АРХИТЕКТУРА СИСТЕМЫ ОБНАРУЖЕНИЯ АТАК ДЛЯ ОБНАРУЖЕНИЯ БОТНЕТОВ

ARCHITECTURE OF THE ATTACK DETECTION SYSTEM FOR DETECTING BOTNETS



УДК 004.056.57

Растамханов Рамиль Наилевич, магистр 2 курс, факультет «Информатики и робототехники», Уфимский государственный авиационный технический университет, Россия, г. Уфа

Rastamkhanov Ramil Nailovich, prm-t@mail.ru

Аннотация

Одной из главных угроз безопасности в IoT являются ботнеты. В сети IoT необходимо применять современные тактики безопасности такие как интеллектуальный анализ сетевого трафика, чтобы обеспечить защитить субъекты в составе IoT. Такая острая проблема нуждается в своевременном устранении. Сетевые атаки со стороны ботнетов довольно серьезный вопрос, к решению которого нужно подходить комплексно. В статье предложена архитектура гибридной системы обнаружения атак, построенной на основе сигнатурного и интеллектуального анализа для обнаружения вредоносного трафика ботнетов. Описываются основные компоненты гибридной системы обнаружения атак, этапы основные этапы построения интеллектуального классификатора.

Annotation

Botnets are one of the main security threats in the IoT. In the IoT network, modern security tactics such as intelligent analysis of network traffic must be applied

to ensure that the actors in the IoT are protected. Such an acute problem requires timely elimination. Network attacks from botnets are quite a serious issue that needs to be addressed in an integrated manner. The article proposes the architecture of a hybrid intrusion detection system based on signature and mining analysis to detect malicious botnet traffic. The main components of a hybrid intrusion detection system, the stages of the main stages of building an intelligent classifier are described.

Ключевые слова: этап аудита, этап обучения, этап обнаружения, Netflow, интеллектуальный анализ, СОА, сигнатурный детектор.

Keywords: audit stage, learning stage, detection stage, Netflow intelligent analysis, ADS, signature detector.

Для анализа особенностей функционирования системы обнаружения атак (далее – СОА) и степени ее влияния на защищаемый объект необходимо составить ее формализованное описание в виде функциональной модели. На Рисунке 1 представлена функциональная модель системы обнаружения атак. Система включает в себя следующие компоненты:

– Сенсоры – осуществляют сбор и первичную обработку сетевого траффика согласно протоколу Netflow;

– Блок извлечения признаков сетевого траффика – служит для извлечения значимых признаков из набора данных и уменьшения размерности данных для дальнейшего обучения классификатора.

– База профилей сетевого траффика – выполняет роль хранилища различного размеченного на нормальный и вредоносный Netflow траффика;

– Журнал предупреждений – хранит предупреждения при обнаружении атаки;

– Интеллектуальная подсистема обнаружения аномалий – выполняет роль интеллектуального анализа сетевого траффика для обнаружения аномалий в сети;

– Хранилище моделей – хранит различные модели машинного обучения для интеллектуального анализа Netflow телеметрии;

– Блок подготовки новой сигнатуры – генерирует подпись сигнатуры обнаруженной атаки для последующего внесения в базу знаний;

– База Знаний – хранит сигнатуры известных атак;

– Сигнатурный детектор – осуществляет сигнатурный анализ захваченной телеметрии сопоставляя их с сигнатурами из базы знаний;

– Станция управления – служит для конфигурирования СОА и реагирования на угрозу;

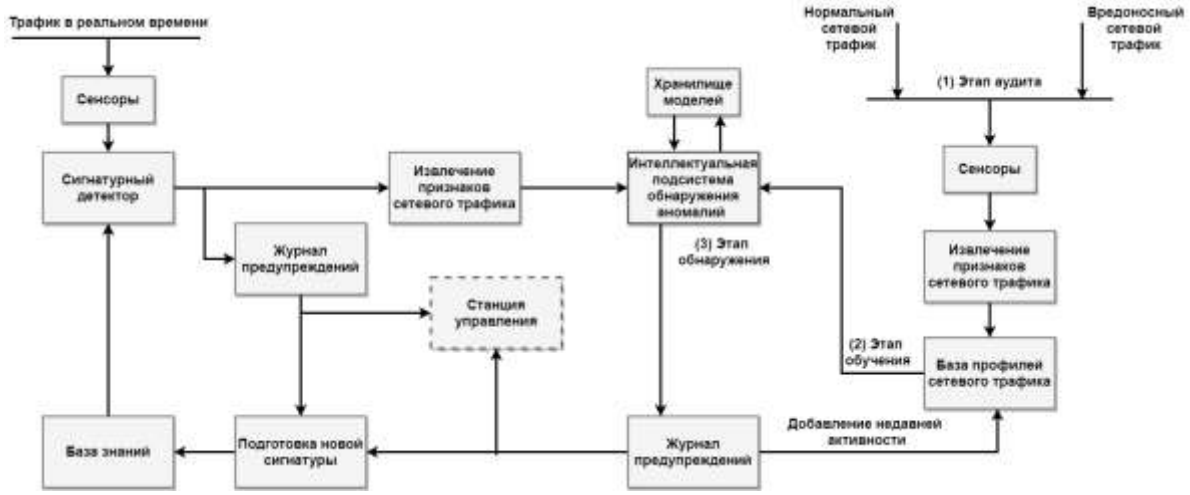


Рисунок 1 – Предлагаемая архитектура СОА

Как показано на Рисунке 1, в данной работе используются сигнатурный детектор и интеллектуальную подсистему обнаружения аномалий, построенную с использованием различных методов машинного обучения и искусственных нейронных сетей. Сигнатурный детектор используется для обнаружения известных атак, тогда как интеллектуальную подсистему обнаружения аномалий предсказывает, является ли данное событие вредоносным, путем наблюдения за ранее сохраненными сетевыми событиями. Обнаружение аномалии состоит из трех этапов, а именно:

– этап аудита;

– этап обучения;

– этап обнаружения;

Этап аудита: на этапе аудита генерируются и сохраняются профили нормального и вредоносного сетевого трафика. Это можно реализовать, получая реальный сетевой трафик данных от предприятия и извлекая NetFlow. Сначала захватывается нормальный трафик и генерируются профили сетевого трафика из телеметрии Netflow и им присваивается метка класса как Normal. Чтобы генерировать вредоносный трафик, выполняются различные атаки и снова захватывается трафик, генерируются профили сетевого трафика и присваивается ярлы класса Intrusion.

В отсутствие реального трафика данных другой вариант – использовать общедоступный набор данных. Для этой цели хорошо подойдут следующие наборы данных:

– CTU-13;

– KDDCUP993;

– CIC COB-20174.

После чего идёт изучение набора данных статистически, чтобы определить общие черты и признаки. Это необработанные атрибуты данных Netflow. Эта группа признаков характеризует трафик:

– StartTime;

– Duration;

– Proto;

– SrcAddr;

– Sport;

– Dir;

– DstAddr;

– Dport;

– State;

– sTos;

– dTos;

– TotPkts;

– TotBytes;

– SrcBytes;

– Label.

После того, как был выбран набор данных начинается извлечение значимых для обнаружения признаков. Данных шаг очень важен, так как данные Netflow содержать категориальные признаки, которые должны быть закодированы в числовые или логические значения, что приведёт к увеличению размера матрицы и проблем с память. Чтобы сократить объем данных для обработки, используется разделения данных по временным окнам. После выбора временного окна идёт извлечение категориальных и числовых признаков описывающие набор данных в заданном временном окне. После чего сохраняем обработанные данные в базу профилей сетевого трафика. Как только получен достаточный объем профилей сетевого трафика, можно переходить к следующему этапу.

Этап обучения: на этом этапе идёт построение модели интеллектуальную подсистему обнаружения аномалий на основе базы профиля сетевого трафика. Но перед тем, как подавать профили на вход классификатора, необходимо выполнить уменьшение размерности входной обучающей матрицы. Для этой цели служат различные методы такие как функции фильтрации с помощью корреляции Пирсона, встроенные методы в классификаторе случайного леса, анализ главных компонент и др. Далее идёт обучение классификатора с использованием различных методов машинного обучения.

Этап обнаружения: после построения классифицирующей модели на этапе обучения, СОА переводится в режим полнофункциональной работы и на входы сенсоров подается реальный сетевой трафик. На этапе обнаружения фиксируется трафик, генерируются профили сетевого трафика и передаются эти профили в качестве входных данных в интеллектуальную подсистему обнаружения аномалий. Интеллектуальная подсистема обнаружения аномалий генерирует предупреждение, если обнаруживает корреляцию входного профиля с вредоносными профилями. При этом по мере функционирования происходит дообучение СОА при анализе подозрительной сетевой активности.

Входящий сетевой трафик проходит через сигнатурный детектор. Здесь все известные атаки идентифицируются путем сопоставления сигнатур. Остальные неизвестные атаки обнаруживаются интеллектуальной подсистемой обнаружения аномалий. При обнаружении неизвестной атаки в журнал вносится запись о предупреждении. Если частота атаки, обнаруженной интеллектуальной подсистемой обнаружения аномалий, превышает пороговое значение частоты Tf, система переходит к генерации сигнатуры на основе интеллектуального анализа для этих соединений. Это увеличивает производительность СОА, поскольку интеллектуальная подсистема обнаружения аномалий способна обнаруживать эти частые атаки за короткое время. После создания подписи обновляется база знаний.

Подготовка новой сигнатуры – это независимый процесс, выполняющийся параллельно. Для частых атак генерируются сигнатуры на основе сигнатурного детектора. Для этого берется поток полезной нагрузки всех случаев атаки, находится самая длинная общая подпоследовательность и представляется в виде регулярного выражения.

После подготовки новой сигнатуры она проверяется при нормальном подключении. Если совпадений не найдено, сигнатура принимается. Если она генерирует большее количество ложных срабатываний, она отбрасывается.

Литература

1. Лукацкий А.В. Обнаружение атак. — М.: БХВ-Петербург, 2003. — 608 с.
2. Barford P., Plonka D. Characteristics of Network Traffic Flow Anomalies. Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. 2001. pp. 69–73.
3. Kim S.S., Reddy A.L. Statistical techniques for detecting traffic anomalies through packet header data. IEEE/ACM TON. 2008. vol. 16. Issue 3. pp. 562–575.
4. Babaie T., Chawla S., Ardon S. Network Traffic Decomposition for Anomaly Detection. Available at: http://arxiv.org/pdf/1403.0157.pdf, 2014 (accessed: 08.03.2016).

5. Крылов В.В., Самохвалова С.С. Теория телетрафика и её приложения — М. : БХВ-Петербург, 2005. — 288 с.
6. Mazurek M., Dymora P. Network anomaly detection based on the statistical self-similarity factor for HTTP protocol. Przeglad elektrotechniczny. 2014. pp. 127–130.
7. Lee K., Kim J., Kwon K.H., Han Y., Kim S. DDoS attack detection method using cluster analysis. Expert Systems with Applications. 2008. vol. 34. Issue 3. pp. 1659–1665.
8. Jyothsna V., Prasad V.V.R. A Review of Anomaly Based Intrusion Detection Systems. International Journal of Computer Applications. 2011. vol. 28, no. 7. pp. 26–35.

Literature

1. Lukatsky A.V. Obnaruzhenie atak [Attack Detection]. SPb.: BHV-Petersburg. 2003. 608 p. (In Russ.).
2. Barford P., Plonka D. Characteristics of Network Traffic Flow Anomalies. Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. 2001. pp. 69–73.
3. Kim S.S., Reddy A.L. Statistical techniques for detecting traffic anomalies through packet header data. IEEE/ACM TON. 2008. vol. 16. Issue 3. pp. 562–575.
4. Babaie T., Chawla S., Ardon S. Network Traffic Decomposition for Anomaly Detection. Available at: http://arxiv.org/pdf/1403.0157.pdf, 2014 (accessed: 08.03.2016).
5. Krylov V.V., Samokhvalova V.V. Teoriya teletrafika i ee prilozheniya [Teletraffic Theory and Its Applications]. SPb.: BHV-Petersburg. 2005. 288 p. (In Russ.).
6. Mazurek M., Dymora P. Network anomaly detection based on the statistical self-similarity factor for HTTPprotocol. Przeglad elektrotechniczny. 2014. pp. 127–130.

7. Lee K., Kim J., Kwon K.H., Han Y., Kim S. DDoS attack detection method using cluster analysis. Expert Systems with Applications. 2008. vol. 34. Issue 3. pp. 1659–1665.
8. Jyothsna V., Prasad V.V.R. A Review of Anomaly Based Intrusion Detection Systems. International Journal of Computer Applications. 2011. vol. 28, no. 7. pp. 26–35.