ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F.A.C.C.T. Threat Intelligence»

Описание функциональных характеристик

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Аннотация

Настоящий документ описывает функциональные характеристики программного обеспечения «F.A.C.C.T. Threat Intelligence» (далее – ПО, Система, Threat Intelligence).

1.2 Назначение ПО

F.A.C.C.T. Threat Intelligence – система учета скомпрометированной информации, предназначена для сбора информации о случаях компрометации учетной информации пользователей информационных систем, компрометации информации о банковских картах, сбора информации о первичных получателях похищаемых денежных средств (далее - дропов), а так же предоставления интерфейса для отображения данных и оповещения о выявленных случаях компрометации данных с целью минимизации рисков мошенничества в отношении финансовых организаций в разных странах.

Основными целями создания Системы являются:

- Предоставление единого интерфейса регистрации фактов компрометации учетных данных пользователей интерактивных информационных систем (дистанционного банковского обслуживания, платежных систем, систем обмена электронными сообщениями, систем хранения данных в сети интернет и прочих электронных интерактивных систем);
- Консолидация разрозненной информации по компрометации информации в сферах финансового обслуживания, хранения данных, оказания государственных услуг и электронной коммерции;
- Генерация правил для систем предотвращения мошеннических операций, используемых организациями, участниками системы;
- Оперативное оповещение участников системы;
- Снижение уровня преступлений в сфере электронной коммерции;
- Ускорение процесс обмена информацией о мошенничестве между банками;
- Повышение качества и количества раскрываемых преступлений;
- Предоставление прозрачной статистической и аналитической информации.

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.

3 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

Для сбора данных Система постоянно мониторит бот-сети различного назначения, вредоносные программы, которые были найдены в результате реагирования на самые опасные инциденты, закрытые хакерские форумы и собирает данные о новых трендах, угрозах. Все эти данные коррелируются между собой и переносятся в соответствующий раздел пользовательского интерфейса Threat Intelligence. Интерфейс системы предоставляет возможность зарегистрировать выявленный инцидент кибербезопасности, получить дополнительную информацию по инциденту, например:

- IP-адрес скомпрометированного пользователя;
- Точное время компрометации сведений;
- Идентификатор копии установленного вредоносного ПО;

- Идентификатор командного центра бот-сети;
- Источник проведения мошенничества;

А также уведомить ответственных лиц о произошедшем событии кибербезопасности.

4 РЕАЛИЗАЦИЯ ПО

Системы состоит из следующих модулей:

- Модуль регистрации инцидентов компрометации учетных данных
- Модуль оповещения о случаях выявления компрометации информации
- Модуль предоставления статистики и отчетности
- Модуль защиты удаленного доступа и контроля изменений

4.1 Модуль регистрации инцидентов компрометации учетных данных

Доступ к модулю регистрации предоставляется через пользовательский веб-интерфейс. Модуль обеспечивает следующие функции:

- Поддержка стандартного формата импорта данных CSV – comma separated value, подразумевающая разделение полей данных стандартным разделителем, с возможностью указания разделителя в диалоге импорта данных;
- Поддержка корректного импортирования даты и времени инцидента из формата unix timestamp;
- Автоматическая ассоциация импортируемых данных с определенной организацией, в соответствии с настройками системы, по следующим идентификаторам:
  - Для аккаунтов систем ДБО и других интерактивных сервисов – по доменному имени;
  - Для банковских карт - по унифицированному международному идентификатору BIN;
  - Для дропов – по банковскому идентификатору, в зависимости от региона: БИК, SWIFT или RTN номера;
- Автоматическое раскодирование импортируемых данных из стандартного способа кодирования POST-запросов;

- Автоматическое определение региона скомпрометированного пользователя по IP-адресу в соответствии с геолокацией;
- Автоматическое определение страны происхождения скомпрометированной карты по идентификатору BIN в соответствии с мировой базой BIN-идентификаторов;
- Корректное импортирование бинарных данных (изображения экрана, сертификаты, ключи доступа) с указанием ассоциированного банка в диалоге загрузки данных;
- Обеспечение целостности и недублирования хранимых данных, с обеспечением уникальности ключевых полей в соответствии с используемой схемой базы данных;
- Возможность указания произвольной даты выявления скомпрометированных данных с подстановкой текущей даты в случае незаполнения соответствующего поля.

4.2 Модуль оповещения о случаях выявления компрометации информации

Модуль создает отчеты по фактам выявления компрометации данных. Оповещение о инциденте кибербезопасности происходит в режиме реального времени. Отчеты отправляются по электронной почте Заказчику, в отношении которого зафиксирован инцидент компрометации данных.

Помимо уведомления Заказчика, в копию письма ставится ответственный сотрудник Разработчика для отслеживания работы системы уведомления и дополнительного учета выявляемых данных.

4.3 Модуль предоставления статистики и отчетности

Данные в системе отображаются на главной странице (Панель управления) в виде аналитической и статистической информации о структуре, количестве и региональном распределении случаев компрометации учетной информации.

Статистическая информация позволяет отслеживать темпы активности злоумышленников, а также распределение по регионам, и включает в себя:

- количество зарегистрированных инцидентов: общее и с разбивкой по типам данных;
- количество инцидентов за определенные промежутки времени;
- общий объем хранимых в системе данных;
- распределение случаев компрометации данных по странам и городам;
- распределение случаев компрометации данных по времени со структурой данных.

4.4 Модуль защиты удаленного доступа и контроля изменений

Модуль защиты удалённого доступа обеспечивает:

- сохранение конфиденциальности и целостности передаваемой информации;
- ограничение доступа к системе для всех адресов, кроме указанных доверенных адресов Заказчика;
- неотключаемый протокол доступа в Систему для каждого участника Системы;
- неотключаемый протокол внесения изменений в Систему и выгрузки данных из системы:
    - загрузка и выгрузка данных;
    - изменение параметров пользователей Системы или создание новых пользователей;
    - выдача пользователю дополнительных прав.