Detection of Zero-Day Attacks on IoT

Shay Reardon ; Murtadha D. Hssayeni ; Imadeldin Mahgoub All Authors

Abstract:
Zero-day attacks are cybersecurity attacks that seek to exploit an unknown vulnerability in Internet of Things (IoT). This makes zero-day attacks inherently difficult to ... **View more**

Metadata

Abstract:
Zero-day attacks are cybersecurity attacks that seek to exploit an unknown vulnerability in Internet of Things (IoT). This makes zero-day attacks inherently difficult to detect and costly to network administrators. Current methods of detection utilize machine learning methodologies for intrusion detection. However, these methods suffer from low performance in specific zero-day attacks. This study proposes novel features built upon network flow and raw packet data aiming to detect zero-day attacks. Our testing approach utilizes fix traditional machine learning algorithms (Decision Tree (DT), Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Logistic Regression (LR), Gaussian Naive Bayes (NB), and Random Forest (RF)) with split-at-scenario cross-validation. We find that our engineered features achieve consistent high detection rates with three models (DT, SVM, and RF), whereas these models fail to detect at least one of the attacks when using raw features. Our results display potential for utilizing the proposed flow-based complex features to detect unknown network attacks with Internet of Battle Things (IoBT) applications.

Published in: 2024 International Conference on Smart Applications, Communications and Networking (SmartNets)

Date of Conference: 28-30 May 2024

DOI: 10.1109/SmartNets61466.2024.10577735

Date Added to IEEE *Xplore*: 05 July 2024

Publisher: IEEE

ISBN Information:

Conference Location: Harrisonburg, VA, USA

ISSN Information:

Contents

Zero-day attacks are cybersecurity attacks that seek to exploit a vulnerability that is unknown to network administrators. This vulnerability is known as a zero-day vulnerability. While the vulnerability remains unknown, the developers cannot patch it, and anti-virus software cannot detect attacks exploiting it. But, by the time developers find the vulnerability or attack, the damage to the company or consumer has already been done. Zero-day cost an average of 1.2 million USD per attack [1], [2] and can last an average of 312 days [3]. It is estimated that every 17 days one of these attacks is discovered [4]. Also, there is a 15 % increase in these attacks. To monitor for these costly attacks, Intrusion Detection Systems (IDS) are required to detect zero-day attacks and vulnerabilities.