



ГАРДА



Гарда Threat Intelligence

**Руководство
пользователя**

garda.ai

2024



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

ООО "Гарда Технологии"
Все права сохраняются за правообладателем.

ООО "Гарда Технологии" оставляет за собой право вносить изменения в содержащуюся в данном документе информацию без предварительного уведомления.

ИНФОРМАЦИЯ О ПРАВЕ СОБСТВЕННОСТИ

Информация, содержащаяся в данном документе, является собственностью ООО "Гарда Технологии". Никакая часть этого документа не может быть воспроизведена или заимствована в какой бы то ни было форме или каким-либо способом – в графическом, электронном виде или механическим путем, включая фотокопирование, запись, в том числе и на магнитные носители, или любые другие устройства, предназначенные для хранения информации – без письменного разрешения ООО "Гарда Технологии". Подобное разрешение не может быть выдано третьей стороной, будь то организация или частное лицо.

Содержание

1 Введение	4
1.1 Аннотация.....	4
1.2 Использование имен, номеров телефонов, сетевых адресов.....	4
1.3 О компании.....	4
1.4 Техническая поддержка.....	4
2 Обзор	5
2.1 Назначение сервиса.....	5
2.2 Личный кабинет пользователя.....	5
2.3 Типы индикаторов.....	5
2.4 Категории данных.....	6
3 Работа с сервисом	7
3.1 ПО для работы пользователя.....	7
3.2 Вход в личный кабинет.....	7
4 Главная	8
5 Индикаторы	10
6 Связи	11
7 Методы и тактики	12
8 События	13
9 Настройки	14

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	Ter	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

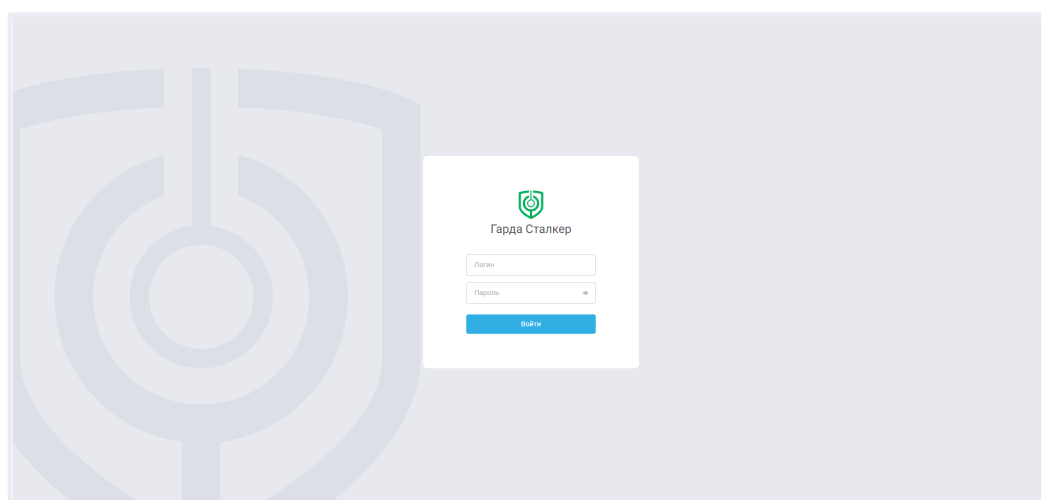
Доступ к интерфейсу оператора комплекса осуществляется с использованием следующего ПО:

- 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:

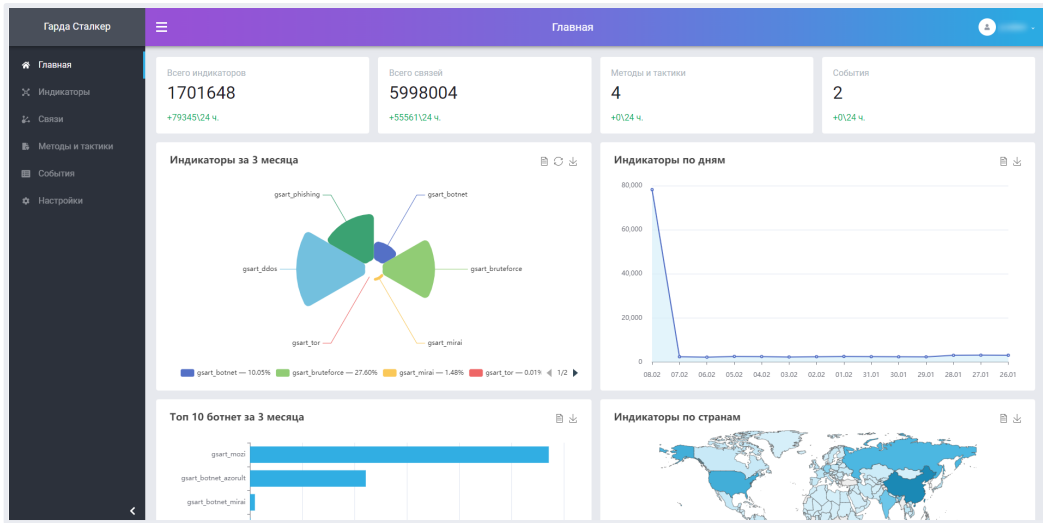
1. Откройте веб-браузер.
2. В адресной строке введите <https://M8wcQMISnvRSae2LLtctNHuB7ExXr5.stalker.gardatech.ru>
3. В открывшемся окне введите имя пользователя и пароль и нажмите кнопку **Войти**.
4. После авторизации пользователя в личном кабинете «Гарда Threat Intelligence» рекомендуется сменить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



5 Индикаторы

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

Страница индикаторов позволяет:

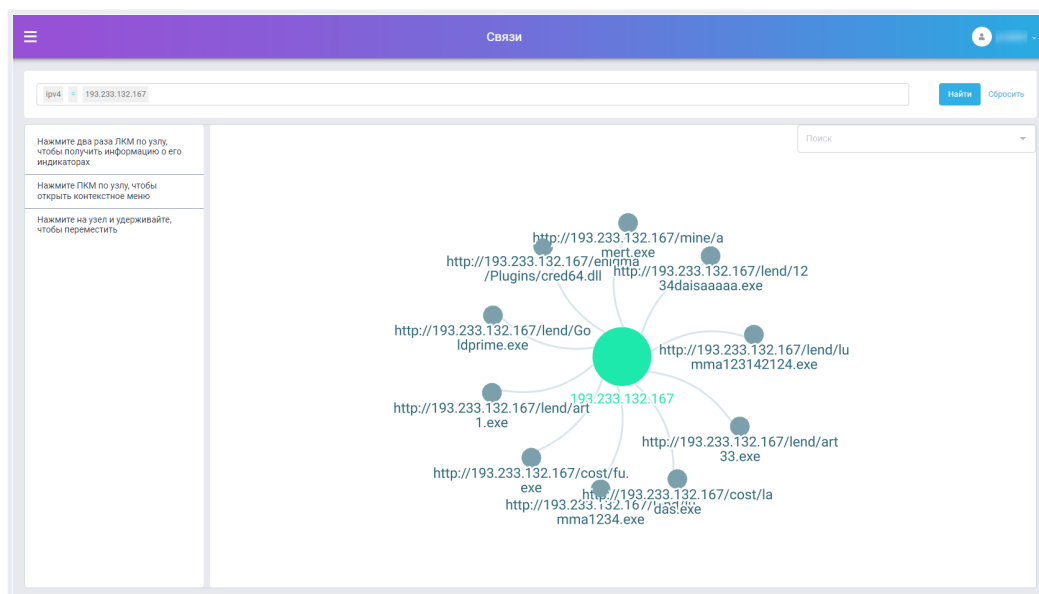
- самостоятельно составить фильтр для поиска данных;
- сохранить составленный фильтр;
- выбрать фильтр для поиска данных из списка сохраненных;
- экспортировать полученные данные в один из доступных форматов (JSON, CSV, TXT, SIG);
- получить строку фильтра в виде выражения для API, чтобы добавить ее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

The screenshot shows the 'Индикаторы' (Indicators) page. At the top, there is a header with a menu icon, the title 'Индикаторы', and a user profile icon. Below the header, there is a filter builder section. It includes a dropdown for 'Выбрать шаблон' (Choose template) and a 'Создать' (Create) button. A search bar contains the filter expression: 'loctype = ip && last_seen_last = 7'. To the right of the search bar are 'Найти' (Find) and 'Сбросить' (Reset) buttons. Below the search bar, there is a section for 'Формат и схема экспорта' (Format and export schema). It shows 'JSON' selected for the format and 'GARDA_Deception' for the schema. There are also buttons for 'Скопировать api-выражение' (Copy api-expression) and 'Экспортировать' (Export). Below this section, it says 'Найдено 56264 записей' (Found 56264 records). The main part of the page is a table with the following columns: 'Значение' (Value), 'Тег' (Tag), 'Тип' (Type), 'Категория' (Category), 'Источник' (Source), and 'Обновлено' (Updated). The table contains 10 rows of data, all with an update date of '9 февраля 2024'.

Значение	Тег	Тип	Категория	Источник	Обновлено
181.233.17.1	gsarL_src_blocklistdeall, gsarT_suspicious	Ip	IoC	GSART_BlocklistdeAll	9 февраля 2024
154.16.248.177	gsarL_src_gsartddos, gsarT_ddosamplification, gsarT_ddos	Ip	IoC	GSART_DDOS	9 февраля 2024
135.148.133.63	gsarL_src_blocklistdeall, gsarT_suspicious	Ip	IoC	GSART_BlocklistdeAll	9 февраля 2024
80.94.95.90	gsarL_src_blocklistdeall, gsarT_suspicious	Ip	IoC	GSART_BlocklistdeAll	9 февраля 2024
118.179.190.57	gsarL_src_blocklistdeall, gsarT_suspicious	Ip	IoC	GSART_BlocklistdeAll	9 февраля 2024
166.164.10.40	gsarL_src_blocklistdeall, gsarT_suspicious	Ip	IoC	GSART_BlocklistdeAll	9 февраля 2024
105.103.54.146	gsarL_src_blocklistdeall, gsarT_suspicious	Ip	IoC	GSART_BlocklistdeAll	9 февраля 2024
195.158.8.66	gsarL_src_gsartddos, gsarT_ddosamplification, gsarT_ddos	Ip	IoC	GSART_DDOS	9 февраля 2024
103.151.47.6	gsarL_src_gsartddos, gsarT_ddosamplification, gsarT_ddos	Ip	IoC	GSART_DDOS	9 февраля 2024
176.194.247.150	gsarL_src_gsartddos, gsarT_ddosamplification, gsarT_ddos	Ip	IoC	GSART_DDOS	9 февраля 2024

6 СВЯЗИ

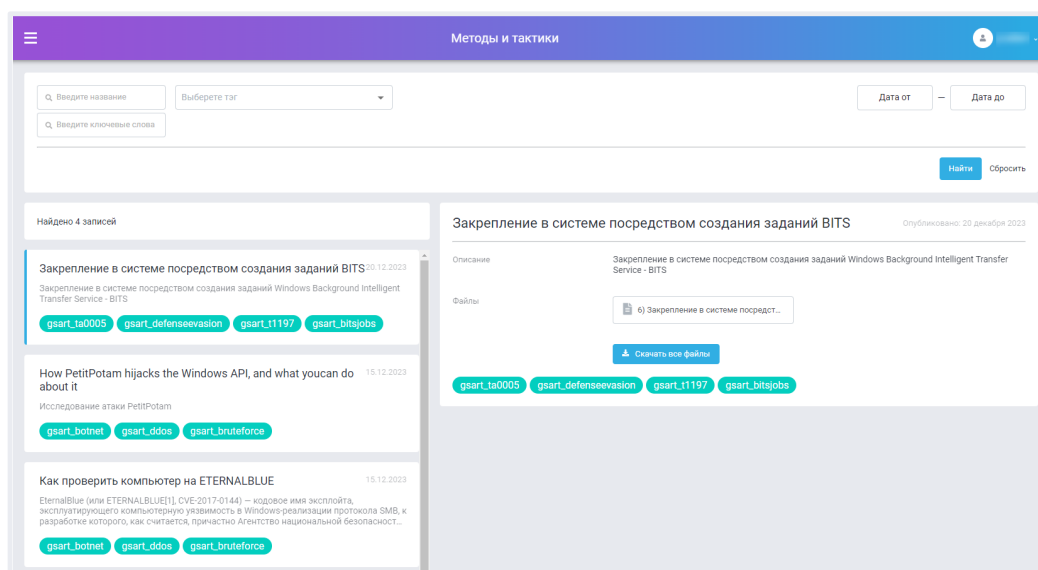
Страница **Связи** демонстрирует в графическом виде информацию о связях между индикаторами, документами, файлами. Страница содержит фильтр для поиска данных по связям, поле графического представления данных и кнопку экспорт для сохранения графического представления данных в виде картинки.



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.

События

Введите название

Выберите тег

Дата от

Дата до

Введите ключевые слова

Найти

Сбросить

Найдено 2 записей

Money-grubbing crooks abuse OAuth apps for BEC, phishing - The Register 15.12.2023

По данным Microsoft, многочисленные злоумышленники злоупотребляют OAuth для автоматизации финансовых киберпреступлений, таких как взлом деловой электронной почты (BEC), фишинг, крупномасштабные спам-кампании, а также развертывают виртуальные машины для незаконного майнинга криптовалют.

Описание

По данным Microsoft, многочисленные злоумышленники злоупотребляют OAuth для автоматизации финансовых киберпреступлений, таких как взлом деловой электронной почты (BEC), фишинг, крупномасштабные спам-кампании, а также развертывают виртуальные машины для незаконного майнинга криптовалют.

Файлы

Money-grubbing crooks abuse OAuth a...

Скачать все файлы

qsart_botnet qsart_ddos qsart_bruteforce

New NKA Abuse Malware Exploits NKN Blockchain Tech for DDoS Attacks 15.12.2023

Новое вредоносное ПО NKA Abuse использует технологию блокчейна NKN для DDoS-атак

qsart_botnet qsart_ddos qsart_bruteforce

9 Настройки

Раздел содержит две вкладки с информацией о пользователе:

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

