Программное обеспечение

«Bot-Trek Secure Portal»

Описание функциональных характеристик

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание функциональных характеристик программного обеспечения «Bot-Trek Secure Portal» (далее – Bot-Trek Secure Portal, Bot-Trek SP, ПО).

1.2 Назначение ПО

Bot-Trek Secure Portal обеспечивает на устройстве пользователя выполнение следующих защитных функций защищаемого веб-ресурса:

- детектирование несанкционированных изменений в страницах защищаемого веб-ресурса;
- детектирование удаленного подключения к конечному устройству пользователя с использованием протоколов удаленного рабочего стола (RDP, TeamViewer, VNC и т.п.);
- выявления признаков утечки учетных данных пользователя защищаемого веб-ресурса с использованием phishing/pharming-атак;
- детектирования использования автоматизированных средств получения информации и совершения действий на веб-ресурсе;
- детектирования хищений на страницах приема платежей с карт;
- детектирование иных признаков работы вредоносного программного обеспечения на конечном устройстве пользователя.

2 Программно-аппаратные среды функционирования ПО

ПО функционирует в следующих программно-аппаратных средах:

- Windows Internet Explorer версии 8.0 и выше
- Google Chrome версии 4.0 и выше
- Mozilla Firefox версии 3.5 и выше
- Apple Safari версии 4.0 и выше
- Opera версии 10.5 и выше
- iOS Safari версии 3.2 и выше
- Opera Mobile версии 11.0 и выше
- Google Chrome for Android версии 11.0 и выше
- Mozilla Firefox for Android версии 26.0 и выше
- Windows Internet Explorer Mobile версии 10.0 и выше

В браузере устройства пользователя должно быть включено исполнение скриптов JavaScript.

3 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

На Рисунок 1 изображены общие принципы функционирования ПО.

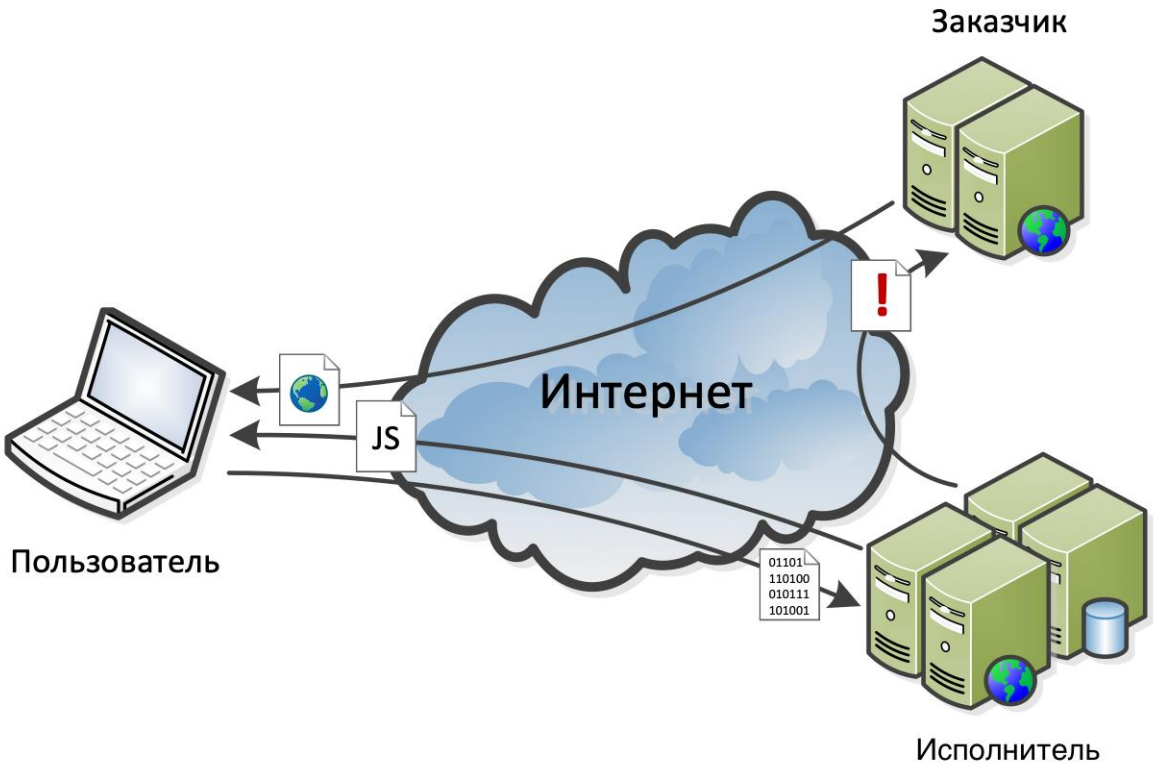

Рисунок 1. Общие принципы функционирования ПО

ПО представляет из себя пользовательский модуль, реализованный на языке JavaScript. ПО загружается совместно со страницами защищаемого веб-ресурса. ПО производит сбор контрольных данных со страницы защищаемого веб-ресурса и устройства клиента, и отсылает их для дальнейшего анализа в автоматизированную систему (далее – АС) АО «БУДУЩЕЕ» (далее – АО «БУДУЩЕЕ», Исполнитель). В случае выявления свидетельств о работе вредоносного ПО на устройстве пользователя или проведения phishing-/pharming-атак, Исполнитель незамедлительно извещает об этом заказчика.

Внедрение ПО не требует внесения каких-либо изменений в инфраструктуру заказчика и в логику работы защищаемого веб-ресурса. ПО не требует инсталляции на устройстве пользователя и работает совершенно прозрачно для него.

4 Реализация ПО

4.1 Назначение ПО

Структура ПО представлена на рис.1.

Рисунок 2. Структура ПО

4.2 Состав ПО

ПО состоит из пользовательского модуля, который реализован на языке JavaScript. Модуль загружается на устройство пользователя совместно с защищаемым веб-ресурсом.

Пользовательский модуль предназначен для сбора контрольных данных, непосредственно в контексте страниц защищаемого веб-ресурса на устройстве пользователя, и их пересылки через сеть Интернет в АО «БУДУЩЕЕ» для последующей обработки и выявления признаков работы вредоносного программного обеспечения на устройстве пользователя.

Пользовательский модуль включает в себя:

- Систему сбора контрольной данных о структуре страницы защищаемого веб-ресурса;
- Систему сбора идентификационных данных пользователя на защищаемом веб-ресурсе;
- Систему защиты обмена данными с АС;
- Систему обмена данными с АС.

4.3 Функции частей ПО

– Система сбора контрольных данных о структуре страницы защищаемого веб-ресурса:
  - Сбор данных о JavaScript-коде;
  - Сбор данных об iframe;
  - Сбор данных о формах.

– Система сбора идентификационных данных пользователя на защищаемом веб-ресурсе:
  - Получение имени учетной записи пользователя на защищаемом веб-ресурсе из форм для ее ввода в целях идентификации пользователя на стороне АС заказчика.

– Система защиты обмена данными с АС:
  - Шифрование идентификационных данных пользователя на публичном RSA-ключе заказчика;
  - Шифрование контрольных данных.

– Система обмена данными с АС
  - Посылка зашифрованных контрольных данных в АС;
  - Периодическая посылка сигнальных данных о работе пользовательского модуля в АС.

5 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПО являются:

Данные от модулей системы и управляющие команды пользователей.

Выходными данными ПО является:

Проанализированная информация от модулей системы, которая разбивается на определенные группы. С их помощью проводится мониторинг, реагирование на инциденты и проведение расследований в защищаемой инфраструктуре.

6 Взаимодействие ПО с автоматизированными системами

Принципиальная схема взаимодействия ПО с АС заказчика и АО «БУДУЩЕЕ» представлена на рис.3.

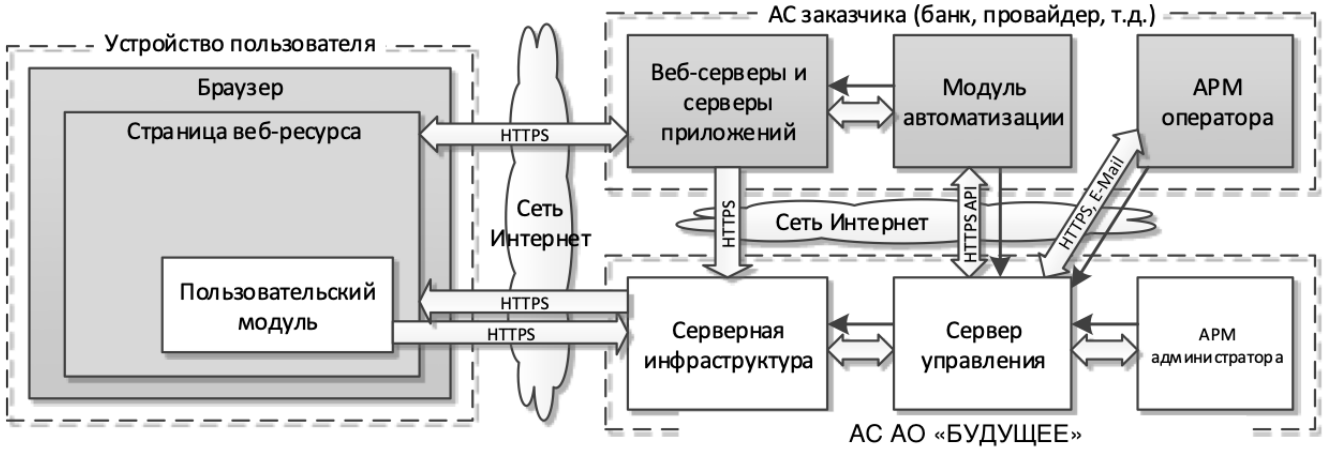

Рисунок 3. Принципиальная схема взаимодействия ПО с автоматизированными системами

6.1 Структура взаимодействия

Во взаимодействии участвуют следующие компоненты:

- Браузер на устройстве пользователя с загруженным пользовательским модулем в составе страницы защищаемого веб-ресурса;
- АО «БУДУЩЕЕ»;
- АС заказчика.

АС АО «БУДУЩЕЕ» состоит из следующих компонент:

- Серверная инфраструктура. Принимает, обрабатывает и анализирует контрольные данные, полученные от пользовательского модуля;
- Сервер управления. Служит для взаимодействия заказчика с АС АО «БУДУЩЕЕ»;
- АРМ администратора. Обеспечивает настройку и сопровождение АС.

АС заказчика состоит из следующих компонент:

- Совокупность веб-серверов и серверов приложений веб-ресурса;

- Модуль автоматизации. Использует API к АС АО «БУДУЩЕЕ» для автоматизации реагирования на выявленные подозрительные события. Необходимость разработки этого модуля и правила реагирования определяются заказчиком;

- АРМ оператора. Служит для ознакомления с подозрительными событиями и управления настройками выявления таких событий.

6.2 Порядок взаимодействия

- Пользовательский модуль загружается на устройство клиента совместно со страницами защищаемого веб-ресурса;

- Пользовательский модуль собирает контрольные данные со страницы веб-ресурса и посылает их для дальнейшего анализа в АС АО «БУДУЩЕЕ»;

- Веб-серверы заказчика отсылают заголовки запросов от пользователя в АС АО «БУДУЩЕЕ» для выявления случаев блокировки работы пользовательского модуля вредоносным программным обеспечением;

- Серверная инфраструктура АС АО «БУДУЩЕЕ» анализирует полученные данные от пользовательского модуля и АС заказчика на предмет наличия признаков вредоносных действий на устройстве пользователя;

- При выявлении таких признаков АС АО «БУДУЩЕЕ» незамедлительно оповещает заказчика по электронной форме;

- Заказчик через сайт сервера управления АС АО «БУДУЩЕЕ» имеет возможность получить детальную информацию о выявленном подозрительном событии с идентификационной информацией о пользователе и его устройстве;

- Заказчик через сайт сервера управления АС АО «БУДУЩЕЕ» имеет возможность дать обратную связь по выявленному событию, которая будет учтена в последующей обработке получаемых данных от пользовательского модуля;

- Оповещение о событиях, их детальная информация и обратная связь по ним так же возможна с использованием API к АС АО «БУДУЩЕЕ».

6.3 Данные, передаваемые пользовательским модулем

Пользовательский модуль передает следующие контрольные данные с устройства пользователя:

- Данные о пользователе:
    - результат применения алгоритма SHA1 к имени учетной записи пользователя;
    - результат применения алгоритма RSA с публичным ключом заказчика к имени учетной записи клиента;
    - характеристики движения курсором.
- Данные о странице защищаемого веб-ресурса:
    - javascript-код, загружаемый на страницы веб-ресурса;
    - структуру и атрибуты веб-форм, размещенных на страницах веб-ресурса;
    - атрибуты следующих HTML-элементов: iframe, object, embed, applet.
- Данные о браузере, через который производится доступ на веб-ресурс:
    - User-Agent, куда входят:
        - Браузер и его версия;
        - Операционная система и ее версия;
        - Разрядность операционной системы;
        - Название и модель устройства клиента.
    - Accept-Encoding;
    - Accept-Language;
    - разрешение экрана;
    - глубина цвета;
    - доступность ActiveX;
    - часовой пояс;
    - шрифты браузера;

- плагины браузера;
- поддерживаемые языки;
- canvas-отпечаток.

– Данные об устройстве, если поддерживается Adobe Flash Player:
  - архитектура процессора;
  - операционная система;
  - используемая версия и ее разрядность (32/64 бита) Adobe Flash Player;
  - размеры экрана;
  - наличие touch-экрана;
  - язык;
  - системные шрифты.

7 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1 Обеспечение конфиденциальности пользовательских данных

В АС АО «БУДУЩЕЕ» не передается пользовательская информация кроме обезличенного имени учетной записи пользователя. Имя учетной записи пользователя передается в виде:

- результата хеш-функции от имени учетной записи;
- и результата шифрования имени учетной записи с использованием публичного RSA-ключа заказчика.

Обе операции производятся непосредственно на устройстве пользователя.

Получаемая заказчиком информация о подозрительном событии содержит зашифрованное имя учетной записи. Используя соответствующий приватный RSA-ключ, только заказчик может получить исходное имя пользователя.

Таким образом, имя пользователя недоступно третьим лицам, в том числе АО «БУДУЩЕЕ».

7.2 Защита передаваемых данных

Весь обмен информации между пользовательским модулем, АС АО «БУДУЩЕЕ» и АС заказчика производится по протоколу HTTPS.

Передаваемые данные из пользовательского модуля в АС АО «БУДУЩЕЕ» дополнительно кодируются в целях защиты от вредоносного программного обеспечения, функционирующего на устройстве пользователя.

7.3 Безопасность периметра АС заказчика

Обмен между АС заказчика и АС АО «БУДУЩЕЕ» всегда инициируется только со стороны Заказчика.

Для защиты периметра заказчика может быть применен любой тип фильтрации, ограничивающий обмен между АС заказчика и ресурсами АС АО «БУДУЩЕЕ».

7.4 Обеспечение доступности

Недоступность АС АО «БУДУЩЕЕ» никак не отражается на доступности и работоспособности защищаемого веб-ресурса как на стороне пользователя, так и на стороне заказчика.

Тем не менее, АС АО «БУДУЩЕЕ» обеспечивает отказоустойчивость своей инфраструктуры.