

---

## НОВОСТИ ИЗ МИРА АРТ

# ЧТО НОВОГО ПРЕДЛАГАЮТ РАЗРАБОТЧИКИ АНТИ-АРТ РЕШЕНИЙ?

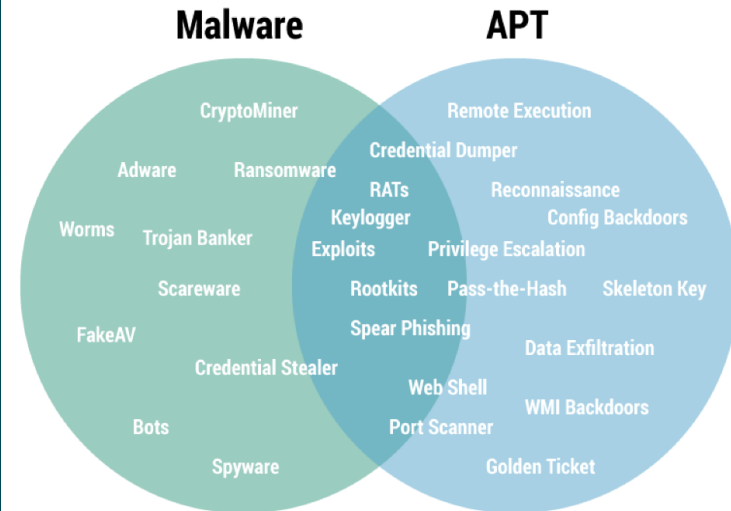
Владимир Соловьев  
Старший специалист АО «ДиалогНаука»  
24 ноября 2020 года

- ❖ 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



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



# Этапы АРТ-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

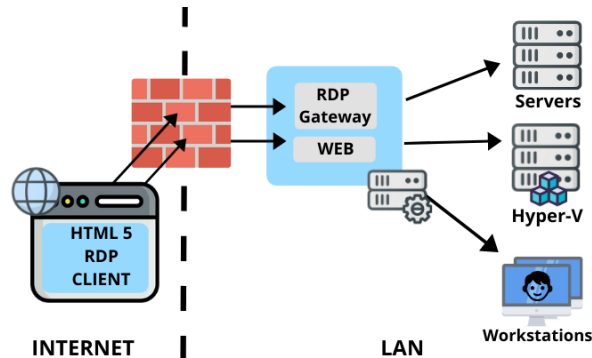
## Достижение цели



- ❖ Хищение данных
- ❖ Изменение данных
- ❖ Связь с управляющими серверами
- ❖ Соккрытие следов
- ❖ Ботнет сеть

# Общая статистика по АРТ-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 АРТ-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



**POSITIVE  
TECHNOLOGIES**

## **НОВОСТИ ИЗ МИРА ART**

ЧТО НОВОГО ПРЕДЛАГАЮТ РАЗРАБОТЧИКИ ANTI-ART РЕШЕНИЙ?

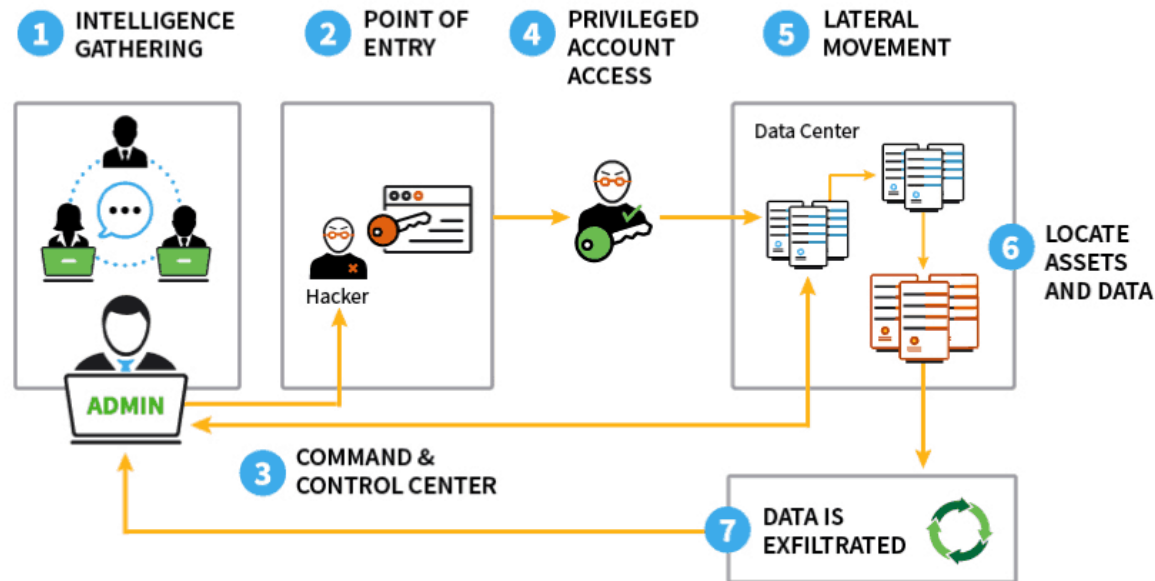


FireEye – американская компания, выпускающая средства защиты информации от атак нового поколения (APT). Основные решения:

- ❖ FireEye EX – система защиты электронной почты
- ❖ FireEye NX – система веб-защиты от вредоносных программ
- ❖ FireEye CM – система централизованного управления
- ❖ FireEye NX – 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 Network SmartVision as of 06/03/2020 17:54:00 Etc/UTC

Group By: name Date Range: 05/03/2020 17:54:00 - 06/03/2020 17:54:00 Severity: all

MAX SEVERITY	NAME	ALERT COUNT	FIRST SEEN	LAST SEEN
●●●●●	Directory Listing Of Users Folder	1	05/15/20 19:13:56	05/15/20 19:13:56

### User Activity Details

Last 2 Logged in User details with this 192.168.99.101

Domain \ User Name	Last Seen Time	AD Server	User Account Properties	Domain \ Group Name
INSECURE \ user3	05/15/20 19:33:31.218914	10.128.44.237	Disabled: false Password Expires: false Password Required: true	INSECURE \ Domain Users INSECURE \ sample DOMAINCONTROLLE \ Administrators
INSECURE \ user1	05/15/20 19:31:07.308661	10.128.44.237	Disabled: false Password Expires: false Password Required: true	INSECURE \ sample DOMAINCONTROLLE \ Administrators INSECURE \ Domain Users

## 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	
Malware Callback	2542		Bot.Grwm	●●●○○	06/05/20 04:44:22	2011::1:74ec:56c5	2011::1:77f6:cec7	http://195.190.13.130/spm/page.php?id=1977&...	

### MITRE

## MITRE ATT&CK™ details

**Exploitation for Privilege Escalation**

**T1068**

Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform Privilege Escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This may be a necessary step for an adversary compromising a endpoint system that has been properly configured and limits other privilege escalation methods.

**Rules Hit**

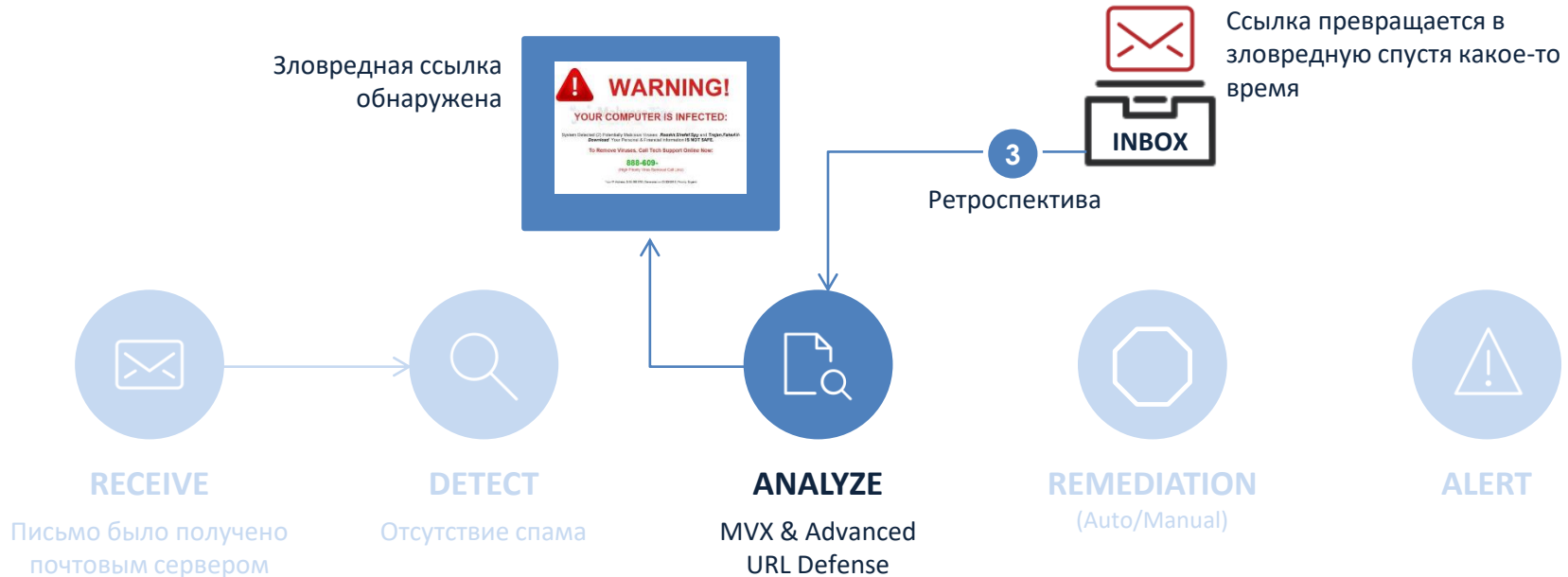
- Heuristic\_Detected\_Suspicious\_MultiDomain\_Similarity

Technique	Impact
Exploitation	Impact

### 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	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>



**FBI: BEC scams accounted for half of the cyber-crime losses in 2019**

Average loss per BEC scam amounted to nearly \$75,000, per complaint, on average.



## Malware Protection для MacOS



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

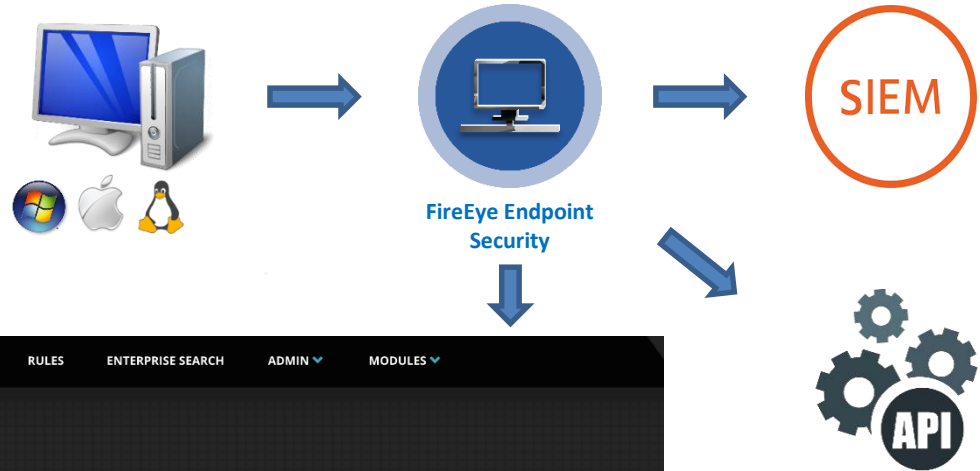
## Дополнительные модули

❖ 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

### ❖ Сбор и отправка журналов :

- ✓ Path
- ✓ Arguments
- ✓ MD5
- ✓ User
- ✓ ... И Т Д.

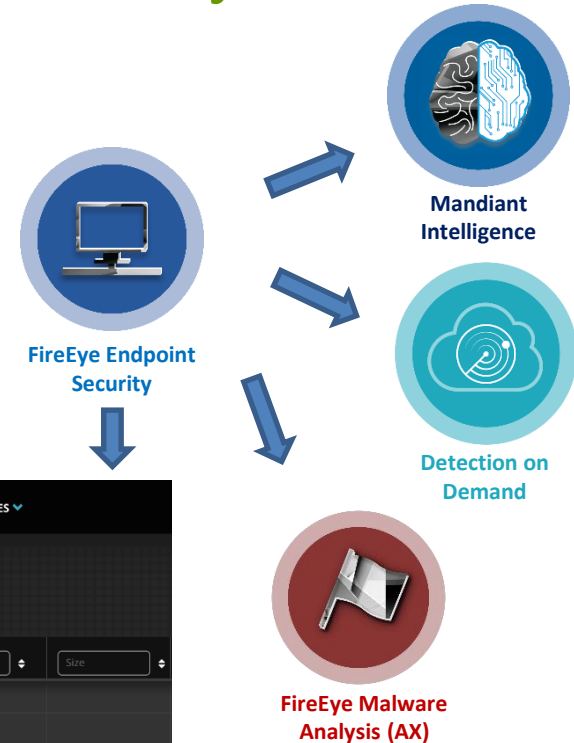


Start Time	Process Path	Args	MD5	Parent Path	User	Owner	File Size in Bytes	Is Signed	Signature Verified
2020-06-16T15:27:33.250Z	C:\Windows\Sy...	\?C:\Windows\system32 \conhost.exe	156f20e7a89573c2fd7cbc305dfc181f	C:\Windows\Sy...	NT AUTHORITY...	NT SERVICE...	271360	No	No
2020-06-16T15:27:48.964Z	C:\ProgramDat...	C:\ProgramData\FireEye\agt\texts EndpointUI\sandbox\spawner.exe --start-for-all C:\Windows\FireEye \xagtui.exe	da9f97c08d0163dcc313734e35a5d618	C:\Program File...	NT AUTHORITY...	BUILTIN\Adm...	806312	Yes	Yes

# FireEye | HX

## Модуль Enricher

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



ENDPOINT SECURITY

DASHBOARD ALERTS HOSTS ACQUISITIONS RULES ENTERPRISE SEARCH ADMIN MODULES

### Enrichment Results

MD5	Status	Created	SHA256	SHA1	Size
262fe1b31ecb43a043bae0818a08265c	BENIGN	2020-05-19T16:26:49.892Z			
0ef4ccede47eaeefe88962817b385af5	MALICIOUS	2020-05-19T16:26:49.953Z			
5dcf26e3fbce71902b0cd7c72c60545b	MALICIOUS	2020-05-19T16:26:49.977Z			
be9387bf647993e501c5d78e49bd4ab5	MALICIOUS	2020-05-19T16:26:50.002Z	c6333c684762ed4b4129c79f49c88c33384b66df...		

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



**T1036 : Masquerading**

**T1088 : Bypass User Account Control**

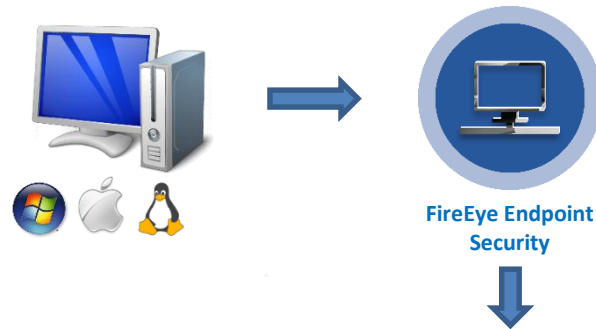
**T1134 : Access Token Manipulation**



## Модуль Host Management

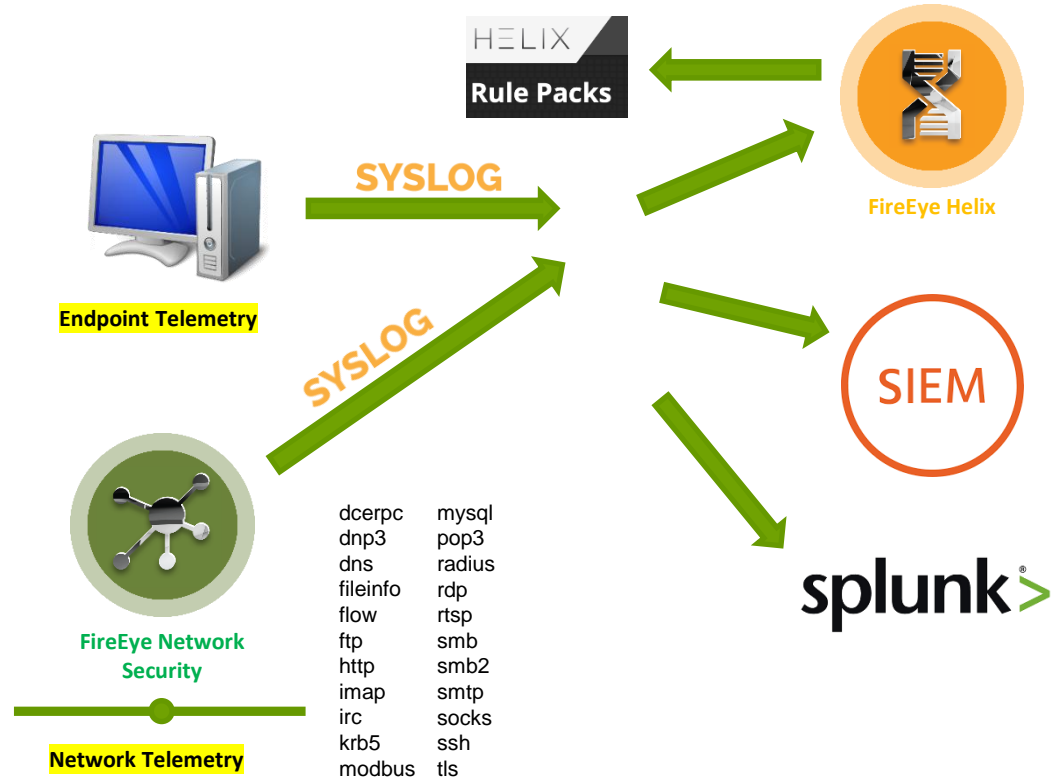
### ❖ Поиск по:

- ✓ 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	Operating Syst...	Patch	Build	Logged on User	Time Zone	Last Check-in
lateral-7c86c4fc	● offline	Windows 7 Professio...	Service Pack 1	7601	LATERAL-7C86C4FAd...	Coordinated Universal Time	2020-05-29T00:59:31Z
victim-d1391f07	● offline	Windows 7 Professio...	Service Pack 1	7601	VICTIM-D1391F07Ad...	Coordinated Universal Time	2020-05-29T00:55:20Z
victim-9bb52481	● offline	Windows 7 Professio...	Service Pack 1	7601	VICTIM-9BB52481Ad...	Coordinated Universal Time	2020-05-28T15:28:22Z
lateral-685640e0	● offline	Windows 7 Professio...	Service Pack 1	7601	LATERAL-685640EAd...	Coordinated Universal Time	2020-05-28T15:28:26Z

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



- ❖ 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**

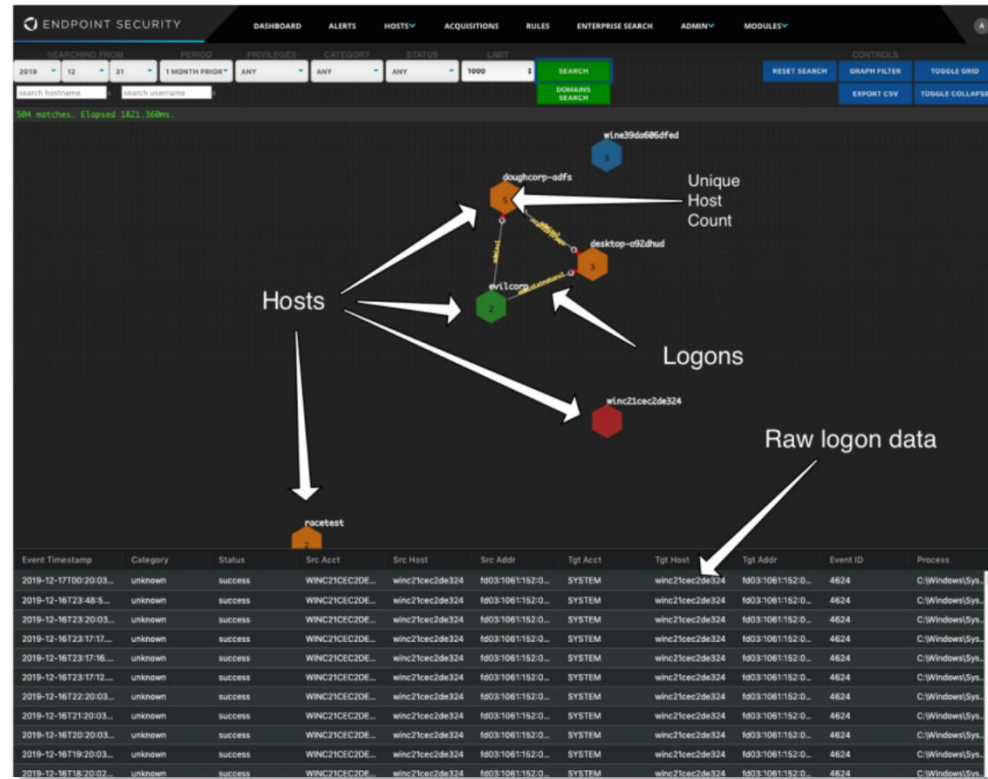
**Process Guard** Version: 1.3.0

Events

First Seen	Agent ID	Source Path	Target Path
2020-03-05 23:10:29 UTC	MwScXAvTv5fGbbxvzbV6	C:\Windows\System32\taskmgr.exe	C:\Windows\System32\lsass.exe
2020-03-05 23:12:25 UTC	MwScXAvTv5fGbbxvzbV6	C:\Program Files (x86)\FireEye\agrt\agrt.exe	C:\Windows\System32\lsass.exe
2020-03-05 23:24:09 UTC	MwScXAvTv5fGbbxvzbV6	C:\Users\admin\Downloads\Process Explorer\procxp64.exe	C:\Windows\System32\lsass.exe
2020-03-05 23:33:32 UTC	I0V81vSHE4cH2RH557GNp	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.1911.3-0\MsMpEng.exe	C:\Windows\System32\lsass.exe

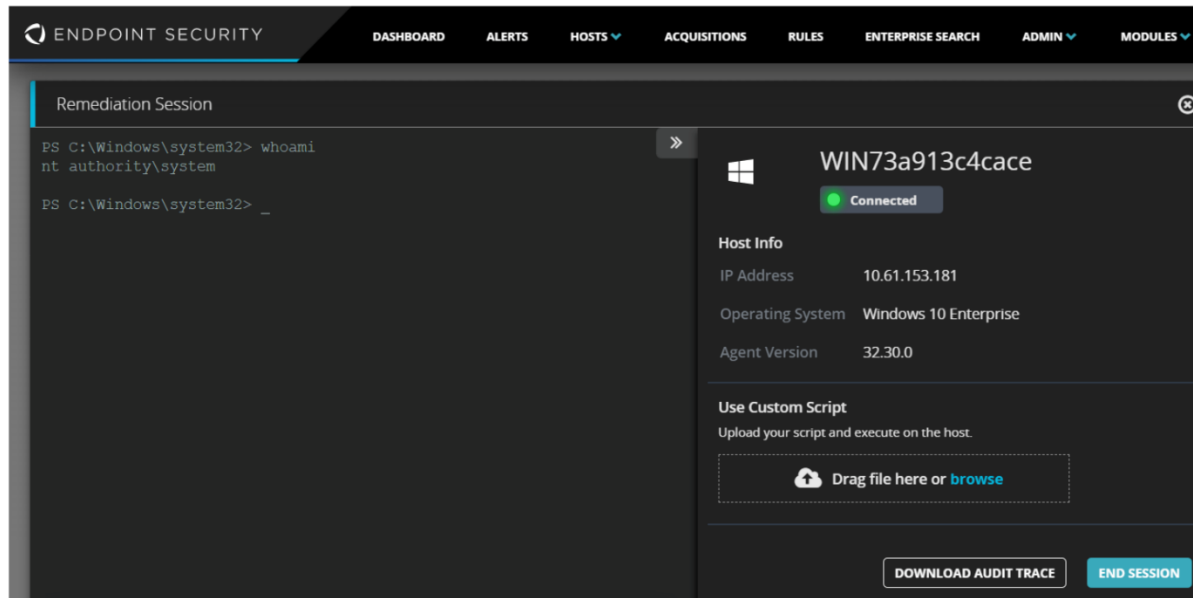


- ❖ Визуализация
- ❖ Сокращение объемов данных
- ❖ История
- ❖ Обогащение данных по событиям входа
- ❖ Инструмент для расследования
- ❖ Поиск/Фильтрация



## Модуль Host Remediation

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



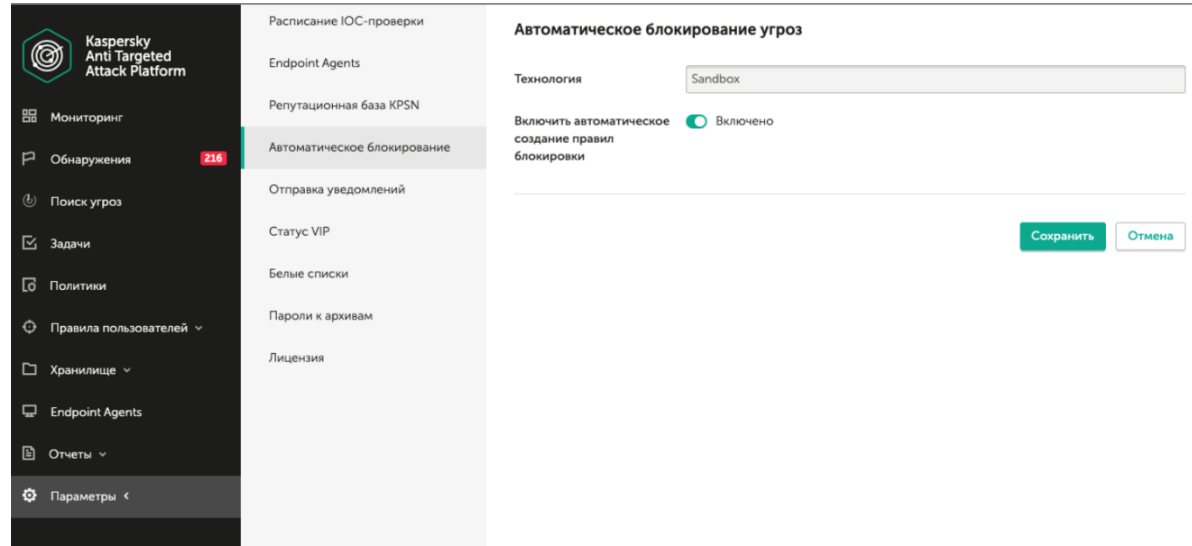
# kaspersky

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»

## Автоматическое предотвращение угроз

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



## 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](https://threats.kaspersky.com)

The screenshot displays the Kaspersky THREATS portal interface. At the top, the logo 'kaspersky THREATS' is visible, along with navigation links for 'Уязвимости' and 'Угрозы', a search bar, and a language selector set to 'RU'. The main heading is 'TROJAN.SCRIPT.GENERIC'. Below this, a breadcrumb trail reads 'Главная > Угрозы > Троян > Trojan.Script.Generic'. A table provides key details:

Дата обнаружения	25/04/2017
Класс	Троян
Платформа	Script
Описание	К данному семейству относят программы, обладающие типовыми характеристиками вредоносных скриптов-троянцев.

Below the table, the section 'География атак семейства Trojan.Script.Generic' features a world map where countries are color-coded to show attack activity. Red indicates high activity, notably in Russia and parts of Europe and Asia. Green and orange indicate lower levels of activity across other regions.

## 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

The screenshot displays the Kaspersky Anti Targeted Attack Platform interface. The left sidebar contains navigation options: Мониторинг, Обнаружения (999), Поиск угроз, Задчи, Политики, Пользовательские правила, Хранилище, Endpoint Agents, Отчеты, and Параметры. The main content area shows details for detection #221471, including its status (Новое), severity (Высокая), host (hdrokuyet1.vpr.ru), and source (SPAN Sensor 127.0.0.1). It lists related rules: Backdoor.Rbot.TCP.CnC and Backdoor.Win32.Rbot.a. A hex dump of the packet data is shown, along with the rule's signature: alert:tcp \$HOME\_NET any -> \$EXTERNAL\_NET 1443. The rule content includes flow, dsize, content, offset, byte\_jump, isdataat, pcre, and reference fields.

Состояние	Новое	Время создания	10 февраля 2020 17:27
Важность	Высокая	Время обновления	10 февраля 2020 17:27
Хост	hdrokuyet1.vpr.ru, 10.64.48.13		
Источник данных	SPAN Sensor 127.0.0.1 (10.02.17.27.25)		

**Результаты проверки**

IDS-правило

```
000 00 4C 4E 00 00 00 00 8C FD 78 FD 1D FD 08 73 .LU.....{...s
010 6E 3F 25 FD 1E FD FD 00 64 68 FD 46 23 FD FD n%.....dk.F..
020 FD 2D FD 08 66 2A FD FD 01 8C FD 66 FD 77 FD 23 ...*F.....F.w.#
030 FD 0A FD 2A 3E FD FD 03 53 3E 24 01 FD FD 7C FD 13 ...*..5$5...|..
040 2F 39 48 79 4C FD 2E FD 4A 18 FD /9tly....3..
```

**Содержание правила**

Заголовок	alert:tcp \$HOME_NET any -> \$EXTERNAL_NET 1443
flow	to_server.established
dsize	>11
content	[7b 9d]
offset	8
byte_jump	4-10.relative.little.from.beginning_post_offset-1
isdataat	!2.relative
pcre	/[\x20-\x7e]{8}[\x7b\x9d]/
reference	url.www.securelist.com/en/descriptions/10155706/Trojan-GameThief.Win32.Magania.eozg
reference	url.www.microsoft.com/security/portals/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32/PcClient.ZR8ThreatID=2147325231

## Загрузка собственных правил IDS

- ❖ Добавлена возможность загрузки на платформу собственных правил IDS

Источник данных SPAN Sensor 127.0.0.1 (10.02.17:27:25)

**Результаты проверки**

IDS [\[Custom\] Backdoor.Win32.Rbot.a](#)

**IDS-правило**

длина = 75

000	00 4C 4E 00 00 00 00 0C FD 7B FD 1D FD 08 73	.LN.....{...s
010	6E 3F 25 FD 1E FD FD 00 64 68 FD 46 23 FD FD	n?%.....dk.F#..
020	FD 2D FD 08 66 2A FD FD 01 8C FD 66 FD 77 FD 23	..-..F*.....F.w.#
030	FD 0A FD 2A 3E FD 03 53 3E 24 01 FD FD 7C FD 13	...*>..5>\$... ..
040	2F 39 48 79 4C FD 2E FD 4A 18 FD	/9HyL...J..

**Содержание правила**

Заголовок	alert tcp \$HOME_NET any -> \$EXTERNAL_NET  443
flow	to_server,established
dsize	>11
content	" 7b 9d "
offset	8
byte_jump	4,-10,relative,little,from_beginning,post_offset-1
isdataat	!2,relative
pcrc	"/[\\x20-\\x7e]+?.{8}\\x7b\\x9d/"
reference	url,www.securelist.com/en/descriptions/10155706/Trojan-GameThief.Win32.Maganla.eogz
reference	url,www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32/PCClient.ZR&ThreatID=-2147325231
reference	md5,1701f8c71b5861a2f2890dc609ef6eda
sid	30288445

Расследование

- Найти похожие события по имени хоста
- Скачать артефакт IDS
- Скачать PCAP-файл

- ❖ 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



## Интеграция с Kaspersky Security для бизнеса

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

Endpoint Detection  
and Response

Sandbox



Endpoint Protection



## POSITIVE TECHNOLOGIES

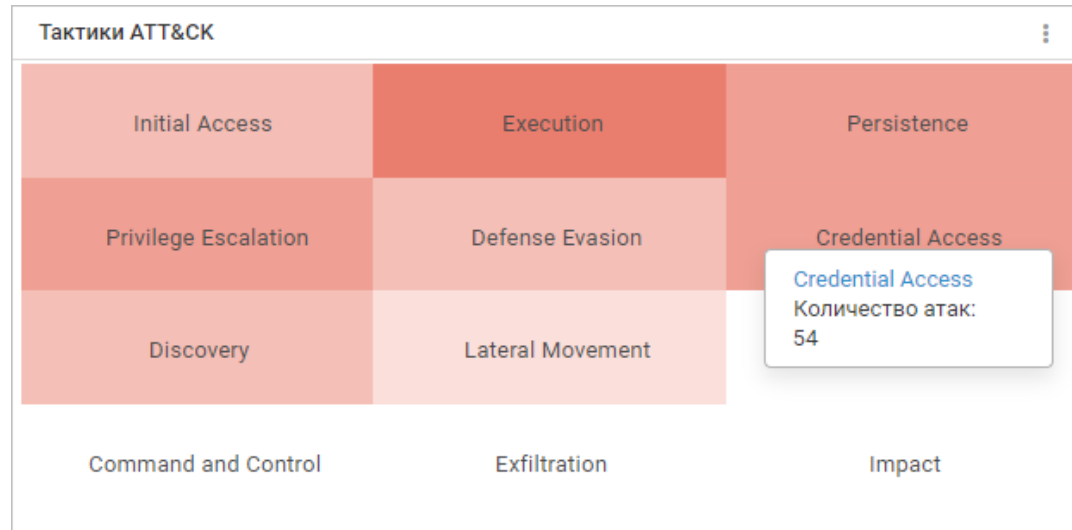
Positive Technologies — международная компания, специализирующаяся на разработке программного обеспечения в области информационной безопасности. Основные решения:

- ❖ 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

# Positive Technologies | PT NAD

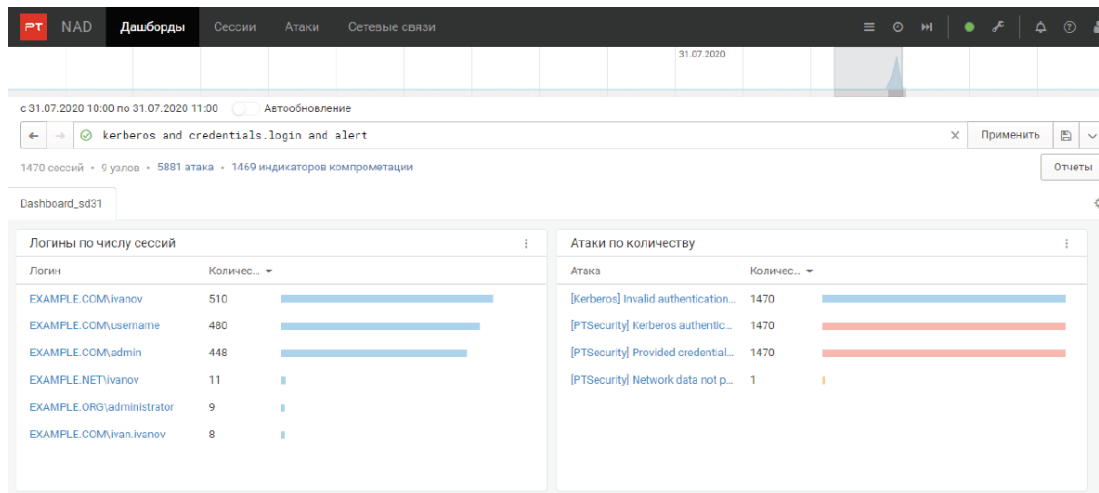
## Стадии атак по матрице ATT&CK

- ❖ 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

The screenshot displays the PT NAD interface for a specific attack rule. The main content area is divided into several sections:

- Общие сведения** (General information):
  - Ошибка обработки сессии** (Session processing error):
    - ASYNC: Не удалось проанализировать часть трафика сессии. Не обнаружена передача данных одной из сторон TCP-соединения.
    - Особенность обработки сессии
    - BREAK: Не удалось завершить анализа TCP-соединения. Потери данных превысили лимит.
  - Общие сведения** (General information):
    - Обнаружена: 29.05.2020 10:47:53
    - Название: ATTACK [PTsecurity] Samba free of uninitialized pointer
    - Опасность: ■ Высокая
    - SID: 19000245 Ревизия: 3
    - Класс: Web Application Attack
- Сессия** (Session):

On the right side, there is a vertical menu with the following options:

- Отметить как ложное срабатывание
- Создать исключение
- Перейти к правилу
- Отправить в хранилище
- Скачать дамп
- Скачать файлы



## 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

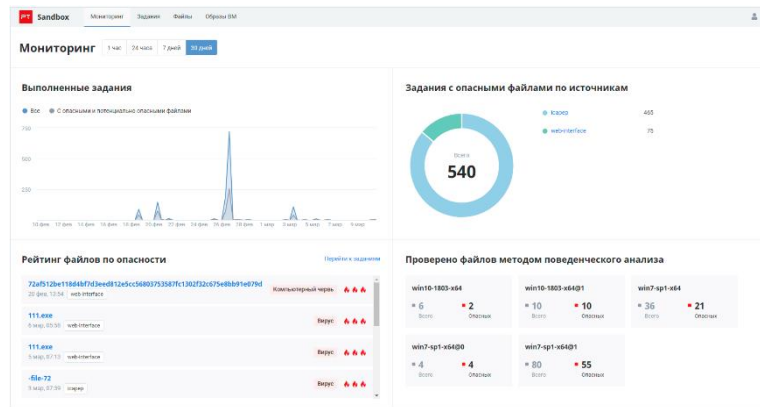




# Positive Technologies | PT Sandbox

## 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 зашифрованный, а также выявляет скрытые и новейшие угрозы с помощью регулярного ретроспективного анализа



---

**СПАСИБО ЗА ВНИМАНИЕ!**

**ПО ВСЕМ ВОПРОСАМ ОБРАЩАЙТЕСЬ НА EMAIL:**

[marketing@dialognauka.ru](mailto:marketing@dialognauka.ru)