講演番号：28

マルウェア解析環境の構築法の検討

A－7　　Study of the configuration of malware detection environment

久保　宏樹†　宮保　憲治†　笠間　貴弘†‡
Hiroki KUBO†　Noriharu MIYAHO†　Takahiro KASAMA†‡
† 東京電機大学　情報環境学部
† School of Information Environment, Tokyo Denki University
‡情報通信研究機構
‡National Institute of Information and Communications Technology

1. はじめに

マルウェアを検出する方法の一つとして,動的解析用の環境を用いて実際にマルウェアを起動し,挙動を監視する方法がある.近年,マルウェアの進化によって動的解析の環境を検知し当該プログラムの終了を行うなど,解析の妨害を行うマルウェアが増加している[1].そのため,マルウェアの動的解析が難しくなりつつある.

本稿では動的解析の環境を構築し,「pafish」(動的解析の環境を検知する OSS(Open-source software))を用いて動的解析の環境を検知する方法を明らかにした.さらに,マルウェアによって動的解析の環境を検知されないような環境設定の変更方法を検討し,評価実験を行った.

2. 動的解析の環境を検知する方法

本検討で,用いた動的解析の環境を図 1 に示す.図1のゲスト OS 上で「pafish」を実行することで判明した動的解析環境の検知方法を表 1 に示す.

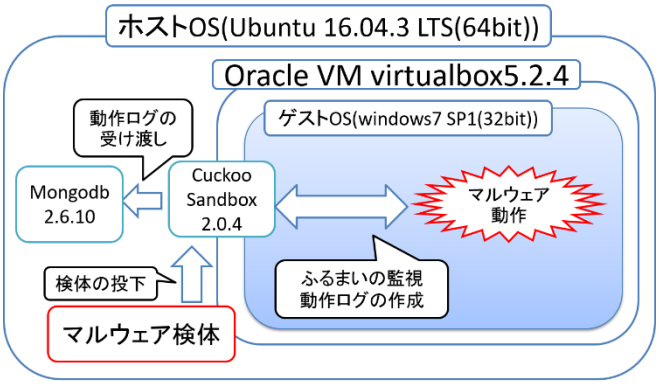

図1 動的解析の環境

表1　動的解析環境の検知方法

1	ドライバのシステムファイルに「Vbox～」の存在を認識、検知
2	MACアドレスが「08:00:27」であるか認識、検知
3	VM特有のプロセス名の認識、検知
4	ホストOS～ゲストOS間のの共有ファイルを認識、検知
5	VM特有のレジストリキーの値を認識、検知
6	一定時間内にマウスの動作があるか

3. 提案手法

表 1 で示した各種の検知方法によって対応付けられるゲスト OS の設定変更方法を表 2 に示す.

表2　ゲストOSの設定変更方法

1	「Vbox～」のシステムファイルの削除	4	ホストOSとゲストOS間の共有フォルダの削除
2	MACアドレスの変更	5	VM特有のレジストリキーの削除
3	VM特有のプロセス名の変更	6	マウスを常に動作させるプログラムを起動

4. 評価実験

4.1 実験方法

設定変更を行わない環境(以下,従来の動的解析環境)と表 2 に示したゲスト OS の設定変更を行うことにより実現した動的解析環境(以下,検討を加えた動的解析環境)とで同一のマルウェアを動作させ,API コール数の比較を行った.

4.2 実験結果

評価にはインターネットで収集した PE フォーマットのマルウェア検体を 300 個使用した.実験結果を表 3 に示す.

表3　実験結果

	検体数(個)	全体の割合(%)
(1)APIコール数が増加	79	26%
(2)APIコール数が減少	111	37%
(3)APIコールの数が同一	95	32%
(4)APIコールの数が計測不能	15	5%

4.3 評価

検討を加えた動的解析環境において API コール数が増加している場合は,マルウェアは本来の悪質な動作を行っていると考えられる.すなわち,表 3 より実験に使用したマルウェアの 26%((1)に相当)が表 2 に示したゲスト OS の設定方法が有効だと考えられる.一方,API コール数が減少,または同一であった全体の 69%((2),(3)に相当)の検体は設定変更が逆効果もしくは無意味であることが判明した

5. まとめ

本検討においては一部のマルウェアに関して,ゲスト OS の設定変更が有効であるということがわかった.今後 API コール数が減少する理由についてはさらに有効な,対処法を検討する予定である.

参考文献

[1] Trend Micro(2017)「巧妙なマルウェアに対抗する最先端のサンドボックス技術」
<http://blog.trendmicro.co.jp/archives/14720>
(2018/1/8 アクセス)