УДК 004.056+681.5 https://doi.org/10.26160/2542-0127-2026-18-42-45

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ АТАК, НАПРАВЛЕННЫХ НА РОБОТОВ

Талтанов А.М.

Автономная некоммерческая организация высшего образования «Московский университет «Синергия», Москва

Ключевые слова: информационная безопасность, компьютерные атаки, угрозы информационной безопасности, уязвимости, технологические роботы, классификация компьютерных атак, нарушители информационной безопасности.

Аннотация. Компьютерные атаки на роботов становятся все более популярными. Для эффективного управления защищенностью промышленных роботов автор проводит аналитику популярных компьютерных атак и описывает их классификацию. Результаты работы призваны сформулировать подход к классификации атак и помочь в описании угроз информационной безопасности промышленных роботов.

CLASSIFICATION OF COMPUTER ATTACKS TARGETED AT ROBOTS

Taltanov A.M.

Autonomous Non-Profit Organization of Higher Education "Moscow University 'Synergy'", Moscow

Keywords: information security, computer attacks, information security threats, vulnerabilities, technological robots, classification of computer attacks, information security violators.

Abstract. Computer attacks on robots are becoming increasingly popular. To effectively manage the security of industrial robots, the author analyzes popular computer attacks and describes their classification. The results of this work are intended to formulate an approach to classifying attacks and to help describe information security threats to industrial robots.

Контекст использования промышленных роботов в реальной эксплуатационной среде зачастую сводится к общим условиям окружения и принципов функционирования, которые подразумевают расположение роботов в отдельном логическом сегменте сети, отсутствие обновлений программного обеспечения и контроля за имеющимися уязвимостями.

Когда архитектура и проблематика известны нарушителю, то остается только подобрать подходящий вектор атаки.

Атаки на технологических роботов можно произвести по каждому уровню модели OSI, однако при атаках чаще используют простые и действенные сценарии [1].

Реальные факты компьютерных атак как раз и показывают определенные тенденции по нарушению функционирования промышленных роботов.

Так в 2025 г. произошла атака по включению роботов Unitree в состав ботнет сети. Атака произошла путем эксплуатации уязвимости, позволяющей выполнить произвольный код от имени суперпользователя. Исследователи смогли получить первоначальный доступ через стандартные протоколы для настройки робота путем анализа кода и отправки авторизационного пакета с содержанием флага для успешного прохождения процесса авторизации [2].

Данная атака показала на сколько несовершенна логика работы программного кода в роботах и насколько мощным оружием может стать распределенная армия зараженных устройств, которая может находиться на технологических предприятиях и обеспечивать критические процессы. При реализации атаки по данному вектору можно добится одновременной остановки производственных автоматизированных процессов на всех предприятиях, где используются уязвимые роботы.

Еще один пример атаки на роботов в 2025 г. публично освещен на хакерском конкурсе в Шанхае. Исследователи, используя интерфейс голосового управления роботом, обошли механизмы защиты ИИ-Агента используя технику Prompt Injection и смогли выполнять произвольные команды.

Данному вектору атаки подвержены в том числе все коллаборативные роботы, имеющие интерфейс голосового управления. При реализации аналогичного вектора атаки можно причинить ни только ущерб жизни и здоровью оператора, но и осуществлять дистанционные террористические атаки на промышленные предприятия [1].

Помимо использования интерфейсов управления как главного источника атаки, сейчас появляются и иные тренды по использованию датчиков роботов в корыстных целях. Пример такого использования был продемонстрирован на научной конференции в 2024 г. Исследователи продемонстрировали атаку по получению несанкционированного доступа к видеокамере домашнего робота пылесоса Ecovacs Deebot X2 (Omni). Реализация данной атаки также возможна благодаря слабым механизмам защиты авторизации при подключении к устройству, что позволяет получить несанкционированный доступ к любому устройству этой модели.

Аналогичный вектор атаки может быть применен и на территории промышленных предприятий. Главным объектом воздействия станут промышленные роботы, оснащенные видеокамерой и встроенными алгоритмами искусственного интеллекта для распознавания объектов. В таком случае данные объекты смогут осуществлять промышленный шпионаж, что может стать серьезной проблемой для высокотехнологичных предприятий военного сектора.

Сейчас в открытом доступе за последние годы был зарегистрирован ряд уязвимостей, относящихся к промышленным роботам: Universal Robots PolyScope 5, Robot Operating System 2 (ROS2), Rockwell Automation FactoryTalk, ABB RobotWare 6 / 7 и иным [3].

Все данные уязвимости можно разделить на следующие типы:

– удаленное выполнение кода;

– выполнение произвольного кода;

– обход аутентификации;

– отказ в обслуживании (DoS).

Учитывая, что тенденции на атаки формируются на стороне хакеров, а только позже появляются в открытом опубликовании, можно сделать вывод, что в данный момент времени аналогичные трендовые уязвимости эксплуатируются нарушителями на промышленных предприятиях по всему миру.

Что касается классификации видов атак на промышленные роботы можно разделить их по ряду параметров.

1. По территориальному признаку:

Атаки в пределах контролируемой зоны.

Атаки такого типа подразумевают наличие определенного доступа к информационным или физическим ресурсам организации, позволяя повышать свои привилегии, осуществлять горизонтальное движение по сетевой инфраструктуре.

Атаки за пределами контролируемой зоны.

Данные атаки подразумевают преодоление физической защиты или получение первоначального доступа к ресурсам компании.

2. По вектору проникновения:

Сетевые атаки.

Данный вид атаки подразумевает за собой работу с пакетами данных, с протоколами обмена информации в сети и сбором информации о конечных узлах.

Атаки через физические интерфейсы.

Данный вид атаки возможен исключительно при проведении атаки в пределах контролируемой зоны, для ее реализации требуется возможность физического взаимодействия.

Атаки через пользовательские интерфейсы.

Данный вид атаки характеризуется выполнением вредоносной активности с использованием интерфейса, с которым взаимодействует работник компании, за частую через графическую оболочку.

Атаки через цепочку поставок.

Данный вид атак характеризуется получением доступа по легитимным каналам, путем компрометации отправителя или поставщика.

3. По категории нарушителя:

Внутренний нарушитель.

Данный вид атак исходит от работника или лица, имеющего авторизованный доступ к информационным и/или техническим средствам.

Внешний нарушитель.

Данный вид атак исходит от внешнего лица по отношению к информационным и физическим активам организации, зачастую это подразумевает отсутствие доступа до компонентов систем.

4. По техническим возможностям нарушителя:

Нарушитель с базовым потенциалом.

Атаки от данной категории нарушителя подразумевают использование общедоступных уязвимостей и эксплойтов при помощи известных утилит и инструментов.

Продвинутый нарушитель.

Атаки от данной категории нарушителя подразумевают более скрытное ведение атаки, более гибкое использование известных утилит и инструментов.

Хакер.

Атаки от данной категории нарушителя подразумевают целенаправленные атаки с поиском и эксплуатированием уязвимостей, в том числе реализация многоуровневых атак с использованием продвинутых и/или самописных утилит и инструментов.

Приступная группировка.

Атаки от данной категории нарушителя подразумевают координированные атаки с поиском и эксплуатированием уязвимостей, в том числе реализация многоуровневых атак с использованием продвинутых и/или самописных утилит и инструментов, а также подразумевают использование инсайдерской информации или информации из даркнет.

Прогосударственная структура.

Атаки от данной категории нарушителя подразумевают координированные атаки с эксплуатированием уязвимостей 0-дня, в том числе реализация многоуровневых атак с использованием секретных решений, а также подразумевают использование высоких мощностей и реализацию сложных APT-атак.

Благодаря классификации атак можно производить моделирование угроз информационной безопасности для промышленных роботов, чтобы лучше понимать контекст состояния защищенности, векторов атаки на промышленных роботов и основные объекты защиты. Простроенная модель атак поможет Компаниям, использующим в том числе промышленных роботов в построении системы защиты и в принятии организационных мер для минимизации риска наступления негативных последствий от компьютерных атак.

Список литературы

1. Xingmao Shao, Lun Xie, Chiqin Li, Zhiliang Wang. A Study on Networked Industrial Robots in Smart Manufacturing: Vulnerabilities, Data Integrity Attacks and Countermeasures // Journal of Intelligent & Robotic Systems. 2023, vol. 109, no. 3, p. 60. doi.org/10.1007/s10846-023-01984-2.
2. Víctor Mayoral-Vilches, Andreas Makris, Kevin Finisterre. Cybersecurity AI: Humanoid Robots as Attack Vectors [Электронный ресурс]. – Режим доступа: https://ar5iv.labs.arxiv.org/html/2509.14139.
3. CISA. Tycon Systems TPDIN-Monitor-WEB2 (Update A) [Электронный ресурс]. – Режим доступа: https://www.cisa.gov/news-events/ics-advisories/icsa-26-202-01.

Сведения об авторе:
Талтанов Антон Михайлович – аспирант.