Программное обеспечение

«F.A.C.C.T. Malware Detonation Platform»

Описание функциональных характеристик

Содержание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Введение

Настоящий документ содержит описание функциональных характеристик программного обеспечения «F.A.C.C.T. Malware Detonation Platform» (далее – ПО, F.A.C.C.T. Malware Detonation Platform, MDP).

1.2 Назначение ПО

F.A.C.C.T. Malware Detonation Platform – программное обеспечение для поведенческого анализа, обеспечивающее выявление ранее неизвестного вредоносного кода с использованием передовых алгоритмов машинного обучения. Решение позволяет эффективно выявлять ранее неизвестные угрозы, осуществляя анализ файлов в изолированной среде. Он позволяет предотвратить заражения в результате фишинговых рассылок, либо загрузки/получения вредоносных файлов, осуществляющих заражения с использованием ранее неизвестных вредоносных программ и инструментов.

Использование модуля F.A.C.C.T. Malware Detonation Platform обеспечивает обнаружение ранее неизвестного вредоносного ПО и сложных целевых атак.

Основными целями создания ПО являются:

1. Предоставление интерфейса с отображением результатов проведения поведенческого анализа объектов
2. Повышение качества и количества раскрываемых преступлений;
3. Предоставление прозрачной статистической и аналитической информации.

1.3 Общие принципы функционирования ПО

Внутри Системы используется набор виртуальных машин с различными операционными системами. Анализируемый объект в автоматизированном режиме запускается на виртуальной машине. После запуска происходит запись следов работы внутри операционной системы в результате запуска объекта, исходя из показателей компрометации. Показатели компрометации могут обновляться в соответствии с понимаем современного ландшафта киберпреступлений. По итогам анализа доступен подробный отчет со следующими информационными блоками:

- Развернутая информация о файле;

- Поведенческие маркеры;
- Сведения о сетевая активности;
- Дерево процессов;
- Видео.

2 Программно-аппаратные среды функционирования ПО

- 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 Реализация ПО

ПО состоит из следующих модулей:

- Модуль предоставления возможности загрузки ПО
- Модуль предоставления результатов анализа
- Модуль защиты удаленного доступа и контроля изменений

В рамках предоставляемого интерфейса операторы системы имеют возможность загружать ПО и файлы в Систему и получать данные по результатам анализа.

3.1 Модуль предоставления возможности загрузки ПО в Систему

В разделе «Управление → Анализ файлов» представлена возможность загрузить ПО и/или набор файлов для проведения поведенческого анализа.

3.2 Модуль предоставления результатов анализа

В разделе «Управление → Анализ файлов» предоставляется список работ по анализу ПО и/или файлов. Каждая строка отражает задачу анализа. По задаче анализа предоставляется детализированная информация:

- Развернутая информация о файле;
- Поведенческие маркеры;
- Сведения о сетевая активности;
- Дерево процессов;
- Видео.

3.3 Модуль защиты удаленного доступа и контроля изменений

Модуль защита удалённого доступа обеспечивает:

- сохранение конфиденциальности и целостности передаваемой информации;
- возможность ограничения доступа к системе для всех адресов кроме указанного в настройках.

- 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.