4ZC-08

IoT マルウェアの長期的な動的活動観測システムの検討

一色千晴　　寺田真敏
東京電機大学

1. はじめに

2016 年マルウェア“Mirai”に感染した IoT 機器が大規模な DDoS 攻撃に利用されて以降[1]，攻撃者が攻撃の踏み台として悪用する事例は後を絶たない．本研究は，IoT 機器のマルウェア感染において，IoT マルウェアの解析だけではなく，攻撃者の活動にも着目し対策を進めていくことを目的としている．本稿では，IoT マルウェアを解析する様々な方法が検討されている一方で，攻撃者の活動に着目した長期観測の取り組みは少ないことから，IoT マルウェアを対象とした観測の取り組みや解析手法を調査し，攻撃者の活動に着目した長期観測における要件を整理した．また，整理した結果を元に攻撃者の活動に着目した長期活動観測システムについて検討した結果を報告する．

2. 関連研究

関連研究では，IoT マルウェアを対象とした解析や観測手法を 3 つの視点から整理した．

2.1 IoT マルウェアに関する研究動向

(1) IoT マルウェア解析・観測の効率化

IoT 機器は機能や機種が多種多様で，IoT マルウェアに特化した解析環境や検知技術を用いた解析・観測をする必要がある．このため，効率化は重要な課題であり，IoT マルウェア向けの汎用的なサンドボックスの開発[2][3]，機械学習を用いた IoT マルウェアの検知・分類の研究[4][5]，IoT マルウェアを収集するハニーポットの研究[6]が行われている．

(2)特定の機器に依存するマルウェアの解析

IoT マルウェアの中には機器特有の機能や構成でなければ意図した挙動をしないものが存在し，機器依存性を考慮した解析・観測が必要となる．このため，特定の機器や機能に依存するマルウェアに対しては実機を用いた手法[7]，機器再起動後も永続的に感染を続けるマルウェアには，マルウェアの動作から IoT 機器の構成を推定しマルウェアの実行環境に仮想環境を適応させる手法[8]が提案されている．また，解析環境を検知するマルウェアに対しては Linux サンドボックスにおける要件の調査[9]や，企業が公開しているファームウェアから IoT 機器の環境を推定し仮想環境で IoT 機器を再現する試み[10]が報告されている．

(3)マルウェアの動作や起因する通信に着目した研究

マルウェアの動作や起因する通信に着目した研究については，マルウェアに感染した IoT 機器の観測と分析に分かれる．観測については，短期間の動的解析ではほとんどの IoT マルウェアは DoS 攻撃命令を受信しない性質があること[11]や IoT 機器での生存競争について報告されている[12]．また，分析については，ダークネット上で観測した通信を元にマルウェアに感染した IoT 機器の実態調査[13]が報告されている．長期的な取り組みについては，長期動的解析によるマルウェアの特徴的な通信の抽出[14]やマルウェアの挙動だけでなく攻撃者の活動に着目した動的活動観測[15]が報告されているが，対象が Windows マルウェアに留まっている状況にある．

2.2 解決したい課題

関連研究に示す通り，IoT マルウェアの解析ならびに観測に関して様々な研究がある一方で，攻撃者の活動に着目した長期観測の取り組みは少ない．本研究では，攻撃者の活動にも着目した長期的な動的活動観測をもとに対策を進めていくことを目的とした．

3. 動的活動観測システム概要

本章では IoT マルウェアの長期的な動的活動観測システムの構成と機能について述べる．

3.1 動的活動観測システムの概要

動的活動観測システムは，IoT マルウェアに対して通常の動的解析だけではなく，攻撃者の活動にも着目することによりセキュリティ対策を進めていくことを目的としている．システム実現にあたっては，関連研究の調査結果に基づき，次に示す機能要件を設定した．

(1)攻撃者視点からの要件

攻撃者視点では，攻撃対象となりえる IoT 機器が多数存在することが魅力となる．実機を用いた観測の場合，マルウェア 1 検体に実機一台を割り当てる必要があること，IoT 機器には MIPS や ARM など PC とは異なり IoT 機器特有のアーキテクチャが多数あることから，多種多様な実機の模擬が可能な仮想環境を用いること．

(2)観測者視点からの要件

長期観測においては，動的活動観測環境が踏み台となったサイバー攻撃を局所化する必要があることから，観測環境自身に考えうるサイバー攻撃の影響を低減する機能を実装すること．

Feasibility Study on a Long-term Behavior Observable System for IoT Malware
CHIHARU ISSHIKI and MASATO TERADA, Tokyo Denki University.

3.2 動的活動観測システムの構成

システム構成を図 1 に示す．動的活動観測システムは，コンテナを用いたマルウェア観測機能(攻撃者視点からの要件)，動的活動観測環境が踏み台となったサイバー攻撃を局所化するアクセス制御機能(観測者視点からの要件)をコンポーネントして持つ仮想環境クラスタから構成する．なお，コンテナ型動的活動観測環境については，レインフォレスト社のマルチ CPU 対応動的解析システムをベースとして使用した[16].

(1)コンテナ型動的活動観測機能

図 2 では，システムの説明上，CPU を明示したコンテナ型動的活動観測機能を提示しているが，図 1 に示す動作で，IoT マルウェアが動作可能な CPU コンテナを選択する．また，IoT マルウェアの活動を長期観測するために，マルウェアのファイルやネットワークアクセスなどのログ記録機能を無効化し，発生した通信データをキャプチャするように特化した．

1. file コマンドでマルウェアの動作するアーキテクチャを特定
2. アーキテクチャに対応したコンテナ型動的活動観測環境を起動
3. IoT マルウェアをコンテナ型動的活動観測環境へ移動させ実行
4. 終了後はコンテナ型動的活動観測を削除

図 1　コンテナの選択手順

(2)アクセス制御機能

アクセス制御機能では長期観測において発生しうる動的活動観測環境が踏み台として悪用される次のケースに対処する．

- スパムメール配信 : 25/tcp を宛先ポート番号とする通信を遮断する．
- DoS 攻撃 : 一定時間で一定量以上の通信があった場合に通信を遮断する．

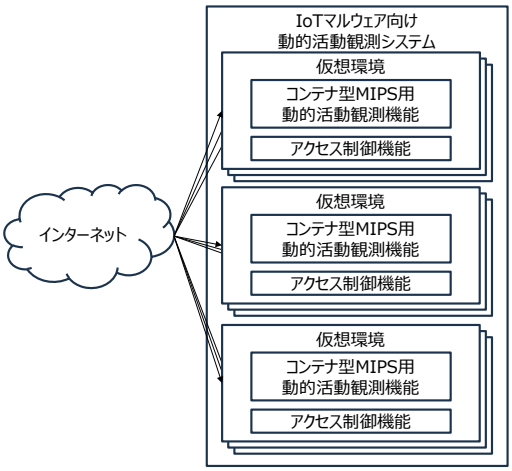

図 2　動的活動観測システムの概要

4. おわりに

本稿では IoT マルウェアを対象とした観測の取り組みや解析手法の調査結果から動的活動観測システムの要件を整理しそれらの要件を元に動的活動観測システムを検討した．

今後は検討したシステムを実環境で稼働できるよう整備を進めるとともに，IoT マルウェアを対象とした長期的な動的活動観測を通して，攻撃者の活動にも注目したセキュリティ対策を検討していく．

謝辞

IoT マルウェアの長期的な動的活動観測システムを検討ならびに構築するにあたりご協力を頂いた株式会社レインフォレストの岡田晃市郎氏，岡田英造氏に感謝します．

参考文献

[1] IPA，“ネットワークカメラや家庭用ルータ等の IoT 機器は利用前に必ずパスワードの変更を”, https://www.ipa.go.jp/security/anshin/attention/2016/mgdayori20161125.html, 2023 年 12 月 29 日参照.
[2]“LiSa”, https://github.com/danielpoliakov/lisa, 2023 年 12 月 29 日参照.
[3]“Limon”, https://github.com/monnappa22/Limon, 2023 年 12 月 29 日参照.
[4] Gaurav, Akshat, et al. “A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system”. Enterprise Information Systems. 2018, vol. 17, no. 3, 2023764.
[5] Su, Jiawei, et al. “Lightweight classification of IoT malware based on image recognition”. 2018 IEEE 42Nd annual computer software and applications conference (COMPSAC). 2018, vol. 2, pp. 664-669.
[6] Pa, Yin Minn Pa, et al. “IoTPOT: A novel honeypot for revealing current IoT threats”. Journal of Information Processing. 2016, vol. 24, no.3, pp. 522-533.
[7] 原悟史ほか. “IoT 機器の実機を用いたマルウェア動的解析手法の検証”. 電子情報通信学会論文 B. 2020, vol. J103-B, no. 8, pp. 272-283.
[8] 井上貴弘ほか. “適応的サンドボックスによる持続感染型 IoT マルウェアの解析”. 研究報告セキュリティ心理学とトラスト(SPT). 2021, vol. 2021-SPT-41, no. 21, pp. 1-6.
[9] Xie, Chenglin, et al. “Envfaker: A method to reinforce linux sandbox based on tracer, filter and emulator against environmental-sensitive malware”. 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). 2021, pp. 667-677.
[10] Chen, Daming D., et al. “Towards automated dynamic analysis for linux-based embedded firmware”. NDSS. 2016.
[11] 鉄穎ほか. “IoT マルウェアによる DDoS 攻撃の動的解析による観測と分析”. 情報処理学会論文誌. 2018, vol. 59, no. 5, pp. 1321-1333.
[12] 安井浩基ほか. “モノの中の戦い: IoT 機器への攻撃の長期観測による マルウェアの生存競争の調査”. コンピュータセキュリティシンポジウム 2023 論文集. vol. 2023, pp. 1325-1332.
[13] 笠間貴弘, 井上大介. “大規模ダークネット観測と能動的スキャンによるマルウェア感染 IoT 機器の分類”. 情報処理学会論文誌. 2017, pp. 1388-1398.
[14] 田辺瑠偉ほか. “長期動的解析によるマルウェアの特徴的な DNS 通信の抽出”. コンピュータセキュリティシンポジウム 2012 論文集, 2012, vol.2013, no. 3, pp. 712-719.
[15] 寺田真敏ほか. “研究用データセット「動的活動観測 2014」の検討”. コンピュータセキュリティシンポジウム 2014 論文集, 2014, vol. 2014, no. 3, pp. 1121-1125.
[16] PR TIMES, “マルチ CPU 対応動的解析システム”, https://prtimes.jp/main/html/rd/p/000000002.000089968.html, 2024 年 01 月 08 日参照.