Анализ сетевых киберпреступлений

Р. Р. Фаткиева[1], А. С. Судаков[1], Д. О. Дедов[2]

[1]*Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина)*
[2]*Санкт-Петербургский государственный университет аэрокосмического приборостроения*

rikki2@yandex.ru, asudakov.mail@gmail.com, dedovdanil3@yandex.ru

Аннотация. **Сетевые киберпреступления представляют собой серьезную угрозу для информационной безопасности в современном цифровом мире. В статье приведен анализ особенностей сетевых киберпреступлений и предложен метод для их анализа. К отличительным особенностям метода можно отнести построение цифрового следа атаки с использованием ориентированного графа, а также цифрового профиля нарушителя. Для этого осуществляется фиксация состояния киберфизической системы в нормальном режиме и выявление момента обнаружения атаки, а также сбор и анализ данных из журналов событий для выделения событий, приводящих к атаке. Построение графа атаки позволяет идентифицировать типичные сценарии атак и характеристики злоумышленников. Предложенный метод позволяет повысить эффективность обнаружения и противодействия сетевым киберпреступлениям, сократить время реакции на инциденты и улучшить уровень безопасности информационных систем.**

Ключевые слова: сетевые киберпреступления, цифровой след атаки, цифровой профиль нарушителя, моделирование инцидента, журналы событий, граф атаки

I. Введение

В современном информационном обществе сетевые технологии играют ключевую роль во многих аспектах нашей повседневной жизни. Однако вместе с их ростом и распространением возрастает и уровень угроз со стороны киберпреступников, которые используют сети для совершения различных преступлений и атак на цифровые системы. В связи с этим, анализ сетевых киберпреступлений становится критически важным для обеспечения безопасности информации и защиты от киберугроз [1]. К отличительным особенностям расследования киберпреступлений можно отнести [2–9]:

- необходимость анализа больших объемов криминалистически значимой информации;
- отсутствие цифрового следа для ряда операций или транзакций;
- необходимость построения цифрового профиля злоумышленника для идентификации образов и закономерностей в сценариях его поведения;
- высокую латентность со стороны пострадавшего;
- необходимость использования цифровой форензики;
- глобализм в источнике атаки и возможность анонимизации в распределенных элементах, участвующих в атаке;
- быстрая эволюция сетевых атак и автоматизация их проведения.

Анализ основных тенденций, методологических подходов, которые исследователи используют для расследования киберпреступлений, представлен в [2]. В [3] показано, что нарушители используют анонимность, препятствуют установлению связей между цифровыми учетными записями и реальными удостоверениями личности. Для решения этой проблемы в [4] затронута задача обнаружения нарушений в облачной инфраструктуре. Предложена интеллектуальная система, формирующая с заданной периодичностью снимок состояний виртуальных машин, расположенных в облачном сервисе, с отправкой их на сервер Trusted Center Server (TCS) для хранения. В случае обнаружения нарушения производится извлечение снимка и его анализ для извлечения доказательств и реконструкции сценария преступления. Предлагаемая система реализована в качестве примера, где криминалистика выступает как услуги (FaaS) для выполнения процесса цифрового расследования за счет использования огромных возможностей облачных вычислительных ресурсов, таких как обработка, вычисления и хранение. Однако такой подход не предусматривает автоматического построения правил обнаружения вторжений, поэтому в работах [5, 6] предложено использовать онтологию цифровых нарушений, что облегчает обнаружение аномалий и автоматизирует обработку следов цифровых доказательств.

Работы [7, 8] посвящены разработке архитектур систем предупреждения на ранней стадии для расследования преступлений с помощью различных процессов сбора и обработки данных и применения инструментов извлечения знаний.

Исследования характеристик сетевых кибернарушений и методов их обнаружения представлены в [9, 10]. Для выявления нарушений в [9] предложено использовать нейронные сети, а в [10] метод растущих пирамидальных сетей. К преимуществам метода можно отнести сочетание статистических и сигнатурных методов обнаружения атак и возможность реконфигурации сетевой инфраструктуры при изменении структурной и функциональной динамики, обусловленной перераспределением соединений между вершинами сети. К недостаткам использование вычислительных ресурсов и длительность анализа.

Методы построения профилей нарушителя с использованием методов кластерных вычислений

рассмотрены в работах [11, 12]. В [11] анализируются 25 атрибутов для обнаружения киберпреступника с помощью различных методов, таких как гауссовская кластеризация, K-средние, нечеткие C-средние и нечеткая кластеризация. В [12] дан систематический обзор литературы по профилированию в качестве основы для разработки методов киберповеденческого анализа.

Обобщая работы [1–12] можно отметить, что разработка систем анализа киберпреступлений является актуальной. В рамках этого целесообразно осуществить интеграцию различных методов обнаружения и анализа киберпреступлений, а также осуществить разработку более эффективных методов построения профилей нарушителей. Сочетание различных подходов значительно улучшит процессы предотвращения и расследования киберпреступлений.

II. Модель сетевых киберпреступлений

Модель инцидента можно представить кортежем

$$M =< M_{\text{КС}}, M_N, M_{\text{A}} >, \quad (1)$$

где $M_{\text{КС}}$ – модель атакуемой киберфизической системы; M_N – модель нарушителя; M_{A} – модель атаки.

В этом случае для выявления инцидентов нарушения безопасности необходимо осуществить анализ точек вхождения в киберфизическую систему, выявить цифровой след сетевой атаки и на основании этого сформировать цифровой профиль злоумышленника или группы нарушителей. Рассмотрим каждый из этапов более подробно.

2.1 Построение модели киберфизической системы и сбор журналов событий.

Для формирования цифрового следа атаки на первом шаге необходимо зафиксировать состояние исследуемой киберфизической системы в нормальном режиме функционирования и временной момент выявления атаки. Это позволит зафиксировать интервал времени, на котором осуществлялась атака, за счет выявления отклонений от нормального режима работы.

$$T_A =< t_{start}, t_{stop} >, \quad (2)$$

где t_{start}. – время начало атаки; t_{stop} – время окончания атаки.

На втором шаге, на интервале времени (2) целесообразно осуществить сбор и анализ данных из журналов событий. Пусть E представляет собой множество всех событий, содержащих информацию о действиях, происходящих в киберфизической системе. Тогда каждое событие e_i можно представить в виде кортежа $e_i =< t_i, s_i, a_i >$, где t_i – временная метка события; s_i – источник события (например, сервер, рабочая станция); a_i – действие или событие (например, попытка доступа к диску, изменение файлов).

Задача анализа заключается в выделении событий, которые могут привести к атаке: $E_A = \{e_i \in E | t_i \geq t_{start}, (\widetilde{s_i}, \widetilde{a_i})\}$, где $\widetilde{s_i}$ – источник события, приводящий к атаке; $\widetilde{a_i}$-событие или действие, приводящее к атаке.

2.2 Построение цифрового следа атаки

Для построения цифрового следа атаки возможно использовать так называемые графы атак и/или сценарии атак. Тогда каждому уникальному событию нарушения $\widetilde{a_i}$ из множества E_A ставится в соответствие вершина v_i в графе атак G. Далее из множества найденных вершин необходимо зафиксировать все возможные совместные события. Для этого для каждой пары события (a_i, a_j), где a_i и a_j имеют определенную зависимость (например, временную $t_i < t_j$) выделяются вершины (v_i, v_j) которые соединяются ребрами. При этом если выявлено, что a_i и a_j имеют временную зависимость $t_i < t_j$, то целесообразно строить ориентированный граф, который лучше отражает последовательность нарушений безопасности. Для отражения этого также возможно использовать вес ребра между этими событиями, отражающий степень их временной зависимостей. Для этого обозначим вес ребра w_{ij} между событиями e_i и e_j.

В качестве альтернативного подхода допускается определить вес исходя из вероятности дуги и/или важности каждого события для процесса атаки.

Процедура является интеграционной и повторяется до тех пор, пока не будут рассмотрены все возможные совместные события. Таким образом, введение весов к ребрам графа позволяет учитывать временные связи между событиями и их важность для анализа структуры атаки и выявить зависимости между различными компонентами атаки.

2.3 Построение цифрового профиля нарушителя:

Получение множества вершин в графе атаки G позволяет для каждой вершины v_i сформировать полный набор характеристик, идентифицирующих знания и умения нарушителя(ей), для проведения атаки, который можно представить в виде множества:

$$\mathrm{C} = (\mathrm{c}_{i1}, \mathrm{c}_{2i}, \ldots, \mathrm{c}_{ij}, \ldots, \mathrm{c}_{in}), \quad (3)$$

где c_{ij} – характеристика знаний и умений нарушителя, например такая, как умение эксплуатировать тип использованной уязвимости, метода атаки, уровень привилегий и т. д.

На этом этапе также целесообразно рассмотреть информацию о возможных используемых инструментах злоумышленника. Это можно представить в виде множества:

$$Tl = (tl_{i1}, tl_{2i}, \ldots tl_{ij} \ \ldots, tl_{iz}), \quad (4)$$

где tl_{ij} – множество инструментов, используемых нарушителем в вершине графа.

Таким образом, введение информации об инструментах злоумышленника позволяет учитывать использованные средства при формировании цифрового профиля нарушителя.

Выделение из множества (3) отдельных поведенческих подмножеств позволяет сформировать набор шаблонов действий, идентифицирующих нарушителя, который определяет типичные последовательности действий или паттерны атаки:

$$X_N = (x_1, x_1, \dots, x_l, \dots, x_k), \quad (4)$$

где x_l – последовательность действий, применяемых нарушителем для реализации сетевой атаки.

Выделение множеств (3–5) позволяет определить цифровой профиль нарушителя M_N как набор характеристик C и поведенческих шаблонов X, представленных в виде:

$$M_N = (C, X, Tl). \quad (5)$$

Модель (5) позволяет описать характеристики и поведение потенциального злоумышленника на основе анализа графа атаки и других источников информации о кибератаках, а также сформировать характеристики для отнесения тех или иных особенностей поведения к определенному кластеру. С другой стороны, это позволит также соотнести профиль нарушителя с конкретным кластером атак или кластером применяемых инструментов, что позволит лучше понять его характеристики и методы действий.

Рассмотрим возможность построения сценария атаки на примере [10] атаки навязывания ложного маршрута за счет несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности, из-за проблемы идентификации сетевых управляющих устройств).

К основному элементу выявления можно отнести изменение исходной маршрутизации на объекте, при которой новый маршрут проходит через ложный объект. Атака осуществляется путем несанкционированного изменения маршрутно-адресных данных как внутри сети, так и во внешних сетях. К характеристикам изменений сетевых настроек можно отнести: изменение IP-адресов устройств, входящих в сеть; используемые в сети протоколы маршрутизации; изменения маски сети; метрики маршрута; используемые на хостах порты; IP-адреса маршрутизаторов; времени передачи данных.

В общем виде при обнаружении нарушения возможно обнаружить и зафиксировать t_{stop} – время окончания атаки. Исходя из этого сформируем конечное событие как $e_n = < \widetilde{t_n}, \widetilde{s_n}, \widetilde{a_n} >$, где $t_n = t_{stop}$, $\widetilde{s_n}$ – хост, $\widetilde{a_n}$ – задержка в передаче данных по сети. Предыдущим по отношению к событию e_n является событие e_{n-1}, которое характеризуется кортежем $e_{n-1} = < \widetilde{t_{n-1}}, \widetilde{s_{n-1}}, \widetilde{a_{n-1}} >$, где s_{n-1} – маршрутизатор сети, через который должен протекать маршрут в нормальном режиме функционирования сети; a_{n-1} – нарушение маршрута. Далее итерационно рассматривая весь путь прохождения пакета по логам работы маршрутизаторов можно зафиксировать все нарушения прохождения сетевого трафика, и построить граф атак. Конечной точной такого графа будет событие, характеризующее начало атаки с временной отметкой. Анализируя все собранные логи и соединяя последовательно все вершины событий, получим ориентированный граф, представленный на рис. 1, характеризующийся t_{start}. – временем начало атаки и событиями e_n – обнаружение в задержке по времени передачи данных; e_{n-1} – анализ пропускной способности сети; e_{n-2} – обнаружение нарушения маршрутизации пакета; e_{n-3} – обнаружение отсутствие/нарушения маршрута в таблице маршрутизации; e_{n-4} – изменение таблиц маршрутизации; e_{n-5} – фиксация формирования сообщения об изменении таблицы маршрутизации; e_{n-6} – установление связи с маршрутизатором хоста с несанкционированным IP.

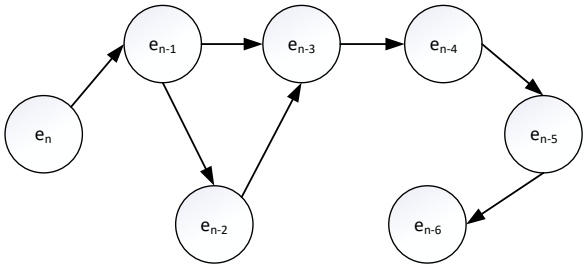

Рис. 1. Граф событий атаки навязывания ложного маршрутизатора

Выявление начального события позволяет зафиксировать время завершения атаки t_{stop} в вершине графа e_{n-6} и перейти к построению цифрового следа атаки. Для этого осуществим противоположное движение по полученному ранее ориентированному графу. Анализ события e_{n-6} позволяет предположить, что для возможности формирования связи с маршрутизатором злоумышленнику требуется как минимум выяснить IP адрес маршрутизатора, и установить с ним связь. В этом случае полученный на рисунке граф целесообразно дополнить вершинами (рис 2), где v_1 – установка программного обеспечения для осуществления атаки; v_2 – перехват трафика; v_3 – получение IP адресов сетевых устройств; v_4 – получение доступа к сетевому устройству (получение пароля маршрутизатора); v_5 – идентификация протоколов маршрутизации и сообщений об ошибках, используемых в сети; v_6 – изменение таблиц маршрутизации; v_7 – «замыкание трафика на себя»; v_8 – анализ трафика на устройстве нарушителя.

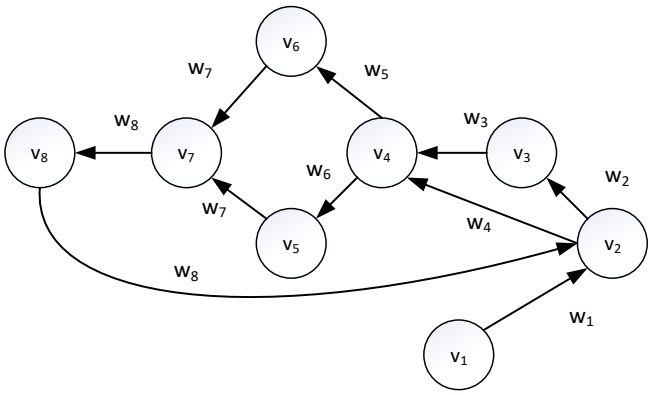

Рис. 2. Граф атаки навязывания ложного маршрутизатора

Оценка маршрутизации в графе (рис. 2) позволяет предположить цифровой след атаки в виде «множества путей передвижения на графе», в зависимости от аргумента ребра w_i и анализа событий зафиксированных в журналах логов и графе на рис 1. Например, в общем случае, анализируя граф атаки (рис. 2) возможно

выделить следующие варианты маршрутов исходя из ребер:

Вариант 1: w_1, w_2, w_3, w_5, w_7, w_8.

Вариант 2: w_1, w_4, w_5, w_7, w_8.

Вариант 3: w_1, w_2, w_3, w_6, w_7, w_8.

Тогда для каждого варианта можно выделить паттерны атаки, например для первого варианта: $X_N = (x_1(w_1), x_2(w_2), x_3(w_3), x_5(w_5), x_7(w_7), x_8(w_8))$.

Далее для каждого элемента из данного множества целесообразно выделить навыки и умения, которые требуются для данного паттерна атаки, что дает возможность получить множество (3). Выделение используемых инструментов позволяет перейти к формированию множества (4). Рассмотрения трех вариантов атаки, представленных ранее, дает возможность построить как минимум три варианта профиля нарушителя, для построения обобщенной базы профилей (5). Однако это не всегда позволяет идентифицировать личностные характеристики нарушителя. В этом случае целесообразно изучить отдельные личностные характеристики, сопоставляя события, происходящие в сети с реакцией нарушителя по логам, и построенным графам событий и атаки (рис. 1 и рис. 2). Например, выделение действий, не входящих в (4), но выявленных по логам событий дает возможность выделить индивидуальные характеристики нарушителя, а в некоторых случаях идентифицировать наличие группы нарушителей.

Таким образом, полученная модель позволяет эффективно анализировать сетевые атаки и строить цифровые профили нарушителей, а предложенный подход обеспечивает комплексный анализ киберпреступлений и создание подробных цифровых профилей нарушителей, что способствует повышению уровня безопасности информационных систем.

III. Заключение

Построение цифрового следа атаки и цифрового профиля нарушителя позволяет идентифицировать типичные сценарии атак, выявлять характеристики и поведенческие шаблоны злоумышленников, а также эффективно реагировать на киберпреступления. К дальнейшим направлениям исследования целесообразно отнести разработку более сложных моделей анализа и предотвращения сетевых киберпреступлений, а также проведение эмпирических исследований на реальных кибератаках для оценки эффективности предложенных подходов.

Список литературы

[1] W.A. Al-Khater, S. Al-Maadeed, A.A. Ahmed, A.S. Sadiq and M.K. Khan, "Comprehensive Review of Cybercrime Detection Techniques," in IEEE Access, vol. 8, pp. 137293-137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[2] Jack Hughes, Sergio Pastrana, Alice Hutchings, Sadia Afroz, Sagar Samtani, Weifeng Li, and Ericsson Santana Marin. 2024. The Art of Cybercrime Community Research. ACM Comput. Surv. 56, 6, Article 155 (June 2024), 26 pages. https://doi.org/10.1145/3639362.

[3] Chetry A., Sharma U. Anonymity in decentralized apps: Study of implications for cybercrime investigations. International Journal of Experimental Research and Review (2023), 32, 195-205. https://doi.org/10.52756/ijerr.2023.v32.017.

[4] Hemdan E.ED., Manjaiah D. An efficient digital forensic model for cybercrimes investigation in cloud computing. Multimed Tools Appl 80, 14255–14282 (2021). https://doi.org/10.1007/s11042-020-10358-x.

[5] Sikos L.F. Artificial intelligence in Digital forensics: Ontology engineering for cybercrime investigation. WIREs Forensic Sci. 2021; 3: e1394. https://doi.org/10.1002/wfs2.1394.

[6] Ayo F.E., Awotunde J.B., Ogundele L.A. et al. Ontology-Based Layered Rule-Based Network Intrusion Detection System for Cybercrimes Detection. Knowl Inf Syst (2024). https://doi.org/10.1007/s10115-024-02068-9.

[7] Fernandez-Basso C., Gutiérrez-Batista K., Gómez-Romero J., Ruiz M.D., Martin-Bautista M.J. An AI knowledge-based system for police assistance in crime investigation. Expert Systems, (2024). e13524. https://doi.org/10.1111/exsy.13524.

[8] Baror Stacey, Adeyemi Ikuesan, Venter Hein. Functional Architectural Design of a Digital Forensic Readiness Cybercrime Language as a Service. European Conference on Cyber Warfare and Security. (2023). 22. 73-82. 10.34190/eccws.22.1.1240.

[9] Shichkina Y.A., Fatkieva R.R, Puzako I.A. Information Threat Recognition Method Using a Neural Network. 2022 III International Conference on Neural Networks and Neurotechnologies (NeuroNT), Saint Petersburg, Russian Federation, 2022, pp. 42-46, doi: 10.1109/NeuroNT55429.2022.9805531.

[10] Y.A. Shichkina, R.R. Fatkieva, "Detection of network attacks using of growing pyramid networks," 2021 10th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, 2021, pp. 1-4, doi: 10.1109/MECO52532.2021.9460188.

[11] Meena K., Veena K. Performance evaluation of cybercriminal detection through cluster computing techniques. J Ambient Intell Human Comput (2019). https://doi.org/10.1007/s12652-019-01605-7

[12] Martineau, M., Spiridon, E., Aiken, M. A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. Forensic Sci. 2023, 3, 452-477. https://doi.org/10.3390/forensicsci3030032