ゼロデイ攻撃の対象となるIoT機器を早期特定するシステムの開発
― ファームウェアの大規模収集・解析による早期対策の実現 ―

1. 背景

近年、IoT(Internet of Things)機器の急速な普及に伴い、IoT機器に存在するセキュリティ上の欠陥である脆弱性を狙ったサイバー攻撃やマルウェア活動による被害が深刻化している。こうしたIoT機器を狙う攻撃の中には、脆弱性の修正プログラムや緩和策が製品ベンダーから公開される前に攻撃が行われるケースが存在する。このような攻撃のことをゼロデイ攻撃といい、有効な対策手段が存在しない無防備な状態の機器が狙われることになるため非常に大きな脅威となりうる。

こうしたサイバー攻撃の動向を把握し適切な対応へと役立てるため、ダークネット上に届く通信パケットの監視やハニーポットによる観測が行われている。観測した攻撃が公知の脆弱性を狙ったものである場合、インターネット上で公開されている脆弱性情報やエクスプロイトコードを調査することにより対象機器の特定を行うことが可能である。一方で観測した攻撃が未知の脆弱性を狙ったもの(ゼロデイ攻撃)である場合、前述の手法では観測した攻撃がどの機器を狙ったものであるかを特定することが困難であるという問題が存在する。

2. 目的

本プロジェクトでは、事前に大規模に収集したIoT機器のファームウェアに対して静的解析及び動的解析を実施し、ハニーポットなどのサイバー攻撃観測網で観測されたゼロデイ攻撃と照合することにより、攻撃の標的となっている機器を速やかに特定するシステムを開発し、脆弱性の早期修正並びにサイバー攻撃による被害の拡大抑止に貢献することを目指す。

3. 開発の内容

本プロジェクトでは、事前にIoT機器のファームウェアを大規模に収集・解析し、ゼロデイ攻撃の観測時にファームウェアの解析結果と攻撃情報を照合することにより、観測されたゼロデイ攻撃のターゲットとなっている機器を早期に特定するシステムを開発した。開発したソフトウェアのシステム構成を図 1に示す。

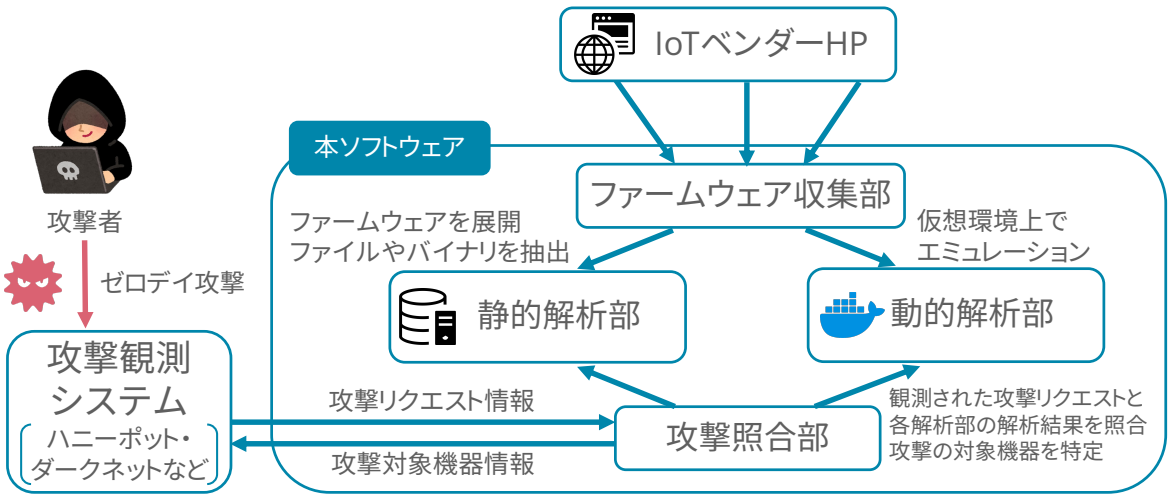

図 1 システム構成

ソフトウェア全体の処理の流れは以下の通りである。はじめに、「ファームウェア収集部」にて、IoT 機器ベンダーのホームページなどで公開されているファームウェアをスクレイピングによって収集し、機器の型番やバージョンなどのメタ情報とともに保存する。収集したファームウェアは「ファームウェア静的解析部」及び「ファームウェア動的解析部」によって解析される。

「ファームウェア静的解析部」では、収集したファームウェアを展開(アンパック)し、ファームウェア内のファイルやバイナリなどを抽出する。さらに、抽出したファイル及びディレクトリ構造の情報を、当該ファームウェア情報と紐づけてデータベースに記録する。

「ファームウェア動的解析部」では、仮想環境上で IoT 機器の CPU をエミュレーションし、実際にファームウェアを起動することにより、ネットワークサービスの稼働状況やレスポンスを取得し、データベースに記録する。

最後に「攻撃照合部」では、ハニーポットなどの攻撃観測システムでゼロデイ攻撃が観測された際にその攻撃リクエストの情報を入力することにより、機器の特定に繋がりうる特徴的な情報(宛先ポート番号、リクエストパス、パラメータ名、リクエストヘッダ内の Cookie や認証情報など)を攻撃リクエストから抽出し、前述のファームウェアの静的解析及び動的解析の結果と照合する。これにより、攻撃の標的となっている可能性のある機器を特定し、その機器の型番やベンダー名、ファームウェアの情報などを出力する。さらに、単に対象機器の情報を提供するだけでなく、攻撃を受けている脆弱な実装が存在している可能性のある実装の箇所(具体的なファイルパスやガ該当箇所周辺の実装内容)を提示する機能や、当該脆弱性の再現や検証などの調査を行うための仮想環境を提供する機能も備える。

4. 従来の技術(または機能)との相違

本開発成果の特徴として以下の 4 点が挙げられる。

- ファームウェアを大規模(17 万件以上)に収集したことにより、幅広い IoT 機器を標的とした攻撃に対応することができる点。

- ファームウェアの静的解析と動的解析を併用することにより、攻撃対象機器の特定速度およびカバレッジを大幅に向上させている点。
- 単に攻撃対象機器を特定するだけでなく、攻撃を受けている脆弱な実装が存在している可能性のある実装の箇所（具体的なファイルパスや該当箇所周辺の実装内容）を推定し提示する機能や、脆弱性の再現や検証のためのより詳しい調査を行うための仮想環境を提供する機能を備えている点。
- 国内の攻撃観測機関との連携・情報共有を積極的に実施し、実際に未知のゼロデイ攻撃の対象機器を特定し関係機関に報告を実施することで悪用状況の早期周知及び脆弱性の修正に貢献した点。

5. 期待される効果

攻撃対象機器が不明なゼロデイ攻撃の観測時に、本ソフトウェアを用いて攻撃の標的となっている機器や脆弱な実装をいち早く特定することにより、当該 IoT 機器のベンダーや開発者に対してゼロデイ脆弱性の存在とその悪用状況を報告することができ、脆弱性を修正するためのファームウェアアップデートやセキュリティパッチの早期提供に貢献することができる（図 2）。

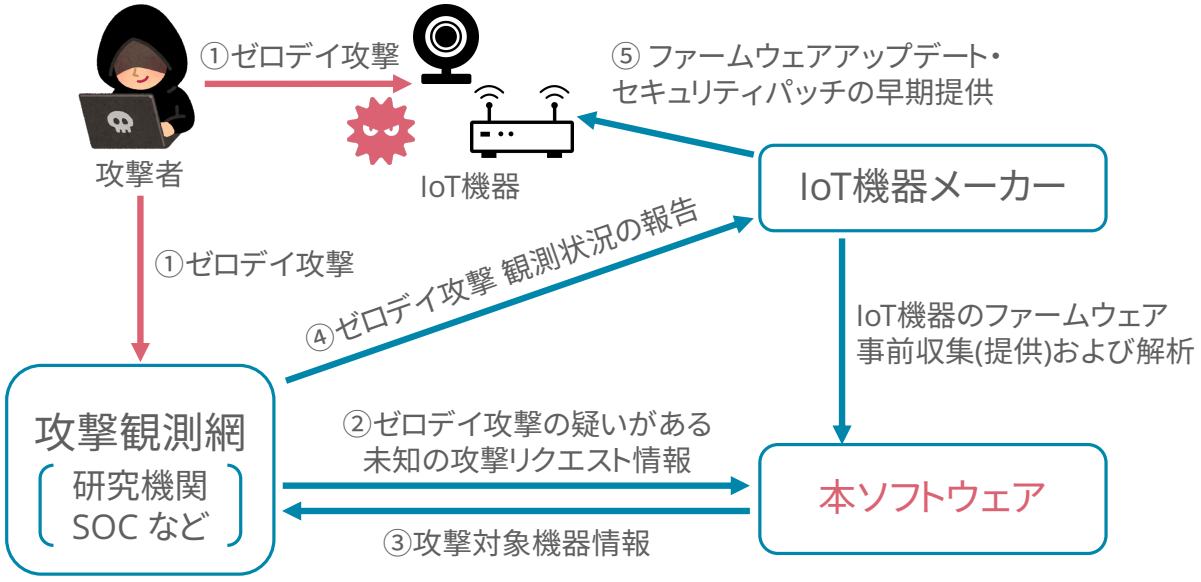

図 2 本ソフトウェアの活用シナリオ

実際に、開発したシステムを国内で観測された未知の攻撃の分析に活用し、これまでに計 4 件のゼロデイ攻撃の対象機器の候補を特定しており、今後も継続的な運用を通じて IoT 機器の脆弱性の早期修正およびサイバー攻撃による被害の拡大防止に寄与することが期待される。

6. 普及（または活用）の見通し

本プロジェクトはその社会的意義からプロジェクト終了後も継続して取り組む価値があることから、今後の展開に向けた技術的および運用面での課題を整理し、ソフトウェアの改善と国内外の攻撃観測網および IoT 機器ベンダーとの連携強化を進めていくことにより、より社会貢献性の高いシステムとして活用していくことを目指す。

7. クリエータ名（所属）

九鬼 琉（横浜国立大学 理工学部 数物・電子情報系学科 / 株式会社オプシス）