Успенский Егор Николаевич
студент
ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ»
г. Москва
Стариков Александр Сергеевич
студент
ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ»
г. Москва
Ромашкина Галина Васильевна
студентка
ГАОУ ВО «Московский городской педагогический университет»
г. Москва
Норкина Анна Николаевна
канд. экон. наук, доцент
ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ»
г. Москва

DOI 10.31483/r-32922

АДАПТИВНОЕ ОБНАРУЖЕНИЕ ВРЕДОНОСНЫХ ЗАПРОСОВ В ВЕБ-АТАКАХ

***Аннотация**: строки веб-запросов (запросы), которые передают параметры указанному ресурсу, всегда обрабатываются злоумышленниками для извлечения конфиденциальных данных и даже для получения полного контроля над веб-серверами и веб-приложениями жертвы. Тем не менее существующие подходы обнаружения вредоносных запросов в современной литературе не могут справиться с постоянным изменением веб-атак. В статье предлагается*

AMODS, адаптивная система, которая периодически обновляет модель обнаружения последних неизвестных атак. Также предлагается адаптивная стратегия обучения, которая называется SVM HYBRID, используемая данной системой для минимизации ручной работы. Оценивается современная модель обнаружения, обученная по десятидневному набору данных, полученному из журналов веб-сервера университета. Эта система превосходит существующие методы обнаружения веб-атак с F-значением 94,79% и частотой FP 0,09%. Общее количество вредоносных запросов, полученных с помощью SVM HYBRID, в 2,78 раза больше, чем в популярном методе адаптивного обучения с использованием опорных векторов поддержки (SVM AL). Полученные вредоносные запросы можно использовать для обновления библиотеки сигнатур брандмауэра веб-приложений (WAF).

***Ключевые слова**: веб-атаки, строки запросов, строки веб-запросов, адаптивное обучение, SVM, обнаружение вторжений, обнаружение аномалий.*

Веб-атаки – это атаки, которые используют исключительно протокол HTTP/HTTPS. Отчет об угрозах для интернет-безопасности от Symantec (ISTR) [1] показывает, что количество атак активно возросло, достигнув 1,1 миллиона ежедневно в 2015 году, что превышает показатели 2014 года более чем вдвое (0,493 млн). Среди веб-атак количество «инъекций» кода против веб-приложений увеличивается с каждым годом и составляет по крайней мере 96,15% веб-атак в 2015 году, согласно отчету об атаках веб-приложений от Imperva (WAAR). В 2015 году Team GhostShell утверждали, что взломали множество веб-сайтов с помощью атак с использованием SQL-инъекций (SQLI) [2] и получили тысячи скомпрометированных данных учетных записей, включая электронные письма, имена пользователей, адреса, номера телефонов и другую конфиденциальную информацию.

Статья посвящена наиболее распространенным типам атак с использованием веб-кода в 2015 году, а именно: атака с использованием межсайтовых сценариев (XSS), атака SQLI, обход каталога (DT) и удаленное включение файлов

(RFI) [4], что составляет соответственно 49,09%, 28,32%, 9,82% и 8,92% от всех веб-атак. Векторы этих атак существуют в пользовательском вводе. Всякий раз, когда пользовательский ввод обрабатывается неправильно, эти атаки могут быть успешными. Поскольку большая часть данных, вводимых пользователем, существует в запросах 1, обнаружение вредоносных запросов является ядром обнаружения атак на основе внедрения кода через Интернет. Для веб-приложений, исходный код которых недоступен или труднодоступен, системы обнаружения вторжений (Web IDS) являются единственным вариантом. Веб-IDS выступает в качестве промежуточного уровня между защищенными веб-приложениями и пользователями и анализирует веб-трафик для выявления возможных вредоносных действий.

Значительные усилия были предприняты для обнаружения вредоносных запросов в веб-запросах с использованием веб-идентификаторов. Используются два основных подхода к обнаружению: обнаружение на основе сигнатур и обнаружение на основе аномалий. Популярным подходом к обнаружению на основе сигнатур является WAF, который поддерживает библиотеку сигнатур известных сигнатур и сравнивает новые веб-запросы с сигнатурами. Подходы на основе сигнатур эффективны при обнаружении известных атак с низкой частотой ложных срабатываний (FP), но не способны обнаружить ранее неизвестные атаки (например, атаки нулевого дня). Подходы обнаружения на основе аномалий [4] обычно полагаются на модель обнаружения для выявления аномальных веб-запросов. В отличие от подходов, основанных на сигнатурах, подходы, основанные на аномалиях, могут обнаруживать неизвестные атаки, но с высокой частотой FP. Два подхода часто применяются взаимодополняющим образом в веб-IDS: обнаружение аномалий служит для обнаружения неизвестных атак, сигнатуры которых затем используются для обнаружения в методе на основе сигнатур. Способность обнаруживать неизвестные атаки привлекла большое академическое внимание к подходам, основанным на аномалиях.

Однако существующие основанные на аномалиях подходы к обнаружению веб-атак постоянны, иными словами, они обычно собирают все обучающие

данные один раз, чтобы создать модель постоянного обнаружения. Поскольку злоумышленники становятся все более изощренными и используют более совершенные инструментарии веб-атак, модель обнаружения может устареть, не способная обнаруживать последние вредоносные запросы в веб-атаках. Предыдущие методы адаптивного обнаружения атак [4] предназначены для сетевых вторжений и не применимы к веб-атакам. Практическое решение для поддержания постоянно обновляемой модели обнаружения веб-атак состоит в том, чтобы включать самые последние важные запросы, включая информативные доброкачественные запросы и репрезентативные вредоносные запросы. Существующий подход к получению последних важных запросов заключается в случайном отборе запросов из веб-трафика и последующей их маркировке вручную. К сожалению, большинство случайно выбранных запросов являются схожими доброкачественными, и существует низкая вероятность того, что запрос будет важным. Поскольку веб-трафик огромен, для получения важных запросов требуется значительная ручная маркировка.

В этой статье будут рассмотрена вопросы, связанные с адаптивным обнаружением вредоносных запросов при веб-атаках. Будет представлена AMODS, адаптивная система для этой цели. AMODS использует эффективную адаптивную стратегию обучения, SVM HYBRID, которая является гибридом выбора подозрительности (SS) и выбора образца (ES). Первый позволяет получать наиболее важные информационные запросы, а именно подозрения, а второй специализируется на сборе репрезентативных вредоносных запросов, образцов. Подозрения и образцы называются важными вопросами. AMODS стремится выявлять атаки как можно раньше, периодически проверяя последние важные запросы. Количество важных запросов тривиально, поэтому ручная маркировка сводится к минимуму. Затем важные запросы включаются в пул обучения для обновления модели обнаружения, которая представляет собой ансамблевый классификатор на основе стеков, состоящий из трех базовых классификаторов и мета-классификатора. SVM используется в качестве мета-классификатора, так что SVM HYBRID может использовать модель обнаружения для получения важных

запросов. Для оценки используется десятидневный набор данных запросов, собранный из журналов веб-сервера веб-сайта университета. Поскольку в журналах регистрируются запросы, проходящие через коммерческий WAF, вредоносные запросы, полученные данной системой, могут использоваться для обновления библиотеки сигнатур WAF.

Основные части проведенного исследования заключаются в следующем:

1. Представлена AMODS, адаптивная система для обнаружения вредоносных запросов в веб-атаках. Насколько известно, это первая работа по адаптивному обнаружению веб-атак.

2. Предложена SVM HYBRID, адаптивная стратегия обучения, разработанная для эффективного выбора важных запросов.

3. Ознакомление со стекированием, основанным на метаобучении [3] ансамблевого классификатора, в качестве базовой модели обнаружения для точного обнаружения вредоносных запросов.

4. AMODS превосходит существующие методы обнаружения веб-атак с F-значением 94,79% и частотой FP 0,09% в реальном наборе запросов за десять дней. Общее количество вредоносных запросов, полученных SVM HYBRID, в 2,78 раза больше, чем SVM AL во время обнаружения в режиме реального времени с использованием AMODS.

Список литературы

1. Symantec, Internet security threat report 2016. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-21–2016-en.pdf

2. Imperva, Analyzing the Team GhostShell Attacks. URL: https://www.imperva.com/blog/analyzing-the-team-ghostshell-attacks/

3. Обнаружение веб-атак с помощью Seq2Seq автоэнкодера [Электронный ресурс]. – Режим доступа: https://habr.com/ru/company/pt/blog/439202/

4. Низамутдинов М. Тактика защиты и нападения на Web-приложения / М. Низамутдинов. – М.: БХВ-Петербург, 2015. – 109 с.