УДК 004.000

Д.В. ШУЛИНИН[1], Н.Г. МИЛОСЛАВСКАЯ[2]

[1]*ООО «Юзергейт», Москва*

[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

ПРОЦЕСС РАЗРАБОТКИ ПРАВИЛ ДЛЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Цель работы – создание процесса разработки контента (правил выявления атак, сигнатур сетевых приложений) для средств защиты информации (СЗИ) на примере UserGate NGFW [1]. Основной результат – формирование систематизированного подхода к разработке контента СЗИ, начиная со сбора данных из открытых и закрытых источников, их оценку и приоритезацию, и заканчивая формированием пакета контента и загрузки его на СЗИ.

Введение

Защитный контент (правила выявления сетевых атак, сигнатуры сетевых приложений, идентификаторы компрометации (списки URL, IP, хэшей файлов, содержащих вредоносный код)) является неотъемлемой частью любого сетевого СЗИ. Благодаря наличию этого контента и функционала, способного его обрабатывать, сетевое устройство может называться СЗИ. Также необходимо помнить, что технологии проведения атак эволюционируют, что говорит о необходимости постоянного развития защитного контента и поддержания его в актуальном состоянии.

Постановка задачи

Цель работы – создание унифицированного процесса по разработке защитного контента для сетевых СЗИ, который бы охватывал полный цикл создания нового правила или сигнатуры, включая поиск информации о новых видах атак, оценку критичности и приоритезацию, моделирование атаки, разработку правила и тестирование его на продуктивном трафике, фильтрацию ложноположительных срабатываний и формирование пакета правил для загрузки на СЗИ.

Пути решения задачи

Разработан процесс, который трансформирует данные из открытых и закрытых источников в пакеты защитного контента, загружаемого на СЗИ, состоящий из следующих этапов:

1) формирование запроса на разработку экземпляра защитного контента. В ходе формирования запроса происходит сбор ключевой информации из

источников данных об атаках, методах защиты, уязвимостях программного обеспечения (ПО) включая, но не ограничиваясь, публикациями производителей ПО и компаний, занимающихся информационной безопасностью (ИБ), общедоступными репозитории, и информационными рассылками регуляторов в сфере ИБ [2];

2) оценка приоритета, для чего используется методика, опирающаяся на ряд критериев, в том числе вектор атаки; сложность реализации; необходимые привилегии; уровень влияния на конфиденциальность, целостность и доступность;

3) стендирование с задачей воспроизведения атаки в лабораторных условиях. Результат данного этапа – полностью сформированная лабораторная среда, которая позволила воспроизвести атаку;

4) сбор и анализ ключевых идентификаторов атаки, в рамках чего осуществляется запись трафика, журналов событий и сбор сопутствующих идентификаторов (например, файлы) в момент проведения атаки;

5) разработка и тестирование с написанием правила выявления атаки, основываясь на собранных на предыдущем этапе, образцах. Для тестирования разработанного правила трафик, имитирующий действия атакующего, пропускается через СЗИ, на котором включено разработанное правило;

6) фильтрация ложноположительных срабатываний правила, для чего используется генератор трафика с образцами трафика, имитирующими работу сети компании. Успешным завершением этапа является отсутствие ложноположительных сработок на тестовом образце трафика;

7) сборка пакета контента. Правило добавляется в пакет контента для централизованной публикации на СЗИ.

Заключение

Созданный процесс разработки контента для СЗИ охватывает полный цикл создания новых правил выявления атак, делая его прозрачным, и измеримым за счет отслеживания ключевых показателей, таких как кол-во производимого контента и время, затраченное на разные этапы разработки.

Список литературы

1. Российские межсетевые экраны нового поколения [Электронный документ]. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/Russian-NGFW-selection-criteria (дата обращения: 23.10.2025).

2. Банк данных угроз безопасности информации [Электронный документ]. – Режим доступа: https://bdu.fstec.ru/vul (дата обращения: 23.10.2025).