ГАРДА
ТЕХНОЛОГИИ

Руководство пользователя сервиса «Гарда Сталкер»

Ноябрь 2022

Нижний Новгород

Дата выпуска: 14.12.2022

Версия документа: 1.1

Оглавление

1. ВВЕДЕНИЕ

1.1. Аннотация

Данный документ представляет собой Руководство пользователя сервиса «Гарда Сталкер».

1.2. Аудитория

Документ предназначен для пользователей сервиса «Гарда Сталкер». Материал, изложенный в документе предполагает у читателя наличие навыков использования web-бразера и инструментов командной строки curl/wget.

1.3. Использование имен, номеров телефонов, сетевых адресов

Все регистрационные имена пользователей, а также номера телефонов, имена и другие данные абонентов, используемые в данном документе, являются вымышленными, а IP-адреса не соответствуют их действительным владельцам. Любые совпадения случайны.

1.4. О Компании

«Гарда Технологии» - российский разработчик систем защиты от внутренних и внешних угроз информационной безопасности, противодействия мошенничеству и расследования инцидентов.

Решения «Гарда Технологии» занимают лидирующие позиции на российских рынках решений информационной безопасности:

- защиты от DDoS-атак операторского класса;
- защиты баз данных;
- фрод-мониторинга порядка пропуска трафика операторов связи;
- DLP-систем.

Разработки аппаратно-программных решений информационной безопасности ведутся с 2005 года. Исследовательский центр компании обладает 5 патентами на уникальные технологии. Решения «Гарда Технологии» внедрены в крупнейших компаниях финансового сектора, промышленных предприятиях, операторах связи и государственных структурах России и СНГ. Подробнее - на gardatech.ru.

1.5. 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: gm.support@gardatech.ru.

2. ОПИСАНИЕ

2.1. Назначение сервиса

Сервис «Гарда Сталкер» 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 (см. Рис.1) предназначен для:

- предоставления пользователю фидов(списков) индикаторов компрометации в соответствии с выбранной лицензией;
- управления учетными данными пользователя (изменение пароля/ключа доступа);
- предоставления пользователю информации о лицензии.

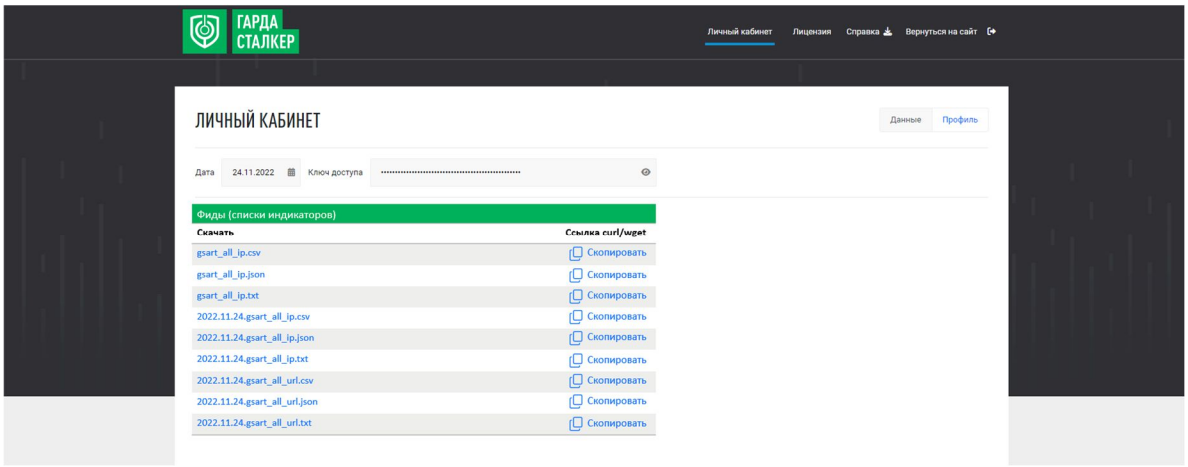

Рисунок 1. Личный кабинет пользователя.

2.3. Типы индикаторов

Доступа информация о следующих типах индикаторов:

- ip – адрес
- url – адрес
- dns – имя

2.4. Категории данных

Предоставляются фиды (списки) следующих категорий:

- C&C botnet host – списки адресов управляющих центров ботнет
- Botnet host – списки адресов узлов задействованных в ботнет сети
- DDoS – списки адресов узлов задействованных в ddos-атаках
- Phising – списки адресов узлов задействованных в фишинге
- Spam – списки адресов узлов задействованных в спам рассылках
- VPN – списки адресов узлов-vpn
- Proxy – списки адресов узлов-proxy
- Tor – списки адресов нод-tor
- Suspicious – списки адресов «подозрительных» узлов. Сюда попадают узлы, которые не удалось идентифицировать по их активности.

Для узлов botnet возможно дополнительное категорирование по принадлежности к ботнету.

2.5. Формат данных

Фиды (списки) предоставляются в следующих форматах:

- json
- csv
- txt
- sig

2.5.1. Формат json

Предоставляет наибольший объем данных. Может быть использован для постобработки данных.

Какие данные передаются в этом формате:

- ip адрес
- Тип ip адреса
- Атакуемые порты и протоколы
- Дата обнаружения первой активности
- Дата обнаружения последней активности
- Теги
- Номера тегов
- Принадлежность к ASN
- Принадлежность к подсети
- Принадлежность к организации
- Географическая принадлежность
- Рейтинг


```
{
    "ip": {
      "v4": "173.10.179.211"
    },
    "services": [
                {
        "protocol": "TCP",
        "port": "22"
      },
      {
        "protocol": "TCP",
        "port": "9530"
      }
    ],
    "firstseen": 1657324800,
    "lastseen": 1668688939,
    "tags": {
      "names": [
        "gsart_botnet",
        "gsart_mirai"
      ],
      "codes": [
        "000003",
        "000017"
      ]
    },
    "asn": {
      "num": "7968",
      "origin": "AS7968",
      "org": "Comtrans Cable Inc.",
      "firstaddr": {
        "ipv4": "173.7.0.0"
      },
      "lastaddr": {
        "ipv4": "173.18.255.255"
      }
    },
    "geo": {
      "city": "Newark",
      "country": "United States",
      "region code": "US"
    },
    "score": "65"
  }
```

2.5.2. Формат csv

Так же содержит значительный объем данных и может использоваться как для постобработки, так и для импорта в программу работы с электронными таблицами.

В качестве разделителя используется запятая (","), в качестве разделителя для однотипных данных, например имен тегов, или пар протокол/порт используется пробел (" ").

Пример индикатора в формате csv:

173.10.145.201,1657324800,1668688939,TCP/22 TCP/9530,gsart_botnet gsart_mirai,000003 000017,AS7968, Comtrans Cable Inc.,Newark,United States,US,65

Атрибут	Значение
ip адрес	173.10.145.201
Дата обнаружения первой активности	1657324800
Дата обнаружения последней активности	1668688939
Атакуемые порты и протоколы	TCP/22 TCP/9530
Теги	gsart_botnet gsart_mirai
Номера тегов	000003 000017
Принадлежность к ASN	AS7922
Принадлежность к организации	Comtrans Cable Inc.
Город	Newark
Страна	United States
Географическая принадлежность	US
Рейтинг	65

2.5.3. Форматы txt и sig

Формат TXT – представляет собой просто список ip-адресов	Формат sig – аналогичен формату txt, но дополнительно содержит информацию о протоколе, исходящем порте, порте получателя
165.232.183.66	148.72.211.177:*/*/*
103.152.164.103	216.245.215.122:*/*/*
103.74.120.192	104.156.155.30:*/*/*
154.21.208.173	194.36.191.196:*/*/*
143.110.137.82	167.99.78.164:*/*/*
67.222.131.158	5.42.246.46:*/*/53
64.235.231.20	185.172.110.230:*/*/*
159.65.147.193	206.81.23.58:*/*/*
184.168.121.5	159.89.2.220:*/*/*
151.80.20.26	196.244.192.13:tcp/*/80
104.156.155.29	196.244.192.13:*/*/554
171.22.30.115	196.244.192.13:tcp/*/3306
128.199.109.135	196.244.192.13:*/*/3389

2.5.4. Дополнительные форматы

По запросу клиента возможно изменение форматов выгрузки, и объема выгружаемых данных.

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 web-интерфейсу сервиса выполните следующие действия:

1. Откройте web-брайзер.
2. В адресной строке введите https://stalker.gartdatech.ru.
3. В открывшемся окне (см. Рис.2) введите имя пользователя и пароль и нажмите кнопку **Войти**.

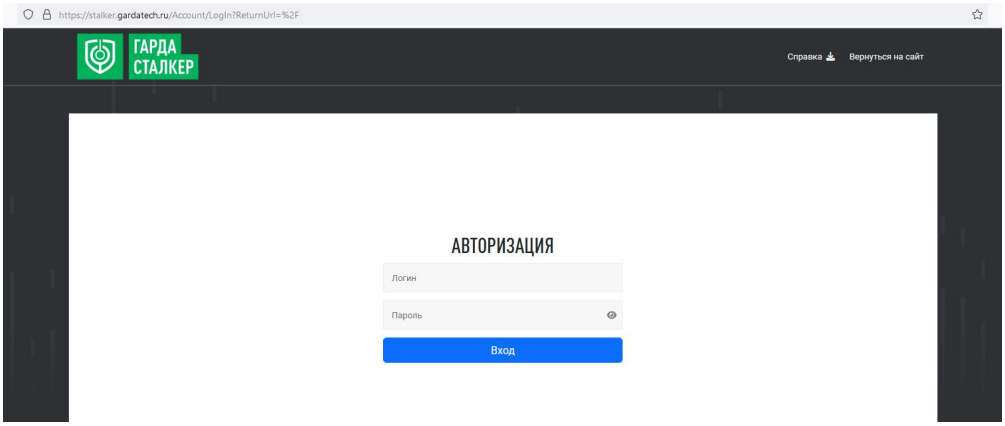

Рисунок 2. Вход в личный кабинет.

4. После авторизации пользователя в личном кабинете «Гарда Сталкер», рекомендуется сменить пароль пользователя.

3.3. Смена учетных данных

Для управления учетными данными выполните следующие действия:

1. Нажмите кнопку **Профиль**, в правом верхнем углу (см. Рис.3)

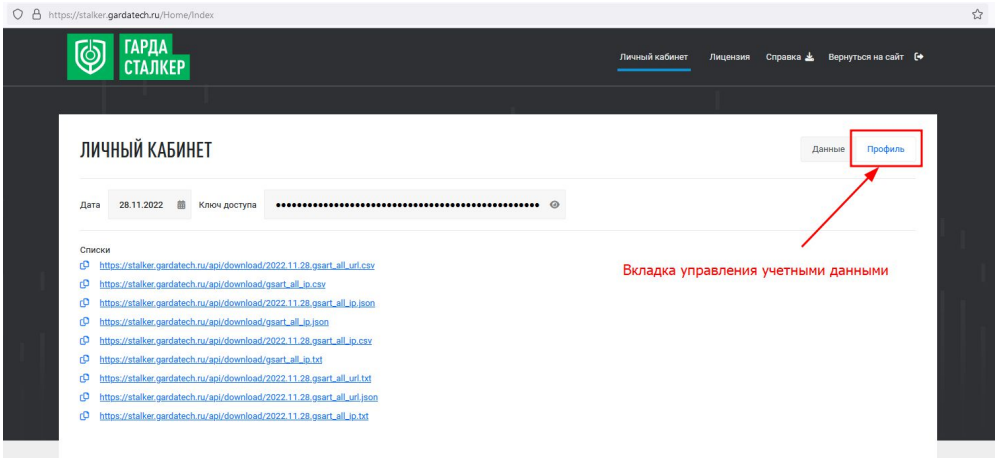

Рисунок 3. Переход на вкладку профиль.

2. На вкладке «Профиль» введите новый пароль пользователя и нажмите кнопку «Сменить пароль» (см. Рис.4).

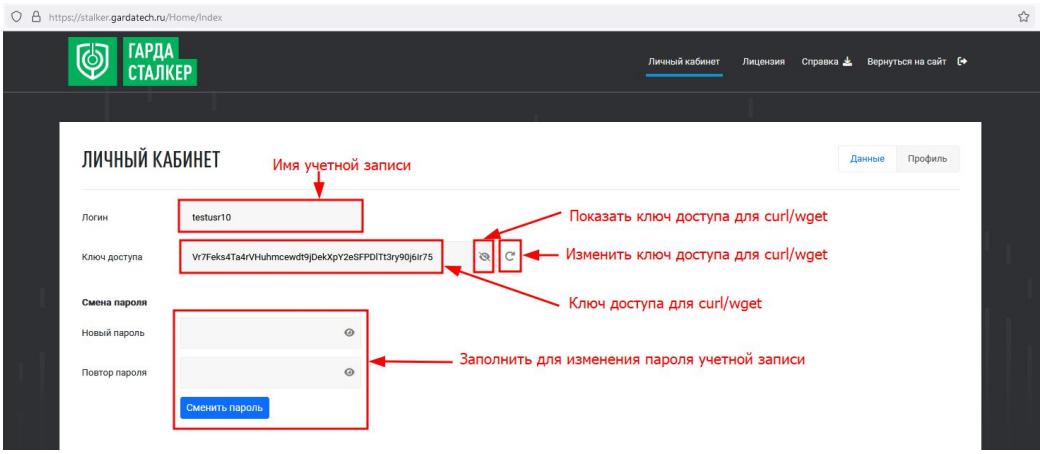

Рисунок 4. Изменение учетных данных.

3. Так же можно посмотреть/изменить ключ доступа (см. Рис.4) к фидам (спискам) для использования с приложениями curl и wget.

3.4. Получение данных

3.4.1. Получение данных из web-интерфейса личного кабинета

Для загрузки данных с использованием web-интерфейса личного кабинет пользователя выполните следующие действия:

1. Перейдите на вкладку «Данные»
2. На вкладке выберите дату, данные за которую вы хотите увидеть, или оставьте текущую (см. Рис.5).
3. В колонке «Скачать» нажмите левой кнопкой мыши на имя фида (списка), который вы хотите получить (см. Рис.5).

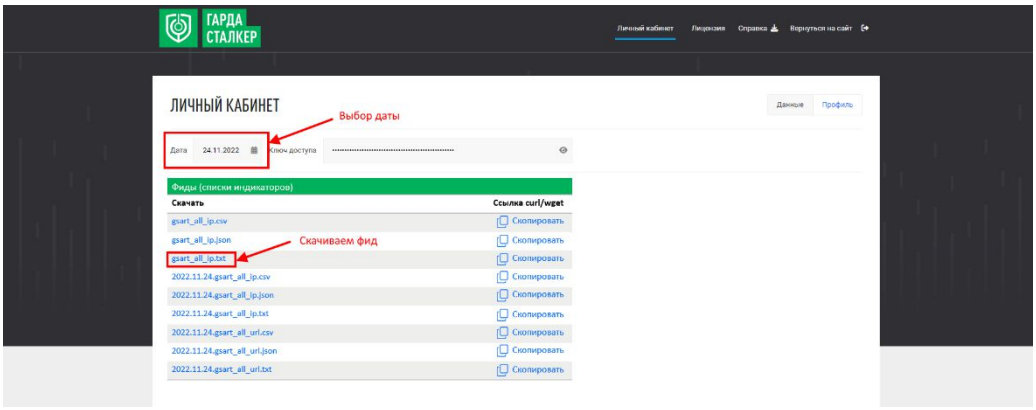

Рисунок 5. Скачивание данных с использованием web-интерфейса личного кабинета.

3.4.2. Получение данных с использованием curl/wget

Для загрузки данных с использованием инструментов командной строки curl/wget необходимо выполнить следующее:

1. Набрать команду для скачивания данных, например:
   a. Пример curl
   ```
   curl -X GET -H "apikey: Vr7Feks4Ta4rVHuhmcewdt9jDekXpY2eSFPDlTt3ry90j6Ir75"
   "https://
   M8wcQMISnvRSae2LLtctNHuB7ExXr5.stalker.gardatech.ru/api/download/gsart_all_ip.csv"
   --output "gsart_all_ip.txt"
   ```
   b. Пример wget
   ```
   wget --header='apikey: Vr7Feks4Ta4rVHuhmcewdt9jDekXpY2eSFPDlTt3ry90j6Ir75' https://
   M8wcQMISnvRSae2LLtctNHuB7ExXr5.stalker.gardatech.ru/api/download/gsart_all_ip.csv
   ```

2. Узнать apikey и получить ссылки на скачивание нужно перейти на вкладку «Данные»
3. Нажать кнопку показать ключ
4. Скопировать ключ и вставить его в поле apikey
5. В столбце «Ссылка curl/wget» нажать кнопку «Скопировать» для соответствующего фида (ссылки) и вставить в команду, как ссылку для скачивания

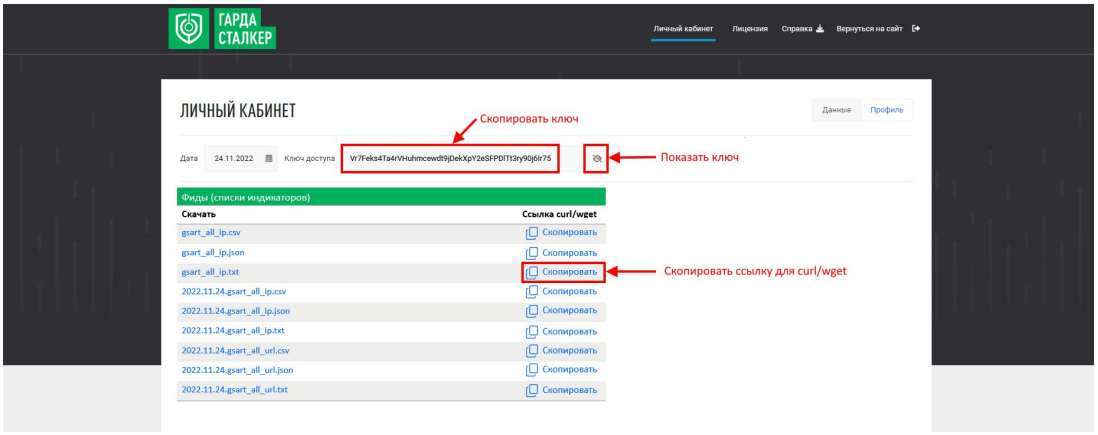

Рисунок 6. Скачивание данных с использованием инструментов командной строки curl/wget.

6. Списки не имеющие в своем наименовании даты, например (gsart_botnet.json), предоставляют данные актуальные на момент выгрузки.
7. Списки имеющие в своем наименовании даты, например (2022.12.12.gsart_botnet.json), предоставляют данные актуальные на указанную дату.

3.5. Доступные категории фидов

Пользователю личного кабинета «Гарда Сталкер» доступны различные категории фидов. Доступ к категориям предоставляется в соответствии с лицензией. Посмотреть доступные категории и иную информацию о лицензии можно в разделе лицензии.

Для просмотра раздела лицензии необходимо перейти с вкладки «Личный кабинет» на вкладку «Лицензия». На вкладке лицензия представлена информация о:

- номере лицензии;
- сроке действия;
- типе лицензии (ограниченная/неограниченная);
- объеме фида (списка) (1000 строк/10000 строк/Максимальный);
- доступных категориях.

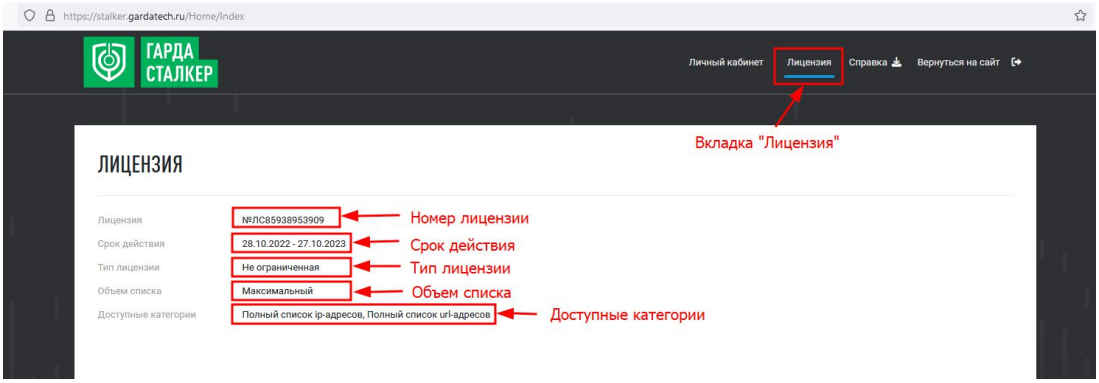

Рисунок 7. Информация о лицензии.