DOI 10.37882/2223-2966.2023.8-2.25

АТРИБУТИВНЫЕ МЕТОДЫ ВЫЯВЛЕНИЯ СЛОЖНЫХ АТАК ПО ДАННЫМ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

ATTRIBUTIVE METHODS FOR DETECTING COMPLEX ATTACKS FROM INTRUSION DETECTION SYSTEM DATA

A. Pavlov

Summary. This article proposes two methods for detecting complex attacks based on data obtained from intrusion detection systems. The first method is based on a combination of rules and allows to identify complex attacks and combine events into meta-events to reduce the sample size. The second method allows to identify complex attacks from meta-events using the DBSCAN clustering method based on the weighted Gower distance. Method metrics are evaluated for the CPTC-2018 dataset. The resulting assessment indicates the practical applicability of the proposed methods in the task of detecting complex attacks and countering advanced threats.

Keywords: information security, cybersecurity, complex attacks, attacker groups, intrusion detection.

Павлов Артем Валерьевич
Аспирант, Университет ИТМО
artempavlov1@gmail.com

Аннотация. В статье предлагаются два метода выявления сложных атак, основанные на данных, полученных из систем обнаружения вторжений. Первый метод основан на комбинировании правил и позволяет проводить выявление сложных атак и объединение событий в метасобытия для уменьшения размерности выборки. Второй метод позволяет выявлять сложные атаки из метасобытий через кластеризацию методом DBSCAN на основании взвешенного расстояния Говера. Приводится оценка метрик методов для набора данных CPTC-2018. Полученная оценка свидетельствует о практической применимости предложенных методов в задаче выявления сложных атак, противодействии продвинутым угрозам.

Ключевые слова: информационная безопасность, кибербезопасность, сложные атаки, группы атакующих, обнаружение вторжений.

На сегодняшний день информационная инфраструктура многих организаций имеет сложное устройство, состоит из различных физических или логических сегментов. Это приводит к тому, что атакующие для достижения целей атаки вынуждены совершать множество действий, перемещаясь между узлами сети [1]. Множество атак, совершаемых атакующим на организацию в рамках одной кампании, называется сложной атакой. Одной из ключевых особенностей сложной атаки является то, что ее нельзя описать менее чем двумя атомарными событиями [2].

Выявление сложных атак является актуальной задачей при противодействии современным угрозам безопасности. Большой поток событий безопасности, получаемых из различных источников, приводит к возникновению у аналитиков явления усталости от тревог, когда аналитик после продолжительной работы начинает пропускать реальные события атак или медленнее применять меры реагирования. Отчасти это вызвано отсутствием связи между событиями, что заставляет рассматривать каждое из них в отдельности. Восстановление хода сложных атак, включая ситуации, когда действия проводят несколько различных атакующих, позволяет показать связи между событиями безопасности, снизить влияние усталости от тревог и принять меры реагирования, более точно соответствующие действиям атакующих. Источником событий для выявления сложных атак могут быть системы обнаружения вторжений.

В данной работе предлагаются два метода выявления сложных атак, полученные в результате анализа набора данных CPTC-2018 [3]. Этот набор был собран в рамках соревнований по тестированию на проникновение и содержит сложные атаки на инфраструктуру, проводимые 7 различными группами атакующих. Рассматриваемые данные получены из системы обнаружения вторжений Surricata. Методы основаны на атрибутивном подходе, к особенностям которого можно отнести отсутствие необходимости сбора сведений об атакуемой системе [4]. Также предлагается метод объединения событий в метасобытия для ускорения анализа.

Задачу выявления сложных атак возможно решать с использованием методов кластеризации. В таком случае в качестве метрик оценки эффективности предлагаемых методов подходят полнота, однородность и V-мера полученной кластеризации [5]. Для их вычисления требуется знание оригинальных меток кластеров.

Однородность (гомогенность) h определяет то, насколько элементы в кластерах похожи. Она вычисляется следующим образом:

$$h = 1 - \frac{H(C|K)}{H(C)},$$

где $H(C|K) = -\sum_{c,k} \frac{n_{ck}}{N} \log\left(\frac{n_{ck}}{n_k}\right)$

$$H(C) = -\sum_c \frac{m_c}{N} \log\left(\frac{m_c}{N}\right),$$

C — эталонная кластеризация, K — полученная кластеризация, $H(C)$ — энтропия, $H(C|K)$ — условная энтропия, N — общее количество объектов в выборке, n_k — количество объектов в кластере k, m_c — количество объектов с меткой c, а n_{ck} — количество объектов с меткой c в кластере k.

Полнота c определяется по следующей формуле:

$$c = 1 - \frac{H(K|C)}{H(K)},$$

C — эталонная кластеризация, K — полученная кластеризация, $H(K)$ — энтропия, $H(K|C)$ — условная энтропия.

Однородность и полнота принимают значение от 0 до 1, где 1 — лучший результат. Для оценки сбалансированности этих параметров используется гармоническая V-мера V, которая определяется следующим образом:

$$V = 2\frac{h \cdot c}{h + c}.$$

Метод выявления сложных атак и объединения событий на основании атрибутов и правил

В рамках метода рассматриваются свойства адреса источника атаки (src_ip), адреса цели атаки (dest_ip) и временной метки (timestamp). Свойства рассматриваемой пары событий имеют нижние индексы 1 и 2.

Определим правила кластеризации. Если группа событий безопасности объединяется в кластер в соответствии с правилом, то такой кластер относится к одной сложной атаке. Для комбинирования правил выдвигается требование к сохранению однородности не ниже 0,98. Исходя из этого значения выбираются значения временных окон.

Правило 1: Если $src\_ip_1 = src\_ip_2$ и адрес не относится к диапазону частных адресов, то события относятся к одной сложной атаке. Правило основано на том, что случаи использования одной и той же инфраструктуры различными атакующими в рамках атаки на одну цель на сегодняшний день неизвестны или крайне редки.

Таблица 1.

Результаты кластеризации с использованием правила 1

Метрика	Значение
Однородность	1
Полнота	0,59
V-мера	0,74
Количество кластеров	45

Метрики оценки правила приведены в Таблице 1. События с адресом источника, относящемся к частным адресам, в расчете метрик не использовались.

Правило 2: если $dest\_ip_1 = dest\_ip_2$, а $|timestamp_1 - timestamp_2| < 3$ сек, то события относятся к одной сложной атаке. Метрики для Правила 1 + Правила 2 представлены в Таблице 2.

Таблица 2.

Результаты кластеризации с использованием правил 1 и 2

Метрика	Значение
Однородность	0,998
Полнота	0,565
V-мера	0,721
Количество кластеров	404

Правило 3: если $dest\_ip_1 = src\_ip_2$, а $|timestamp_1 - timestamp_2| < 5$ сек, то события относятся к одной сложной атаке. Правило показывает задействованные в дальнейших атаках захваченные ресурсы.

Метрики для Правила 1 + Правила 2 + Правила 3 приведены в Таблице 3.

Таблица 3.

Результаты кластеризации с использованием правил 1, 2 и 3

Метрика	Значение
Однородность	0,997
Полнота	0,58
V-мера	0,733
Количество кластеров	344

На основании полученной кластеризации возможно провести объединение событий безопасности в метасобытия. Необходимость проведения подобной операции обуславливается тем, что многие методы, использующиеся при кластеризации, включая вычисление матрицы расстояний, имеют вычислительную сложность, квадратично зависящую от числа элементов в выборке. Таким образом, объединение событий без потери существенных свойств позволяет существенно снизить требуемые для вычисления ресурсы.

Определим метод объединения. Если у группы событий безопасности совпадают следующие атрибуты:

- метка кластера;
- src_ip;
- dest_port (порт цели атаки);
- dest_ip;
- src_ip;
- proto (протокол транспортного уровня);

— alert.signature (сработавшее правило);
— alert.category (категория сработавшего правила),

то такие события объединяются в метасобытие, содержащее все эти атрибуты, кроме метки кластера. На основании минимальной и максимальной временной метки событий в группе к метасобытию добавляются свойства start_time и end_time.

Применение предложенного метода объединения к кластеризации набора CPTC-2018 позволило уменьшить размер выборки в 10 раз без существенных потерь в возможности выявления сложных атак.

Метод выявления сложных атак из метасобытий на основании взвешенного расстояния

Метасобытия, полученные методом объединения, имеют смешанный тип данных. Для такого типа подходит лишь небольшое количество методов кластеризации. Содержащиеся в метасобытиях свойства имеют гетерогенную природу, поэтому их вклад при кластеризации может быть различным. Для определения весов использовалась комбинация методов K-прототипов и подход к поиску весов, описанный в [6]. В результате были получены веса свойств, представленные в Таблице 4:

Таблица 4.

Веса свойств метасобытия

Свойство	Вес
start_time	$3 \cdot 10^{-10}$
end_time	$3 \cdot 10^{-10}$
src_ip	0,617
dest_ip	0,26
dest_port	$1{,}47 \cdot 10^{-4}$
proto	$9{,}7 \cdot 10^{-12}$
alert.signature	0,073
alert.category	0,05

Далее на основании полученных весов была построена матрица расстояний. Для вычисления использовалось взвешенное расстояние Говера. К полученной матрице применялись различные методы кластеризации, их метрики представлены далее в Таблице 5:

Таблица 5.

Метрики различных методов кластеризации

Метод	Гиперпараметры	Однородность	Полнота	V-мера
HDBSCAN	*min_cluster_size=130, min_samples=1*	0,96	0,56	0,71
OPTICS	*min_samples=5, metric=minkowski*	0,85	0,29	0,43
DBSCAN	*eps=0,5, min_samples=1*	**0,991**	**0,573**	**0,727**

Для дальнейшего использования была выбрана кластеризация, полученная методом DBSCAN, как обладающая самыми высокими показателями однородности и V-меры кластеризации.

Поскольку предложенные методы имеют высокую однородность, возможно провести объединение кластеров, полученных двумя предложенными в статье методами. Такое объединение имеет следующие метрики: однородность — 0,99, полнота — 0,585, V-мера — 0,735, количество кластеров — 53.

В работе предложены два метода выявления сложных атак по данным систем обнаружения вторжений. Методы, как по отдельности, так и вместе, позволяют выявить сложные атаки с высокими показателями однородности и полноты, что говорит о высокой практической применимости методов. Причины объединения событий легко интерпретировать аналитикам при работе. Дальнейшие исследования могут быть направлены на поиск других методов выявления, основанных на других свойствах и подходах, а также на анализ и предсказание действий, атакующих на основании выявленных сложных атак.

ЛИТЕРАТУРА

1. Cuppens, F. Alert correlation in a cooperative intrusion detection framework / F. Cuppens, A. Miege // Proceedings of the 2002 IEEE Symposium on Security and Privacy (SP). — 2002. — P. 202–215.
2. Jaeger, D. Multi-step attack pattern detection on normalized event logs / D. Jaeger, M. Ussath, F. Cheng, C. Meinel // 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE. — 2015. — P. 390–398.
3. Munaiah, N. A Cybersecurity Dataset Derived from the National Collegiate Penetration Testing Competition / N. Munaiah [et al.] // Hawaii International Conference on System Sciences. — 2019.
4. Pavlov A., Voloshina N. Analysis of IDS Alert Correlation Techniques for Attacker Group Recognition in Distributed Systems // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) — 2020, Vol. 12525, pp. 32–42
5. Rosenberg, A. V-Measure: A conditional entropy-based external cluster evaluation measure / A. Rosenberg, J. Hirschberg // Proceedings of the 2007 Joint Conference on Empirical Methods in Natural Language Processing and Computational Natural Language Learning. — 2007. — P. 410–420.
6. Huang, J.Z. Automated variable weighting in k-means type clustering / J.Z. Huang [et al.] // IEEE Transactions on Pattern Analysis and Machine Intelligence. — 2005. — Vol. 27, No. 5. — P. 657–668.

© Павлов Артем Валерьевич (artempavlov1@gmail.com)
Журнал «Современная наука: актуальные проблемы теории и практики»