BinGrep：制御フローグラフの比較を用いた関数の検索によるマルウェア解析の効率化の提案

羽田 大樹[1,2]　後藤 厚宏[1]

概要：近年，日本においても APT 攻撃による大規模な被害を経験し，インシデント対応の重要性が再認識された．インシデントにおいてマルウェアの亜種が共通的に使用された場合，過去に解析したマルウェアの関数に相当するコードの場所を特定できると速やかに解析が行える．このコード特定のために，BinDiff に代表されるパッチ解析用のコード「比較」ツールを利用できるが，貪欲アルゴリズムにより対応付けを連鎖的に間違えてしまう場合や，間違えた場合に利用できる情報がないという課題があった．マルウェア解析に適したコード比較アルゴリズムとして，関数における制御フローグラフの編集距離と命令列の最長共通部分列を用いて関数を「検索」する BinGrep を提案する．BinGrep は，GNU bash と binutils では 11,049 個の関数のうち 90.3%について正解を出力できた．実際に APT 攻撃で使用されたマルウェアで評価したところ，Emdivi の 11 検体の評価では，インシデント対応において重要であった 27 個の関数の 85%について正解を出力できた．また，Emdivi と PlugX のそれぞれ 2 検体の全関数について評価を実施し，マルウェア解析において提案方式が有効であることを示した．

本招待論文は，情報処理学会論文誌に掲載されました「BinGrep：制御フローグラフの比較を用いた関数の検索によるマルウェア解析の効率化の提案」[1] についてご紹介いただくものです．

参考文献

[1] 羽田大樹，後藤厚宏：BinGrep：制御フローグラフの比較を用いた関数の検索によるマルウェア解析の効率化の提案，情報処理学会論文誌，Vol. 58, No. 5, pp. 1151–1162 (2017).

[1] 情報セキュリティ大学院大学
[2] NTT セキュリティ・ジャパン