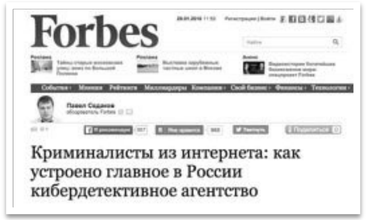


GROUP-IB

13 лет
опыта в сфере компьютерной криминалистики, консалтинга и аудита информбезопасности

100+
успешных расследований в России и Европе

125000+
инцидентов, обработанных круглосуточным Центром реагирования CERT-GIB

$70M
сохранили наши клиенты в 2015 году с помощью решений Bot-Trek

Крупнейшая и самая опытная **Лаборатория компьютерной криминалистики** в Восточной Европе

Круглосуточный Центр реагирования на инциденты информационной безопасности **CERT-GIB**

Система раннего предупреждения киберугроз Bot-Trek™ с использованием данных кибервразведки и машинного обучения

Интеллектуальная защита бренда и цифрового контента – сервисы **GIB Brand Protection** и **AntiPiracy**

Официальный партнер Europol, полицейской службы Евросоюза

Компания, рекомендованная Организацией по безопасности и сотрудничеству в Европе (ОБСЕ)

Одна из 7 самых влиятельных компаний в области кибербезопасности по версии Business Insider UK

Первый российский поставщик threat intelligence решений, вошедший в отчеты Gartner

НАМ ДОВЕРЯЮТ

Лауреат «Премии Рунета 2013»

Лауреат премии «Компания года 2012»

Финансовый сектор
Сбербанк, ВТБ24, Альфа-Банк, QIWI, Открытие

Промышленность и связь
Ростех, Газпром, Роснефть, Базовый элемент, Норникель

Государственный сектор

Зарубежные клиенты
Microsoft, citi, Raiffeisen BANK, Capital One, HUAWEI, orange

Связь, IT, технологии
Ростелеком, МТС, Билайн, Avito, hh.ru, Одноклассники

Медиа, развлечения, спорт
sochi 2014, Первый, Центр партнерства, СТС, Sony Pictures, Condé Nast, Amedia

BOT-TREK TDS

Система обнаружения целевых атак и угроз в корпоративной сети

Позволяет сосредоточиться на реагировании
на критические события, доверив обработку логов профессионалам

Обеспечивает круглосуточную поддержку вашей службы безопасности
и сопровождение процесса реагирования опытными специалистами Group-IB

Bot-Trek TDS выявляет все виды вредоносных программ, распространяющихся или уже работающих в вашей сети

- целевые угрозы
- 0-day атаки
- банковские трояны
- шпионское ПО
- мобильные трояны
- средства скрытого удаленного управления
- бекдоры

и другие угрозы.

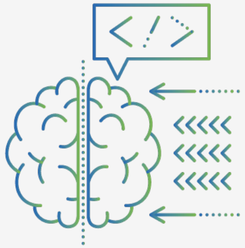
Уникальные источники данных об угрозах

Кибербразведка

Эксклюзивные данные кибербразведки Bot-Trek Intelligence™ о новых вредоносных программах и инструментах атак, изменениях в известных вирусах и поведении преступных групп

Криминалистика

Самые полные данные об инструментах актуальных целевых атак от аналитиков Лаборатории компьютерной криминалистики Group-IB, участвующих в их расследовании



Машинное обучение

Выявление ранее неизвестных вредоносных объектов с помощью технологии Bot-Trek Machine Mind, основанной на современных алгоритмах поведенческого анализа и машинного обучения

95%

данных из закрытых источников

100,000+

профайлов преступных групп и индивидов

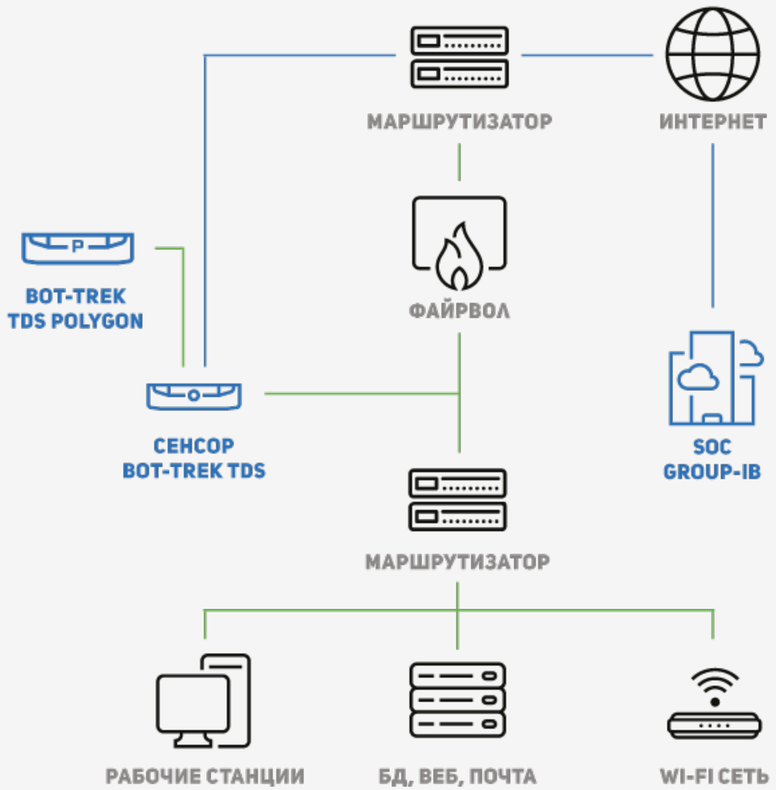
80%

высокотехнологичных преступлений в России и СНГ расследуется с нашим участием

Как работает Bot-Trek TDS

Сенсор анализа трафика

- выявляет зараженные узлы, устанавливая их взаимодействия с командными центрами по признакамвредоносной активности, разрабатываемым на основе данных из уникальных источников.
- детектирует сетевые аномалии, генерируемые вредоносными программами, при помощи алгоритмов машинного обучения.
- интегрируется с системой поведенческого анализа Polygon для выявления ранее неизвестного вредоносного кода.
- передает информацию о выявленных инцидентах в SOC Group-IB по безопасному каналу.



SOC GROUP-IB

Сведения об инцидентах, полученные от сенсора, классифицируются и коррелируются в Центре обработки данных.

События анализируются квалифицированными специалистами Group-IB вручную.

24 Анализ данных ведется круглосуточно, без выходных

Эксперты SOC уведомят ваших специалистов о критичных угрозах по телефону и e-mail, а все результаты анализа будут доступны в удобном web-интерфейсе.

Опытные специалисты Group-IB берут на себя работу по выявлению критичных инцидентов, позволяя вашей службе ИБ сосредоточиться на реагировании.

Команда профессионалов на вашей стороне

Специалисты с уникальной квалификацией

Глубокое понимание угроз, forensic-компетенции, многолетний опыт и знание лучших международных практик реагирования.

Оперативный отклик службы поддержки

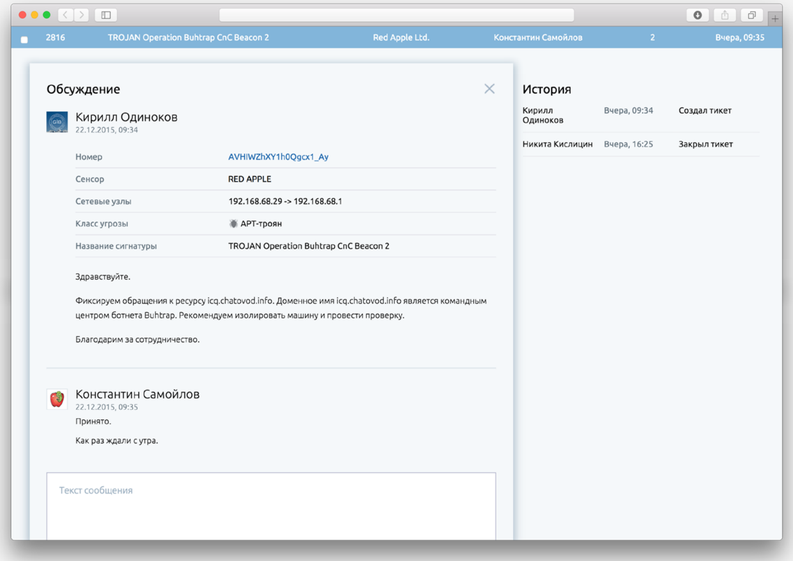
Большая часть вопросов решается за 10 минут. Удобная тикет-система гарантирует, что ни один вопрос не останется без ответа.

Выезд мобильной бригады реагирования

Криминалисты и инженеры могут выехать на место инцидента для полной нейтрализации угрозы и сбора цифровых доказательств.

24

Круглосуточная поддержка специалистов через удобную тикет-систему



CERT-GIB

первый в России частный центр круглосуточного реагирования на инциденты информационной безопасности

Компетентная организация Координационного центра национального домена сети Интернет

Аккредитованный член международных сообществ команд реагирования FIRST и Trusted Introducer

Партнер IMPACT – международного партнерства по противодействию киберугрозам

Максимальное удобство использования

Облачный интерфейс

Вся информация о выявленных угрозах доступна в веб-интерфейсе, через который удобно отслеживать уведомления в течение дня.

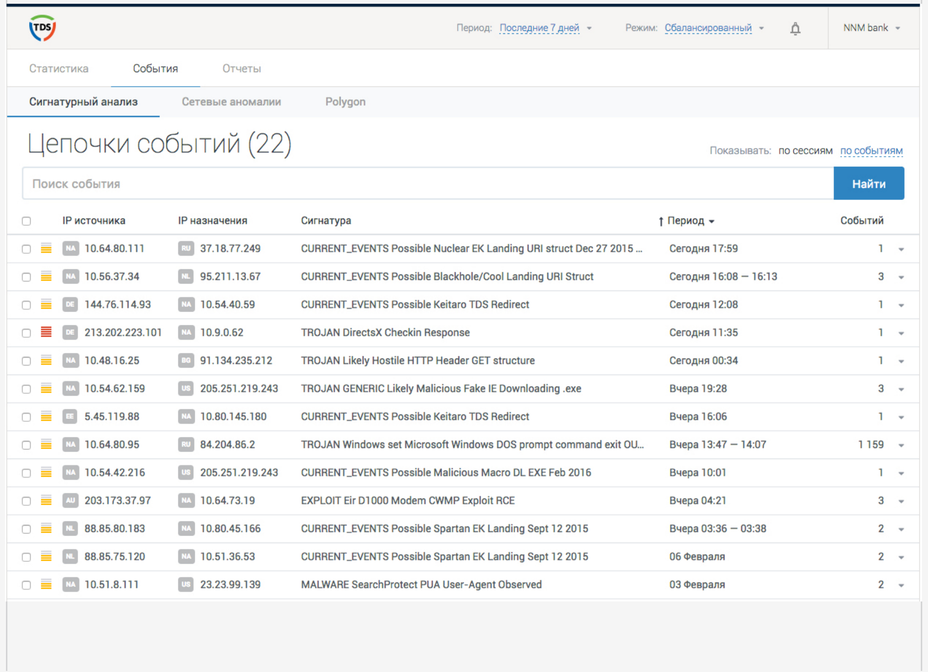
Наглядные отчеты

Интерфейс позволяет выгружать наглядные отчеты по периодам и по типам событий, позволяя отслеживать и анализировать динамику атак так же просто, как посещаемость сайта.

Интеграция с SIEM и системами хранения логов

Поток событий, фиксируемых сенсором Bot-Trek TDS, может быть автоматически направлен в любую SIEM или систему хранения логов через стандартный механизм syslog.

Детальная информация о каждой подозрительной сессии



Сохраняйте полный контроль с оперативными уведомлениями об инцидентах

ПО ТЕЛЕФОНУ

Критические заражения устройств (банковские троянские, дропперы, шпионское ПО, скрытое ПО для удаленного управления)

Подтверждение эксплуатации технической уязвимости

ПО ЭЛЕКТРОННОЙ ПОЧТЕ

Попытки эксплуатации узявимостей в ПО, сетевом оборудовании и сетевых сервисах

Нежелательная, но не критичная активность

Проведите тест-драйв Bot-Trek TDS

Объективный контроль трафика и поддержка реагирования опытными специалистами – бесплатно на 14 дней

Даже если за период пилота не будет выявлено активных заражений, вы получите информацию о потенциальных угрозах для компаний вашего сектора, которая поможет скорректировать вашу стратегию ИБ.

1
Установка и настройка

Наши специалисты согласуют схему внедрения сенсора и установят его.

Вы увидите все активные заражения сразу после подключения TDS.

2
Консультация эксперта

Мы покажем возможности веб-интерфейса и ответим на ваши вопросы.

При необходимости мы можем протестировать корректность заведения трафика и провести эмуляцию атаки.

3
Поддержка реагирования

При обнаружении критических угроз наш CERT будет уведомлять вас по выбранному каналу связи.

Оперативные ответы на вопросы, касающиеся реагирования, вы сможете получить через удобную тикет-систему.

4
Отчет о результатах пилотного проекта

После успешного завершения пилота мы подготовим отчет о выявленных инцидентах с описанием потенциальных угроз вашей информационной безопасности.

BOT-TREK TDS Polygon

Система выявления ранее неизвестного вредоносного кода с использованием передовых алгоритмов машинного обучения

Полная конфиденциальность – обработка и анализ файлов внутри вашего контура безопасности

Круглосуточная поддержка вашей службы безопасности и сопровождение процесса реагирования опытными специалистами Group-IB

Почтовые вложения

Вредоносные файлы, получаемые пользователями через почтовую систему в ходе целевых атак и применения социальной инженерии

Скачиваемые файлы

Объекты, скачиваемые пользователями и их компьютерами при атаке их браузеров

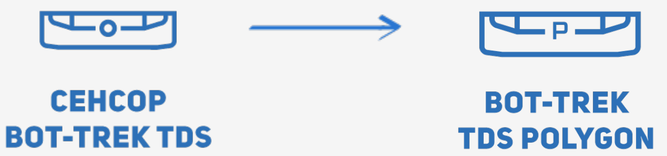
Целевые атаки

Вредоносное ПО, нацеленное эксклюзивно на вашу инфраструктуру

и другие ранее неизвестные вредоносные объекты, не определяемые антивирусами и сигнатурным подходом.

Как работает Bot-Trek TDS Polygon

Polygon запускает файлы, полученные от TDS,
в изолированной среде, анализирует их поведение
и **выносит объективное заключение о степени опасности объекта**



Ферма виртуальных машин

Потенциально вредоносные файлы запускаются в безопасной тестовой среде, настраиваемой и обновляемой исходя из специфики вашего бизнеса и региона

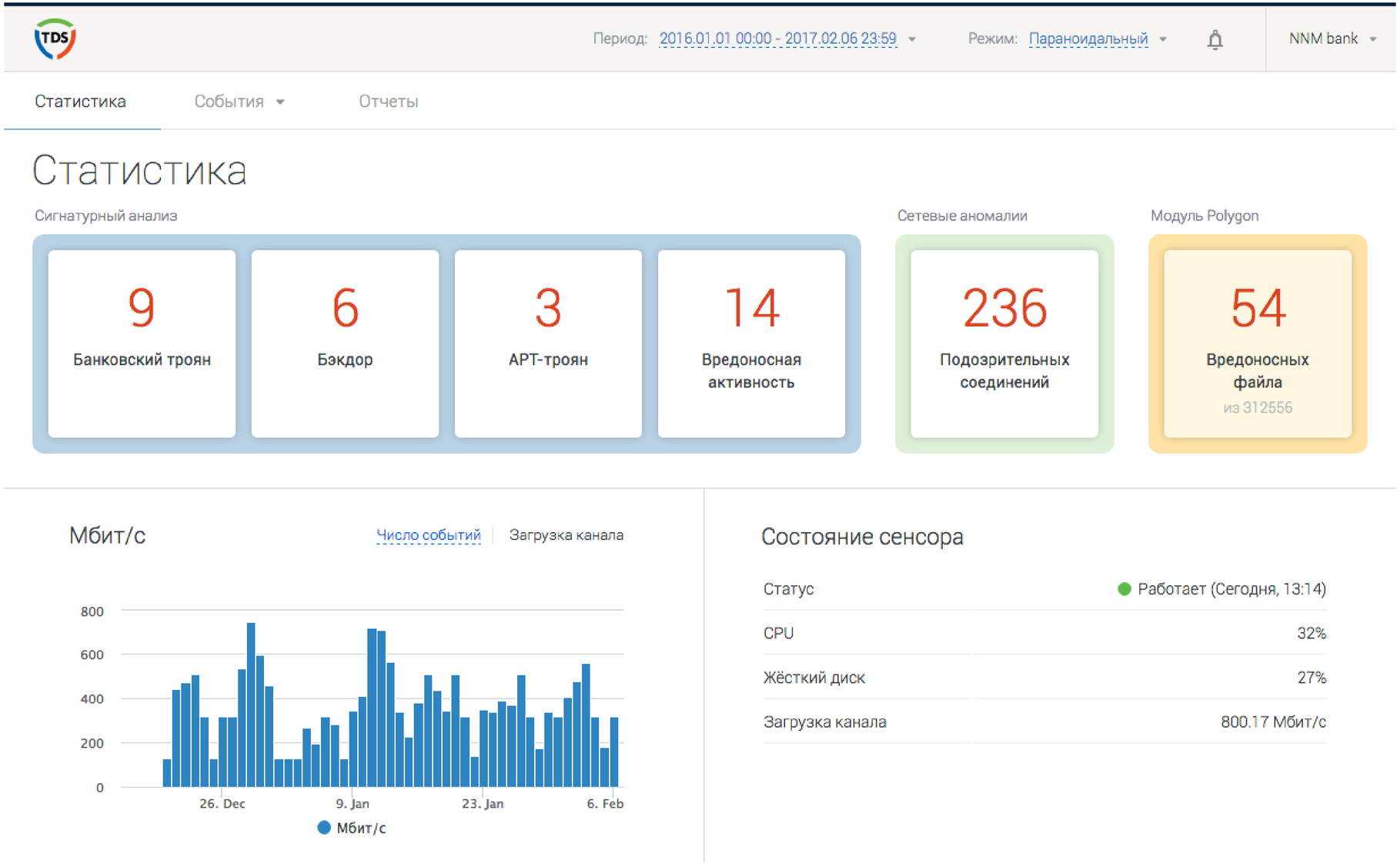
Низкоуровневый системный монитор

Не раскрывая своего присутствия, монитор отслеживает поведение вредоносных объектов на самом низком уровне

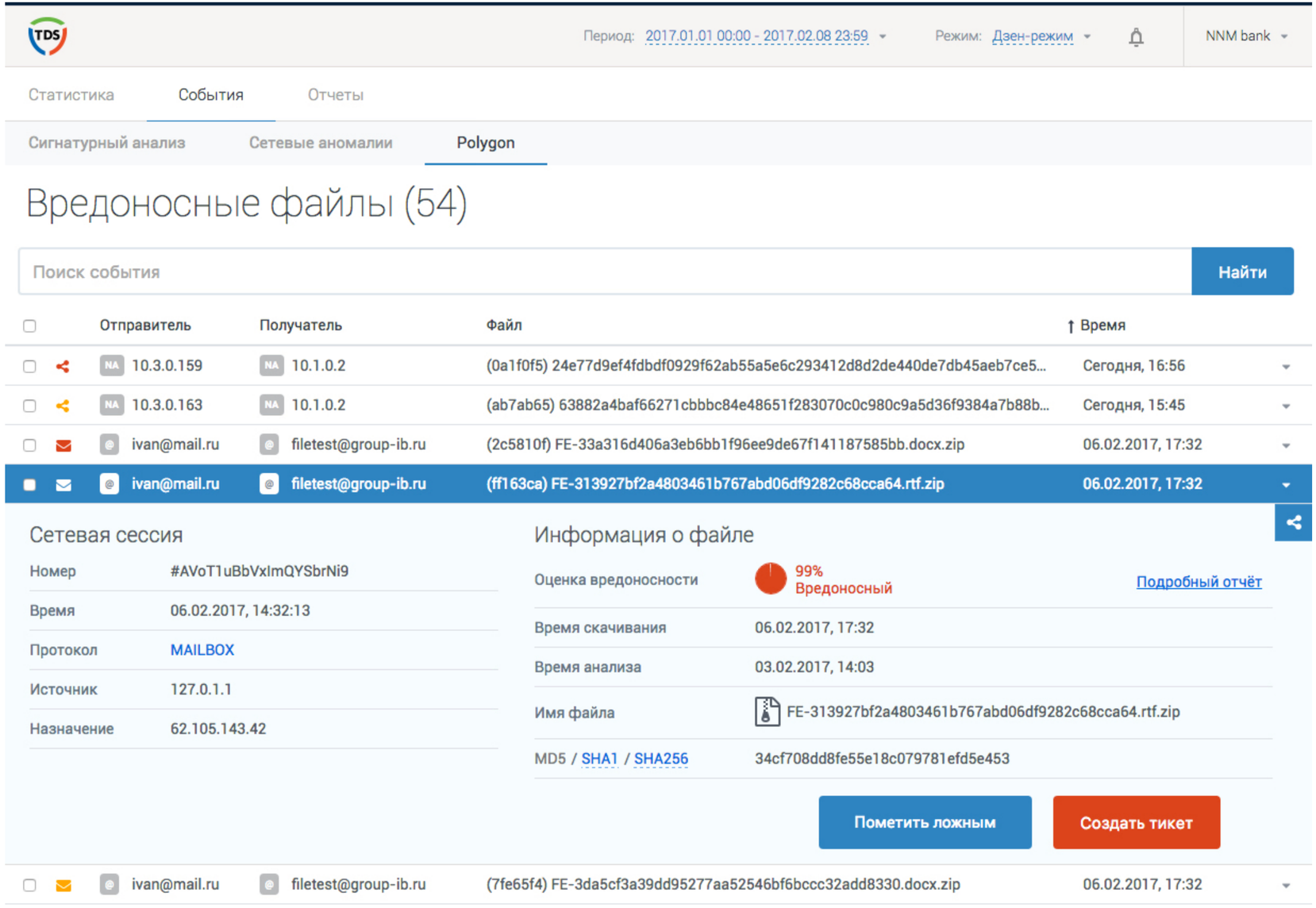
Регулярно обновляемый классификатор

Вердикт об опасности объекта выносится на основании классификатора, формируемого с помощью технологии Bot-Trek Machine Mind

Интерфейс: Главная страница



Интерфейс: Модуль Polygon



Интерфейс: Модуль Polygon, отчёт о вредоносном файле

Сигнатурный анализ | Сетевые аномалии | Polygon

Вредоносный файл FE-33a316d406a3e9de67f141187585bb.docx.zip

Информация о файле

Оценка вредоносности	95.19999999999999%
Время анализа	03.02.2017, 14:02
Имя файла	FE-33a316d406a3eb6bb1f96ee9de67f141187585bb.docx.zip 40,1 КБ
MD5 / SHA1 / SHA256	d06d1bc06f1b001447ac042a4b1fc641

- Информация о файле
- Поведенческие маркеры
- Сетевая активность
- Дерево процессов
- Видео

Поведенческие маркеры

Вредоносные 14 | Прочие 10

- ● В трафике обнаружены вредоносные признаки 1
- ● Создаёт подозрительный powershell-процесс 2
- ○ Wscript.exe начала сетевую активность, говоряшую о загрузке payload с помошью скрипта 6
- ○ В офисном файле есть контейнер с исполняемым файлом 1
- ○ Изымает приватную информацию из локальных Internet браузеров 4
- ○ Ишёт Windows Idle Time, чтобы определить uptime 1
- ○ Определяет IP с помошью внешних ресурсов 1
- ○ Перезаписывает настройки Mozilla Firefox 2
- ○ Подозрительный HTTP-траффик 1
- ○ Пробует создать или модифицировать системные сертификаты 2
- ○ Регистрирует новый корневой (ROOT) сертификат 1
- ○ Создаёт отложенную задачу с помошью планировшика задач 15

Интерфейс: Модуль Polygon, отчёт о вредоносном файле

Сетевая активность

DNS 5 | HTTP 3 Скачать PCAP

Domain	IP	Type
dist.torproject.org	78.47.38.226	A
	154.35.132.70	A
download-codeplex.sec.s-msft.com	e4949.g.akamaiedge.net	CNAME
	wildcard.sec.s-msft.com.edgekey.net	CNAME
	23.223.34.202	A
proxifier.com	162.144.216.241	A
chocolatey.org	104.20.74.28	A
	104.20.73.28	A

Дерево процессов

● Исследуемый файл ● Созданный файл

312 C:\Program Files\Microsoft Office\Office12\WINWORD.EXE c:\users\john\appdata\local\temp\tmpr_l4iy\FE-33a316d406a3eb6bb1f96ee9de67f141187585bb.doc

Новый | Файлы | Ключи реестра | Мьютексы | Буферы

1508 C:\Windows\System32\wscript.exe C:\Users\John\AppData\Local\Temp\DOC\Quittung_sbb_ch_14.09.2016.js

Новый | Завершился | Файлы | Ключи реестра | Мьютексы

1748 C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -ExecutionPolicy Unrestricted -File "C:\Users\John\AppData\Local\Temp\Z9TN0mmG.ps1"

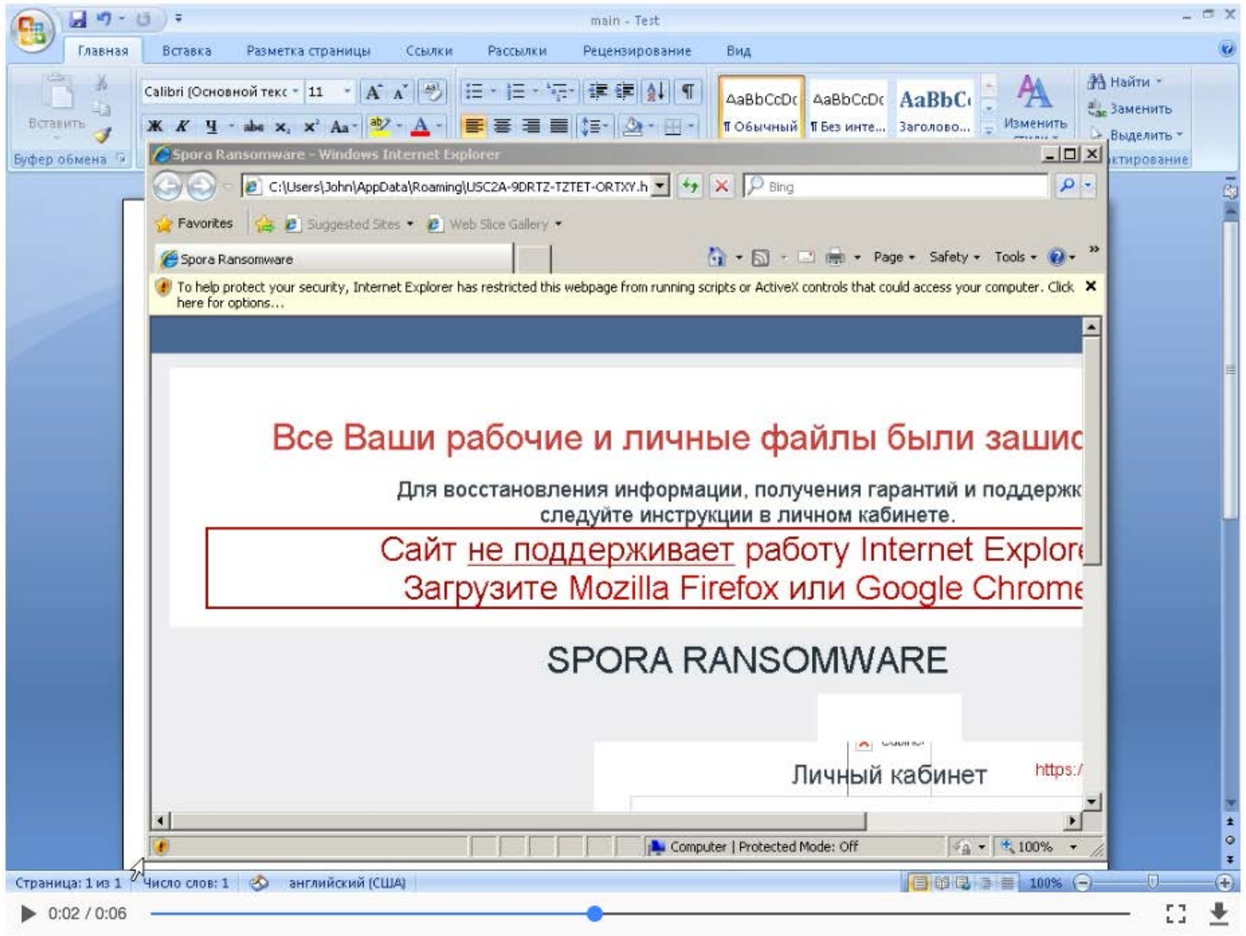
Новый | Завершился | Файлы | Ключи реестра | Мьютексы

496 C:\Users\John\AppData\Local\Temp\7za.exe x -o"C:\Users\John\AppData\Roaming\TP" -y "C:\Users\John\AppData\Local\Temp\pl.zip"

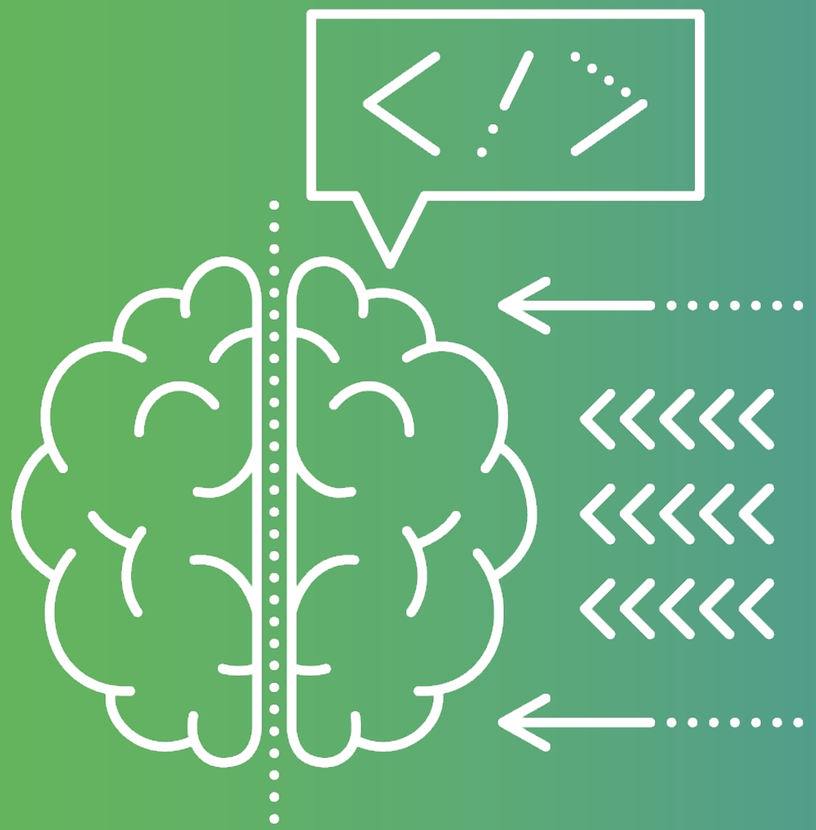
Новый | Завершился | Файлы

Интерфейс: Модуль Polygon, отчёт о вредоносном файле

Видео



Машинный интеллект на страже вашей безопасности



SYSTEM MONITOR

Системный монитор

Низкоуровневый драйвер регистрирует вызовы и изменения, происходящие в системе при выполнении анализируемого кода.

DATA MINING

Интеллектуальный анализ данных

Обновляемая база поведенческих маркеров позволяет о выделять из всего объема системных событий те, которые могут сигнализировать о потенциально опасной активности

SUPERVISED LEARNING

Обучение под контролем специалистов

Матмодели и логика классификатора корректируются опытными аналитиками, что сводит к минимуму количество ложных срабатываний

Спасибо!

Алексей Цивилев
Руководитель отдела
инфраструктурных решений

tsivilev@group-ib.ru
+7 963 999 14 18