**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ  
«Bot-Trek Intelligence»**

**Версия 1.0**

**РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ**

**СОДЕРЖАНИЕ**

[1. Аннотация 3](#_Toc460501995)

[2. Настройки доступа и учетных записей 3](#_Toc460501996)

[2.1. Разграничение прав доступа 3](#_Toc460501997)

[2.2. Настройки учетной записи 3](#_Toc460501998)

[3. Раздел Учетные записи 5](#_Toc460501999)

[3.1. Учетные записи 5](#_Toc460502000)

[3.2. Кредитные карты 6](#_Toc460502001)

[3.3. Черный обнал 7](#_Toc460502002)

[3.4. IMEI 8](#_Toc460502003)

[3.5. Файлы 10](#_Toc460502004)

[4. Раздел угрозы 11](#_Toc460502005)

[5. Раздел атаки 13](#_Toc460502006)

[5.1. DDoS-атаки 13](#_Toc460502007)

[5.2. Фишинг (Phishing) 13](#_Toc460502008)

[5.3. Фишинг комплекты (Phishing kits) 15](#_Toc460502009)

[6. Раздел Хактивизм 17](#_Toc460502010)

[7. Раздел Целевые вредоносные программы 18](#_Toc460502011)

[8. Раздел Подозрительные IP (Suspicious IP) 19](#_Toc460502012)

[8.1. Tor nodes 19](#_Toc460502013)

[8.2. Open proxy 19](#_Toc460502014)

[8.3. Private/Botnet Socks 20](#_Toc460502015)

[9. Раздел Нарушение бренда (Brand Abuse) 21](#_Toc460502016)

[9.1. Домены (Domains) 21](#_Toc460502017)

[9.2. Фишинг (Phishing) 22](#_Toc460502018)

[9.3. SSL сертификаты (SSL certificates) 23](#_Toc460502019)

[9.4. Реклама (Advertising) 24](#_Toc460502020)

[9.5. Мобильные приложения (Mobile applications) 26](#_Toc460502021)

[9.6. Фишинг комплекты (Phishing kits) 27](#_Toc460502022)

# Аннотация

Настоящий документ содержит руководство пользователя по использованию программного обеспечения «Bot-Trek Intelligence» версии 1.0 (далее – ПО).

# Настройки доступа и учетных записей

Доступ к системе предоставляется через Веб или API интерфейсы. Доступ к Веб-интерфейсу доступен всем клиентам. Доступ через API-интерфейсу предоставляется по запросу.

# Разграничение прав доступа

**Разграничение прав на сетевом уровне**

Доступ к системе через Веб или API интерфейсы разрешен только по белому списку IP-адресов. Все IP-адреса вашей компании, указанные в анкете для подключения, добавляются в список разрешенных и их можно посмотреть в настройках учетной записи.

Если вы пытаетесь получить доступ с IP-адреса, который не добавлен в список разрешенных, то вы получите сообщение об ошибке с кодом 403.

**Разграничение прав на уровне компаний**

Доступ можно разграничить и на уровне компании в виде иерархической структуры, когда головная компания видит все данные, а дочерние компании видят только свои данные. Это позволяет разделить доступ к данным, например, по территориальному признаку. Например, компания Contoso USA будет видеть все данные, которые относятся к USA, компания Contoso Singapore только свои данные, а головная компания Contoso будет видеть данные обоих компаний.

Для каждой компании назначается доступ к определенным разделам. Принадлежность данных к определенной компании определяется настройками компании, где указаны домены, IP-адреса, BIN-номера и телефоны, по которым происходят поиск и сравнение.

**Разграничение прав на уровне пользователей**

Количество пользователей в системе не ограничивается и определяется желаниями клиента. Каждому пользователю могут назначаться отдельные права, но не больше чем компании, к которой он относится. Т.е. если в компании есть два пользователя, то каждому из них можно предоставить доступ к разным разделам и данным.

# Настройки учетной записи

Для перехода в раздел настройки учетной записи необходимо в правом верхнем углу нажать на иконку шестерёнки .

Страница состоит из следующих блоков: информация по пользователе, информация о компании, информация о дочерних компаниях и о пользователях компаний.

**Информация о пользователе**

Первый блок этого раздела показывает настройки вашего пользователя и права доступа. Значение часового пояса используется для отображения сведений о времени обнаружения угроз в вашей временной зоне. В этом же блоке вы можете изменить пароль для своей учетной записи, для чего необходимо нажать на кнопку «Изменить пароль».

**Информация о компании**

В следующем блоке вам доступны для просмотра данные о настройке вашей компании. Особое внимание надо уделить заполнению списков, описанных ниже:

|  |  |
| --- | --- |
| Список | Описание |
| Домен | По списку указанных доменов происходит поиск логинов и паролей, вредоносных программ, которые имеют отношение к вашей компании. Если атакующими будет перехвачен пароль от учетной записи в домене, который не указан в данном списке, вы об этом не будете оповещены. |
| Внешние IP-адреса | Список внешних IP-адресов компании используется для поиска зараженных устройств анализируя подключения к серверам управления вредоносными программами. |
| BIN-номера | Это первые 6 цифр номера банковской карты идентифицирующие банк, который ее выпустил. По данному списку осуществляется поиска скомпрометированных банковских карт, выпущенных вашей организацией. |
| Номер телефонов | Данный список содержит полные и короткие номера телефонов вашей компании. Короткие номера могут использоваться для отправки уведомлений и приема SMS-команд. Использую номера из этого списка мы осуществляем поиск среди конфигурационных файлов вредоносных программ. |

Пользователи компаний не имеют прав на внесение настроек в описанные списки, чтобы избежать ошибочного получения данных, которые не имеют отношения к их компании. Все изменения вносятся администраторами системы по запросу через форму обратной связи или иным удобным для вас способом.

Для компании определяются права доступа к разным разделам и подразделам системы. Пользователи этой компании не могут иметь доступа к разделам, к которым не предоставлен доступ для самой компании.

**Информация о дочерних компаниях и о пользователях компаний**

В следующем блоке отображаются данные о дочерних компаниях, если они созданы и пользователях, входящих в каждую из компаний. Если дочерних компаний не создано, то все пользователи будут иметь отношение к головной компании. По каждому пользователю можно посмотреть какими правами он обладает и активна ли его учетная запись.

# Раздел Учетные записи

Мы постоянно собираем сведения о новых вредоносных программах, исследуем сетевые инфраструктуры бот-сетей и применяем специальные технические меры для извлечения информации о скомпрометированных идентификаторах клиентов заказчика и оперативной информации для предотвращения случаев мошенничества. Такие данные включают в себя:

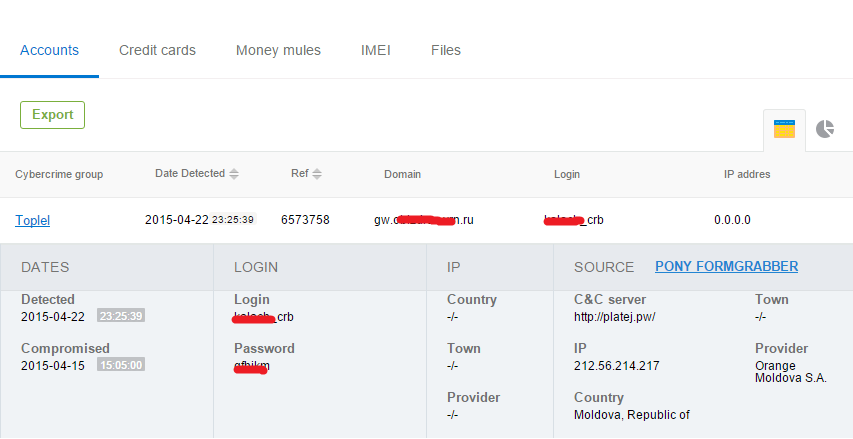
* Логины и пароли.
* Номера банковских карт.
* Счета, куда переводятся похищаемые денежные средства.
* Копии ключей электронной цифровой подписи и сертификаты.
* Снимки экранов с компьютеров клиентов заказчика.
* IP-адреса инфицированных клиентов заказчика.
* Другие данные, ассоциированные с корпоративными доменами и диапазонами IP-адресов заказчика: корпоративные аккаунты e-mail, реквизиты доступа к intranet-ресурсам и т.д.

Для удобства разграничения доступа к обнаруженным данным, все записи разбиваются на отдельные категории и предоставляются в разных секциях настоящего раздела.

# Учетные записи

В разделе учетные записи предоставляются сведения о перехваченных вредоносными программами логинов и паролей. Ниже приведено описание отображаемых в каждой строке полей:

|  |  |
| --- | --- |
| Название поля | Описание |
| Cybercrime group | Название преступной группы. Если поле не заполнено, значит мы не можем отнести используемую вредоносную программу и ее сервер управления к конкретной группе. Если название группы указано, то при нажатии на ее название вы попадете на страницу с ее описанием. |
| Дата обнаружения | Дата обнаружения. |
| Домен | Домен или IP-адрес ресурса, от которого перехвачен логин и пароль. |
| Логин | Перехваченный логин от ресурса, указанного в поле Домен. |
| IP-адрес | данные об IP-адресе зараженного клиента. Если IP-адрес не был установлен, то значение этого поля равно 0.0.0.0. |



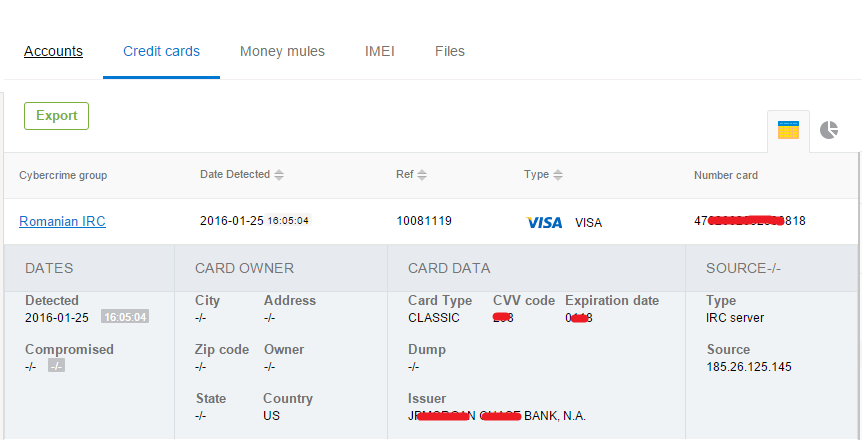
Если нажать на записи, то раскрываются дополнительные детали, разбитые на насколько блоков:

|  |  |
| --- | --- |
| Login | содержит непосредственно логин и пароль, которые перехватила вредоносная программа. Данные сохраняются и предоставляются в том виде, как они были перехвачены вредоносной программой. Если вы видите ошибку с кодировкой или опечатку в логине или пароле – это означает, что именно в таком виде их получил атакующий. |
| Даты | всегда присутствует дата обнаружения факта компрометации. Дополнительно может быть известна дата и время самой компрометации, при условии, что эти сведения собираются атакующим. |
| Source | данном блоке указываются названия вредоносной программы, адрес сервера, куда вредоносная программа передает сведения. При нажатии на название вредоносной программы откроется статья с ее описанием. |
| IP | данные об IP-адресе зараженного клиента. Если IP-адрес не был установлен, то данные отсутствуют. |

# Кредитные карты

В разделе кредитные карты предоставляются сведения о перехваченных атакующими данных банковских карт. В этот раздел попадают данные, скомпрометированные с использование банковских трянов для ПК и мобильных устройств, троянов для POS-терминалов, фишинговых страниц, хакерских форумах. Ниже приведено описание отображаемых в каждой строке полей:

|  |  |
| --- | --- |
| Название поля | Описание |
| Cybercrime group | Название преступной группы. Если поле не заполнено, значит мы не можем отнести используемую вредоносную программу и ее сервер управления к конкретной группе. Если название группы указано, то при нажатии на ее название вы попадете на страницу с ее описанием. |
| Дата обнаружения | Дата обнаружения. |
| Тип карты | Тип банковской карты. Определяется по BIN-номеру. |
| Номер карты | Полный номер банковской карты |



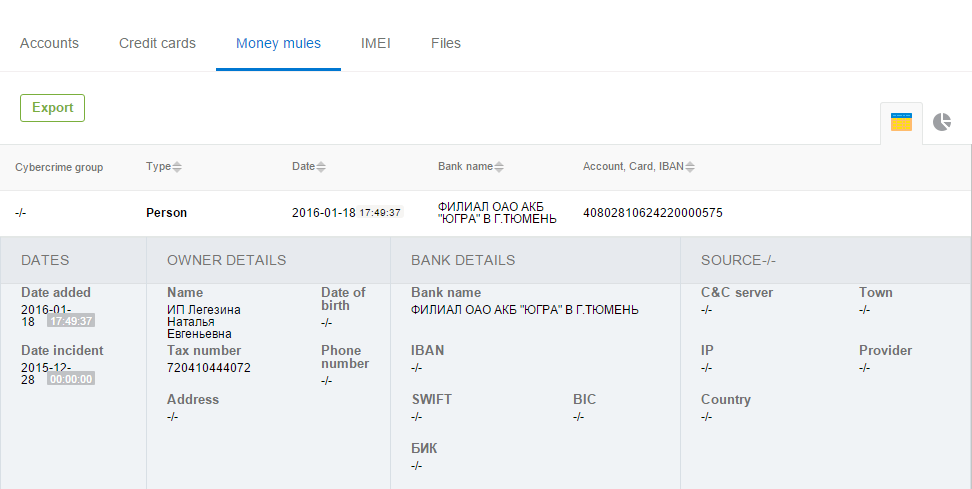
Если нажать на записи, то раскрываются дополнительные детали, разбитые на насколько блоков:

|  |  |
| --- | --- |
| Даты | всегда присутствует дата обнаружения факта компрометации. Дополнительно может быть известна дата и время самой компрометации, при условии, что эти сведения собираются атакующим. |
| Владелец карты | Данные о имени и адреса владельца карты. |
| Данные карты | Данные банковской карты, включая CVV код и срок действия карты. В поле дамп приводится копия дорожки магнитной полосы. Дамп может присутствовать только если для его получения использовалась вредоносная программа для POS-терминалов. |
| Source | данном блоке указываются названия вредоносной программы, адрес сервера, куда вредоносная программа передает сведения. При нажатии на название вредоносной программы откроется статья с ее описанием. |

# Черный обнал

В разделе Черный обнал предоставляются сведения счетах, куда атакующие переводят похищаемые денежные средства. Атаки man-in-the-browser (MITB), мобильные трояны, а также некоторые фишинговые наборы позволяют хакерам совершать денежные переводы со скомпрометированных счетов в автоматическом режиме. Исследование бот-сетей, ориентированных на банки, позволяет нам извлекать из файлов настроек данные о счетах, куда злоумышленники планируют переводить похищаемые деньги. Ниже приведено описание отображаемых в каждой строке полей:

|  |  |
| --- | --- |
| Название поля | Описание |
| Cybercrime group | Название преступной группы. Если поле не заполнено, значит мы не можем отнести используемую вредоносную программу и ее сервер управления к конкретной группе. Если название группы указано, то при нажатии на ее название вы попадете на страницу с ее описанием. |
| Тип | Тип счета. Может относится к банковскому счету физического, юридического лица или номеру электронного кошелька. |
| Дата обнаружения | Дата обнаружения. |
| Банк | Наименования банка. |
| Номер счета | Номер счета, куда переводятся похищаемые денежные средства. |



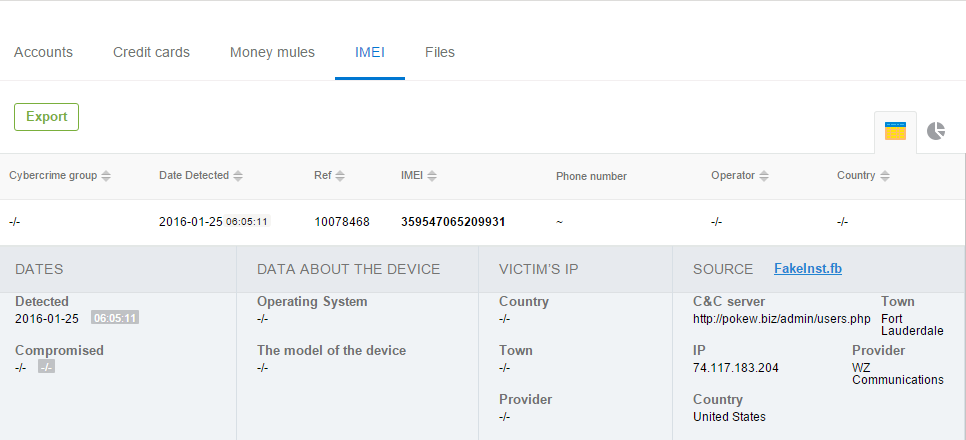
Если нажать на записи, то раскрываются дополнительные детали, разбитые на насколько блоков:

|  |  |
| --- | --- |
| Даты | всегда присутствует дата обнаружения факта компрометации. Дополнительно может быть известна дата и время самой компрометации, при условии, что эти сведения собираются атакующим. |
| Владелец счета | Данные о владельце счета. |
| Детали банка | Данные о банке или компании, где открыт счет и его детали. |
| Source | данном блоке указываются названия вредоносной программы, адрес сервера, куда вредоносная программа передает сведения. При нажатии на название вредоносной программы откроется статья с ее описанием. |

# IMEI

В этом разделе предоставляются данные о зараженных мобильных устройствах под операционной системой Android. Как и в случае с обычными бот-сетями мы исследуем мобильные бот-сети и предоставляем нашим заказчика списки мобильных устройств их клиентов и сотрудников, зараженных вредоносными программами. Информация из этого раздела не содержат персональных данных и всем клиентам отдается полный список скомпрометированных устройств. При необходимости, их можно отфильтровать, используя панель фильтров в правой части экрана. Ниже приведено описание отображаемых в каждой строке полей:

|  |  |
| --- | --- |
| Название поля | Описание |
| Cybercrime group | Название преступной группы. Если поле не заполнено, значит мы не можем отнести используемую вредоносную программу и ее сервер управления к конкретной группе. Если название группы указано, то при нажатии на ее название вы попадете на страницу с ее описанием. |
| Дата обнаружения | Дата обнаружения. |
| IMEI | Домен или IP-адрес ресурса, от которого перехвачен логин и пароль. |
| Номер телефона | Перехваченный логин от ресурса, указанного в поле Домен. |
| IP-адрес | данные об IP-адресе зараженного клиента. Если IP-адрес не был установлен, то значение этого поля равно 0.0.0.0. |



Если нажать на записи, то раскрываются дополнительные детали, разбитые на насколько блоков:

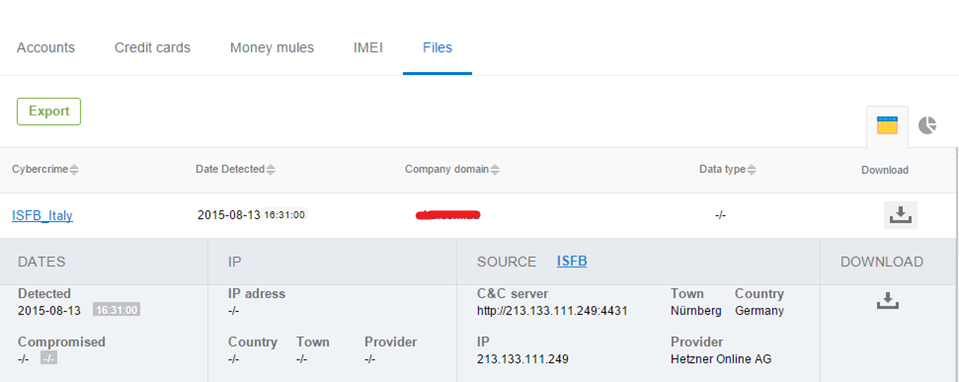
|  |  |
| --- | --- |
| Даты | всегда присутствует дата обнаружения факта компрометации. Дополнительно может быть известна дата и время самой компрометации, при условии, что эти сведения собираются атакующим. |
| Данные об устройстве | Данные о модели скомпрометированного устройства, операционной системе и ее версии, если таковые сведения собираются вредоносной программой. |
| IP | IP-адрес скомпрометированного устройства. |
| Source | данном блоке указываются названия вредоносной программы, адрес сервера, куда вредоносная программа передает сведения. При нажатии на название вредоносной программы откроется статья с ее описанием. |

# Файлы

В некоторых случаях вредоносная программа может создавать снимки экранов, перехватывать сессии, копировать сертификаты, СМС-сообщения или записывать видео файлы. Такие данные не поддаются автоматическому анализу и из них невозможно извлечь логины, пароли, номера карт. Однако, если в результате ручного анализа удается определить компанию к которой относятся перехваченные данные, то они попадают в этот раздел в виде архивов. Для загрузки архива необходимо начать на кнопку Download.

Ниже приведено описание отображаемых в каждой строке полей:

|  |  |
| --- | --- |
| Название поля | Описание |
| Cybercrime group | Название преступной группы. Если поле не заполнено, значит мы не можем отнести используемую вредоносную программу и ее сервер управления к конкретной группе. Если название группы указано, то при нажатии на ее название вы попадете на страницу с ее описанием. |
| Дата обнаружения | Дата обнаружения. |
| Домен | Домен или IP-адрес ресурса, от которого перехвачен логин и пароль. |
| Тип данных | Обозначает тип данных: снимки экранов, видео файлы, сертификаты, SMS или иное. |



Если нажать на записи, то раскрываются дополнительные детали, разбитые на насколько блоков:

|  |  |
| --- | --- |
| Даты | всегда присутствует дата обнаружения факта компрометации. Дополнительно может быть известна дата и время самой компрометации, при условии, что эти сведения собираются атакующим. |
| IP | IP-адрес скомпрометированного устройства. |
| Source | данном блоке указываются названия вредоносной программы, адрес сервера, куда вредоносная программа передает сведения. При нажатии на название вредоносной программы откроется статья с ее описанием. |

# Раздел угрозы

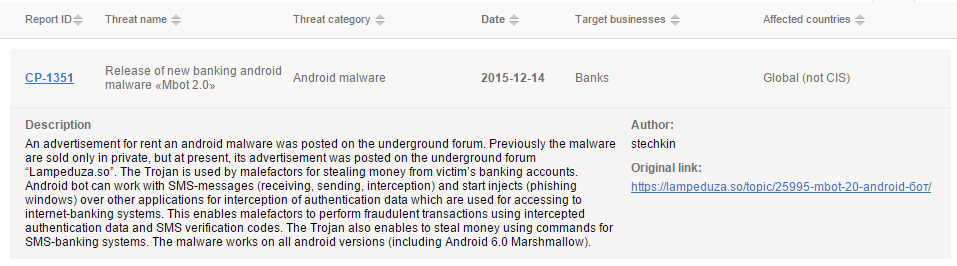
За счет участия в расследованиях и реагирований на инциденты мы узнаем о новых угрозах одними из первых. За последние годы мы получили доступы к самым закрытым хакерским сообществам, что позволяет нам следить за их активностью и доставлять эти знания нашим заказчикам. К сведениям об угрозах относятся:

* Утечки и продажи корпоративных данных.
* Объявления о поиске инсайдеров в разных компаниях или исполнителей атак.
* Появление новой вредоносной программы или сервиса для хакерского сообщества.
* Изменения в тактике проведения атак.
* Обсуждение уязвимостей.

По каждой угрозе создается отдельная запись со следующим кратким описанием:

|  |  |
| --- | --- |
| ReportID | Номер отчета. При нажатии на него, вы подаете на отдельную страницу с подробным описанием угрозы. |
| Threat name | Название угрозы. |
| Threat category | Категория, к которой мы отнесли данную угрозу. Используется для фильтрации и поиска. |
| Date | Дата составления отчета об угрозе. |
| Targeted businesses | Затрагиваемые секторы бизнеса, на которое нацелена угроза. |
| Affected countries | Страны, к которым относятся данная угроза. |
| Description | Краткое описание угрозы. |
| Author | Псевдоним человека, ассоциированный с данной угрозой. |
| Original link | Ссылка на источник, где были обнаружены сведения об угрозе. |

При нажатии на номер отчета вы подаете на отдельную страницу с подробным описанием



В детальном описании угрозы данные разбиваются на несколько блоков:

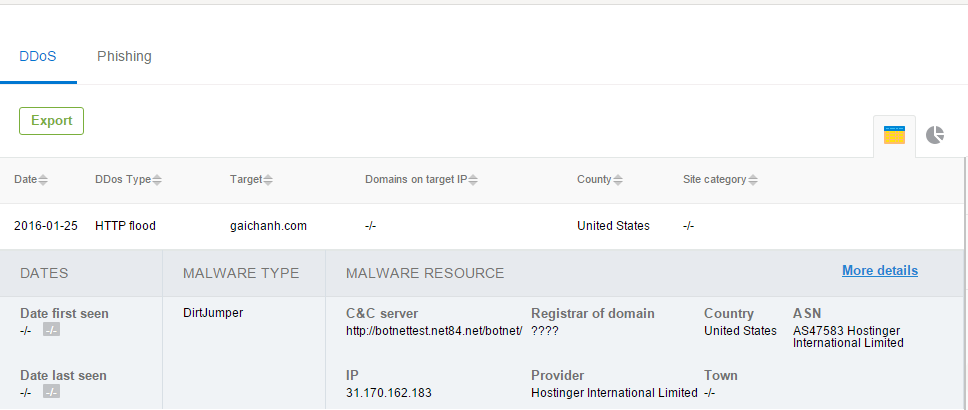
|  |  |
| --- | --- |
| Название блоков | Описание |
| Personal profile | Общее описание угрозы. |
| Screenshots | Содержит изображения полученные в результате исследования угрозы. Может содержать: объявления на хакерском форуме, изображения систем управления вредоносными программами, фрагменты переписки с злоумышленником и т.п. |
| Описание угрозы | Полное описание угрозы. |
| Рекомендации | Общие рекомендации по предотвращению реализации этой угрозы. |
| Индикаторы | Раздел содержат данные, которые могут быть использованы для обнаружения действия данной угрозы. |

# Раздел атаки

# DDoS-атаки

Для обнаружения DDoS атак мы используем сенсоры, установленные в разных странах. Сенсоры представляют из себя неправильно настроенные серверы, по аналогии с серверами используемые злоумышленниками для проведения атак через усилители: NTP Amplification, DNS Amplification или через неправильно настроенные CMS-системы, например, Wordpress Pingback. Пропуская через наши сенсоры вредоносный сетевой трафик, мы видим атакуемые цели и сообщаем о них в режиме реального времени.

Кроме того, мы осуществляем мониторинг бот-сетей и смотрим за командами получаемые вредоносными программами с своих серверов управления, расшифровываем, что позволяет нам видеть не только атакуемые цели, но и точно сказать какая вредоносная программа использовалась для атаки и где находится ее сервер управления.

Ниже приведено описание отображаемых в каждой строке полей:

|  |  |
| --- | --- |
| Название поля | Описание |
| Дата | Дата проведения атаки. |
| Тип атаки | Тип атаки. Например, HTTP POST flood, DNS Amplification и т.п. |
| Цель | Домен или IP-адрес атакуемого ресурса. |
| Домены на IP | Домены на IP-адресе. Если в качестве атакуемого ресурса мы видим IP-адрес, то для определения категории ресурсы мы пытаемся получить список сайтов размещенных на нем. |
| Страна | Страна определяется на основе IP-адреса. |
| Категория сайта | Категория сайта определяется по домену и используется для фильтрации ресурсов. |

# Фишинг (Phishing)

В данный раздел попадает информация о фишинговых ресурсах в результате анализа сетевого трафика с использование наших сенсоров Bot-Trek TDS, оповещений приходящих в наш CERT, отслеживания СПАМ сообщений, вредоносной контекстной рекламы, появляющихся новых доменных имен, открытых источников, а также наших партнеров.

Для некоторых клиентов мы персонально анализируем журналы Веб-сервера, что позволяет значительно повысить скорость обнаружения фишиговых страниц.

Ниже приведено описание отображаемых полей:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Fav | Favicon (сокр. от англ. FAVorite ICON — «значок для избранного») — значок веб-страницы. |
| Дата | Дата и время обнаружения фишингового ресурса |
| Домен | Домен на котором расположен фишинговый ресурс |
| Статус | Текущий статус фишинговой страницы. Может принимать значения: Обнаружен, На реагировании, Реагирование завершено с указанием причины завершения реагирования. |
| Бренд | Название бренда под который создан фишинговый ресурс |
| Проверка на VT | Результат проверки домена на VirusTotal. Например, 4/68 означает что 4 из 68 производителей средств защиты распознали домен как вредоносный. |

Если нажать на записи, то раскрываются дополнительные детали по домену, содержимому фишинговой страницы, снимок экрана и копия HTML страницы:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата регистрации | Дата регистрации домена |
| URL | Полный URL-адрес на фишинговую страницу |
| Регистратор | Регистратор через которого был зарегистрирован домен |
| IP (хостер) | IP-адрес домена. В скобках указывается хостинг компания, если она была определена. |
| TITLE on url | Заголовок страницы при переходе на полный URL. Может отличается от следующего заголовка. |
| TITLE on home page | Заголовок страницы при переходе на домашнюю страницу домена. |
| Фавикон MD5 | Хэш сумма с изображения Favicon (сокр. от англ. FAVorite ICON — «значок для избранного») — значок веб-страницы. Используется для поиска аналогичных изображений на других страницах. |
| Фишинг-кит | Хэш сумма с архива с исходными скриптами фишинговой страницы. |
| Адрес данных кита | Адрес, куда отправляются данные с фишинговой страницы. Адреса автоматически извлекаются из конфигурационных файлов фишинг-кита. |
| Наименование сигнатуры | Название сигнатуры по которой сработала привязка к определенному бренду. |
| Снимок экрана | Снимок экрана созданный при переходе на фишинговую страницу. Под снимком экрана есть кнопка html. Если нажать на это кнопку, то произойдет загрузка сохраненной html страницы соответствующей снимку экрана. |
| Источник | Внутренне обозначение источника откуда была получена ссылка на фишингую страницу |
| История изменения статуса | История изменения статуса фишинговой страницы. Может принимать значения: Обнаружен, На реагировании, Реагирование завершено с указанием причины завершения реагирования. |

# Фишинг комплекты (Phishing kits)

Фишинг комплект или фишинг кит – это набор страниц, скриптов и изображений, обеспечивающих работу фишингового сайта. Т.е. это готовый фишинговый сайт с файлом настроек, в котором могут указываться параметры отображения страницы и настройки по сохранению/отправке данных введённых жертвой на фишинговых сайтах. Атакующий может настроить сайт на запись полученной информации в локальный файл, базу данных или отправку данных на заданный адрес электронной почты. Последний вариант - самый распространенный.

В этот раздел попадают архивы фишинговых комплектов, полученных нами в рамках реагирования. Из фишинговых комплектов мы автоматически анализируем конфигурационные файлы и определяем куда атакующий перенаправляет данные.

Ниже приведено описание отображаемых полей:

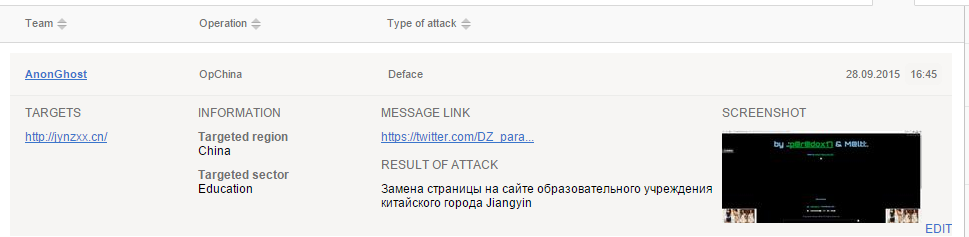
|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Добавлен | Дата и время получения фишингового комплекта. |
| Фишинг-кит | Хэш сумма с архива с исходными скриптами фишинговой страницы. |
| Email из фишинг кита | Адрес, куда отправляются данные с фишинговой страницы. Адреса автоматически извлекаются из конфигурационных файлов фишинг-кита. |
| Бренд | Название бренда, под который создан фишинговый ресурс. |

# Раздел Хактивизм

Хактивизм – это синтез социальной активности и хакерства. Часто используется для продвижения радикальных идей путем проведения компьютерных атак с целью привлечения внимания к определенному вопросу. Наши аналитики постоянно следят за действиями хактивистов и предоставляют данные:

* О начале новой операции.
* Об успешных атаках в рамках отдельной операции или независимо от нее.
* О том, как проводились атаки и каковы ее результаты.
* Взаимосвязи между разными группами.

Подобные сведения позволяют следить за утечками, изучать тактику проведения атак, оценивать риски быть атакованными в рамках определенной операции, оценивать уровень подготовки лиц, участвующих в атаках по их прошлому опыту и подготовиться им противостоять.

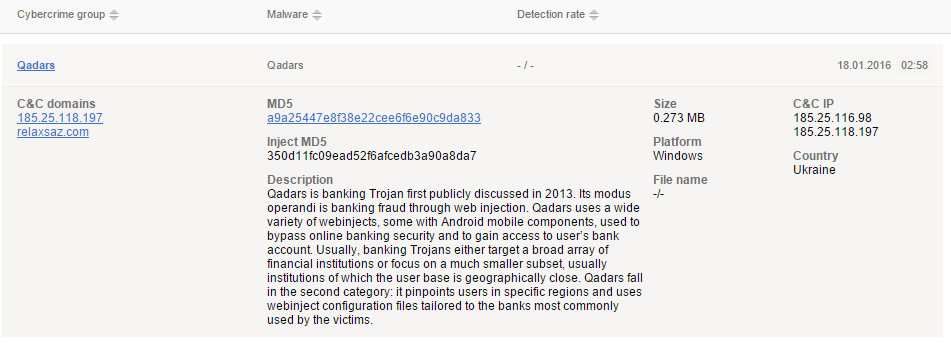


Ниже приведено описание отображаемых в каждой строке полей:

|  |  |
| --- | --- |
| Название поля | Описание |
| Team | Название команды или псевдоним атакующего |
| Operation | Операция в рамках которой была проведена атака |
| Type of attack | Тип атаки |
| Targets | Адрес атакованного ресурса |
| Targeted region | Регион к которому относится атакованный ресурс |
| Targeted sector | Сектор к которому относится атакованный ресурс |
| Message link | Ссылка на сообщение, где опубликованы данные об атаке |
| RESULT OF ATTACK | Краткая информация об атаке |
| SCREENSHOT | Снимок экрана, подтверждающий факт успешной атаки |

# Раздел Целевые вредоносные программы

Ежедневно мы исследуем тысячи вредоносных файлов, участвуем в расследованиях разных инцидентов, что позволяет нам получать сведения о вредоносных программах, нацеленных на вас и ваших клиентов. Если мы видим, что вредоносная программа имеет файл настроек, где затрагиваются ваши системы, IP-адреса, домены или ваши внешние телефоны вы немедленно узнаете об этом. Даже если вредоносная программа не имеет настроек, но мы в результате реагирования на инцидент узнали, что она может быть причастна к атаке на вас, вы также получите подробные сведения об этой вредоносной программе.

Ниже приведено описание отображаемых в каждой строке полей:

|  |  |
| --- | --- |
| Название поля | Описание |
| Cybercrime group | Название преступной группы. Если поле не заполнено, значит мы не можем отнести используемую вредоносную программу и ее сервер управления к конкретной группе. Если название группы указано, то при нажатии на ее название вы попадете на страницу с ее описанием. |
| Malware | Название вредоносной программы |
| MD5 | MD5 хэш экземпляра вредоносной программы. При нажатии на MD5 будет открыто подробное описание вредоносной программы в котором будет раздел с полным раскрытием файла настроек трояна, содержащий упоминания ваших ресурсов. |
| Inject MD5 | MD5 хэш с файла настроек вредоносной программы, содержащий упоминания ваших ресурсов. |
| Size | Размер экземпляра вредоносной программы. |
| Platform | Операционная система под которую написан вредоносная программа. |
| C&C domains | C&C-адреса для этого экземпляра вредоносной программы. |
| C&C IP | IP-адреса для этого экземпляра вредоносной программы. |
| Country | Страна определяется по IP-адресам из C&C IP. |

# Раздел Подозрительные IP (Suspicious IP)

Мы предоставляем ежеминутно обновляемые списки непубличных Socks-прокси и взломанных серверов, которые используются хакерами для проведения атак и обеспечения собственной анонимности. В дополнение к этому мы собираем для вас данные об открытых прокси серверах, выходных узлах сети Tor.

При этом открытые прокси серверы и Tor для проведения атак будут использовать новички, а вот профессионалы воспользуются Socks -прокси на ботах или взломанными серверами, чтобы замаскироваться под обычных пользователей и обеспечить себе наивысший уровень анонимности.

Используя эти данные вы можете фиксировать у себя подозрительную сетевую активность, выявлять и блокировать атаки на самых ранних этапах.

# Tor nodes

Последние в цепочке серверы Tor называются выходными узлами. Они выполняют роль передаточного звена между клиентом сети Tor и публичным Интернетом.

Ниже приведено описание отображаемых полей:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата обнаружения | Дата и время последнего обнаружения |
| IP адрес | IP адрес |
| Провайдер | Интернет провайдер. Определяется по IP адресу |
| Страна | Страна, соответствующая IP адресу |

Если нажать на записи, то раскрываются дополнительные детали по этом IP адресу

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата первого фиксирования | Дата и время, когда этот IP адрес впервые попал к нам в базу |
| Источник | Адрес ресурса, откуда был получен адрес. |
| ASN | Номер и название автономной системы, в которую входит IP адрес |
| Город | Город, соответствующий IP адресу |

# Open proxy

Сеть Интернет постоянно сканируется с целью поиска серверов, настроенных как открытые прокси. Эти списки открыто распространяются на различных ресурсах, посвященных анонимности в сети. Серверы могут быть настроены как открытые прокси в результате ошибок конфигурирования, в результате взлома или специально. Мы собираем списки таких серверов из множества ресурсов, наиболее популярных среди хакеров.

Ниже приведено описание отображаемых полей:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата обнаружения | Дата и время последнего обнаружения |
| IP адрес | IP адрес |
| Порт | Порт прокси сервера |
| Тип | Тип прокси сервера. Может быть HTTP, HTTPS, SOCKS4 или SOCKS5. От типа зависеть какой трафик будет проксироваться. |
| Анонимность | Степень анонимности. Задается на ресурсе опубликовавшем этот прокси сервер. |
| Страна | Страна, соответствующая IP адресу |

Если нажать на записи, то раскрываются дополнительные детали по этом IP адресу

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата первого фиксирования | Дата и время, когда этот IP адрес впервые попал к нам в базу |
| Источник | Адрес ресурса, откуда был получен адрес. |
| ASN | Номер и название автономной системы, в которую входит IP адрес |
| Город | Город, соответствующий IP адресу |
| Провайдер | Интернет провайдер. Определяется по IP адресу |

# Private/Botnet Socks

В данный раздел попадают адреса, где была установлена вредоносная программа, которая превращает компьютер в Socks прокси. Такие компьютеры сдаются в аренду и используются в различных атаках, обеспечивая максимальный уровень анонимности атакующего.

Ниже приведено описание отображаемых полей:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата обнаружения | Дата и время последнего обнаружения |
| IP адрес | IP адрес |
| Провайдер | Интернет провайдер. Определяется по IP адресу |
| Страна | Страна, соответствующая IP адресу |

Если нажать на записи, то раскрываются дополнительные детали по этом IP адресу

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата первого фиксирования | Дата и время, когда этот IP адрес впервые попал к нам в базу |
| Источник | Адрес ресурса, откуда был получен адрес. |
| ASN | Номер и название автономной системы, в которую входит IP адрес |
| Город | Город, соответствующий IP адресу |

# Раздел Нарушение бренда (Brand Abuse)

# Домены (Domains)

Мы автоматически получаем данные о новых доменах от крупнейших регистраторов. В дополнение мы осуществляем мониторинг Passive DNS для выявления доменов в специфичных доменных зонах, а также доменов третьего уровня. Если доменное имя или регистрационные данные содержат сведения, относящиеся к вашему бренду, то начинает процесс реагирования. Домены могут быть использованы в фишинговых атаках, вредоносных программах или различных мошеннических схемах.

Ниже приведено описание отображаемых полей:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Fav | Favicon (сокр. от англ. FAVorite ICON — «значок для избранного») — значок веб-страницы. |
| Дата обнаружения | Дата обнаружения домена |
| Домен | Название обнаруженного доменного имени |
| Контакт | Контактное лицо, указанное в whois для этого домена |
| Email | Адрес электронной почты, указанный в whois для этого домена |
| IP адрес | Последний IP адрес для этого домена |
| Проверка на VT | Результат проверки домена на VirusTotal. Например, 4/68 означает что 4 из 68 производителей средств защиты распознали домен как вредоносный. |
| Категория | Категория, к которой отнесен данный домен. Может принимать значение:   * Не определено (No defined) * Нет контента (No content) * Вредоносная программа (Malware) * Легальный домен (Legal domain) * Фишинг (Phishing) * Безопасное использование бренда (Safe brand usage) * Нелегальное использование бренда (Illegal brand usage) |

Если нажать на записи, то раскрываются дополнительные детали по домену:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата регистрации | Дата регистрации домена |
| Дата истечения регистрации | Дата окончания срока регистрации домена |
| Регистратор | Регистратор через которого был зарегистрирован домен |
| IP | IP-адрес домена |
| Поисковая фраза | Поисковая фраза по которой был найден этот домен. Для каждого клиента свой набор поисковых фраз |
| Контактное лицо | Контактное лицо указанное в whois для этого домена |
| Организация | Организация указанная в whois для этого домена |
| Телефон | Телефон указанный в whois для этого домена |
| Email | Email указанный в whois для этого домена |
| Адрес | Адрес указанный в whois для этого домена |
| DNS | DNS серверы домена |
| IP history | История изменения IP адреса |
| Скриншот ресурса | Снимок экрана созданный при переходе на домашнюю страницу домена. Под снимком экрана есть кнопка html. Если нажать на это кнопку, то произойдет загрузка сохраненной html страницы соответствующей снимку экрана. |
| TITLE страницы | Заголовок страницы при переходе на домашнюю страницу домена |
| Фавикон MD5 | Хэш сумма с изображения Favicon (сокр. от англ. FAVorite ICON — «значок для избранного») — значок веб-страницы. Используется для поиска аналогичных изображений на других страницах. |
| История изменения статуса | История изменения статуса фишинговой страницы. Может принимать значения: Обнаружен, На реагировании, Реагирование завершено с указанием причины завершения реагирования. |

# Фишинг (Phishing)

В данный раздел попадает информация о фишинговых ресурсах в результате анализа сетевого трафика с использование наших сенсоров Bot-Trek TDS, оповещений приходящих в наш CERT, отслеживания СПАМ сообщений, вредоносной контекстной рекламы, появляющихся новых доменных имен, открытых источников, а также наших партнеров.

Для некоторых клиентов мы персонально анализируем журналы Веб-сервера, что позволяет значительно повысить скорость обнаружения фишиговых страниц.

Ниже приведено описание отображаемых полей:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Fav | Favicon (сокр. от англ. FAVorite ICON — «значок для избранного») — значок веб-страницы. |
| Дата | Дата и время обнаружения фишингового ресурса |
| Домен | Домен на котором расположен фишинговый ресурс |
| Статус | Текущий статус фишинговой страницы. Может принимать значения: Обнаружен, На реагировании, Реагирование завершено с указанием причины завершения реагирования. |
| Бренд | Название брэнда под который создан фишинговый ресурс |
| Проверка на VT | Результат проверки домена на VirusTotal. Например, 4/68 означает что 4 из 68 производителей средств защиты распознали домен как вредоносный. |

Если нажать на записи, то раскрываются дополнительные детали по домену, содержимому фишинговой страницы, снимок экрана и копия HTML страницы:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата регистрации | Дата регистрации домена |
| URL | Полный URL-адрес на фишинговую страницу |
| Регистратор | Регистратор через которого был зарегистрирован домен |
| IP (хостер) | IP-адрес домена. В скобках указывается хостинг компания, если она была определена. |
| TITLE on url | Заголовок страницы при переходе на полный URL. Может отличается от следующего заголовка. |
| TITLE on home page | Заголовок страницы при переходе на домашнюю страницу домена. |
| Фавикон MD5 | Хэш сумма с изображения Favicon (сокр. от англ. FAVorite ICON — «значок для избранного») — значок веб-страницы. Используется для поиска аналогичных изображений на других страницах. |
| Фишинг-кит | Хэш сумма с архива с исходными скриптами фишинговой страницы. |
| Адрес данных кита | Адрес, куда отправляются данные с фишинговой страницы. Адреса автоматически извлекаются из конфигурационных файлов фишинг-кита. |
| Наименование сигнатуры | Название сигнатуры по которой сработала привязка к определенному бренду. |
| Снимок экрана | Снимок экрана созданный при переходе на фишинговую страницу. Под снимком экрана есть кнопка html. Если нажать на это кнопку, то произойдет загрузка сохраненной html страницы соответствующей снимку экрана. |
| Источник | Внутренне обозначение источника откуда была получена ссылка на фишингую страницу |
| История изменения статуса | История изменения статуса фишинговой страницы. Может принимать значения: Обнаружен, На реагировании, Реагирование завершено с указанием причины завершения реагирования. |

# SSL сертификаты (SSL certificates)

В этот раздел попадают все ресурсы на которых был найден SSL-сертификат, имеющий отношение к вашему бренду. Если в регистрационных данных SSL сертификата или в имени домена к которому он относится есть упоминание вашего бренда, то вы об этом будете оповещены. Такие SSL сертификаты могут быть использованы в фишинговых атаках, вредоносных программах или различных мошеннических схемах.

Ниже приведено описание отображаемых полей:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Fav | Favicon (сокр. от англ. FAVorite ICON — «значок для избранного») — значок веб-страницы. |
| Домен | Название обнаруженного доменного имени |
| Отпечаток сертификата | Уникальный отпечаток SSL сертификата. Генерируется при его выпуске. |
| IP адрес | Последний IP адрес для этого сертификата |
| Провайдер | Интернет провайдер. Определяется по IP адресу. |
| Категория | Категория, к которой отнесен данный домен. Может принимать значение:   * Не определено (No defined) * Вредоносная программа (Malware) * Легальный сертификат (Legal certificate) * Мошенничество (Fraud) * Партнерский сервис (Service of a partner) |

Если нажать на записи, то раскрываются дополнительные детали по домену:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата регистрации | Дата регистрации домена |
| Дата истечения регистрации | Дата окончания срока регистрации домена |
| Регистратор | Регистратор через которого был зарегистрирован домен |
| IP | IP-адрес домена |
| Организация | Организация на которую выдан сертификата |
| Страна | Страна указанная в регистрационных данных сертификата |
| Город | Город указанный в регистрационных данных сертификата |
| Местонахождение | Местонахождение указанное в регистрационных данных сертификата |
| Действителен | Срок действия сертификата |
| Количество хостов | Количество хостов, где этот сертификат был найден. |
| Поисковая фраза | Поисковая фраза, по которой был найден этот сертификат |
| Common name | Название центра, выпустившего сертификат |
| Организация | Организация выпустившая сертификат |
| IP history | История изменения IP адреса |
| Скриншот ресурса | Снимок экрана созданный при переходе на домашнюю страницу домена. Под снимком экрана есть кнопка html. Если нажать на это кнопку, то произойдет загрузка сохраненной html страницы соответствующей снимку экрана. |
| TITLE страницы | Заголовок страницы при переходе на домашнюю страницу домена |
| Фавикон MD5 | Хэш сумма с изображения Favicon (сокр. от англ. FAVorite ICON — «значок для избранного») — значок веб-страницы. Используется для поиска аналогичных изображений на других страницах. |
| История изменения статуса | История изменения статуса фишинговой страницы. Может принимать значения: Обнаружен, На реагировании, Реагирование завершено с указанием причины завершения реагирования. |

# Реклама (Advertising)

Используя контекстную рекламу, мошенники могут добиться чтобы при определенных поисковых запросах ссылка на их ресурс была на первом месте. Таким образом могут продвигаться различные мошеннические ресурсы, фишинговые сайты, а также специальные сайты для распространения вредоносных программ. Для атак на определенную аудиторию мошенники используют хорошо известные бренды. Мы постоянно отслеживаем рекламу в разных странах и поисковых системах.

В этот раздел попадают данные обо всех новых рекламах с упоминанием вашего бренда.

Ниже приведено описание отображаемых полей:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Fav | Favicon (сокр. от англ. FAVorite ICON — «значок для избранного») — значок веб-страницы. |
| Обнаружена | Дата обнаружения рекламы |
| Домен | Название доменного куда попадает пользователь после перехода по рекламному объявлению |
| Заголовок объявления | Заголовок рекламного объявления. |
| Категория | Категория, к которой отнесен данный домен. Может принимать значение:   * Не определено (No defined) * Вредоносная программа (Malware) * Легальный реклама (Legal advertising) * Мошенничество (Fraud) * Нелегальное использование бренда (Illegal brand usage) |

Если нажать на записи, то раскрываются дополнительные детали по домену:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Дата регистрации | Дата регистрации домена |
| Ресурс | Ресурс на который осуществляется переход при клике на объявление |
| Регистратор | Регистратор через которого был зарегистрирован домен |
| IP (хостер) | IP-адрес домена. В скобках указывается хостинг компания, если она была определена. |
| Скриншот рекламы | Снимок участка страницы с рекламой |
| TITLE рекламного объявления | Заголовок рекламируемого объявления |
| Source | Название поисковой системы в которой показывается реклама |
| Условия воспроизведения | Страна, Город и устройство которые использовались для получения этой рекламы. Выдача рекламы зависит от указанных параметров. |
| Снимок экрана | Снимок экрана созданный при переходе на фишинговую страницу. Под снимком экрана есть кнопка html. Если нажать на это кнопку, то произойдет загрузка сохраненной html страницы соответствующей снимку экрана. |
| TITLE on url | Заголовок страницы на который осуществляется переход при клике на объявление |
| Фавикон MD5 | Хэш сумма с изображения Favicon (сокр. от англ. FAVorite ICON — «значок для избранного») — значок веб-страницы. Используется для поиска аналогичных изображений на других страницах. |
| История изменения статуса | История изменения статуса страницы. Может принимать значения: Обнаружен, На реагировании, Реагирование завершено с указанием причины завершения реагирования. |

# Мобильные приложения (Mobile applications)

В этот раздел попадают данные обо всех мобильных приложениях, которые используют ваш бренд. Поиск мобильных приложений осуществляется по официальным и неофициальным магазинам приложений.

Ниже приведено описание отображаемых полей:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Иконка | Иконка приложения |
| Название приложения | Название обнаруженного приложения |
| Обнаружен | Дата обнаружения приложения |
| Автор | Автор приложения, указанный в магазине приложений |
| Источник | Название магазина в котором было найдено приложение |
| Тип | Категория к которой относится приложение в магазине |
| Категория | Категория, к которой отнесено приложение. Может принимать значение:   * Не определено (No defined) * Легальное приложение (Legal application) * Вредоносная программа (Malware) * Безопасное использование бренда (Safe brand usage) * Нелегальное использование бренда (Illegal brand usage) |

Если нажать на записи, то раскрываются дополнительные детали по домену:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Последнее обновление | Дата, когда приложение было обновлено в магазине приложений |
| Полный URL | URL адрес по которому доступно приложение |
| Количество загрузок | Показывает сколько раз приложение было загружено |
| Количество оценивших | Количество пользователей магазина поставивших оценку этому приложению |
| Версия | Версия приложения |
| Размер | Размер приложения |
| Рейтинг | Рейтинг приложения в магазине |
| Найденные вхождения | Поисковая фраза, по которой было найдено приложение |
| Описание приложения | Описание приложения, представленное в магазине |
| MD5 | Хэши приложений. Собираются все доступные версии |
| Изображения | Изображения приложения, представленные в магазине |
| Источники | Название магазина в котором было найдено приложение |
| История изменения статуса | История изменения статуса страницы. Может принимать значения: Обнаружен, На реагировании, Реагирование завершено с указанием причины завершения реагирования. |

# Фишинг комплекты (Phishing kits)

Фишинг комплект или фишинг кит – это набор страниц, скриптов и изображений, обеспечивающих работу фишингового сайта. Т.е. это готовый фишинговый сайт с файлом настроек, в котором могут указываться параметры отображения и настройки по сохранению/отправке данных введённых жертвой на фишинговых сайтах. Атакующий может настроить сайт на запись полученной информации в локальный файл, базу данных или отправку данных на заданный адрес электронной почты. Последний вариант - самый распространенный.

В этот раздел попадают архивы фишинговых комплектов, полученных нами в рамках реагирования. Из фишинговых комплектов мы автоматически анализируем конфигурационные файлы и определяем куда атакующий перенаправляет данные.

Ниже приведено описание отображаемых полей:

|  |  |
| --- | --- |
| **Название поля** | **Описание** |
| Добавлен | Дата и время получения фишингового комплекта. |
| Фишинг-кит | Хэш сумма с архива с исходными скриптами фишинговой страницы. |
| Email из фишинг кита | Адрес, куда отправляются данные с фишинговой страницы. Адреса автоматически извлекаются из конфигурационных файлов фишинг-кита. |
| Бренд | Название бренда, под который создан фишинговый ресурс. |