ГАРДА

Гарда Threat Intelligence

Руководство пользователя

garda.ai

2024

Тип документа:	Руководство пользователя
Дата выпуска:	28.05.2024
Статус документа:	Released
Версия:	2.0

Содержание

1 Введение

1.1 Аннотация

Данный документ представляет собой Руководство пользователя сервиса «Гарда Threat Intelligence».

1.2 Использование имен, номеров телефонов, сетевых адресов

Приведенные в настоящем документе сведения о юридических и физических лицах, включая любые их данные, являются вымышленными, а IP-адреса и номера телефонов не соответствуют их действительным владельцам. Любые совпадения случайны.

1.3 О компании

Гарда Технологии (входит в группу компаний Гарда) – разработчик семейства продуктов в области защиты данных и сетевой безопасности. Решения Гарда защищают данные крупнейших государственных организаций и корпораций, защищают 50% всего российского интернета от DDoS-атак, обеспечивают защиту цифровых сервисов и мероприятий федерального масштаба. Продуктовый портфель холдинга построен на основе технологий собственной разработки, которые не требуют сторонних лицензий, включены в Единый реестр российского ПО и сертифицированы ФСТЭК.

1.4 Техническая поддержка

По всем вопросам, связанным с работой продукта, обращайтесь в Службу технической поддержки компании "Гарда Технологии":

- Тел. +7(831) 422-12-20 (с 9-00 до 18-00 по московскому времени).
- Email: gs.support@gardatech.ru.

2 Обзор

2.1 Назначение сервиса

Сервис «Гарда Threat Intelligence» предназначен для предоставления пользователю фидов (списков) индикаторов компрометации, полученных в результате реализации мероприятий по сбору, обогащению, анализу и фильтрации данных как из открытых источников, так и из собственных источников компании.

2.2 Личный кабинет пользователя

Личный кабинет пользователя предназначен для:

- работы с индикаторами компрометации:
  - поиск и фильтрация;
  - выгрузка в системы заказчика;
- получения информации применяемых техниках и тактиках атак и защиты от них;
- получения информации о событиях в мире информационной безопасности;
- управления учетными данными пользователя (изменение пароля/ключа доступа);
- предоставления пользователю информации о лицензии.

2.3 Типы индикаторов

Тип индикатора	Описание
ip	IP-адрес
hostname	доменное имя
url	адрес ресурса в сети Интернет
hash	хэш-сумма файла или отпечаток сетевого сервиса
autonomussystem	система IP-сетей и маршрутизаторов, управляемых одним или несколькими операторами, имеющими единую политику маршрутизации с Интернетом
email	адрес электронной почты

2.4 Категории данных

Категория	Тег	Описание
Botnet host	gsart_botnet	списки индикаторов задействованных в ботнет сети
DDoS	gsart_ddos	списки индикаторов задействованных в ddos-атаках
Phising	gsart_phising	списки индикаторов задействованных в фишинге
Spam	gsart_spam	списки индикаторов задействованных в спам рассылках
VPN	gsart_vpn	списки индикаторов vpn
Proxy	gsart_proxy	списки индикаторов proxy
Tor	gsart_tor	списки адресов нод-tor
Suspicious	gsart_suspicious	списки адресов «подозрительных» индикаторов. Сюда попадают индикаторов, которые не удалось идентифицировать по их активности

Для узлов botnet возможно дополнительное категорирование по принадлежности к ботнету.

3 Работа с сервисом

3.1 ПО для работы пользователя

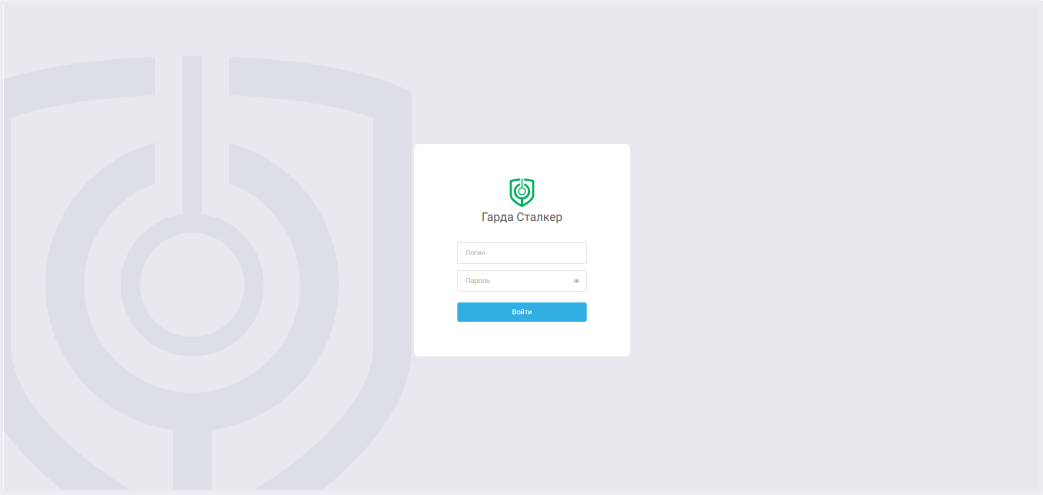
Доступ к интерфейсу оператора комплекса осуществляется с использованием следующего ПО:

- Google Chrome версии 42.0.2311.90 и выше;
- Яндекс Браузер версии 18.9.1 и выше;
- Mozilla Firefox версии 41.0.1 и выше;
- Opera версии 29.0.1795.60 и выше;
- Curl версии 7.61.1 и выше;
- Wget версии 1.19.5 и выше.

3.2 Вход в личный кабинет

Для доступа к веб-интерфейсу сервиса выполните следующие действия:

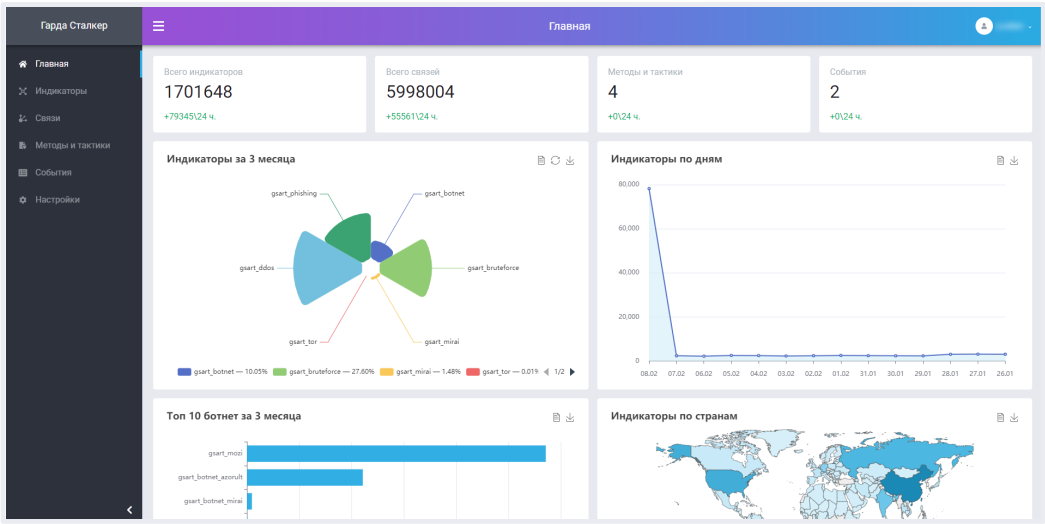
1. Откройте веб-браузер.
2. В адресной строке введите https://M8wcQMISnvRSae2LLtctNHuB7ExXr5.stalker.gardatech.ru
3. В открывшемся окне введите имя пользователя и пароль и нажмите кнопку **Войти**.
4. После авторизации пользователя в личном кабинете «Гарда Threat Intelligence» рекомендуется сменить пароль пользователя.



4 Главная

Главная страница содержит общую информацию о системе в виде следующих информационных виджетов:

- **Всего индикаторов** - содержит данные о количестве индикаторов в системе, так же показывает добавленные/обновленные индикаторы за последние 24 часа. При клике по виджету открывает вкладку **Индикаторы**.
- **Установлено связей** - содержит данные о количестве связей, установленных индикаторами в системе, также показывает добавленные /обновленные связи новых индикаторов за последние 24 часа. При клике по виджету открывает вкладку **Связи**.
- **Методы и практики** - содержит данные о количестве новых документов с описанием методов практик, количество добавленных документов за последние 24 часа. При клике по виджету открывает вкладку **Методы и практики**.
- **События** - содержит данные о количестве новостей, количество добавленных новостей за последние 24 часа. При клике по виджету открывает вкладку **События**.
- **Индикаторы за последние 3 месяца** - виджет с распределением индикаторов по категориям за последние три месяца.
- **Статистика по индикаторам** - виджет статистических данных в виде графика с линиями трендов по удаленным, добавленным/обновленным индикаторам.
- **Топ 10 ботнет за 3 месяца** - показывает наиболее активные ботнеты за последние 3 месяца.
- **Интерактивная карта** - показывает количество вредоносных индикаторов в соответствии с государством. В зависимости от интенсивности то или иное государство подсвечивается от нейтрального до красного. При клике по государству остальные виджеты показывают информацию по нему. При клике по виджету в фильтр на соответствующей виджету странице автоматически добавляется выбранное государство.

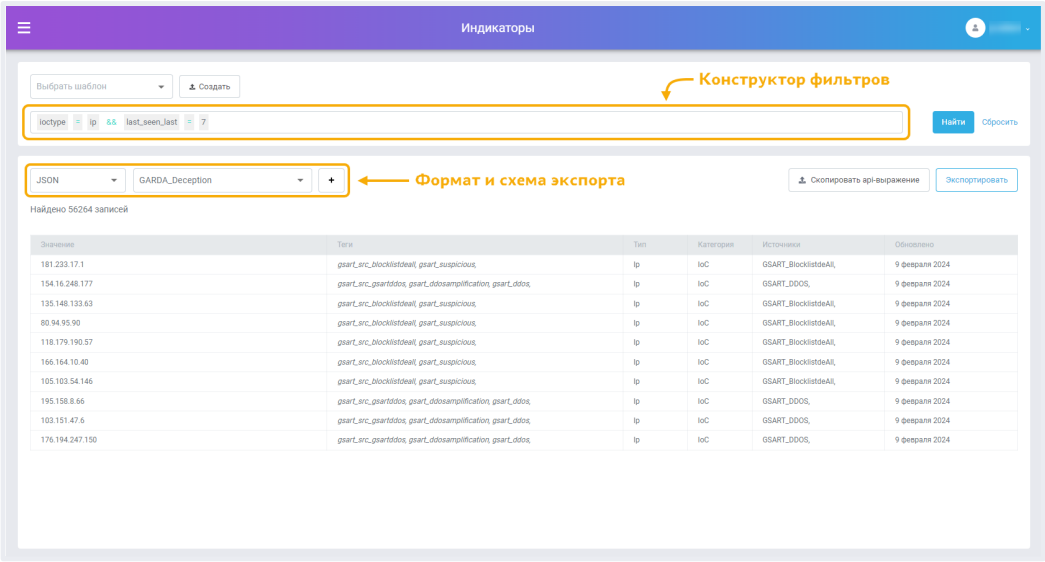

Гарда Сталкер
Главная
Индикаторы
Связи
Методы и тактики
События
Настройки
Главная
Всего индикаторов
1701648
+79345\24 ч.
Всего связей
5998004
+55561\24 ч.
Методы и тактики
4
+0\24 ч.
События
2
+0\24 ч.
Индикаторы за 3 месяца
gsart_phishing
gsart_botnet
gsart_ddos
gsart_bruteforce
gsart_tor
gsart_mirai
gsart_botnet — 10.05%
gsart_bruteforce — 27.60%
gsart_mirai — 1.48%
gsart_tor — 0.01%
1/2
Индикаторы по дням
80,000
60,000
40,000
20,000
0
08.02
07.02
06.02
05.02
04.02
03.02
02.02
01.02
31.01
30.01
29.01
28.01
27.01
26.01
Топ 10 ботнет за 3 месяца
gsart_mozi
gsart_botnet_azorult
gsart_botnet_mirai
Индикаторы по странам

5 Индикаторы

Основная рабочая страница, предназначенная для получения информации по конкретным индикаторам и отобразить информацию об индикаторе.

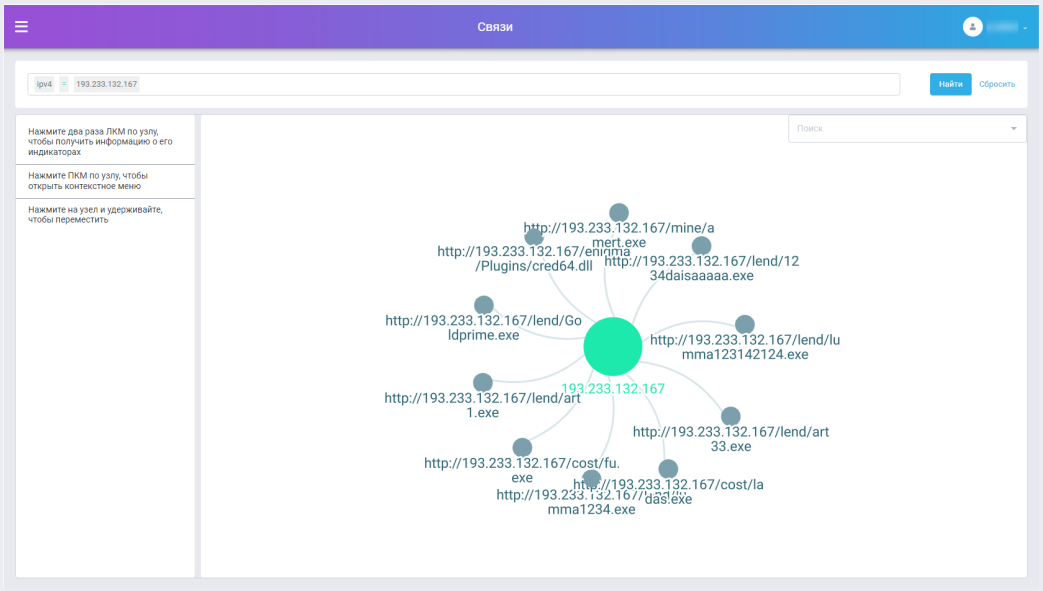
Страница индикаторов позволяет:

- самостоятельно составить фильтр для поиска данных;
- сохранить составленный фильтр;
- выбрать фильтр для поиска данных из списка сохраненных;
- экспортировать полученные данные в один из доступных форматов (JSON, CSV, TXT, SIG);
- получить строку фильтра в виде выражения для API, чтобы добавить ее в запрос получения данных с использованием curl/wget;
- посмотреть информацию об индикаторе в формате JSON и его расшифровке.



6 Связи

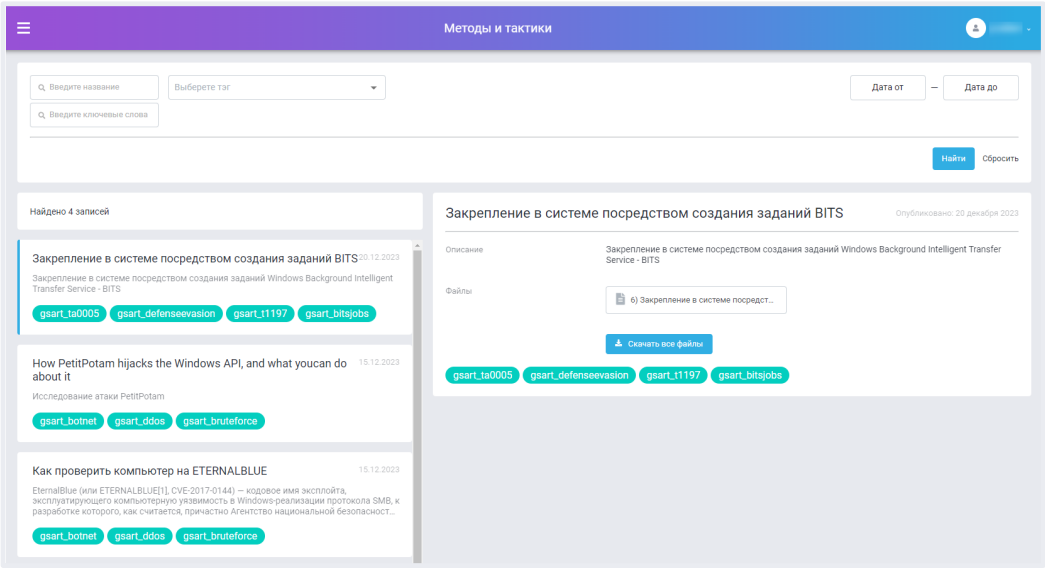
Страница **Связи** демонстрирует в графическом виде информацию о связях между индикаторами, документами, файлами. Страница содержит фильтр для поиска данных по связям, поле графического представления данных и кнопку экспорт для сохранения графического представления данных в виде картинки.



7 Методы и тактики

Страница предназначена для представления информации связанной с методами, практиками, рекомендациями по обнаружению и защите от атак, в том числе с использованием продуктов компании, а также информацию с описанием вредоносных объектов.

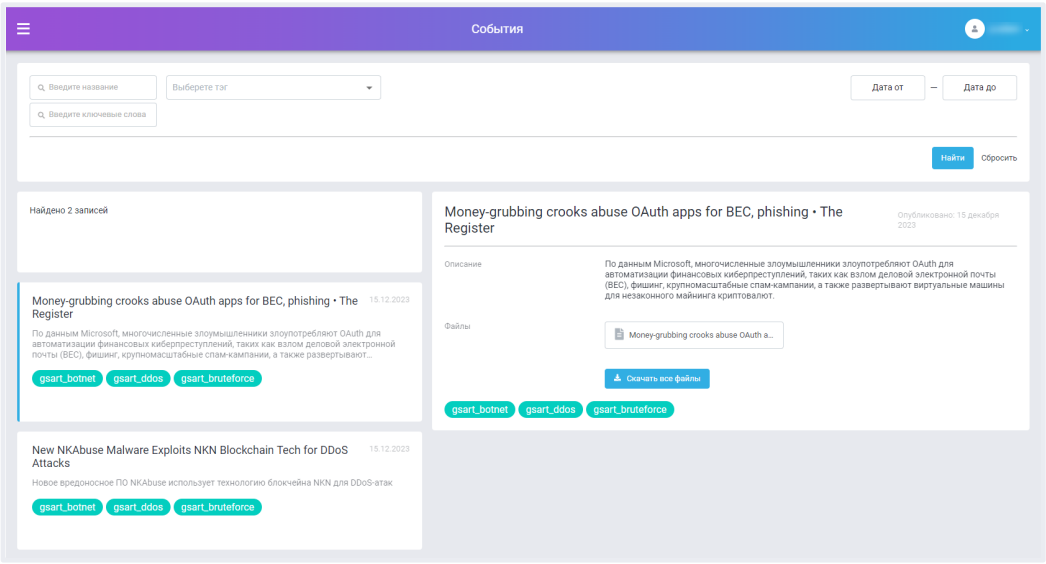
Имеется строка фильтрации данных. При клике на объект разворачивается более подробное описание и ссылки на файлы.



8 События

Раздел содержит информацию о новых уязвимостях, проводимых атакующих кампаниях, утечках данных и т.п.

Страница имеет фильтр для поиска данных. Содержит виджеты с кратким описанием новости. При клике новость разворачивается в подробное описание с ссылками на документы и внешние ресурсы.



9 Настройки

Раздел содержит две вкладки с информацией о пользователе:

- **Профиль**
- **Информация о лицензии**