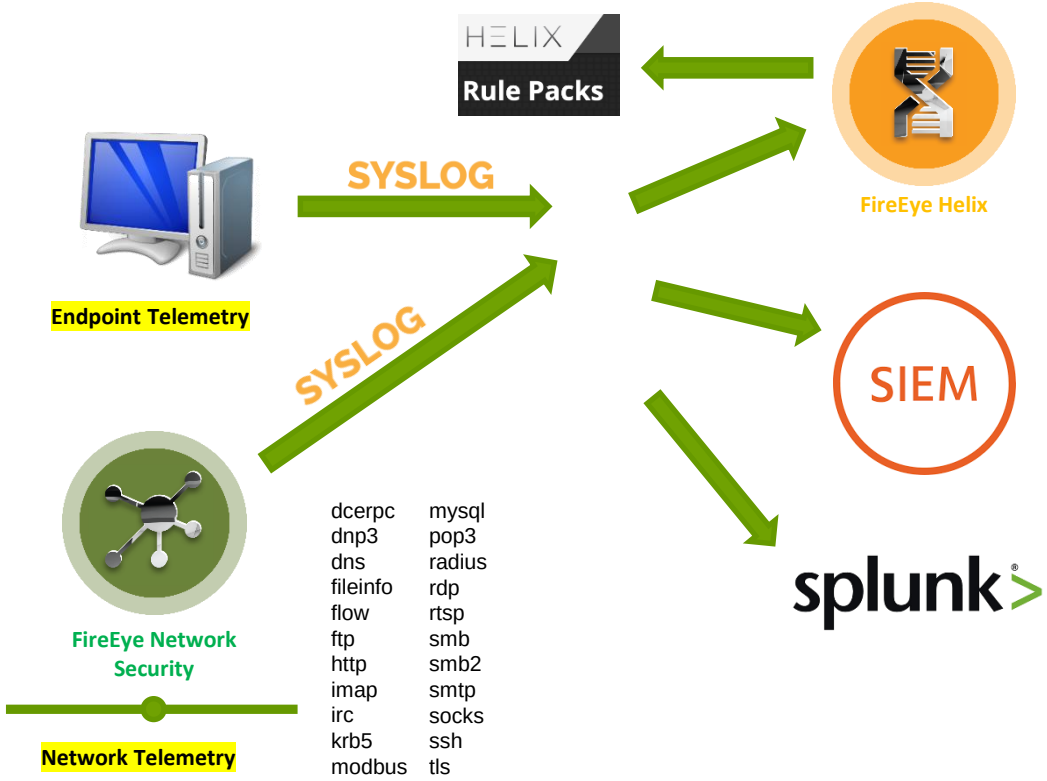
## Host Management

| Hostname | Online Status (All) | Operating Syst... | Patch | Build | Logged on User | Time Zone | Last Check-in |
|---|---|---|---|---|---|---|---|
| lateral-7c86c4fc | offline | Windows 7 Professio... | Service Pack 1 | 7601 | LATERAL-7C86C4F\Ad... | Coordinated Universal Time | 2020-05-29T00:59:31Z |
| victim-d1391f07 | offline | Windows 7 Professio... | Service Pack 1 | 7601 | VICTIM-D1391F07\Ad... | Coordinated Universal Time | 2020-05-29T00:55:20Z |
| victim-9bb52481 | offline | Windows 7 Professio... | Service Pack 1 | 7601 | VICTIM-9BB52481\Ad... | Coordinated Universal Time | 2020-05-28T15:28:22Z |
| lateral-685640e0 | offline | Windows 7 Professio... | Service Pack 1 | 7601 | LATERAL-685640E\Ad... | Coordinated Universal Time | 2020-05-28T15:28:26Z |

# FireEye | HX, NX

## Модуль Event Streamer

- Application
- Application Experience
- AppLocker
- PowerShell
- Print Service
- Security
- System
- Task Scheduler
- Terminal Services
- Windows Defender



# Модуль Process Guard

- Защита от утечки учетных данных
- Обнаружение и блокировка
- Работает по поведению – не по файлам
- MITRE ATT&CK Technique T1003

MITRE ATT&CK™

**T1003 : Credential Dumping**

**Process Guard** Version: 1.3.0

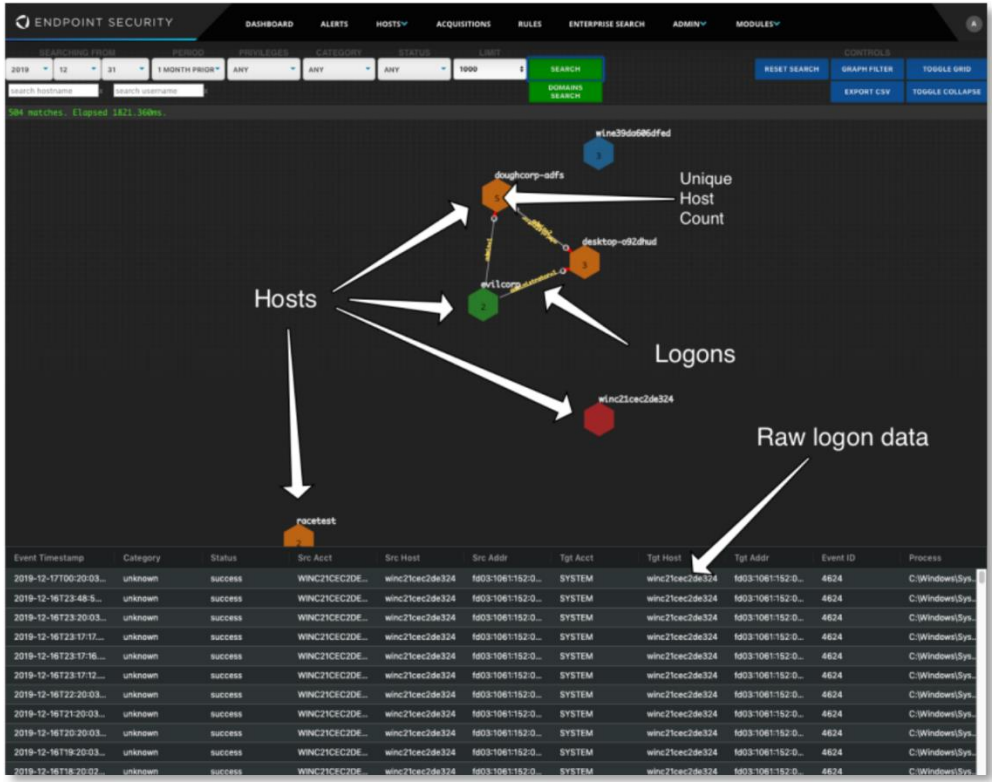
**Events**

| First Seen | Agent ID | Source Path | Target Path |
|---|---|---|---|
| 2020-03-05 23:10:29 UTC | Mw5cXAvTtv5fGbbxvlzbV6 | C:\Windows\System32\taskmgr.exe | C:\Windows\System32\lsass.exe |
| 2020-03-05 23:12:25 UTC | Mw5cXAvTtv5fGbbxvlzbV6 | C:\Program Files (x86)\FireEye\xagt\xagt.exe | C:\Windows\System32\lsass.exe |
| 2020-03-05 23:24:09 UTC | Mw5cXAvTtv5fGbbxvlzbV6 | C:\Users\admin\Downloads\ProcessExplorer\procexp64.exe | C:\Windows\System32\lsass.exe |
| 2020-03-05 23:33:32 UTC | I0V81v5HE4cfH2RH557GNp | C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.1911.3-0\MsMpEng.exe | C:\Windows\System32\lsass.exe |

# FireEye | HX

## Модуль Logon Tracker

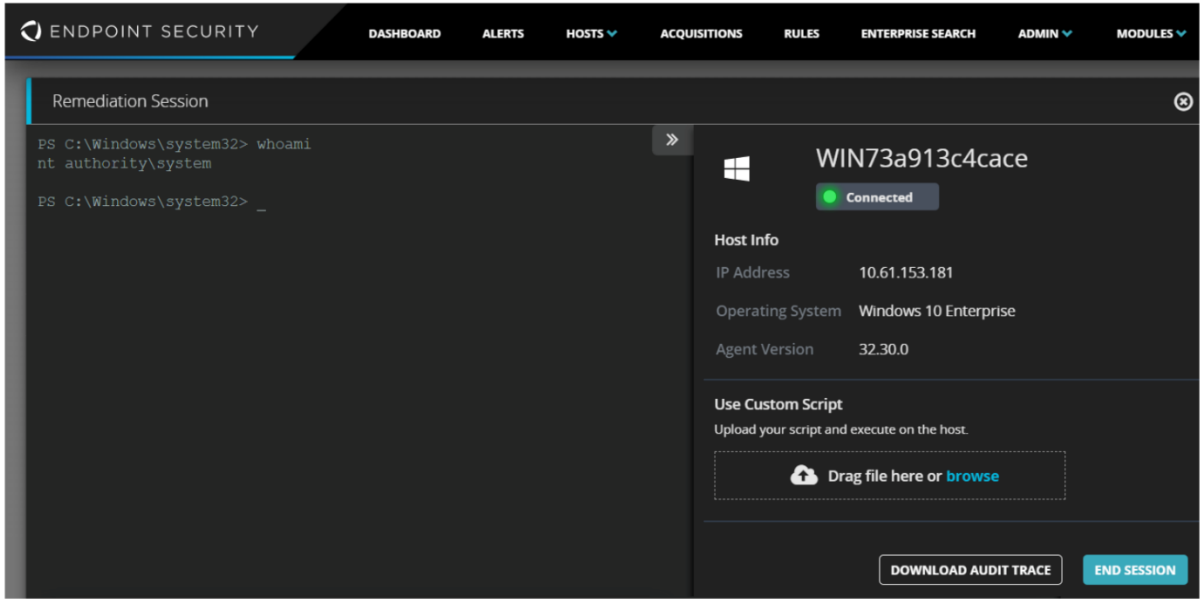
- Визуализация
- Сокращение объемов данных
- История
- Обогащение данных по событиям входа
- Инструмент для расследования
- Поиск/Фильтрация



# FireEye | HX

## Модуль Host Remediation

- Удаленная консоль
- Аудит
- Завершение процесса
- Удаление файлов
- Запуск скриптов



kaspersky

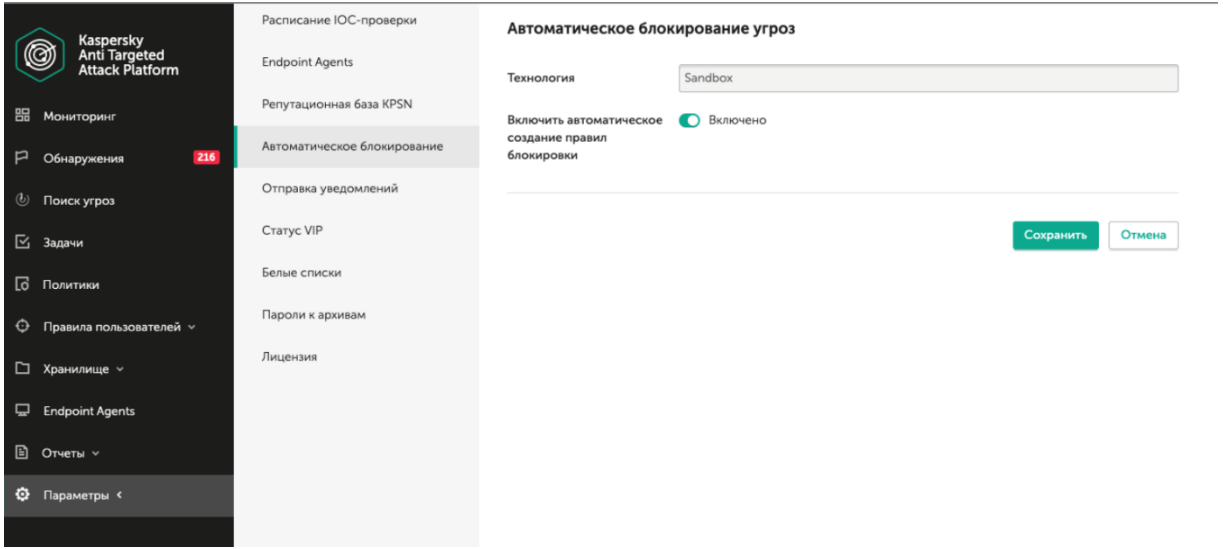
АО «Лаборатория Касперского» — международная компания, специализирующаяся на разработке систем защиты от компьютерных вирусов, спама, хакерских атак и прочих киберугроз. Основные решения:

- Kaspersky Anti Targeted Attack (KATA) Platform – платформа для защиты от комплексных целевых атак любой сложности
- Kaspersky Endpoint Detection and Response (EDR) – решение для выявления угроз и реагирования на киберинциденты на конечных устройствах
- Kaspersky Sandbox – «песочница»

# Kaspersky | KATA, KEDR

## Автоматическое предотвращение угроз

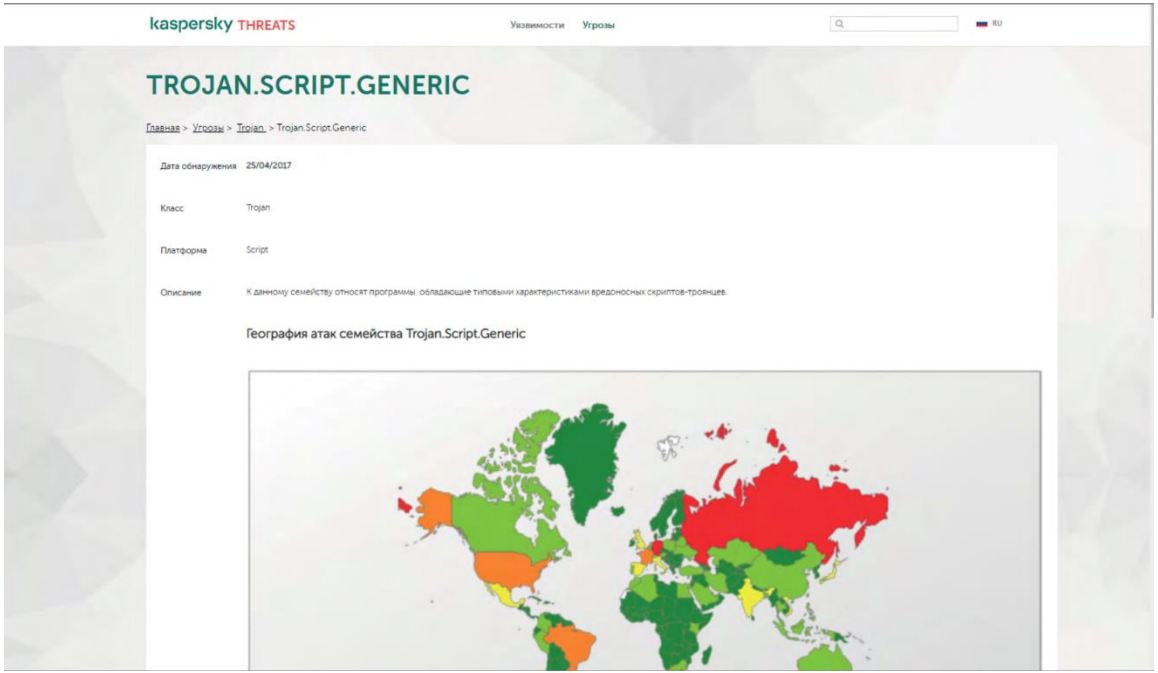
- Добавлена возможность запрета запуска подозрительных файлов на всех хостах в соответствии с заданными правилами автоматического реагирования, если песочница обнаружила угрозу



# Kaspersky | KATA, KEDR

## Просмотр описаний обнаруженных угроз

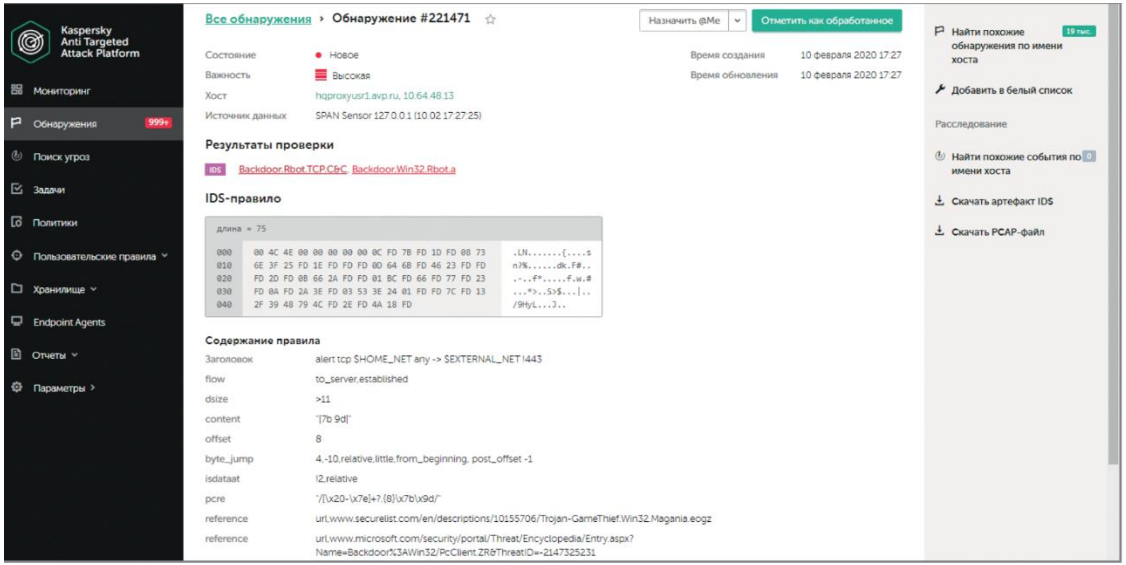
- Добавлена возможность просмотра подробного описания всех обнаруженных угроз в интерфейсе платформы Kaspersky Anti Targeted Attack / Kaspersky Endpoint Detection and Response за счет глубокой интеграции с порталом threats.kaspersky.com



# Kaspersky | KATA, KEDR

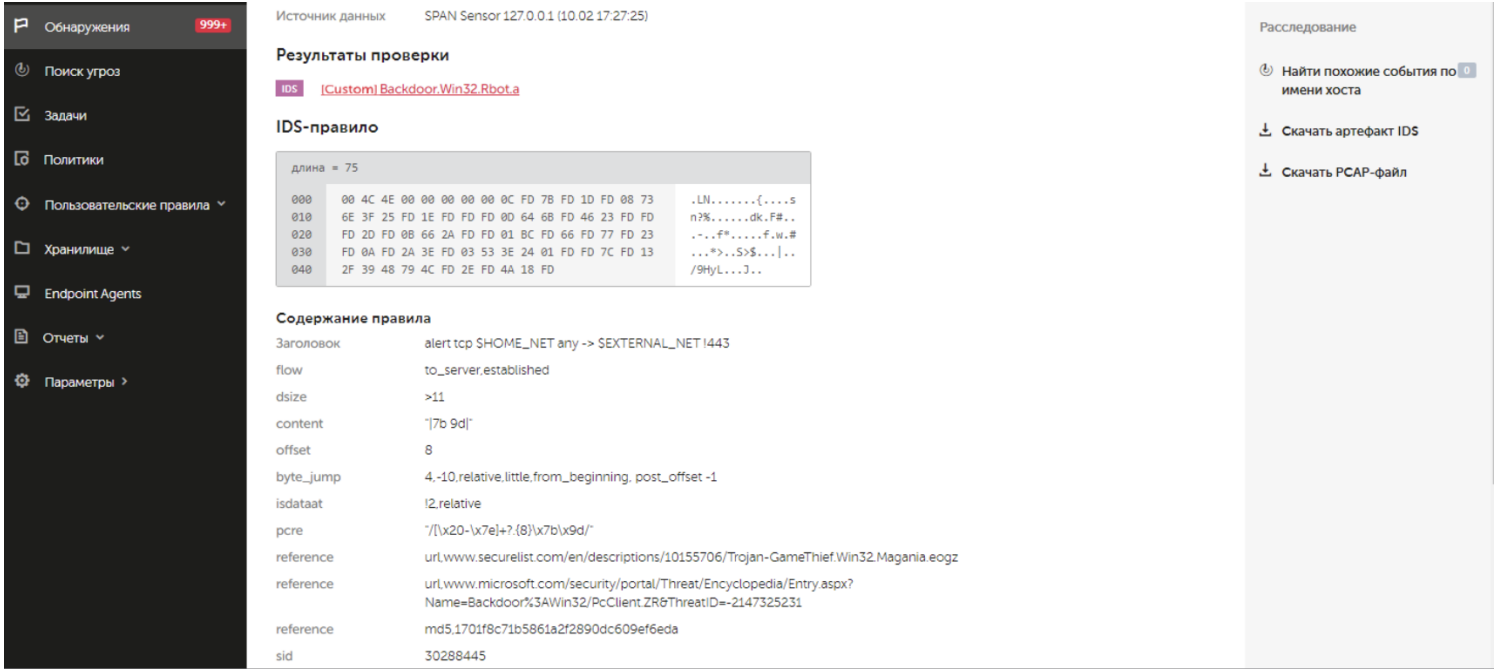
## Просмотр подробной информации о правилах IDS и загрузка файла PCAP

- Добавлена возможность просмотра пользователями описания правила, связанного с конкретным оповещением. Пакет подозрительных данных конвертируется в формат PCAP, который открывается стандартными утилитами вроде Wireshark. Пользователи затем могут скачать файл PCAP



# Загрузка собственных правил IDS

- Добавлена возможность загрузки на платформу собственных правил IDS



# Новый агент

- Новый агент был разработан для поддержки ряда других продуктов «Лаборатории Касперского». Администрировать агент можно с помощью единого интерфейса Kaspersky Security Center. Команды по установке (развертыванию), обновлениям, удалению агента и управлению настройками теперь выдаются агенту в виде единых задач (независимо от того, в какое решение он встроен)

# Kaspersky | KATA, KEDR

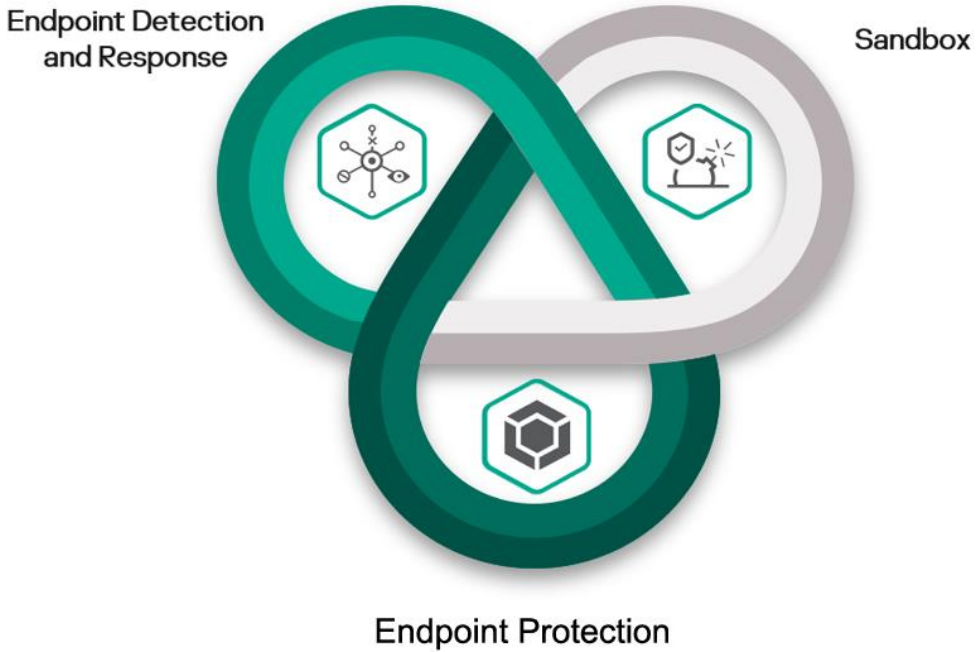
## Распределенный карантин

- Больше не нужно отправлять подозрительные файлы в центральный узел Kaspersky Endpoint Detection and Response для помещения на карантин – теперь каждый агент может помещать файлы на карантин самостоятельно

# Kaspersky | Sandbox

## Интеграция с Kaspersky Security для бизнеса

- Решение позволяет проводить углубленный динамический анализ угроз и автоматически блокировать сложные атаки, которые обходят средства защиты рабочих мест



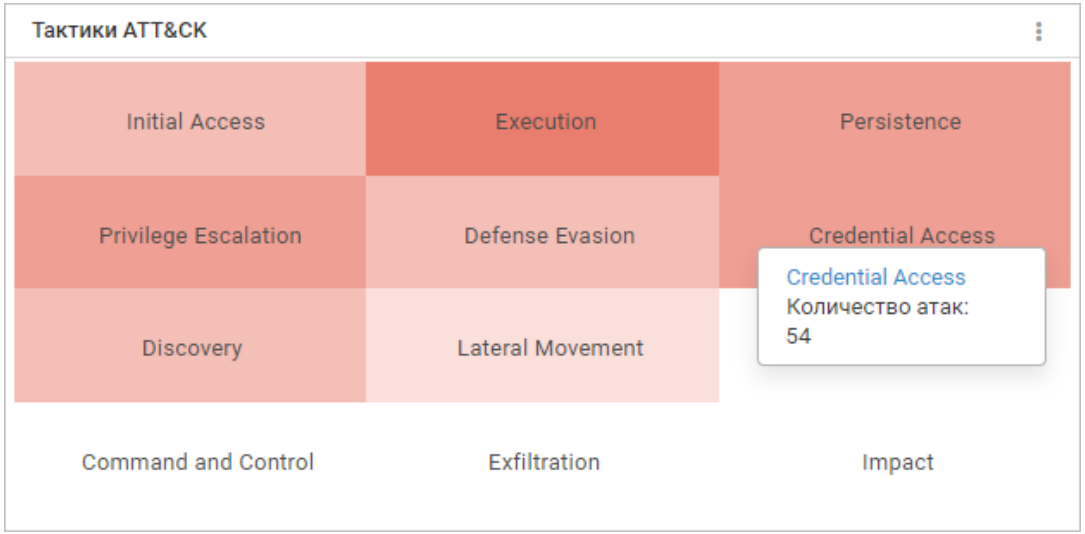

Positive Technologies — международная компания, специализирующаяся на разработке программного обеспечения в области информационной безопасности. Основные решения:

- PT MS – многоуровневая система защиты от вредоносных программ
- PT NAD – система глубокого анализа сетевого трафика для выявления атак на периметре и внутри сети
- PT Sandbox – «песочница»

- PT MS и PT NAD вместе образуют решение Anti-APT

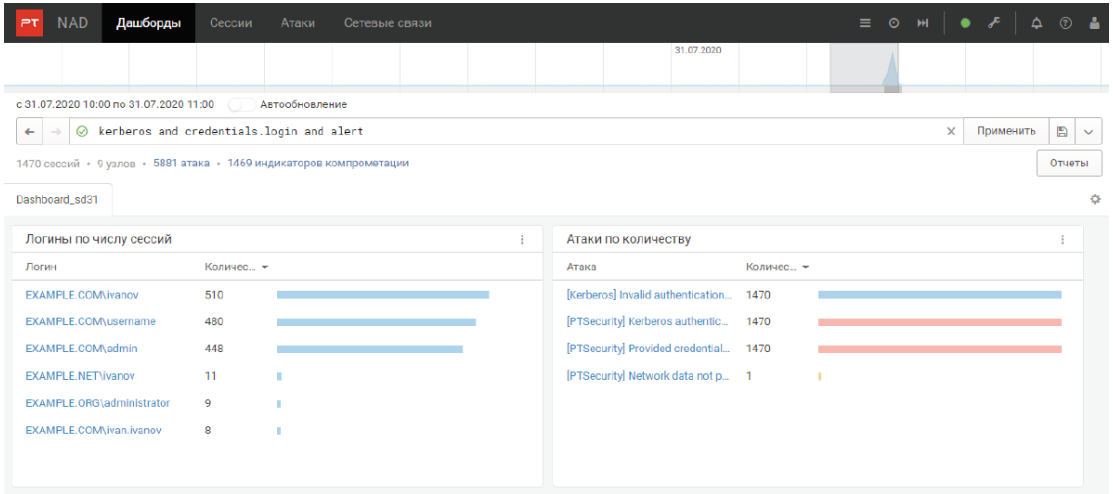
# Стадии атак по матрице ATT&CK

- В новой версии PT NAD (10 версия) появилась тепловая карта с тактиками по модели MITRE ATT&CK



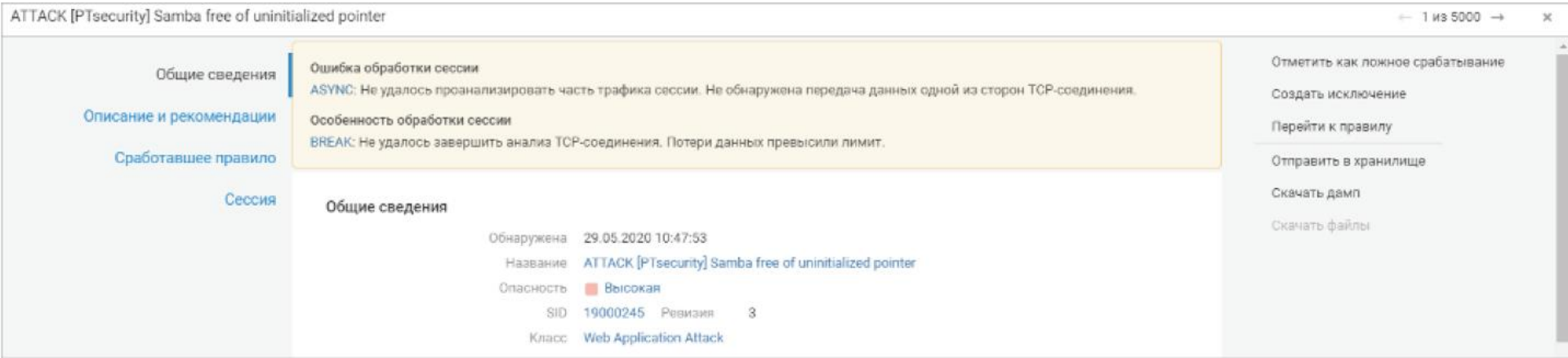
## Определение учетных данных пользователя при аутентификации Kerberos

- Теперь PT NAD может определять учетные данные пользователя при аутентификации по протоколу Kerberos. В результате у любого сетевого соединения, использующего этот тип аутентификации, появляется дополнительный признак — логин доменной учетной записи пользователя. Эти данные упрощают выявление фактов несанкционированного доступа.



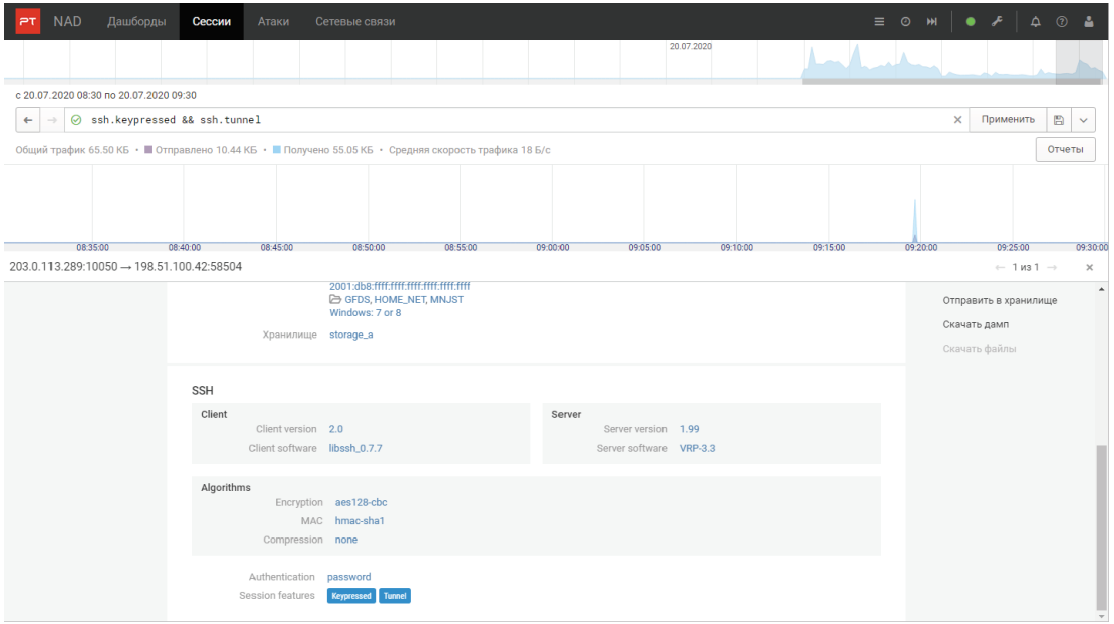
## Улучшения в отображении флагов и ошибок обработки сессий

- Начиная с версии 10.0 в карточках сессий и атак флаги и ошибки обработки сессии отображаются в отдельных блоках



# Расширенный анализ SSH-сессии

- PT NAD может проводить расширенный анализ SSH-сессии, который включает в себя:
  - ✓ определение типа трафика в зашифрованном соединении
  - ✓ получение информации об аутентификации: как прошла, сколько было неудачных попыток
  - ✓ обнаружение интерактивных данных в сессии, передачи файлов и создания туннелей

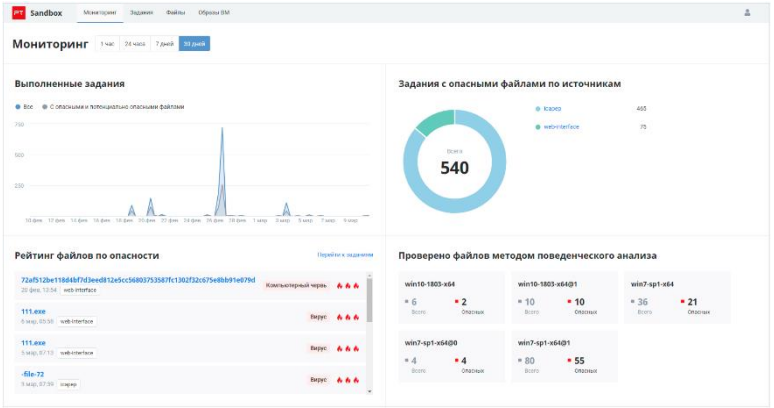


# Автоматическое обновление образов ловушек

- Начиная с версии 2.7 PT MS обновление образов ловушек теперь выполняется в автоматическом режиме: обновление гипервизора, удаление неподдерживаемых образов ловушек и повторная генерация подобразов ловушек более не требуются

# PT Sandbox как отдельный продукт

- PT Sandbox — песочница для защиты от целевых и массовых атак с применением неизвестного вредоносного ПО. Поддерживает гибкую настройку виртуальных сред в соответствии с реальными рабочими станциями и надежно защищена от техник обхода песочниц. Продукт обеспечивает комплексный анализ файлов и трафика, включая шифрованный, а также выявляет скрытые и новейшие угрозы с помощью регулярного ретроспективного анализа



**СПАСИБО ЗА ВНИМАНИЕ!**

**ПО ВСЕМ ВОПРОСАМ ОБРАЩАЙТЕСЬ НА EMAIL:**

marketing@dialognauka.ru