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 マルウェア基礎情報の調査
Investigation of Basic Information on IoT Malware

周 家興* 寺田 真敏 †
Jiaxing Zhou Masato Terada

キーワード IoT マルウェア，脆弱性，オペコード

あらまし

Internet of Things（IoT）デバイスの普及に伴い、IoT デバイスを狙ったサイバー攻撃も急増しており、被害を抑制するための対策を講じる必要がある．サイバー攻撃の一種である IoT マルウェアに関する研究においては、IoT マルウェアのライフサイクル分析、IoT マルウェア解析手法，IoT マルウェア検知と分類手法など、非常に多くの研究がなされている．また、IoT マルウェア対策の研究を進めるにあたり、IoT マルウェアの特徴を把握するための表層解析情報や動的解析情報について調査は進められてきてはいるが、その報告は 2017 年～2018 年の IoT マルウェアに留まっている．本研究では、2021 年時点で IoT マルウェアの特徴を把握するため、表層解析情報や静的解析情報として、IoT マルウェアのアーキテクチャ、ファミリー名、Operation Code（オペコード）、関数名および実装された脆弱性の種類について調査する．

調査手法としては、(1)表層解析では、各検体から実行可能なアーキテクチャ情報を抽出する．(2)静的解析では、検体ごとに、使用しているオペコードおよび関数名を抽出する．(3)各検体が攻撃に使用する脆弱性の判定では、各検体のバイナリファイルに保存されている文字列を抽出し、公開されている脆弱性データベースと突き合わせて特定する．(4)上述までの調査に加えて、AVClass というツールで検体のファミリー名の抽出し、アーキテクチャ種類ごとに、検体のファミリーごとに、ELF フォーマットごとに、脆弱性の実装状況と傾向、および検体のオペコードと関数名の使用傾向を調査する．本研究で使用する検体（ファイルタイプは Executable and Linkable Format(ELF)である）は、Virusshare という公開されているマルウェアレジポトリから入手し、総数は 52,617 件である．

調査結果としては、(1)52,617 件中 10,213 件検体から合計 46 種類の攻撃に使用する脆弱性を特定した．攻撃に使用する脆弱性のうち、利用された回数が最も多い脆弱性は CVE-2017-17125（Huawei HG532 における入力確認に関する脆弱性）で、9,060 検体に利用されたことが分かった．二番目は CVE-2014-8361(Realtek SDK の miniigd SOAP サービスに任意のコードを実行される脆弱性)で 2,358 検体，三番目は Linksys E-series の Remote Code Execution 脆弱性(CVE 番号の付与なし)で 2,225 検体に利用されたことが分かった．(2)実行可能なアーキテクチャごとで見た場合、アーキテクチャ Aarch64 以外の検体では攻撃に使用する脆弱性のうち最も多い脆弱性が CVE-2017-17215 であった．一方、Aarch64 ベースの検体では Linksys E-series の Remote Code Execution 脆弱性が一番多い．また、ARM、I386 と MIPS ベースの検体には、今回の調査で特定した 46 種類の攻撃に使用する脆弱性すべてが存在することが分かった．(3)検体のファミリーごとで見た場合、ファミリーMirai が脆弱性 CVE-2017-17215、Linksys E-series の Remote Code Execution、CVE-2014-8361 をよく利用し、Gafgyt と Tsunami が脆弱性 CVE-2017-17215 をよく利用していることが分かった．(4)Virustotal のスキャン結果では ELF フォーマットとして Android タイプと Linux タイプが提示されている．この ELF フォーマットごとに、IoT マルウェア間の差分を攻撃に使用する脆弱性と関数名の使用状況から調査した結果、Android タイプは Linux タイプよりも 3 倍くらい該当する検体数が多かった．しかし、Android タイプと Linux タイプの検体母数の比率がおおよそ 3:1 であることから、ELF フォーマットで見た場合、2 タイプの検体の動作上の差分は、特にないことが分かった．

本研究では IoT マルウェアのアーキテクチャ情報、使用しているオペコード、関数名および攻撃に使用する脆弱性の利用状況から IoT マルウェアの基礎情報と動作特徴を調査した．今後は大規模の均衡データセットでアーキテクチャごとにより深い分析を行う．

* 東京電機大学, 〒125-0051 東京都足立区千住旭町 5 番 {syuu, terada}@isl.im.dendai.ac.jp