ISS-SP-040

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に関する研究

房安　良和† 　　滕　琳†† 　　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，本研究では，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構築を目的とする．

2. ハニーポット/マルウェア解析システム構成

先行研究[3]で構築したハニーポット(マシン A)と本研究で構築するマルウェア解析システム(マシン B)の構成を図 1 に示す．マシン B では，QEMU を用いて IoT デバイスを模した Linux デバイスをエミュレートし，マシン A で捕獲したマルウェアの解析を行う．

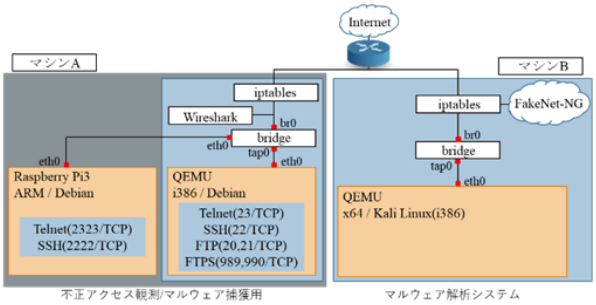

図 1. ハニーポットとマルウェア解析システムの構成

3. ハニーポット/マルウェア解析システム構成

マシン 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た各解析方法の解析内容を表 1 に示す．

表 1. 解析内容(マシン 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

静的解析結果を用いたマルウェアの書換え及び，動的解析を繰り返すことで，マルウェア内のコードを網羅的に実行する．なお，マルウェアの実行で発生する外部との通信に対応するため，FakeNet-NG を用いてインターネット及び C&C サーバ等との通信で発生する通信のエミュレートを行う．マシン B での解析結果は，ハッシュ値や保有機能等をまとめ，マルウェア情報としてデータベース化する．

4. 静的解析と動的解析の組み合わせ

動的解析に使用する単純な strace の実行のみでは，C&C サーバからの命令で動作するマルウェアや，解析妨害機能を持つマルウェア等については不十分である．そこで，静的解析として radare2 を用いた条件分岐(jmp 系命令)等の情報取得・書換えを行い(図 2, 3)，再度動的解析をする．これにより，マルウェアの網羅的な実行及び解析が可能となる．なお，全条件分岐に対して書換えを行うと，while 等のループ処理が存在する場合に変数の値が正しく取得されない等の問題が生じるため，書換えの必要/不要の判別を行う必要がある．

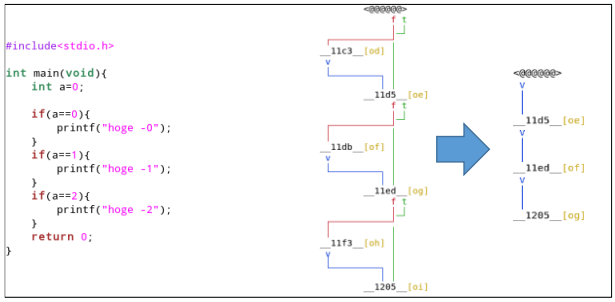

図 2. 実行したソースコードと条件分岐への書き換え前後に radare2 で作成したフローグラフ

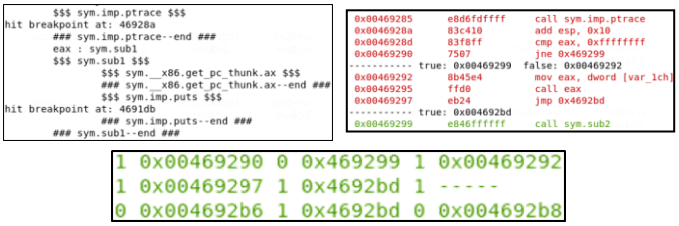

図 3. 実行したソースコードでの取得情報(左上: 実行時に呼び出された関数の可視化，右上: 実行/未実行命令についての可視化，下: 各分岐(jmp 系命令)における実行結果の可視化)

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/,2020-02
[2] radware:「Bricker PDoS Attack: Back With A Vengence」, https://security.radwarecom/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/, 2020-02
[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, 2020-02