УДК 004.056

АНАЛИЗ ЭФФЕКТИВНОСТИ HONEYPOT-СИСТЕМЫ T-POT ДЛЯ ИЗУЧЕНИЯ ВЕКТОРА АТАК НА УСТРОЙСТВА IOT И IIOT

Баринова Я.В. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Менщиков А.А. (Университет ИТМО)

Введение. Сегодня, в результате стремительного развития технологии Интернет-вещей и её внедрения во все сферы жизни, возрастает и количество устройств промышленного контроля, которые выставлены в Интернете зачастую без должного обеспечения безопасности, что делает их открытыми и уязвимыми для атак с потенциально катастрофическими последствиями.

Основная часть. Одним из способов прогнозирования и предотвращения атак на устройства промышленной инфраструктуры может выступать технология ловушек (honeypot). Главная цель технологии – привлечение внимания злоумышленников к контролируемой системе, для дальнейшего исследования их методов атаки, обнаружения уязвимостей и разработки более эффективных мер защиты. Использование honeypot имеет несколько преимуществ:

1. Раннее обнаружение уязвимостей: технология может обнаружить уязвимости, которые могут быть использованы злоумышленниками до того, как они будут использованы в реальной атаке на реальную систему.
2. Увеличение безопасности: технология может помочь улучшить безопасность системы, путем обнаружения слабых мест и уязвимостей, а также предоставления дополнительного времени для реагирования на атаку.
3. Сбор данных: использование honeypot может предоставить множество ценных данных, которые могут быть использованы для анализа методов атаки и улучшения мер безопасности.

В ходе экспериментальных исследований, на облачном сервере была развернута honeypot-система с открытым исходным кодом T-Pot в исследовательских целях. T-Pot – это honeypot-платформа, которая включает несколько известных ловушек (а также вспомогательных инструментов) и объединяет их вместе с помощью docker. Для анализа трафика в T-Pot, все поступающие атаки перенаправляются в контейнер, который наилучшим образом реагирует на инциденты и обрабатывает их.

Выводы. В работе рассмотрена актуальность и ключевые возможности существующей open-source honeypot системы – T-Pot, проведена установка и запуск системы на облачном сервисе. В результате развертывания системы в течение 7 дней были зафиксированы данные свыше чем о 300.000 инцидентах. Полученные данные помогают понять основные методы атак злоумышленников, а полученный анализ атак впоследствии может быть применим для обеспечения безопасности устройств Интернет-вещей.

Список использованных источников:

1. Javier F., Ahmet A., Berk C., A. Uluagac «A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems» (PDF) // arXiv – CS – Cryptography and Security (IF), DOI: arxiv-2108.02287
2. T-Pot Version 22.04 released // [Digital resource]. https://github.security.telekom.com/2022/04/honeypot-tpot-22.04-released.html#t-pot-installer, free.

Баринова Я.В. (автор)

Менщиков А.А. (научный руководитель)