ISS-SP-051

静的解析と動的解析を組み合わせた IoT デバイスに対するマルウェア解析システムの検討

房安　良和†　　小寺　建輝†　　泉　隆††
† 日本大学大学院理工学研究科　　†† 日本大学理工学部

1. まえがき

近年，IoT の普及によって様々なデバイスがインターネットに接続されるようになった．これに伴い，IoT デバイスに感染し DDoS 攻撃等を実行させる「Mirai」[1]や，ストレージを破壊し，デバイスを使用不可能にする「BrickerBot」[2]をはじめとするマルウェアの出現が確認され多くの IoT デバイスへと感染被害が拡がった．多種多様なマルウェアの実行を阻止する必要があるが，IoT デバイスに対するセキュリティ対策は，現状，十分に行われていない．そこで，セキュリティ対策を講じるために，まず IoT デバイスに対するサイバー攻撃を分析する必要があると考え，先行研究[3]では不正アクセスやマルウェアを収集するハニーポットを構築した．本研究では，そのハニーポットで収集したマルウェアを解析するシステムの検討・構築を目的とする．

本稿では，上述したマルウェア解析システムの構成及び使用する解析手法について検討した．

2. ハニーポット/マルウェア解析システム構成

先行研究で構築したハニーポット(Machine A)と本研究で構築するマルウェア解析システム(Machine B)の構成を図 1 に示す．

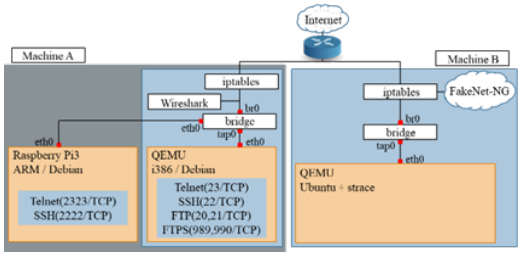

図 1.　ハニーポットと解析システムの構成

マルウェア解析システム(Machine B)では，QEMU を用いて IoT デバイスを模した Linux (Ubuntu)デバイスをエミュレートし，ハニーポット(Machine A)で捕獲したマルウェアの解析を行う．なお，エミュレートするデバイスの CPU アーキテクチャについては，解析対象のマルウェアに合わせたものを選択する．マルウェア解析システム(Machine B)を構築するために使用するソフトウェアを表 1 に示す．

表 1.　使用ソフトウェア(Machine B)

カテゴリ	使用ソフトウェア	目的
アクセスコントローラ	iptables	・マルウェアの実行によって発生する通信の FakeNet-NG への転送 ・インターネットとの通信の遮断
インターネットサービスエミュレータ	FakeNet-NG	・インターネットのエミュレーション ・通信パケットの取得(pcap ファイル)

マルウェア解析用システム(Machine B)で使用する解析ソフトウェアとそのソフトウェアを用いて解析する内容について，表層解析，動的解析，静的解析に分け，表 2 に示す．なお，マルウェアの実行で発生する各種サーバとの通信に対応するため，FakeNet-NG を用いたインターネットのエミュレートを行う．

表 2.　解析方法(Machine B)

解析方法	解析手段	解析内容
表層解析	PEframe	マルウェアに直接記述されている情報
動的解析	strace	マルウェアの実行で発生するシステムコール
	pcapファイル	・C&Cサーバの設置地域 ・マルウェアの実行で発生する通信パケット
静的解析	radare2[4]	マルウェアの実行で発生する処理内容の推定

3. 静的解析と動的解析の組み合わせ

動的解析のみでは，C&C サーバからの命令で動作をするマルウェアや，解析妨害機能を持つマルウェア等については，主要機能の解析を行うことができない．そのため，静的解析を用いることでマルウェアの動作内容について推定を行う．また，radare2 を用いたマルウェア内の条件分岐等への書き換えを行い(図 3)，網羅的に実行可能にした上で再度動的解析を行う．これにより，動的解析のみを実行した場合に実行されなかった機能の解析が可能となる．

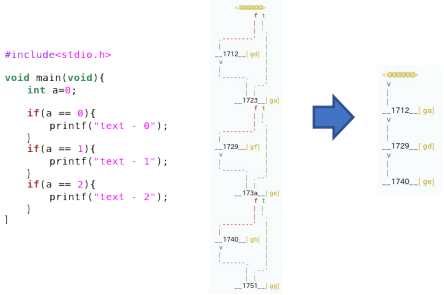

図 3.　実行したソースコードと条件分岐への書き換え前後に radare2 で作成したフローグラフ

4. まとめ

本稿では，マルウェア解析システムの構成及び解析手法の提案を行った．今後は，実際のマルウェアに対して本手法の導入を行うために，手動でのマルウェア解析並びに自動化への検討を行う．

文　献

[1] WIRED:「The Reaper IoT Botnet Has Already Infected a Million」, https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/,2018-12
[2] radware:「Bricker PDoS Attack: Back With A Vengence」, https://security.radwarecom/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/, 2018-12
[3] 房安良和・小寺建輝・泉隆:「ハニーポットを用いた IoT デバイスに対するサイバー攻撃の分析」, 平成 30 年電気学会全国大会,3-089,2018-03
[4] radare2:「radare/radare2 : unix-like reverse engineering framework and commandline tools security」,https://github.com/radare/radare2, 2018-12