環境依存型マルウェア解析システムの機能向上に向けたサンドボックスの構成検討

徳山 喜一† 重本 倫宏†
鬼頭 哲郎† 磯部 義明† 仲小路 博史†

†日立製作所
244-0817 横浜市戸塚区 吉田町 292
kiichi.tokuyama.vg@hitachi.com

あらまし 近年、動作環境依存型マルウェアに代表される、ターゲットとされた組織向けにカスタマイズされたマルウェアにより、組織のITシステムが突破され重要な情報を盗み取られる被害が増加の一途をたどっている。これらの被害を引き起こす高度なサイバー攻撃に対し迅速な対策を支援するための技術として、我々の研究グループでは、多種環境においてマルウェア解析を並列的に実行することで、動作環境依存型マルウェアの挙動を明らかにするマルウェア自動解析技術を開発している。本稿では、我々の保有するマルウェア自動解析システムを構成するサンドボックス77種類に対して、構成サンドボックス数と検知精度に関する分析を行い、検知精度を維持しながら構成サンドボックス数を削減できる可能性について検証した。

Configuration study of the sandbox for the function improvement of environment-dependent malware analyzing system

Kichi Tokuyama† Tomohiro Shigemoto†
Tetsuro Kito† Yoshiaki Isobe† Hirofumi Nakakoji†

†Hitachi, Ltd.
292 Yoshida-cho, Totsuka Ward, Yokohama City, Kanagawa 244-0817, JAPAN
kiichi.tokuyama.vg@hitachi.com

Abstract In recent years, theft of important information from IT system of the organization has been increasing owing to cyber attacks which utilize malwares customized for targeted organization as typified by the environment dependent malware. Against this background, in order to support the rapid measures against sophisticated cyber attacks, our research group has developed the automated malware analyzing system that can reveal the behavior of the environment dependent malware by executing them in parallel in various environments. In this paper, we performed the research about the detection accuracy and number of constructed sandboxes for the 77 types of sandbox that make up the malware automatic analysis system, and verified the possibility that it is possible to reduce the number of configuration sandbox while maintaining the detection accuracy.

1　はじめに

近年、民間企業や、防衛関連企業、公的機関を狙ったサイバー攻撃が顕在化しており、個人、企業、国家の利益や安全性を損なうリスクが高まっている。また、攻撃手法も益々巧妙化しており、標的型攻撃、特に APT（Advanced Persistent Threat）攻撃[1]は、秘密裏に、そして執拗に長期間攻撃を続ける点で従来の脅威とは性質が異なる。さらに近年では、新種のマルウェアの半数以上が既存のウイルス対策ソフトでは検知できないと報告されている[2]。このような状況下でマルウェアが組織の中に侵入してしまった場合には、侵入したマルウェアの特性を解明して被害拡大防止策を講じることが重要となる。

マルウェアの特性を解明する手法として、マルウェアを特殊な解析環境で実行して挙動を観測する動的解析手法が用いられているが、最近のマルウェアは実行環境を限定することで解析環境での解析を逃れるタイプが増えている[3,4]。このような背景から、我々の研究チームでは、最新のサイバー攻撃の性質をいち早く把握し、防御に生かすことを目的として、マルウェアの自動解析技術（M3AS）の開発を行っている。本技術では、多種環境のサンドボックス上でマルウェアの並列解析を実施することで、動作環境に応じて挙動を変化させるマルウェア（動作環境依存型マルウェア）の検知が可能である。

マルウェアを多種環境上で並列解析するシステムにおいては、サンドボックスの構築コストとの兼ね合いから、並列解析を行うサンドボックスの個数と検知精度との兼ね合いが重要である。そこで今回は、M3AS の保有するサンドボックス 77 種類に対して、構成サンドボックス数と検知精度に関する分析を行い、検知精度を維持しながら構成サンドボックス数を削減できる可能性について検証した。本報告では、これらの取り組みの結果を述べる。

2　関連研究

動作環境依存型マルウェアとは、特定の組織を攻撃することを目的として、特定の端末環境でのみ動作するよう仕組まれたマルウェアのことである。これらの動作環境依存型マルウェアの解析にあたり、特定の環境しか用意されていない既存の動的解析ソフトウェアやサービスによる解析ではその挙動が明らかにできないという課題があった。動作環境依存型マルウェアの解析アプローチとして、Zhaoyan Xu らは、環境調査を行う API を監視し、様々な値を返すことで、環境依存型のマルウェアを効率的、効果的に解析する手法を示している[5]。我々の研究チームでは、動作環境依存型マルウェアを解析するために、多種環境のサンドボックスを備えたマルウェア解析システムを開発している[6]。

3　マルチモーダルマルウェア解析システム

ここでは、我々の研究チームが開発するマルウェア解析システム[6]について述べる。

3.1　M3AS の概要

我々の開発するマルウェア解析システム（M3AS）の概要を図 1 に示す。

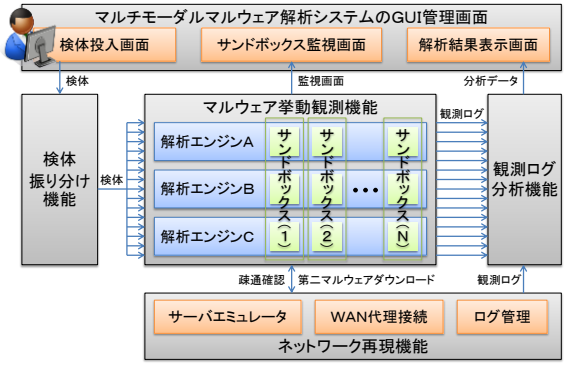

図 1　M3AS の概要

M3AS では様々な OS やソフトウェアを組み合わせた複数の解析環境上でマルウェアを解析する。解析環境の構築にあたっては、公開された脆弱性情報や攻撃傾向に基づいてマルウェアが動作しや

すい環境を選定している。また、マルウェア解析のノウハウをスクリプト化することで、観測結果からマルウェアの挙動を自動抽出する技術を実装している。この技術によりマルウェアによるネットワーク接続などの不正行動を容易に解明することができ、被害の発生や拡大の防止に役立てることができるようになる。

3.2　環境依存型マルウェア検知方法

M3AS によるマルウェア解析によって、M3AS を構成する各サンドボックスからマルウェアの挙動情報がそれぞれ出力される。ここで M3AS では、被解析検体がインターネット上の不審な接続先（あらかじめ定めたホワイトリストのいずれにも合致しない通信先）へ通信を行う挙動をマルウェアの挙動とみなす。また、動作環境依存型マルウェアの判定には、各環境ごとに導出するピアソンの相関係数を用いる。あるマルウェアに対して、特定の動作環境におけるピアソンの相関係数が 0.4 を上回った場合に、当該マルウェアを動作環境依存型マルウェアとして検知する。

3.3　環境依存型マルウェア解析評価実験

動作環境依存型マルウェア検知方法を用いて、実施した評価実験の結果を図２、図３に示す。本評価実験では、2014 年の 10 月の間、我々の所属する組織で観測したマルウェア検体 631 件を用いて解析を行っている。図２、図３に示すように、動作環境が、物理環境、もしくは仮想環境に依存する検体が 631 検体中 23 検体、また、いずれかの OS 環境への依存性が確認されたマルウェアが

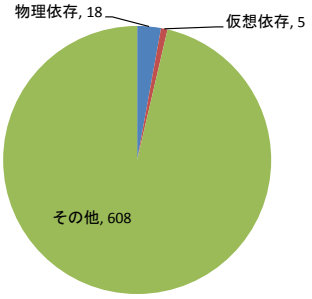

図 2 物理/仮想環境依存性検体の分布

631 検体中 115 検体観測された。

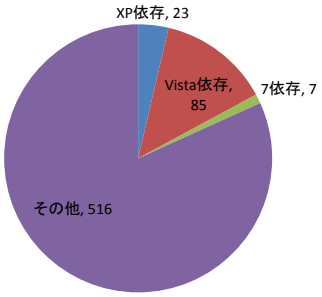

図 3 OS 依存性検体の分布

4　環境依存型マルウェアを検知するサンドボックスの構成検討

我々の研究チームで開発するマルウェア解析システム M3AS では、様々な環境依存型マルウェアの挙動を検知するために、多種類の動作環境をサンドボックス上で実装しており、その種類数は 77 種類に及ぶ。M3AS を構成するサンドボックスの動作環境について、解析エンジンは Threat Analyzer および Cuckoo Sandbox[7,8]のいずれか、OS は Windows XP(Service Pack 2/Service Pack 3), Windows Vista (Service Pack 1 / Service Pack 2) , Windows 7 (Service Pack 1)のいずれか、インストールアプリケーションは JRE (1.4, 5, 6, 7), Microsoft Office(2007, 2010, 2013), Adobe Flash Player(9, 10, 11), Adobe Reader (8, 9, 10, 11), Microsoft Internet Explorer(6, 7, 8, 9, 10)である。

M3AS を構成する各サンドボックスに対するマルウェアの挙動検知結果を得るために、これまでに本システムにより解析した 3,000 件超の被解析検体の解析結果データを、サンドボックスごとに蓄積してきた。M3AS を構成する各サンドボックスで検知した検体数（検知検体数）のデータを表１に示す。なお、M3AS を用いてこれまでに解析した検体の中で、不審なネットワークへの通信を検知した検体の総数は 2,117 件であり、表１の第３列には、各サンドボックスにおける検知検体数

の、2,117 件に対する割合（検知率）を示している。

表 1 サンドボックスごとのマルウェア検知率

	サンドボックス検知数(個別)	サンドボックス検知率(個別)
#1	1146	54.13%
#2	1145	54.09%
#3	1132	53.47%
#4	1131	53.42%
#5	1128	53.28%
#6	1109	52.39%
#7	937	44.26%
#8	871	41.14%
#9	862	40.72%
#10	858	40.53%
#11	857	40.48%
	.	.
	.	.
	.	.
#68	272	12.85%
#69	262	12.38%
#70	229	10.82%
#71	220	10.39%
#72	219	10.34%
#73	196	9.26%
#74	167	7.89%
#75	147	6.94%
#76	1	0.05%
#77	1	0.05%

表 1 の結果より、最も検知率の高いサンドボックスは、全検体 2117 件のうち 50%程度を検知可能であることがわかる。

M3AS において多種環境のサンドボックスを構築するためには、通常はコストの制約を受けるため、より少ない数のサンドボックスで構成する必要がある。これを受けて、本報告では、より少ないサンドボックスの組合せでも高い全体検知率（組合せに含まれるサンドボックスのいずれかで検知可能なマルウェア数の割合）が得られるようなサンドボックスの組合せの選定を試みる。

4.1 サンドボックス選定方法の提案

表 1 の結果を用いて、検知率の高いサンドボックスを順に選択して組合せを作成する方式（検知率順選択方式）を策定する。検知率順選択方式でサンドボックスの組合せを選定した際の、選定サンドボックスの個数に対する全体検知率の推移を図 4 に示す。

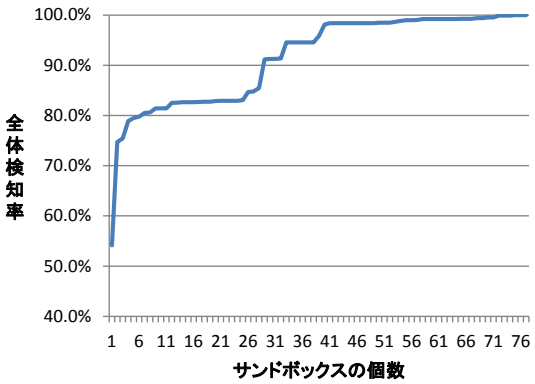

図 4 全体検知率の分布

図 4 より、検知率順選択方式では、サンドボックスの個数に対する全体検知率の増加の滞りが断続的に発生することが確認できる。これは、類似のサンドボックス間では検知可能な検体の種類に重複が見られるためだと考えられる。そこで、これらの問題を解決するサンドボックスの組合せ選定の方法として、以下の 2 つを策定し、評価を行った。

- 最大検知器選択方式
  - ➢ すでに選択したサンドボックスの組合せにより検知可能な検体を検体全体の集合から除外、その補集合の中で最も検知数の大きいサンドボックスを選択
- 重複排除選択方式
  - ➢ あるサンドボックスの検知可能検体で、他のいずれのサンドボックスの検知可能な検体とも重複を起こさない検体の数が、最も大きいサンドボックスを選択

最大検知器選択方式は、検知率の高いサンドボックスを優先的に選ぶという方針のもと、他のサンドボックスとの検知検体の種類の重複を考慮するよう、手法を改良したものである。単純に検知検体数の大きなサンドボックスを順に選ぶ手法に対して、すでに選択したいずれのサンドボックスにも検知されていないマルウェア検体を検知可能なサンドボックスを、より優先的に選定できる。

重複排除選択方式は、各サンドボックスにおいて、固有に検知可能なマルウェア検体を多く持つ

サンドボックスに着目し、これを優先的に選定する手法である。検知可能な全検体を漏れなく検知することを前提とする場合、本手法はより効率的にサンドボックスの組合せを選定できる。

以後、各方式におけるアルゴリズムの内容とその評価結果をそれぞれ述べる。なお、アルゴリズムの内容説明にあたっては以下の表記記号を用いる。

- U:マルウェアの全体集合.
- m(i):マルウェア. iはマルウェアの序列番号を表す.
  (U = {m(1), m(2), …, m(2117)})
- W:サンドボックスの全体集合.
- s(j):サンドボックス. jはサンドボックスの序列番号を表す.
  (W = {s(1), s(2), …, s(77)})
- S(j): s(j)によって検知可能なマルウェアの集合.
  (S(j) = {m(p), m(q), m(r)…} ,
  0≦p, q, r≦2117)
- #:集合の要素の個数を表す記号.
  たとえば、#S(j)はs(j)によって検知可能なマルウェアの個数を表す.
  (0≦#S(j)≦2117)
- Y:選定したサンドボックスの集合.
  Yの初期値は空集合である(Y = ϕ).
  なお、Yの要素となるサンドボックスをx(k)と記述する.(1≦k≦77) また、S(j)と同様、x(k)により検知可能なマルウェアの集合をX(k)と表す.

4.1.1 最大検知器選択方式

アルゴリズム

- n = 1 とする.
- (開始)
  x(n) =
  〔s(i) | #S(i) = max(#{S(i)∩U} | s(i) ∈W)〕
  とする.
- U = U ∩ {X(n)}^{C} とする.
- Wから要素s(i)を取り除く.
- (終了条件)
  U＝ϕ であれば終了し、
  Y={x(1), ・・・, x(n)}を出力する.
- n＝n＋1 として(開始)に戻る.

4.1.2 重複排除選択方式

アルゴリズム

- n = 1 とする.
- 1 ≦i, j≦77 に対し、S(i) ⊂S(j) ならば、s(i)をWから取り除く.
- (開始)
  x(n)
  =〔s(i) | #S(i) =
  max(#{ S(k)∩{$\cup_{l\neq k}$S(l)}^{C} ∩U} | s(k) ∈ W) 〕
  とする.
- Wから要素x(n)を取り除く.
- (終了条件)
  U＝ϕ であれば終了し、
  Y={x(1), ・・・, x(n)}を出力する.
- ∀s(k) ∈W に対して#{ S(k)∩{$\cup_{l\neq k}$S(l)}^{C} ∩U} = 0 であれば、(分岐1)へ移動し、
  そうでなければ、(分岐2)へ移動する.
- (分岐1)
  U = U ∩ {$\cup_j$ X(j)}^{C} として(分岐2)へ移動する.
- (分岐2)
  n＝n＋1 として(開始)に戻る.

4.2　各方式の評価結果

最大検知器選択方式と、重複排除選択方式とをそれぞれ用いて、サンドボックスの組合せを決定した結果を図５に示す。なお比較対象として、4.1節で述べた、検知率順選択方式を用いた場合の全体検知率の推移も図５に示す。

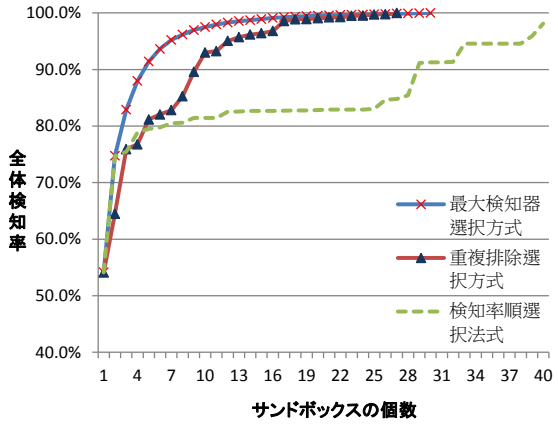

図 5 全体検知率の分布

最大検知器選択方式では、30個のサンドボックスで全検体2,117件を検知した。一方、重複排除選択方式では、27個のサンドボックスで全検体2,117件を検知し、最大検知器選択方式と比べて3個少ないサンドボックスの組合せとなった。なお、サンドボックスの個数が少ない場合において、重複排除選択方式での全体検知率は最大検知器選択方式を下回る結果となった。

5　考察

5.1　両者の方法における相違

最大検知器選択方式については、サンドボックスの個数が少ない場合に大きな増加率を示すものの、残存の未検知検体の数が少なくなる毎に、全体検知率の増加率は単調に減少する。このため最大検知器選択方式は、すべての検体を漏れなく検知することを前提とせず、限られたサンドボックスで高い全体検知率を持つ組合せを選定する場合に有効である。

重複排除選択方式の場合、最大検知器選択方式に対してサンドボックスの組合せ個数に対する全体検知率の増加パターンがまばらである。これは、この方法が、単純に全体検知数の大きなサンドボックスを順番に選ぶ方法ではないことによる。

さらに重複排除選択方式においては、固有の検知検体を持つサンドボックスがより早い段階で選択される。このために、最大検知器選択方式、重複排除選択方式の双方による選択サンドボックスの組合せからそれぞれ上位のみを抽出した場合、前者に対し後者の方が、より多くの動作環境依存型マルウェアを検知するサンドボックス群となることが考えられる。

5.2　今後の課題

今回行った重複排除選択方式の評価においては、あるマルウェアの解析に対して一部のサンドボックスを使用しなかった場合や、一部のサンドボックスにおいてエラーが発生した場合も、「検知なし」として扱った。これは、あるマルウェアを固有に検知するサンドボックスを選定する際に、誤った選定を引き起こす原因となっている。このため、解析エラー、もしくは解析なしの場合を「検知なし」の場合と区別した上で、選定方法を検討することが課題となる。

重複排除選択方式のアルゴリズムでは、他のサンドボックスでは検知できなかった固有の検知検体を持つサンドボックスを選定し、それらによって検知された検体を全体から取り除くという処理を繰り返しているが、上述のサンドボックスが存在しない場合は、アルゴリズムが破綻してしまう。いずれのサンドボックスにも固有の検知検体が存在しない場合は、検知されたサンドボックスの種類数が最も少ない検体について、それを検知したサンドボックスを選定する、といった方針での改良が考えられる。

また、今回行ったサンドボックス選定の評価では、これまでに M3AS で検知した検体を標本としたため、本選定方法によって構成されたサンドボックスで今後現れる検体を 100%検知できるとは限らない。このため、マルウェアの動向に応じて必要となるサンドボックスの種別を予測し、安全

マージンとして追加することも必要である。これらの予測方法も、今後の検討課題となる。

6 まとめ

我々の研究チームが開発したマルウェア自動解析システム(M3AS)について、構成するサンドボックスの個数に対する全体検知率をより大きくするサンドボックス選定方法の策定に取り組み、複数のサンドボックス間での検知検体の重複を考慮した、サンドボックスの選定方式を2つ提案した。1つ目の最大検知器選択方式は、少ないサンドボックスの個数でより検知率の高いサンドボックスの組合せを選定するために有用である。また2つ目の重複排除選択方式は、最大検知器選択方式よりも少ない個数のサンドボックスで全検体を検知でき、また、動作環境依存型マルウェアを検知するサンドボックスを優先的に選定する手法であると考えられる。

77個のサンドボックスで構成されるM3ASによって検知した、不正なネットワーク通信を行うマルウェアはこれまでに2,117件存在したが、最大検知器選択方式の場合は合計30個、重複排除選択方式の場合は合計27個のサンドボックスで、これら2,117件のマルウェア全体を検知可能であることが分かった。このため、重複排除選択方式を採用した場合、多種環境マルウェア解析システムにおいて構築するサンドボックスの数を、65%削減できることが分かった。

参考文献

[1] IPA: 標的型攻撃/新しいタイプの攻撃の実態と対策. http:// www.ipa.go.jp/files/000024542.pdf

[2] Symantec: Antivirus software is dead, says security expert at Symantec, http://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec

[3] Rodrigo Rubira Branc: Scientific but Not Academical Overview of Malware Anti-Debugging, Anti-Disassembly and Anti-VM Technologies, Black Hat USA Conference 2012.

[4] Chen,X., Andersen,J., Mao,Z.M. et al.: Towards an Understanding of Anti-Virtualization and Anti-Debugging Behavior in Modern Malware, The 38th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp.177 - 186(2008).

[5] Zhaoyan Xu, Jialong Zhang, Guofei Gu, Zhiqiang Lin : GoldenEye - Efficiently and Effectively Unveiling Malware's Targeted Environment

[6] 仲小路博史, 重本倫宏, 鬼頭哲郎, 林直樹, 寺田真敏, 菊池浩明: 多種環境マルウェア動的解析システムの提案, コンピュータセキュリティシンポジウム2014論文集, pp. 984-991(2014).

[7]ネクストイット:"GFI Sandbox Top" https://www.nextit.jp/product/gfi/sandbox/

[8]Cuckoo Sandbox:"Automated Malware Analysis – Cuckoo Sandbox" http://www.cuckoosandbox.org/

商標等に関する表示