Исхаков С.Ю., Мельников А.К., Исхаков А.Ю.

О применении техник проактивного поиска угроз в работе робототехнических комплексов

Аннотация: Рассмотрены техники проактивного поиска угроз для выявления таргетированных атак без использования вредоносного программного обеспечения. Проводится анализ возможности их интеграции в инфраструктуру робототехнических комплексов. Результаты проведенного эксперимента на киберполигоне РТК подтверждают эффективность обнаружения сложных целенаправленных атак, при этом отмечается важность применения не только множества источников индикаторов, но и необходимость комплексирования методов обогащения событий и тактик.

Ключевые слова: кибербезопасность, индикаторы компрометации, робототехнические комплексы, сервисные данные, модель атак

Введение

Одним из ярко выраженных трендов в решении задач информационной безопасности сегодня является развитие методов выявления угроз, в реализации которых не задействовано вредоносное программное обеспечение (ПО). Основной целью является выравнивание темпов конверсии проактивных техник обнаружения и инструментов автоматизации управления ИТ-инфраструктурой. При этом одной из сфер применения алгоритмов, позволяющих выявлять ранее неизвестные кибератак, являются высокоавтоматизированные отрасли промышленности, такие как робототехника и киберфизические системы.

Среди причин подобных тенденций можно выделить, в первую очередь, ограниченность использования классической антивирусной защиты на базе сигнатур и эвристического анализа (не позволяют выявить бесфайловые атаки и несанкционированное применение легитимного ПО). Кроме того, количество внедряемых на объектах средств защиты зачастую так велико, что генерируемые ими данные о возможных инцидентах сложно поддаются анализу.

В данной работе рассматриваются проактивные техники поиска угроз и проводится анализ возможности их применения в инфраструктуре робототехнических комплексов.

Состояние исследований

Общим фактором в современных техниках поиска угроз является формирование наборов индикаторов компрометации, которые позволяли бы выявить ранее неизвестную атаку на ранних стадиях. Поскольку эффективность таких обнаружений сводится к реальной возможности реагировать на угрозу, то необходимо ранжировать подобные индикаторы в соответствии с их значимостью. Проведенный обзор литературы выявил широкую вариативность методов, подходов и техник моделирования различных угроз [1]. В работе [2] поднимается проблема высокой сложности индикаторов компрометации для представленных моделей, формализующих базовый набор действий для детектирования злоумышленника. Но еще более сложной задачей является задача интерпретации индикаторов для различных гетерогенных инфраструктур, в том числе с применением робототехнических комплексов различного класса [3].

Аспекты проактивного анализа и его организации на объектах критической инфраструктуры, а также в системах реального времени рассмотрены в [4-5]. В исследованиях [6-8] отмечаются методологические аспекты внедрения Threat Intelligence для повышения уровня информационной безопасности, рассматриваются основные факторы влияния на данный процесс.

Очевидно, что подходы, ориентированные на комплексирование информации о злоумышленниках и ресурсах, могут быть использованы для моделирования как технических, так и нетехнических угроз. При этом одна из основных целей применения таких подходов – обеспечить возможность предоставления полезного базиса для оценки риска.

Постановка задачи

В качестве исследуемого объекта была выбрана действующая георасределенная ИТ-инфраструктура, в состав которой входит также несколько киберфизических систем – робототехнических комплексов. Авторами был проведен предварительный поиск

достоверных источников сведений об индикаторах кромпрометации, в результате чего было выделено 90 платформ. При этом 12 из них в результате детального анализа были исключены из перечня вследствие низкой частоты актуализации информации. Исследованные платформы применяют общепринятые форматы описания и структурирования данных (STIX/MISP, JSON, CSV, TXT и т.д.).

Для сокращения разрыва между успешными случаями проведения атак и возможностями их обнаружения необходимо не только опираться на различные типы индикаторов компрометации, но и использовать потенциальные источники обогащения данных. На исследуемом объекте был внедрен прототип системы класса SOAR, которая позволяет связать их вместе и определить критичность отдельного оповещения, придавая больше контекста путем объединения данных из различных источников. В таблице 1 представлена применяемая в ходе исследования классификация приоритетов инцидентов.

Таблица 1 – Примеры детектирования инцидентов

Тип оповещения (инцидента)	Вероятность реализации угрозы	Возможные действия
1	2	3
Фиксация нежелательного ПО (класс “not-a-virus”) средствами классических антивирусов без признаков ущерба для затронутых сегментов	Низкая	Запрос к вендорам АВЗ на корректировку логики обнаружения; Внесение исключений в правила детектирования; Автоматизированное восстановление объекта
Обнаружение вредоносного ПО (класс шифровальщиков, кейлоггеров и т.д.) с признаками ущерба для затронутых сегментов	Средняя	Анализ вредоноса (песочницы, поиск по источникам индикаторов компрометации, запрос вендору) Внесение исключений в правила детектирования

Продолжение таблицы 1

1	2	3
Выявление индикаторов, относящихся к классу техник и процедур различных APT-группировок, а также вредоносная активность, связанная с применением легитимного ПО	Высокий	Оперативно реагирование, принятие мер по локализации заражения; Организация расследования с применением техник форензики; Восстановление объектов вручную

При формировании таблицы 1 использовались следующие критерии классификации выявленных инцидентов:

– определение этапа атаки по модели Cyber Kill Chain, на котором была зафиксирована активность;

– результат обогащения индикаторов компрометации данными из смежных систем (периодичность и количество связанных событий, аномалии в поведенческом анализе сущностей);

– степень критичности сегмента и влияние угрозы на нарушение защищенности смежных участков инфраструктуры;

– возможность и сложность восстановления затронутых систем (требуемые показатели доступности информационных систем).

Эксперимент

В ходе исследования за 10 месяцев было зафиксировано 1259 оповещений, большая часть которых сгенерирована в результате анализа событий от узлов инфраструктуры РТК с применением техник проактивного поиска угроз на основе индикаторов типа TTP (фиксация техник, тактик и процедур). При этом окончательно подтвержденными инцидентами среди них было признано менее 3%.

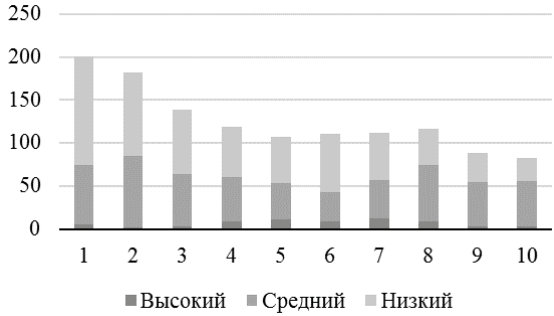

Рисунок 1 – Распределение инцидентов по вероятности реализации угрозы

С одной стороны, основная причина низкого уровня конверсии связана со сложностью задачи отличить легитимную активность в работе РТК от злонамеренной, что является вычислительно трудоемкой задачей и требует расчета точных распределений либо их точных приближений [9]. С другой стороны, несмотря на то, что большая часть инцидентов относится к низкой и средней вероятности реализации угрозы (рисунок 1), та малая доля реально подтвержденных инцидентов, обнаруженных проактивными методиками относилась в основном к высокому уровню реализации угрозы. Диаграмма на рисунке 2, в свою очередь, отражает значительное преимущество проактивных техник на основе индикаторов компрометации (*K1*) по общему количеству детектов (*K2* – эмуляция угроз, *K3* – ручное обнаружение, *K4* – анализ трафика).

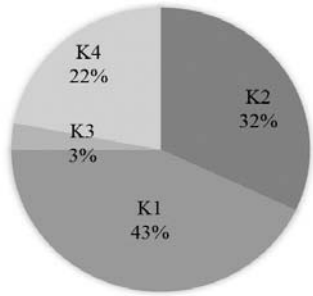

Рисунок 2 – Распределение инцидентов по методам обнаружения

Заключение

В ходе исследования была проведена оценка применения техник проактивного поиска угроз в работе робототехнических комплексов. Результаты эксперимента показали, что методы обнаружения сложных целенаправленных атак, а также ранее неизвестных векторов угроз являются высокоэффективными в данной отрасли промышленности, но требуют не только использования множества источников индикаторов, но и методов обогащения событий и тактик проактивного поиска угроз.

Исследование выполнено при частичной финансовой поддержке гранта Президента Российской Федерации в рамках научного проекта №МК-2421.2020.9 (исследование проактивных алгоритмов), а также гранта РФФИ №19-01-00767 (апробация алгоритмов на робототехнических комплексах)

Литература:

1. *Tatam M., Shanmugam B., Azam S., Kannoorpatti K.* A review of threat modelling approaches for APT-style attacks // Heliyon. – 2021. – Vol. 7. Issue 1. – P. 1-19.

2. *Liao X., Yuan K., Wang Z., Li Z., Xing L., Beyah R.* Acing the IOC game: Toward automatic discovery and analysis of open-source cyber threat intelligence / Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. – 2016. – P. 755-766.

3. *Hughes J., Cybenko G.* Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity // Technology Innovation Management Review. – 2013. – Vol. 3(8). – P. 15-24.

4. *Bianco D.J.* The Pyramid of Pain // Enterprise Detection & Response. – 2013. – URL: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html (дата обращение 01.10.2021).

5. *Mokaddem S., Wagener G., Dulaunoy A., Iklody A.* Taxonomy driven indicator scoring in misp threat intelligence platforms // arXiv. – 2019. – Vol. 1902.03914. – P. 1-10.

6. *Belur J., Tompson L., Thornton A., Simon M.* Interrater Reliability in Systematic Review Methodology: Exploring Variation in Coder Decision-Making // Sociological Methods & Research. – 2018. – Vol. 50. Issue 2. – P. 837-865.

7. *Hoffmann R.* Markov Models of Cyber Kill Chains with Iterations / Proceedings in the 2019 International Conference on Military Communications and Information Systems (ICMCIS). – 2019. – P. 1-6.

8. *Дрянных Ю.Ю., Жуков В.Г.* О необходимости внедрения threat intelligence // Решетневские чтения. – 2017. – №21-2. – С. 398-399.

9. *Левин И.И., Дордопуло А.И., Писаренко И.В., Мельников А.К.* Управление расчетом точных приближений распределений вероятностей значений статистик на гибридных вычислительных системах / XIV Всероссийская мультиконференция по проблемам управления (МКПУ-2021): материалы XIV мультиконференции (27 сентября-2 октября 2021 Дивноморское, Геленджик) в 4 т. / Т. 2. – Управление в распределенных и сетевых системах (УРСС-2021). – Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2021. – С. 261-266.

Пискурева Т.А., Махов А.Н.

Цифровая трансформация и импортозамещение во взаимосвязи обеспечения безопасности ядерного объекта

Аннотация: Переход на импортонезависимые решения и цифровая трансформация идут в ногу с обеспечением безопасности на базе использования отечественных программных продуктов и технических средств.

В работе рассматривается взаимосвязь стратегии цифровой трансформации и импортозамещения с задачами по обеспечению безопасности ядерного объекта, обращается внимание на роль человеческого фактора при переходе на использование новых импортонезависимых решений, на важность формирования организационной культуры и культуры безопасности.

Ключевые слова: цифровизация, цифровая трансформация, импотрозамещение, цифровые продукты, системы защиты, ядерный объект, культура безопасности

Изменения, которые происходят в мировом порядке, глобальный кризис и пандемия сформировали новую повестку, следуя которой Россия вступила на путь глубокой цифровой трансформации государства.