SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

IoT マルウェア配布サーバの継続的監視による検体遷移の調査
Investigation of Malware Transitions through Continuous Monitoring of IoT Malware Download Servers

徐　競博 *　　鄭 俊俊 *　　毛利 公一 †
Jingbo XU　　Junjun ZHENG　　Koichi MOURI

キーワード IoT，マルウェア，マルウェア解析，ハニーポット

あらまし

IoT(Internet of Things) 機器の普及とともに，Mirai に代表される IoT 機器を侵入対象としたマルウェア (以下「IoT マルウェア」という) が増加傾向にあり，それに伴う被害の影響拡大が懸念されている．実際に，「Mirai」や「Bashlite」[1](別称:Gafgyt，Qbot，Lizkebab など) などのソースコード [2][3] の公開されており，そのため，亜種が次々と生まれている．今後も，攻撃者の目的の変化に伴い，IoT マルウェアの侵入方法や攻撃方法の傾向も変化していくと考えられる．

本論文では，IoT マルウェア配布サーバごとの検体の遷移を調査する目的で，2021 年 8 月 24 日〜11 月 30 日の期間に，図 1 に示したような IoT 機器を狙ったサイバー攻撃を観測するためのハニーポットを用いて，IoT マルウェア配布サーバを継続的に監視した．その結果，1405 件の IoT マルウェア検体を収集することができた．また，同一の配布サーバでも検体が続々と更新されていることが明らかになった．本稿では，さらに検体に含まれる特徴的な文字列に着目し，攻撃に利用される認証情報や脆弱性と，攻撃用コマンドなどの変化に基づいても調査を行った．

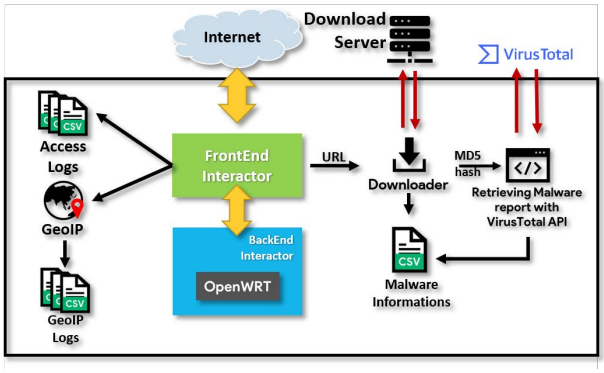

図 1: IoT 機器を狙ったサイバー攻撃を観測するためのハニーポットの構成

参考文献

[1] Eduard Kovacs, “BASHLITE Malware Uses ShellShock to Hijack Devices Running BusyBox”, https://www.securityweek.com/bashlite-malware-uses-shellshock-hijack-devices-running-busybox, 2014.

[2] Jerry Gamblin, “Mirai-Source-Code”, https://github.com/jgamblin/Mirai-Source-Code, 2017.

[3] Zehra Array,“BASHLITE”, https://github.com/ifding/iot-malware/tree/master/BASHLITE, 2016.

* 立命館大学 〒 525-8577 滋賀県草津市野路東 1-1-1. Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu, Shiga, 525-8577 Japan. jxu@asl.cs.ritsumei.ac.jp
† mouri@asl.cs.ritsumei.ac.jp