ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«F6 Threat Intelligence»

Описание функциональных характеристик

Содержание

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термин	Описание
Заказчик	Лицо, заключившее договор на использование ПО
Инцидент/событие кибербезопасности	Событие, когда злоумышленники получают несанкционированный доступ к информации с целью её дальнейшего использования в злонамеренных целях, а также нарушение работы IT-систем. Угроза внедрения или неудачная попытка получения доступа тоже считаются инцидентами
Исполнитель	Работы Исполнителя на протяжении всего жизненного цикла могут исполняться: • АО «БУДУЩЕЕ»; • Компанией-интегратором, по выбору Заказчика
ПО, Система, «F6 Threat Intelligence»	Программа для ЭВМ «F6 Threat Intelligence»
Пользователь	Лицо, непосредственно использующее ПО
Разработчик	АО «БУДУЩЕЕ»
Угроза или Киберугроза	Потенциально возможное происшествие, преднамеренное или нет, которое может оказать нежелательное воздействие на систему или хранящуюся информацию
API (Application Programming Interface)	Описание способов взаимодействия одной компьютерной программы с другими
C2 (Control&Command) сервера	Сервера, с помощью которых злоумышленники управляют скомпрометированной системой
CSV	Текстовый файл, который позволяет сохранить данные в виде структурированной таблицы

DarkWeb (даркweб)	«Темная сеть», скрытая анонимная сеть интернета, где действуют злоумышленники, а также форумы в открытом Интернете, посвященные хакерской тематике
IoC (Indicators of Compromise)	Индикаторы компрометации. Информация, связанная с вредоносной активностью, такая как хэши образцов вредоносных программ, IP-адреса и доменные имена, связанные с атаками. Они используются для обновления систем обнаружения и защиты, таких как брандмауэры, а также для анализа методов, которые используют злоумышленники
OSINT (Open-Source Intelligence)	Разведка по открытым источникам. То есть сбор и анализ информации, полученной из разных общедоступных информационных каналов
POST-запрос	Метод HTTP для отправки данных на сервер

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Аннотация

Настоящий документ описывает функциональные характеристики «F6 Threat Intelligence».

1.2 Назначение ПО

«F6 Threat Intelligence» — это система киберразведки, предназначенная для сбора, анализа и распространения информации о событиях безопасности, Киберугрозах и уязвимостях.

Система представляет собой обширную базу знаний, содержащую информацию по злоумышленникам, Угрозам и возможным уязвимостям, а также предоставляет данные о вредоносном программном обеспечении. По выявленным событиям кибербезопасности Система генерирует оповещения.

Кроме того, в Системе представлены аналитические отчеты о последних Киберугрозах, что позволяет выстроить наиболее эффективную защиту инфраструктуры.

1.3 Программно-аппаратные среды функционирования ПО

Требования для работы ПО как облачного интернет-сервиса:

- 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;
- Яндекс.Браузер версии 20 и выше;
- Microsoft Edge версии 105 и выше.

Требования для работы ПО с помощью API-интерфейса:

- Python 3.5.3.

2 ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ПО

На Рисунок 1 изображены общие принципы функционирования ПО.

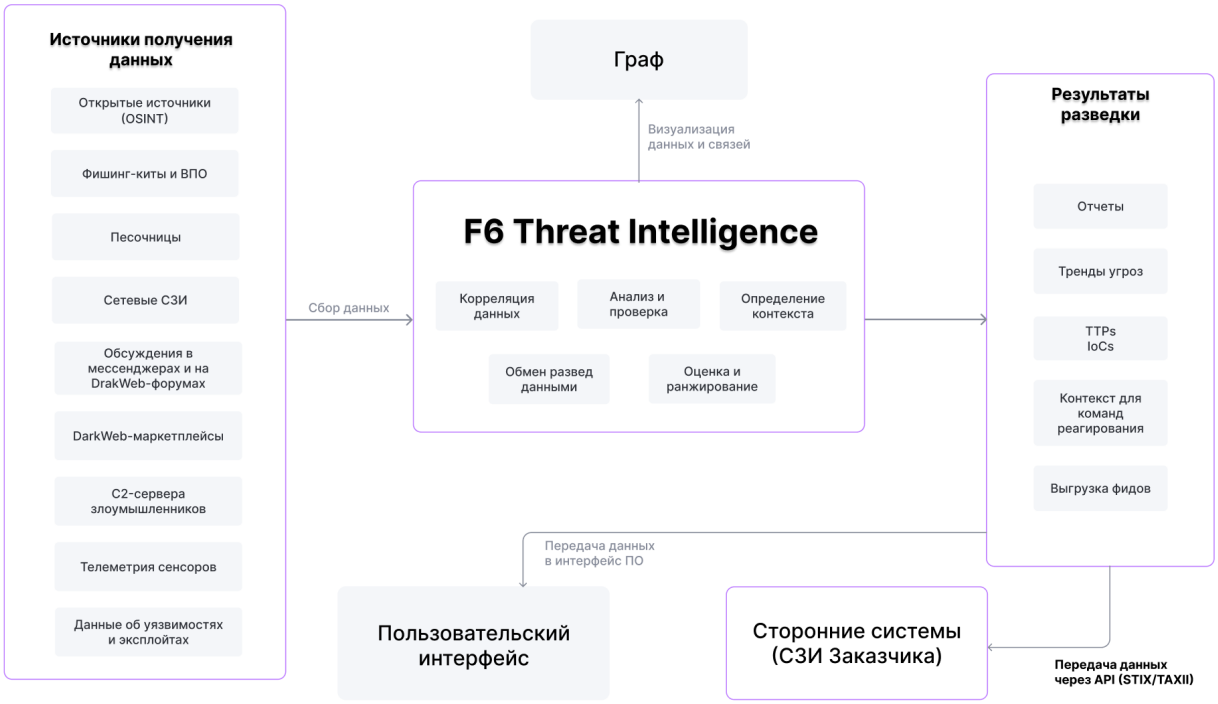

Рисунок 1. Общие принципы функционирования ПО

ПО «F6 Threat Intelligence» собирает данные из различных источников, таких как:

- Открытые источники (OSINT);
- Фишинг-киты и вредоносное ПО (далее — ВПО);
- Песочницы — системы для безопасного запуска файлов в виртуальной среде для выявления потенциального ВПО;
- Сетевые СЗИ;
- Мессенджеры и DarkWeb-форумы («теневые», подпольные форумы злоумышленников);
- DarkWeb-маркетплейсы (торговые площадки злоумышленников в теневом сегменте сети Интернет);
- C2 (Control&Command) сервера злоумышленников — сервера, с помощью которых злоумышленники управляют скомпрометированной системой;
- Телеметрия сенсоров;
- Данные об уязвимостях и эксплойтах.

Затем ПО перерабатывает полученные данные в осмысленную и практически полезную информацию для дальнейшего обнаружения и реагирования на Угрозы, а также минимизации последствий от возможных атак злоумышленников. ПО коррелирует между собой полученные данные, оценивает и ранжирует данные по уровню их потенциальной опасности, а также проверяет на достоверность.

Результатом такой переработки становятся данные кибербразведки: индикаторы компрометации (IoC), техники, тактики и процедуры злоумышленников по матрице MITRE ATT&CK, а также данные для составления отчетов по трендам Угроз, последним атакам и т. п. При возникновении события кибербезопасности, ПО незамедлительно оповещает ответственных лиц.

Результаты кибербразведки переносятся в соответствующие разделы пользовательского интерфейса ПО для дальнейшего использования Пользователем, а также отправляются в сторонние системы через API. В ПО «F6 Threat Intelligence» реализованы два API-интерфейса — API 1.0 и API 2.0.

«F6 Threat Intelligence» позволяет использовать графовый анализ с помощью инструмента Граф. Граф визуализирует связи между данными, чтобы найти источник актуальной Угрозы, отследить существующие связи участников киберпреступных группировок.

ПО позволяет интегрировать полученные данные с системами безопасности (СЗИ) Заказчика с помощью API для оптимизации обмена информацией об Угрозах и повышения эффективности борьбы с возникающими Угрозами.

3 РЕАЛИЗАЦИЯ ПО

ПО «F6 Threat Intelligence» представляет из себя комплексную систему, состоящую из нескольких модулей. ПО реализовано на следующих языках программирования:

- PHP;
- Golang;
- JavaScript;
- Python.

Система состоит из следующих модулей:

- Модуль регистрации Инцидентов событий кибербезопасности;
- Модуль поиска информации по ключевым словам в определенных массивах данных;
- Модуль оповещения о случаях упоминаний ключевых слов;
- Модуль предоставления статистики и отчетности;
- Модуль предоставления аналитических данных об активности злоумышленников;
- Модуль защиты удаленного доступа и контроля изменений.

3.1 Модуль регистрации Инцидентов кибербезопасности

Модуль позволяет зарегистрировать в Системе Инциденты кибербезопасности для реагирования, защиты от подобных Инцидентов и их дальнейшего изучения. Доступ к модулю предоставляется через веб-интерфейс. Интерфейс обеспечивает обязательные и необязательные поля для заполнения (список полей приведен ниже).

Модуль поддерживает стандартный формат импорта данных CSV, корректное импортирование даты и времени Инцидента из формата unix timestamp.

Кроме того, модуль обеспечивает:

- Автоматическое раскодирование импортируемых данных из стандартного способа кодирования POST-запросов;
- Автоматическое определение региона пользователя, ставшего целью атаки, по IP-адресу в соответствии с геолокацией;
- Корректное импортирование бинарных данных (изображения экрана, сертификаты, ключи доступа);
- Целостность и недублирование хранимых данных, с обеспечением уникальности ключевых полей в соответствии с используемой схемой базы данных;

– Возможность указания произвольной даты выявления события кибербезопасности с подстановкой текущей даты в случае незаполнения соответствующего поля.

Для пользователей систем ДБО (дистанционного банковского обслуживания) и иных интерактивных интерфейсов при регистрации Инцидентов обязательными для заполнения являются следующие поля:

– Доменное имя либо IP-адрес, на котором развернута система;
– Идентификатор пользователя;
– IP-адрес;
– Дата и время Инцидента.

Следующая информация является необязательной для заполнения, однако интерфейс предусматривает данные поля:

– Коды подтверждения операций;
– Идентификатор копии вредоносного ПО;
– Иные данные.

3.2 Модуль поиска информации по ключевым словам в определенных массивах данных

Модуль позволяет зарегистрировать в Системе факты выявления ключевых слов, обнаруженных на определенных ресурсах в сети Интернет. Доступ к модулю предоставляется через веб-интерфейс.

ПО производит мониторинг по ключевым словам, заданным для Заказчика, в ряде источников, таких как:

– Открытые источники (OSINT);
– Мессенджеры и DarkWeb-форумы;
– DarkWeb-маркетплейсы;
– Телеметрия сенсоров.

Модуль поддерживает стандартный формат импорта данных CSV, корректное импортирование даты и времени Инцидента из формата unix timestamp. Импортируемые данные автоматически ассоциируются с определенной организацией, в соответствии с настройками Системы, по заданным доменным именам, IP-адресам и ключевым словам.

Кроме того, модуль обеспечивает:

– Автоматическое раскодирование импортируемых данных из стандартного способа кодирования POST-запросов;

– Целостность и недублирование хранимых данных, с обеспечением уникальности ключевых полей в соответствии с используемой схемой базы данных;
– Возможность указания произвольной даты выявления данных с подстановкой текущей даты в случае незаполнения соответствующего поля.

3.3 Модуль оповещения о случаях упоминаний ключевых слов

При выявлении случаев упоминаний ключевых слов Пользователям Системы отправляются отчеты для предотвращения Инцидентов кибербезопасности в режиме реального времени. Оперативное оповещение позволяет в значительной степени снизить количество успешных случаев мошенничества, снизить потенциальные риски атаки.

При регистрации в Системе случая упоминания ключевых слов, принадлежащих или связанных с Пользователем, Пользователю немедленно приходит оповещение на электронную почту, указанную в настройках Системы.

Оповещение по электронной почте содержит в себе как минимум следующую обязательную информацию:

– Тип выявленных данных;
– Количество выявленных данных;
– Название организации.

Помимо уведомления на почтовый адрес Пользователя, в копию уведомления ставится ответственный сотрудник Разработчика для отслеживания работы системы уведомления и дополнительного учета выявляемых данных.

3.4 Модуль предоставления статистики и отчетности

Зарегистрированные в Системе данные позволяют предоставлять аналитическую и статистическую информацию о структуре, количестве и региональном распределении случаев совершенных или планируемых кибератак. Аналитическая информация выводится, прежде всего, на главной странице (Панель управления) в виде краткой сводки по количеству, типам, региональному и временному распределению данных. Статистическая информация позволяет отслеживать темпы роста/спада активности злоумышленников в этой сфере, а также различные распределения по регионам.

Модуль предоставления статистики и отчетности предоставляет следующую информацию:

– Количество зарегистрированных Инцидентов: общее и с разбивкой по типам данных;
– Количество Инцидентов за определенные промежутки времени;
– Общий объем хранимых в системе данных;

– Распределение случаев кибератак по странам;
– Распределение случаев кибератак по времени с отображением структуры данных;
– Время отображения статистических показателей.

3.5 Модуль предоставления аналитических данных об активности злоумышленников

Модуль предоставления аналитических данных об активности злоумышленников предоставляет актуальные данные об используемых техниках, тактиках и инструментах злоумышленников. Такие данные повышают осведомленность пользователей ПО о текущих трендах кибератак, используемых ВПО и т.п., и позволяют выстроить эффективную защиту инфраструктуры Пользователей для противодействия потенциальным кибератакам.

Действия атакующих важно отслеживать на временной шкале, чтобы иметь возможность оценивать не только их активность, но и сферу интересов, приоритетные регионы, эволюцию используемых тактик по методологии MITRE ATT&CK. Описание тактик атакующих (злоумышленников) позволяет внутренним командам Разработчика и пользователям Системы эффективно проверять состояние защищенности инфраструктуры, разрабатывать и адаптировать планы по ее улучшению.

Доступ к модулю предоставляется через веб-интерфейс в соответствующем разделе (Атакующие).

Модуль предоставляет следующие данные:

– Название группировки;
– Псевдонимы - перечень псевдонимов, под которыми группировка вела свою деятельность;
– Первое появление - первая зафиксированная активность группировки;
– Последнее появление - последняя активность группировки;
– Источник Угрозы - страна, из которой группировка ведет свою деятельность;
– Отрасль - основные отрасли деятельности жертв;
– География - страны, в которых группировка проявляла свою активность;
– Последние Угрозы - даты последних зафиксированных атак группировки;
– Список используемого группировкой вредоносного программного обеспечения;
– Иные сведения.

3.6 Модуль защиты удаленного доступа и контроля изменений

Модуль защиты удаленного доступа обеспечивает защиту от несанкционированного доступа в Систему, защиту конфиденциальных данных Пользователей, а также записывает изменения в Системе, что помогает в выявлении проблем и предотвращении потенциальных событий кибербезопасности.

Модуль защиты удалённого доступа обладает следующими функциями:

- Сохранение конфиденциальности и целостности передаваемой информации;
- Возможность ограничения доступа к системе для всех адресов, кроме указанного в настройках, причем ограничение работает на канальном уровне;
- Неотключаемый протокол доступа в Систему для каждого участника Системы. Для контроля удачных/неудачных попыток авторизации в личном кабинете отображается история авторизации;
- Неотключаемый протокол внесения изменений в Систему и выгрузки данных из системы:
    - Загрузка новых данных;
    - Изменение параметров пользователей Системы;
    - Выгрузка данных в отдельный файл со скачиванием через клиентский браузер;
    - Создание новых пользователей Системы;
    - Выдача пользователю дополнительных прав.