ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «Preventive Proxy»

Версия 1.0

ОПИСАНИЕ РЕАЛИЗАЦИИ

СОДЕРЖАНИЕ

Аннотация

Настоящий документ содержит описание реализации программного обеспечения «Preventive Proxy» версии 1.0 (далее – ПО).

Краткое описание и назначение ПО

Preventive Proxy – программное обеспечение для обнаружения интеллектуальных автоматизированных программ (ботов) и защиты от них, а также для снижения прямых убытков и издержек от мошеннической активности на веб-порталах и в мобильных приложениях (далее – АС Заказчика), которая происходит с использованием автоматизированных действий. В ПО используются машинное обучение и нейронные сети для анализа сессионных данных, экспертные скоринговые модели, анализ трафика, графовый анализ связанных ресурсов.

Основными целями создания ПО являются:

- снижение уровня мошенничества и хищений денежных средств у пользователей АС Заказчика;
- повышение защищенности пользователей АС Заказчика от мошеннической активности и хищений, производимых с помощью автоматизированных действий;
- повышение показателей Заказчика по противодействию мошенничеству в его АС;
- повышение уровня автоматизации по принятию решения о наличии вредоносной бот-активности в АС Заказчика.

Функциональные требования к ПО

Функциональность ПО должна предусматривать выполнение следующих действий:

- проверка легитимности пользователя и его окружения;
- выявление и блокировка бот-активности;
- предоставление дополнительных вердиктов и скоринговых оценок в систему противодействия мошенничества Заказчика в целях снижения уровня ложно положительных выявлений мошенничества;
- обеспечение защиты от фишинг/фарминг-атак;
- предотвращение извлечения данных со страниц приложения (защита от скрапинга);
- предотвращение перегрузки запросами всего ресурса или его составляющих в результате бот-активности (защита от отказа в обслуживании);
- предотвращение получения закрытой информации из серверной части мобильного или веб-приложения (защита от атак на мобильный API);
- выявление прямых обращений к программному интерфейсу или его использование из сторонних или поддельных мобильных приложений (защита от несанкционированного использования API);
- мониторинг обращений из браузера пользователя к вредоносным доменам;
- выявление доступа со скомпрометированных выделенных серверов или устройств компаний, предоставляющих услуги хостинга и коллокации;
- выявление использования средств для автоматизации пользовательских действий (Selenium, PhantomJS и т.д.).

Эксплуатационные требования к ПО

В ходе эксплуатации ПО должны выполняться следующие требования:

- Совместимость – ПО должно быть совместимо с наиболее популярными программно-аппаратными средами (указаны в п.5 «Программно-аппаратные среды функционирования ПО);
- Универсальность – возможность обмена данными с АС Заказчика для выполнения действий, указанных в п.3 «Функциональные требования к ПО»;
- Надежность – обеспечение бесперебойной работоспособности ПО не ниже 95% времени на протяжении года.

Программно-аппаратные среды функционирования ПО

ПО функционирует в программно-аппаратных средах, отвечающих хотя бы одному из следующих требований:

- Среда поддерживается компилятором языка программирования Golang. Этому требованию соответствуют операционные системы на платформах Linux, Windows и macOS.
- Среда позволяет запустить Docker. ПО может функционировать в среде с ядром, поддерживающим контрольные группы и изоляцию пространств имён (namespaces); существуют сборки для Windows, MacOS (Intel and Apple chipset), популярных дистрибутивов Linux и ARM.

Общие принципы функционирования ПО

Для работы Preventive Proxy понадобятся:

- клиентский модуль Fraud Hunting Platform (Web Snippet или Mobile SDK) - получает и передает в серверную часть поведенческие характеристики пользователя и окружения, в котором работает приложение;
- серверная часть Fraud Hunting Platform (Processing Hub) - в ответ на данные, полученные из клиентского модуля, формирует и передает новый серверный файл cookie с вердиктом о наличии или отсутствии признаков бот-активности. При запросе из приложения клиентский модуль дополнительно формирует и передает клиентский файл cookie на базе серверного.

На основе данных, полученных из клиентского и серверного модулей Fraud Hunting Platform, Preventive Proxy проверяет наличие, корректность и уникальность файлов cookie на запросах с устройства пользователя, и на их основе принимает решение о наличии или отсутствии бот-активности в текущей пользовательской сессии.

Реализация ПО

Архитектура ПО представляет собой сервис-ориентированную архитектуру, основанную на использовании распределенных, слабо связанных, заменяемых компонентов, оснащенных

стандартизированными интерфейсами для взаимодействия по стандартизированным протоколам.

Унификация программных интерфейсов осуществляется на уровне, как минимум, но не ограничиваясь:

- браузера пользователя;
- мобильных приложений Заказчика;
- АС Заказчика;
- ПО.

В состав ПО входят следующие подсистемы:

- Подсистема получения данных с устройства пользователя. Подсистема предназначена для получения токенов пользователей в рамках их сессии работы в АС Заказчика, содержащих первичные данные о мошеннической активности на стороне пользователей, дополнительные идентификационные данные пользовательских устройств и другие параметры;
- Подсистема обработки данных. Подсистема предназначена для обработки данных, полученных от подсистемы получения данных с устройств пользователей АС Заказчика – проверки токенов на валидность и целостность;
- Подсистема управления. Подсистема, предназначенная для выполнения настроек и администрирования ПО;
- Подсистема аналитики. Подсистема предназначена для работы Аналитиков АС с выявленными событиями бот-активности, получения отчетов и статистики, настройки модели выявления бот-активности;
- Подсистема информационного обмена. Подсистема предназначена для экспорта/импорта данных между АС Заказчика и ПО как в режиме реального времени, так и в диалоговом (запросном) режиме и передачи в АС Заказчика вердиктов и скоринга выявленных фактов бот-активности;
- Подсистема защиты информации. Подсистема представляет собой программно-технический комплекс, предназначенный для защиты технических средств, программного обеспечения и данных от несанкционированного доступа к данным АС. Выполняет функции по идентификации и аутентификации сторон, производящих обмен ин-формацией, функции по разграничению прав доступа к информационным ресурсам АС.

Подсистемы получения данных, обработки данных, передачи данных, управления, аналитики, информационного обмена, защиты информации должны иметь возможность размещаться как в облачной инфраструктуре Исполнителя, так и в инфраструктуре Заказчика. Решение принимается на этапе внедрения.

Устранение неисправностей ПО

Устранение неисправностей ПО происходит в 2 этапа:

- Устранение критических неисправностей. Производится непосредственно при обнаружении неисправности, выпуск исправляющего обновления производится незамедлительно.
- Устранение неисправностей не являющихся критическими. Производится в запланированные промежутки времени одновременно с выпуском других обновлений.

Среднее временной интервал доступности продукта за год – 95%.

Для обеспечения бесперебойной работы ПО необходима команда технической поддержки, состоящая не менее чем из двух специалистов разработки, а также не менее чем из одного DevOps инженера.

Сообщить об обнаруженной неисправности можно на адрес электронной почты sp@group-ib.com. В письме необходимо указать следующие данные:

- название компании-заказчика и контакты;
- на каком ресурсе обнаружена проблема;
- описание проблемы, если возможно - диагностические сообщения от системы;
- критичность проблемы.

Совершенствование ПО

ПО находится в состоянии непрерывного совершенствования. План совершенствования утверждается на год, впоследствии становится доступен для конечных пользователей.

Фактическое размещение инфраструктуры и команды разработки

Команда и инфраструктура разработки размещены по адресу: г. Москва, ул. Шарикоподшипниковская д.1.