Научная статья
Original article

Принципы и методы обнаружения вредоносных программ в киберфизических системах

Нафиков Р.Х.[1,2], Назаров Д.М.[2,*]
[1]*ООО «Уралкомлектэнергомаш», Екатеринбург, Россия*
[2]*ФГБОУ ВО «Уральский государственный экономический университет», Екатеринбург, Россия*
[*] *Автор-корреспондент: slup2005@mail.ru*

Аннотация: В статье рассматриваются основные подходы и технологии, используемые для обнаружения вредоносных программ в контексте киберфизических систем. Цель статьи заключается в анализе и синтезе существующих методов обнаружения вредоносных программ, а также выявлении их преимуществ и недостатков в контексте киберфизических систем. Статья представляет собой комплексное изучение темы, начиная с определения киберфизических систем и особенностей угроз, связанных с вредоносными программами, и заканчивая кратким обзором существующих методов обнаружения таких угроз. Основное внимание уделяется принципам и методам обнаружения вредоносных программ, таким как сигнатурное обнаружение, эвристический и метаэвристический подходы, а также механизмы обнаружения, основанные на машинном обучении и анализе поведения. В результате анализа и обзора методов обнаружения вредоносных программ авторы систематизирую материал в области обнаружения вредоносных программ в киберфизических системах.

Ключевые слова: киберфизическая система, вредоносное программное обеспечение, эвристические, метаэвристические методы.

Для цитирования: Нафиков Р.Х., Назаров Д.М., Принципы и методы обнаружения вредоносных программ в киберфизических системах. Умная цифровая экономика. 2023. Т.3, №2, с. 97-102

Principles and methods for detecting malware in cyber-physical systems

Nafikov R.Kh.[1,2], Nazarov D.M.[2,*]
[1]*OOO Uralkomlektenergomash, Yekaterinburg, Russia*
[2]*Ural State University of Economics, Yekaterinburg, Russia*
** Corresponding author: slup2005@mail.ru*

Abstract: The article discusses the main approaches and technologies used to detect malware in the context of cyber-physical systems. The purpose of the article is to analyze and synthesize existing malware detection methods, as well as to identify their advantages and disadvantages in the context of cyber-physical systems. The article is a comprehensive study of the topic, starting with the definition of cyber-physical systems and features of threats associated with malware, and ending with a brief overview of existing methods for detecting such threats. The focus is on the principles and methods of malware detection, such as signature detection, heuristic and metaheuristic approaches, as well as detection mechanisms based on machine learning and behavior analysis. As a result of the analysis

and review of malware detection methods, the authors systematize the material in the field of malware detection in cyber-physical systems.

Keywords: cyber-physical system, malicious software, heuristic, metaheuristic methods.

For citation: Nafikov R.Kh., Nazarov D.M., Principles and methods for detecting malware in cyber-physical systems. Smart digital economy. 2023. Vol. 3, №2, pp. 97-102

В киберфизических системах (CPS) вредоносные программы могут представлять серьезную угрозу для безопасности и надежности работы таких систем. Это связано с тем, что киберфизические системы представляют собой интеграцию физических процессов с информационными системами, что может привести к нежелательным последствиям при атаке на них. Сложность и разнообразие киберфизических систем создает дополнительные проблемы для обнаружения и устранения вредоносных программ.

Актуальность вопроса о изучении различных аспектов вредоносного программного обеспечения (ПО) в контексте обеспечения безопасности киберфизических систем неоспорима, поскольку угрозы в Интернете и киберпространстве постоянно растут и усложняются.

Главная цель данного исследования заключается в анализе и синтезе существующих методов обнаружения вредоносных программ, а также выявлении их преимуществ и недостатков в контексте киберфизических систем для обеспечения их безопасности и надежной работы.

Вредоносное ПО представляет собой опасность для компьютерных систем и Интернета в целом. Это программное обеспечение создается с целью проникновения в компьютерные системы, нарушения их работы или кражи конфиденциальных данных без согласия владельца системы [5].

Существует множество различных видов вредоносных программ, включая вирусы, черви, ботнеты, троянские кони, эксплойты, шпионское ПО, рекламное ПО, руткиты и многое другое [5, 6, 7, 2]. Каждый из этих типов вредоносных программ имеет свои уникальные характеристики и точки входа, которые используются для заражения системы (см. таблицу 1).

Таблица 1 - Характеристики вредоносного программного обеспечения

Вид вредоносного ПО	**Характеристики**	**Точки входа**
Вирусы	Распространяются посредством программ или файлов	Загрузка инфицированных файлов, передача через почту или чаты
Черви	Подключаются к сети без согласия пользователя	Загрузка инфицированных файлов, использование пораженных сайтов
Ботнеты	Устанавливаются на компьютер без согласия пользователя	Загрузка инфицированных файлов, посещение пораженных сайтов
Троянские кони	Удаленный контроль над компьютером	Загрузка инфицированных файлов, посещение пораженных сайтов

Эксплойты	Используют уязвимости в программном обеспечении	Посещение пораженных сайтов, открытие инфицированных файлов
Шпионское ПО	Следит за действиями пользователя и сбор личных данных	Загрузка инфицированных файлов, посещение пораженных сайтов
Рекламное ПО	Показывает нежелательную рекламу и перенаправляет на нежелательные сайты	Загрузка инфицированных файлов, посещение пораженных сайтов
Руткиты	Получают полный доступ к компьютеру	Загрузка инфицированных файлов, посещение пораженных сайтов, уязвимости в программном обеспечении
Мистификации	Представляются как нечто другое, чтобы получить доступ к компьютеру	Загрузка инфицированных файлов, посещение пораженных сайтов, поддельные оповещения о безопасности, поддельные уведомления в электронной почте или чате
Кейлоггеры	Следят за вводом клавиатуры	Загрузка инфицированных файлов, посещение пораженных сайтов

Вредоносное ПО различных групп обладает уникальными способами маскировки, которые затрудняют его обнаружение. Современные инструменты для выявления вредоносных программ используют несколько механизмов обнаружения, чтобы обеспечить возможность своевременного деактивации вредоносного программного обеспечения. Каждый из этих механизмов обнаружения направлен на использование различных характеристик в соответствии с типом зловредных программ (см. табл. 1).

Заметим, что вирусы как наиболее массовый вид вредоносного ПО могут быть классифицированы как резидентные или нерезидентные[7].

Нерезидентные вирусы рнеализуют простые атаки, которые можно легко идентифицировать на точке входа с использованием инструментов обнаружения, таких как скалыватель (англ. "heuristic scanner") [5]. Такие атаки обычно менее сложны и легко обнаруживаются.

В отличие от них, резидентные атаки на память являются более сложными и эффективными, так как они способны проникать в систему и оставаться в памяти, маскируя свое присутствие от антивирусных и других средств обнаружения. Такие атаки обладают высокой скоростью распространения, что делает их особенно опасными, поскольку их целью является поражение максимально возможного числа файлов как на локальном уровне внутри зараженного хоста, так и удаленно через сетевые хосты и общие сетевые ресурсы. Вторая категория резидентных атак включает медленные вирусы, которые являются одним из наиболее опасных типов вредоносных программ [5]. Их основная характеристика – применение методов скрытности и шифрования для длительного незамеченного пребывания в системе. Медленные вирусы могут быть особенно коварными, так как они могут разрабатываться с целью избежать обнаружения антивирусными программами, путем маскировки своих действий или модификации своих сигнатур.

Эти мощные атаки могут быть составными, включая комбинацию нескольких процессов, работающих совместно для достижения определенных целей. Например, медленные вирусы могут использовать полиморфное или метаморфное шифрование, постоянно изменяя свой код, чтобы затруднить его обнаружение. Кроме того, они могут использовать различные уровни защиты, такие как криптование, обфускация и руткиты, для обеспечения дополнительной защиты от обнаружения.

Из-за своей сложности и способности длительное время оставаться незамеченными, медленные вирусы могут нанести серьезный ущерб инфраструктуре и данным, а также могут быть использованы для кражи конфиденциальной информации или для проведения других злонамеренных действий. Чтобы снизить риск заражения медленными вирусами, необходимо применять комплексные стратегии безопасности, включая регулярное обновление антивирусного программного обеспечения, использование многоуровневых защитных мер и обучение пользователей основам кибергигиены.

Системы обнаружения вредоносных программ применяют различные методы, основанные на сигнатурах, для идентификации известных атак. С течением времени, обнаружение сигнатур стало весьма результативным подходом для определения известных угроз [5, 6, 7]. Распознавание конкретной сигнатуры в коде позволяет точно определить угрозы, ассоциированные с этим кодом. Атакующие сигнатуры регулярно обновляются и сохраняются в базе данных для обеспечения защиты от вредоносного ПО. Тем не менее, данный метод становится неэффективным, когда сигнатура атаки искажена с помощью специальных механизмов «мутаций» кода или программистом.

Эвристические подходы представляют собой один из самых действенных методов обнаружения мутировавших вирусов и вирусных атак. Эвристические и метаэвристические методы применяются для выявления неизвестных или известных атак с так называемыми полиморфными характеристиками [1, 3, 4]. В своей сути, эвристический метод представляет собой неформальный подход к решению проблем защиты от вирусных атак, приближенный к оптимальному решению. Эвристические методы обычно применяются для быстрого достижения решения, которое в любом случае является приближенным к наиболее оптимальному. Метаэвристический метод включает эвристический подход к решению множества вычислительных задач, путем совмещения определенных пользователем процедур "черного ящика" с целью достижения эффективного решения.

Большинство современных методов обнаружения вредоносных программ, которые используют метаэвристику для выявления атак, включают в себя набор изолированных инструментов. Эти инструменты применяют разнообразные методы в попытке обнаружить атаки, для которых нет специфического метода обнаружения. В основном, эти инструменты применяют один из следующих механизмов: сравнение с образцами, автоматическое обучение, эмуляция среды, нейронные сети, интеллектуальный анализ данных, байесовские сети и скрытые марковские модели. Хотя существуют и другие метаэвристические методы, большая часть из них основана на одном или нескольких упомянутых выше механизмах (см. табл. 2).

Таблица 2 - Классификация механизмов обнаружения вредоносных программ

Категория	Методы обнаружения
Сигнатурные методы	- Сопоставление с образцом (Pattern Matching)
	- Обнаружение на основе хэшей (Hash-based Detection)
	- Статическое анализирование кода (Static Code Analysis)
Эвристические методы	- Эмуляция среды (Environment Emulation)
	- Нейронные сети (Neural Networks)
	- Интеллектуальный анализ данных (Data Mining)
	- Байесовские сети (Bayesian Networks)
	- Скрытые марковские модели (Hidden Markov Models)
Метаэвристические методы	- Генетические алгоритмы (Genetic Algorithms)
	- Муравьиные алгоритмы (Ant Colony Algorithms)
	- Частицы роя (Particle Swarm Optimization)
	- Иммунные алгоритмы (Immunological Algorithms)
Системы экспертных знаний	- Базы знаний (Knowledge Bases)
	- Экспертные системы (Expert Systems)
	- Логика нечетких множеств (Fuzzy Logic)
Машинное обучение	- Обучение с учителем (Supervised Learning)
	- Обучение без учителя (Unsupervised Learning)
	- Обучение с подкреплением (Reinforcement Learning)

Таким образом, современные системы обнаружения вредоносных программ стремятся комбинировать различные методы и инструменты для повышения вероятности успешного обнаружения атак, особенно тех, которые могут изменять свои сигнатуры или поведение. Использование метаэвристических подходов в совокупности с традиционными методами обнаружения на основе сигнатур позволяет обеспечить более надежную защиту от многообразных и постоянно эволюционирующих угроз вредоносного ПО. Это особенно актуально в современном мире, где киберпреступники постоянно разрабатывают новые и более изощренные атаки, чтобы обойти существующие системы безопасности и проникнуть в защищенные сети.

В заключение, был проведен анализ и синтез различных методов обнаружения вредоносных программ, исследованы их преимущества и недостатки в контексте киберфизических систем. В результате проведенного анализа авторы сделали вывод о важности разработки новых и усовершенствование существующих методов обнаружения вредоносных программ для обеспечения безопасности киберфизических систем. Понимание принципов и методов обнаружения вредоносных программ имеет большое значение для специалистов в области кибербезопасности и разработчиков киберфизических систем, а также для тех, кто отвечает за обеспечение безопасности критически важных инфраструктур организаций.

Список литературы

1. Андреев, С. А. Методы защиты пользователей в сети Интернет: темные паттерны / С. А. Андреев, Д. М. Назаров // BI-технологии и корпоративные информационные системы в оптимизации бизнес-процессов цифровой экономики : Материалы X Международной научно-практической очно-заочной конференции, Екатеринбург, 02 декабря 2022 года / Ответственные за выпуск: А.Ю. Коковихин, Д.М. Назаров, ответственный редактор: С.В. Бегичев. – Екатеринбург: Уральский государственный экономический университет, 2023. – С. 3-6. – EDN PRNDDC.
2. Комашинский Д. В. Подход к обнаружению вредоносного программного обеспечения на основе позиционно-зависимой информации / Д. В. Комашинский, И. В. Котенко, А. В. Шоров // Труды СПИИРАН. – 2009. – № 10. – С. 131-147. – EDN NBMCBP.
3. Смирнов Д. В. Исследование особенностей поведения вредоносного программного обеспечения класса крипторов-вымогателей / Д. В. Смирнов, И. А. Лубкин // Решетневские чтения. – 2016. – № 2. – С. 271–273.
4. Умницын М. Ю. Отслеживание состояния информационной системы на основе анализа данных о событиях / М. Ю. Умницын, С. В. Михальченко // Прикаспийский журнал: управление и высокие технологии. – 2017. – № 4. – С.165–173 (http://hi-tech.asu.edu.ru/files/4(40)/165-173.pdf).
5. Цветков В. Я. Эвристический анализ как инструмент информационной безопасности / В. Я. Цветков, С. В. Булгаков // Современные наукоемкие технологии. – 2010. – № 1. – С. 53.
6. Chen, X, Andersen, J. Mao, Z. M. Bailey, M. and Nazario, J. Towards an understanding of anti- virtualization and anti-debugging behavior in modern malware, in International Conference on Dependable Systems and Networks, 2008.
7. Podgórski, W. Artificial intelligence methods in virus detection and recognition—Introduction to heuristic scanning, 2012. Available at http://podgorski.wordpress.com.
8. Sze S. and Tiong, W. A comparison between heuristic and metaheuristic methods for solving the multiple traveling salesman problem," World Academy of Science, Engineering and Technology, 2007.