УДК 004.492
А. Бельма, О. Кареліна
(Тернопільський національний технічний університет імені Івана Пулюя)

ВИЯВЛЕННЯ ЗАГРОЗ ДЛЯ IOT-ПРИСТРОЇВ ЗАСОБАМИ HONEYPOTS

UDC 004.492
A. Belma, O. Karelina
(Ternopil Ivan Puluj National Technical University, Ukraine)

DETECTION OF THREATS TO IOT DEVICES USING HONEYPOTS

В останні роки поява Інтернету речей (IoT) викликала велику стурбованість з приводу безпеки мережевих вбудованих пристроїв. Кількість пристроїв IoT зростає в геометричній прогресії, і, згідно з оцінками, протягом 2020 року кількість підключених пристроїв перевищить 40 мільярдів, а загальний потенційний економічний ефект складе від 3,9 трильйонів до 11,1 трильйонів доларів на рік. Інтернет речей був названий наступною промисловою революцією, і він вплине на те, як всі підприємства, уряд і споживачі будуть взаємодіяти з фізичним світом. Однак, якщо, з одного боку, у нас є ідея світу, в якому всі пристрої мають цифрове з'єднання, що дозволяє нам робити те, про що ми ніколи раніше не уявляли, існує інша, зворотна сторона: через відсутність необхідних заходів безпеки, Інтернет речей стає все більш привабливою ціллю для кіберзлочинців. Зростаюча кількість підключених пристроїв прямо пропорційна кількості векторів атак і можливостям для хакерів націлюватися на користувачів і компанії. Якщо ця проблема безпеки не буде чим швидше вирішена – виникне складне питання. Тому існує досить гостра необхідність в розробці відповідних і економічно ефективних методах пошуку вразливостей в пристроях IoT для їх усунення до того, як зловмисники ними скористаються.

Honeypot - це інструмент з ізольованою і розділеною мережею, який імітує реальну мережу, привабливу для зловмисників. Цю мережу можна розглядати як фальшиву систему, яка виглядає як справжня, щоб привернути зловмисників і бути атакованою, і таким чином контролювати взаємодію між ними і зараженим пристроєм. В традиційній IT-безпеці honeypot зазвичай використовуються для розуміння динамічного ландшафту загроз без розкриття важливих ресурсів. Тому головною метою дослідження є адаптація honeypot для підвищення безпеки IoT і пояснення того, чому honeypot є найкращим і найефективнішим методом в питаннях безпеки IoT-пристроїв. Можливість реалізації honeypot на IoT розглядається по декількох причинах: популярність IoT платформи, наявність цільових зловмисників та привабливість IoT-пристроїв через низький рівень безпеки.

Через неоднорідність пристроїв IoT створення приманки з низьким рівнем взаємодії вручну є недоступним. З іншого боку, купівля всіх фізичних пристроїв IoT для створення honeypot з високим рівнем взаємодії також неможлива. Ця дилема змусила шукати інноваційний спосіб створення honeypot для пристроїв IoT – використання технології машинного навчання для автоматичного вивчення поведінкових знань про пристрої IoT і створення honeypot з «інтелектуальною взаємодією». Також для поліпшення якості результатів дослідження використовується кілька методів машинного навчання.

Література

1. URL: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world