Программное обеспечение

«Bot-Trek Secure Portal»

Руководство по установке и эксплуатации

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание процесса установки и эксплуатации 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.

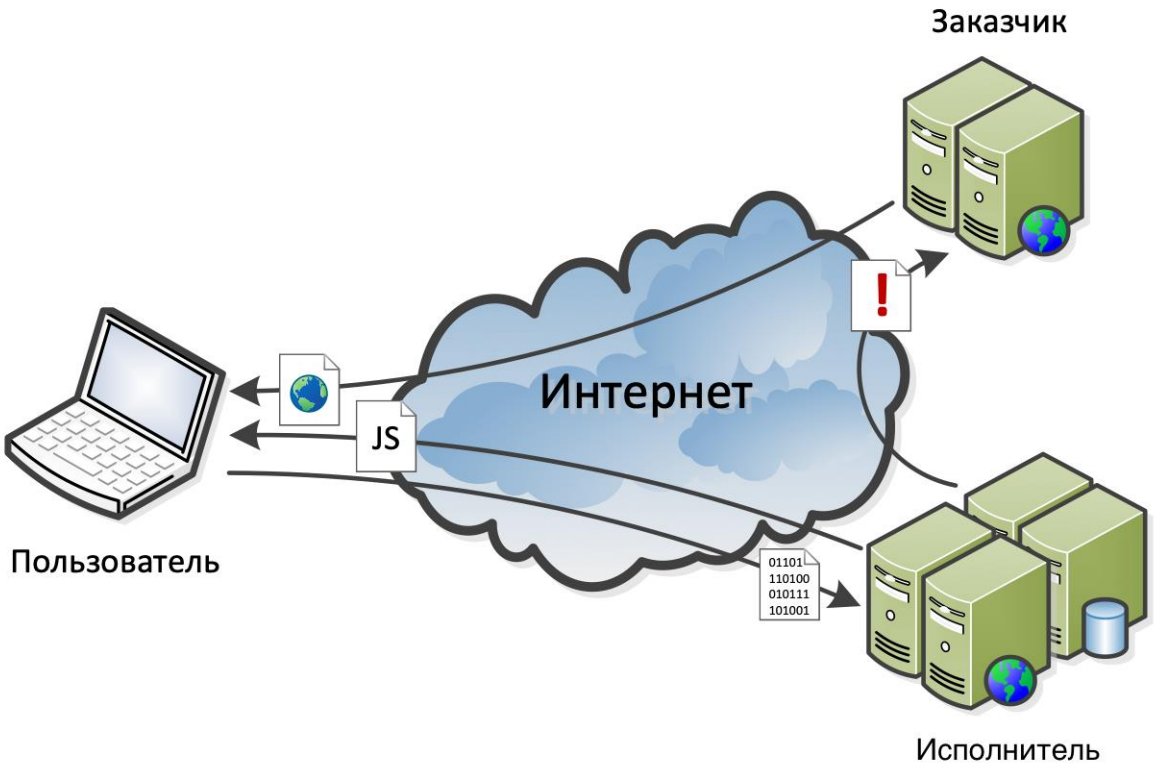

Рисунок 1. Общие принципы функционирования ПО

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 Обязанности и функции администратора заказчика

В обязанности администратора входит следующее:

a. Произвести встраивание ПО в защищаемый веб-ресурс

b. Поддерживать функционирование ПО

5 Порядок встраивания

Для встраивания ПО в защищаемый веб-ресурс необходимо выполнить следующие шаги:

- Выбрать схему встраивания в инфраструктуру;
- Выработать приватный и публичный RSA-ключи;
- Создать две тестовые учетные записи на защищаемом веб-ресурсе;
- Определить перечень IP-подсетей заказчика, которые будут использоваться при взаимодействии с АС АО «БУДУЩЕЕ» (далее АО «БУДУЩЕЕ»);
- Передать полученные ранее регистрационные данные заказчика в АО «БУДУЩЕЕ»;
- Получить в ответ ссылку на настроенный под веб-ресурс пользовательский модуль;
- Сконфигурировать веб-серверы заказчика на дублирование заголовков HTTP-запросов от пользователя на адрес https://fp-back.facct.ru;
- Вставить в каждую необходимую страницу защищаемого веб-ресурса ссылку на пользовательский модуль.

5.1 Выбор схемы встраивания в инфраструктуру

Существует три схемы встраивания ПО в инфраструктуру заказчика:

- Загрузка клиентского модуля и передача контрольных данных происходит на домены *.facct.ru;
- IP-адресы серверов АО «БУДУЩЕЕ» регистрируются как домен следующего уровня в основной домен заказчика;
- Загрузка клиентского модуля и передача контрольных данных производится через веб-серверы заказчика.

У каждой из схем есть свои достоинства и недостатки, оптимальное сочетание которых определяется заказчиком исходя из условий использования защищаемого веб-ресурса:

Схема	Достоинства	Недостатки
I	• Минимальные настройки на стороне заказчика; • Отсутствие дополнительной нагрузки на ИТ-инфраструктуру заказчика; • Быстрый вариант для пилотного использования ПО.	• На стороне браузера видны обращения на сторонние по отношению к заказчику ресурсы; • Неработоспособность ПО при использовании дополнительных настроек политики или плагинов браузера, которые ограничивают обмен со сторонними веб-ресурсами по отношению к основному; • Неработоспособность в IE6 и IE7, или в некоторых режимах обратной совместимости с более ранними версиями в IE8 и старше.
II	• Весь обмен между браузером пользователя и веб-ресурсом происходит с использованием доменов заказчика; • Отсутствие блокировок работы клиентского модуля сторонним ПО; • Средний уровень скрытности использования ПО для мошенника; • Отсутствие дополнительной нагрузки на ИТ-инфраструктуру заказчика.	• В некоторых случаях требуется дополнительно выпускать ssl-сертификат на новые домены (описано ниже); • Неработоспособность в IE6 и IE7, или в некоторых режимах обратной совместимости с более ранними версиями в IE8 и старше.
III	• Весь обмен между браузером пользователя и веб-ресурсом происходит с использованием его домена; • Отсутствие блокировок работы клиентского модуля сторонним ПО; • Высокий уровень скрытности использования ПО для мошенника; • Работоспособность в IE6 и IE7, а также в режимах обратной совместимости с более ранними версиями в IE8 и старше.	• Требуются дополнительные настройки по трансляции запросов, относящихся к ПО, на web-серверах заказчика; • Дополнительная нагрузка на инфраструктуру заказчика.

В случае выбора схемы II, если действие ssl-сертификат защищаемого веб-ресурса не распространяется на домены следующего уровня, то необходимо выпустить отдельный ssl-сертификат на созданный домен.

Необходимые настройки в случае выбора схемы III будут предоставлены отдельно по запросу заказчика.

По выбору заказчика, незначительная часть серверной функциональности ПО генерации полиморфного клиентского модуля и его раздачи может быть передана заказчику. Это дает заказчику полный контроль над изменениями клиентского модуля и перечнем

передаваемых данных с устройства пользователя. Инструкции по настройке вышеозначенного функционала будут предоставлены заказчику отдельно по запросу.

Далее указаны все общие шаги по внедрению ПО вне зависимости от выбранной схемы его внедрения.

5.2 Выработка RSA-ключей

Публичный RSA-ключ заказчика используется пользовательским модулем для шифрования имени учетной записи пользователя. Шифрование производится на устройстве пользователя. Зашифрованное имя учетной записи пользователя передается в АС АО «БУДУЩЕЕ» с другими контрольными деталями страницы защищаемого веб-ресурса.

Приватный RSA-ключ заказчика используется для расшифрования имени учетной записи пользователя при получении извещения из АС АО «БУДУЩЕЕ» о выявлении подозрительного события. Расшифрование производится на стороне заказчика. Таким образом, обеспечивается конфиденциальность пользовательских учетных данных.

Размерность ключей, срок действия и выбор программного обеспечения для выработки пары RSA-ключей определяется заказчиком.

Далее приведены команды для выработки ключей на примере свободного программного обеспечения OpenSSL (www.openssl.org):

a. Для создания приватного RSA-ключа необходимо выполнить команду:

```
openssl genrsa -out privkey.pem 1024
```

b. Для получения публичного RSA-ключа необходимо выполнить команду:

```
openssl rsa -pubout -in privkey.pem -out pubkey.pem
```

5.3 Создание тестовых учетных записей

Для настройки пользовательского модуля необходим доступ в защищаемый веб-ресурс. Для достоверной проверки, что пользовательский модуль не будет собирать контрольные данные, которые зависят от пользователя, необходимо использовать две различные учетные записи.

Условия предоставления тестовых учетных записей определяется заказчиком.

5.4 Взаимодействие ПО с автоматизированными системами

В целях обеспечения информационной безопасности, помимо использования протокола HTTPS при взаимодействии между компонентами АС заказчика и АО «БУДУЩЕЕ», используется ограничение на публичные IP-адреса/подсети заказчика, с которых это взаимодействие возможно.

На рисунке 2 представлена принципиальная схема взаимодействия между АС заказчика и АО «БУДУЩЕЕ»:

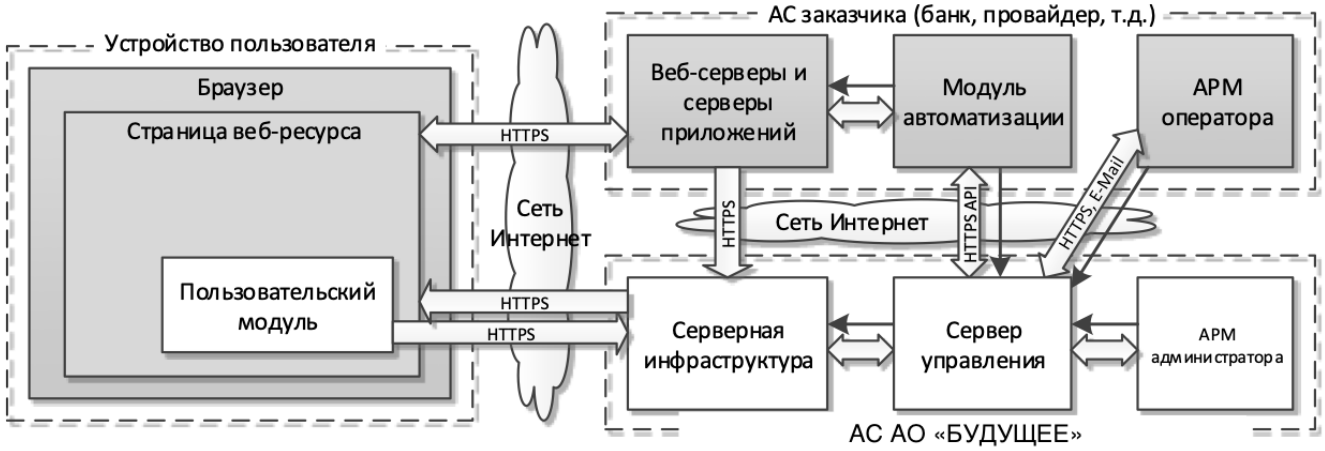

Рисунок 2. Принципиальная схема взаимодействия ПО с автоматизированными системами

Необходимо определить все IP-адреса/подсети заказчика, которые будут участвовать в обмене между следующими компонентами АС:

- Веб-серверы АС заказчика и Серверной инфраструктурой АС АО «БУДУЩЕЕ»;
- Модуль автоматизации АС заказчика и Сервером управления АС АО «БУДУЩЕЕ»;
- АРМ оператора АС заказчика и Сервером управления АС АО «БУДУЩЕЕ».

При определении IP-адресов/подсетей необходимо учесть существующие сценарии обеспечения непрерывности функционирования АС заказчика.

Политика ограничений по доступу к АС АО «БУДУЩЕЕ» со стороны компонент АС заказчика определяется заказчиком самостоятельно. При этом необходимо учитываться следующее:

- все взаимодействие с АС АО «БУДУЩЕЕ» инициируется со стороны компонент АС заказчика по протоколу HTTPS;

- доменным именам АС АО «БУДУЩЕЕ» соответствует несколько IP-адресов в целях обеспечения бесперебойности работы АС и распределения нагрузки на нее.

5.5 Передача регистрационных данных заказчика в АО «БУДУЩЕЕ»

Через портал защищенной электронной почты АО «БУДУЩЕЕ» (https://smail.facct.ru) необходимо отправить письмо с заголовком «Bot-Trek FACCT registration» со следующими сведениями:

- Публичный RSA-ключ заказчика. Передача приватного RSA-ключа строго запрещена и потребует выработки новой пары RSA-ключей;

- Две тестовых учетных записи с паролями к защищаемому веб-ресурсу;

- Публичные IP-адреса/подсети заказчика, которые участвуют в обмене с АС АО «БУДУЩЕЕ».

Если портал защищенной электронный почты АО «БУДУЩЕЕ» используется в первый раз, то необходимо пройти процесс регистрации на портале.

5.6 Получение настроенного пользовательского модуля

Для настройки пользовательского модуля под защищаемый веб-ресурс потребуется некоторый период времени, который зависит от сложности веб-ресурса. Данный период согласовывается с заказчиком отдельно.

В ответ на исходное письмо заказчика с регистрационными данными, по окончании настройки пользовательского модуля, АО «БУДУЩЕЕ» вышлет ссылку на него через портал защищенной почты.

5.7 Вставка ссылки на пользовательский модуль в страницы защищаемого веб-ресурса

Пользовательский модуль написан на языке JavaScript. Для его использования необходимо вставить в раздел HEAD необходимых HTML-страниц веб-ресурса следующую директиву:

<script type=”text/javascript” src=[ссылка на пользовательский модуль]></script>

ВНИМАНИЕ: указанная директива должна находиться сразу за <HEAD>.

6 Поддержание функционирования ПО

Поддержание функционирования ПО состоит в контроле действия настроек, произведенных в рамках встраивания ПО. Иных регламентных мероприятий со стороны администратора заказчика ПО не требует.