マルウェアのポート待ち受け状態を考慮した 並列動的解析環境のネットワーク制御

鉄 穎† 吉岡 克成† 松本 勉†
†横浜国立大学
240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7
{tie-ying-fc, yoshioka, tsutomu }@ynu.ac.jp

あらまし NATにより同一のグローバルIPアドレスを共有してネットワーク接続する複数の実行環境においてマルウェア動的解析を行う際，NAT下の実行環境においてポート待ち受け状態となったマルウェアに対して，外部からの接続要求が届かず，解析に影響を与える場合がある．そこで，本研究では，実行環境のポート待ち受け状態監視とNATを実現しているルータのルーティング自動変更により，ポート開放可能な解析環境を作り，外部からの接続要求が適切に実行環境に届く仕組みを提案する．提案手法が解析結果に大きな影響を与える例として，独自のP2P通信により感染ホスト間でデータ共有を行うZeroAccess検体をポート開放可能な解析環境で1か月以上動かし，500万近い感染疑いホストを見つけた事例についても説明する．

Network Control of Multiple Sandboxes Corresponding to Port Listening States of Malware

Ying Tie† Katsunari Yoshioka† Tsutomu Matsumoto†

†Yokohama National University.
79-7 Tokiwadai, Hodogaya, Yokohama, Kanagawa 240-8501, Japan
{ tie-ying-fc, yoshioka, tsutomu }@ynu.ac.jp

Abstract When multiple malware sandboxes connect the Internet with the same global IP address by using NAT, incoming connection requests from an outside host do not reach any of them even if a malware sample executed in these sandboxes listens on a port expecting to receive the requests. In this paper we propose a method in which incoming connection requests can be properly delivered to an expected sandbox through the NAT device by monitoring port listening states of each sandbox and changing network routing dynamically. We show several analysis cases using our method, including the ZeroAccess case, in which nearly 5 million hosts suspected to be infected by ZeroAccess malware are identified by observing its P2P communications between the sample executed in the sandbox and the infected hosts in the Internet.

1　はじめに

スパムメールや Dos 攻撃のようなインターネット上の大規模な不正活動は，ボットネットを利用して効率的に行われている．ボットネットは攻撃者により制御されるマルウェア感染ホストからなるネットワークであり，攻撃命令を出す指令サーバ，これらのサーバの追跡を困難にする為のプロキシサーバやマルウェア配布用のサーバなどからなる．

我々はこのように攻撃者によって操作されるマルウェアの振る舞いを解析するため，実行環境内でマルウェア検体を長期解析し，その挙動を観測することを試みているが，多数のマルウェア検体の長期動的解析を行うためには計算機資源とネットワーク資源の効率的利用が重要である．前者については，仮想化技術の効率的利用により，限られた実マシン上に多数の実行環境を実現する方法を提案している[4]．本稿ではネットワーク資源としてマルウェア実行環境（以降，実行環境）がインターネット接続に用いるグローバル IP アドレスに着目する．

基本的には NAT により限られたアドレスを多数の実行環境で共有するが，この際，インターネット側から接続要求が各実行環境に届かないという問題点がある．そのため，ポート待ち受け状態となり，外部からの接続要求に応えて動作するマルウェアの挙動が観測できない．そこで，各実行環境のポート待ち受け状態を監視し，その状況に応じてNATを実現しているルータのルーティングを自動変更することで，外部からの接続要求が適切に実行環境に届く仕組みを提案する．また，外部からの要求を実行環境に転送しない従来方式に比べ，提案方式が有効に働き，解析結果に大きな影響を与える実マルウェアの解析例をいくつか示す．

本論文の構成は以下のとおりである．まず，2章で先行研究とその問題点について説明する．3 章で提案方式を詳細に説明し，4 章では 3 章の提案方式に対する評価実験について述べる．5 章では，評価実験結果について考察を述べ，最後に，6 章でまとめと今後の課題を述べる．

2　マルウェア動的解析時の外部からの接続要求の重要性

マルウェア動的解析は解析対象のマルウェア検体を解析用の実行環境内で動作させて，その挙動を観測する手法であり，マルウェアを用いた攻撃の動作の把握や攻撃先の特定には，効率的な手法といえる．ボットのように攻撃者に操作されて動作するマルウェアの通信を観測し，感染ホストを検知する手法が多数検討されている．

また，動的解析は，完全に隔離された環境（閉環境）で行われるもの[3]と，実インターネットへ接続が許可された環境（開環境）で行われるものがある．前者は，インターネットに接続できないため，攻撃者の指令を受けて行われる不正活動を観測できず，一方後者は，インターネットへのアクセスを許可されているため多くの情報を得られるが，外部に攻撃等の悪影響を与えるリスクがある．近年では，インターネットへの接続を制御し，擬似サーバを含む半開環境で解析を行うもの[1,2,4,5]が主流である．

これらのインターネット接続型動的解析においては，実行環境からインターネット上のホストに対して開始される通信だけでなく，インターネット上のホストから実行環境に対して開始される通信が重要となる場合がある．例えば，解析対象の検体がプロキシサーバや Web サーバといったサーバ機能を有する場合や，P2P 通信を行う場合には，外部ホストから実行環境に対してセッションが開始される場合がある．

本稿では，多数の実行環境が限られたグローバル IP アドレスをNATにより共有してインターネット接続を行っている状況を想定し，このような場合でも外部からの接続要求を適切に処置する手法を提案する．

3　提案方式

本章では，多数の実行環境をインターネット

接続する際，限られたグローバル IP アドレスを共有するために NAT を利用することを想定し，このような場合にもインターネット上のホストからの接続要求が各実行環境に適切に転送される仕組みを提案する．具体的には，各実行環境のポート待ち受け状態を監視し，状況に応じてルータのルーティングを動的に制御することによって，外部からの接続を待ち受けするマルウェア検体の解析を行えるようにする．3.1 節では並列動的解析環境について説明し，3.2 節では提案方式を説明する．

3.1 並列動的解析環境

並列動的解析環境(図 1)は，並列解析環境サーバ，L2 スイッチ，ルータ，管理サーバといった機器により構成する[4]．

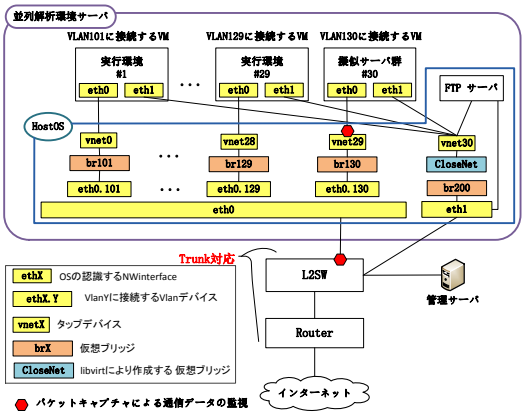

図1. 並列動的解析環境構成図

並列解析環境サーバは仮想化技術により多数の実行環境を実現している．現在構築済みのシステムでは 1 台の並列解析環境サーバ上に 29 個の実行環境（図 1 の実行環境#1～実行環境#29）を動作させることができる．Host OS(CentOS5.9)上で，iptables[15]を利用し，危険性が高い通信を擬似サーバ群（図 1 の擬似サーバ群#30）に転送する．危険度の判定には参考文献[1]の手法等を利用する．さらに各実行環境間は仮想ネットワークで接続されており，タグ VLAN を導入する．ルータ側では，VLAN 間の通信をブロックすることで，各実行環境がお互いに通信することを防ぎ，独立したネットワーク環境でマルウェア検体を解析できるようにしている．また，実行環境群はルータの外側の NIC に割り当てられたグローバル IP アドレスを NAT により共有している．

管理サーバは L 2 スイッチを流れるトラヒックのキャプチャや各ネットワーク・サーバ機器の運用管理等を行う．Host OS 上の FTP サーバは動的解析時の設定ファイルやバッチファイルなどを一時保存するために用いる．

3.2 提案方式

図 2 に，提案方式による各実行環境の待ち受け状態監視とルーティング設定変更の流れを示す．

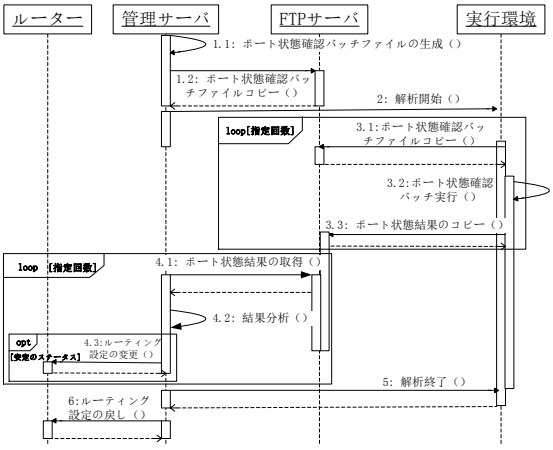

図 2. 提案方式におけるポート待ち受け監視とルーティング設定変更処理の流れ

(1.1)まず各実行環境に応じたポート状態確認用のバッチファイル（以降，バッチファイル）を生成する．バッチファイル内ではポート状態確認用コマンドとして「netstat」を使い，「-ano」オプションを付けて，ポート状態及び対応するプロセス ID を取得する．また，当該コマンドの実行間隔と実行回数もバッチファイル作成時に設定できるようにする．

(1.2)生成されたバッチファイルを FTP サーバに転送する．

(2)解析を開始する．

(3.1-3.2)FTP サーバに格納されたバッチファイルを実行環境にコピーし，これを実行する．

(3.3) バッチファイル実行の結果を FTP サーバに保存する．手順 3 を(1.1)により設定され

た実行回数に達成するまで，繰り返す．

(4.1) 上記のステップ 3.3 により FTP サーバに保存されたポート待ち受け状態監視結果ファイル（以降，結果ファイル）を管理サーバにコピーする．

(4.2)上述のとおり，ポート待ち受け状態確認コマンドの実行回数は任意に設定できるため，複数の結果ファイルが存在する場合がある．そこで，一定時間経過すると，FTP サーバに新しい結果ファイルが生成されているかをチェックし，新しいファイルがある場合にはこれを取得し，事前に取得されたベース結果ファイル（マルウェアを解析する前のポート待ち受け状態）と比較し，マルウェア実行により待ち受け状態となった TCP 及び UDP のポートリストファイルを出力する．

(4.3)ステップ 4.2 で得られるポートリストファイル群の中で一定回数以上現れた待ち受けポートのみ，ルータ上で開放設定を行う．一方，開放されたポートで待ち受けをしなくなったら，当該設定を削除する．なお，複数の実行環境で同一のポートで待ち受けを始めた場合，事前に設定した優先順位に従い，転送設定を行う．手順 4 も，(1.1)で設定された実行回数分繰り返す．

(5)動的解析を終了する．

(6)当該実行環境に対するルーティングの設定を削除する．

4 評価実験

評価実験では，NAT においてポート開放処理が行われない環境(以降，ポート非開放環境)と，提案方式のポート開放の環境(以降，ポート開放環境)とで得られる解析結果の違いに着目する．Virus Total[12]から提供を受けた 189 検体と低対話型ハニーポット Nepenthes で 2007 年 8 月から 2010 年 7 月の間に収集した 36 検体，合計 225 検体に対して，事前実験として 10 分間の動的解析を行い，ポート待ち受け状態が確認できた 22 検体のうち，通信量が多い ZeroAccess，Pramro，Zeus の 3 検体を選定して実験対象とした．検体情報を表 3，表 4，表 6 に示す．

4.1 実験環境

ポート開放環境には 3 章で説明した並列動的解析環境を用いた．ポート開放環境の設定を表1に示す．なお，当該環境はマルウェアのホストベース挙動を観測するための API フック機能を有している．

表 1. ポート開放環境

実行環境 OS/SP	Windows XP/SP3
ポート開放	する
API フック機能	あり
ISP 回線	回線 1

ポート非開放環境の設定を表 2 に示す．ポート非開放環境では，API フック機能の実装は準備が間に合わず行っていない．また，ポート開放環境と同じ ISP 回線を使うと互いの実験結果が干渉する恐れがあるため，別の ISP 回線を用いた．

表 2. ポート非開放環境

実行環境 OS/SP	Windows XP/SP3
ポート開放	しない
API フック機能	なし
ISP 回線	回線 2

4.2 解析結果の比較

ZeroAccess, Pramro, Zeus の 3 検体のポート開放環境とポート非開放環境での解析結果を比較する．

ZeroAccess は独自の P2P 通信により感染ホスト間で通信を行い，攻撃者からの命令を実行したり自身を更新しつつ，クリック詐欺や Bitcoin の採掘をすることにより金銭を取得することが報告されている[6]．

表 3. ZeroAccess 検体情報

検体名	ZeroAccess.ib（McAfee[8]）
MD5 値	cd10050574974a441cc89d1a5a41ba59
解析期間	（開）2013/07/21~29, 08/02~14(22days) （閉）2013/08/02~23(22days)
待ち受けポート	16471/tcp,16471/udp

当該検体の待ち受けポートは TCP，UDP と

もに 16471 番である．表中の(開)はポート開放環境で，(非)はポート非開放環境を指す．なお，以降の表でも同様に記述する．解析環境の運用の都合から 2 つの実験環境における解析期間がずれているが，以降では同じ日数分(22 日分の通信データ)を用いて比較を行う．なお，ポート開放環境は，07/30~08/01 の間，ルータの再起動により，ルーティング設定が失われており，ポート開放状態になかったため，比較対象外とする．

実験で得られたプロトコル別通信先数について，図 3~6 に示す．図中の枠内の数字は，図 5 では，問い合わせたドメイン数を表しており，その他の図では，実行環境と通信したホスト数を表している．

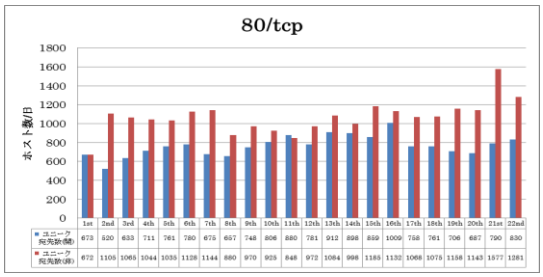

図 3. 宛先ホスト数の推移(80/tcp)

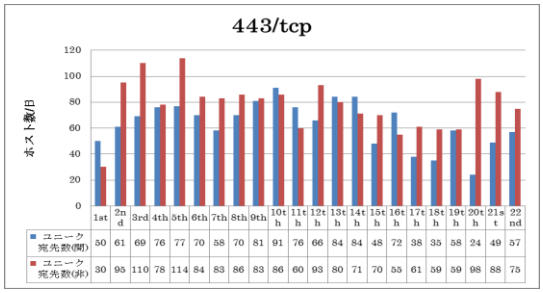

図 4. 宛先ホスト数の推移(443/tcp)

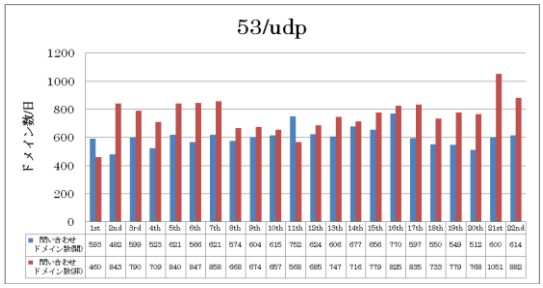

図 5. 名前解決されたドメイン数の推移

まず，ZeroAccess のクリック詐欺に関わると思われる通信，80/tcp，443/tcp に関して，通信先ホスト数の推移の比較を図 3，図 4 に示す．また，名前解決されたドメイン数の推移の比較を図 5 に示す．2つの実行環境で通信先ホスト数に大きな差は見られないものの，80/tcp 宛の通信先数及び名前解決されたドメイン数はポート非開放環境の方が若干大きくなった．この原因については調査中である．

次に，P2P 通信に関する比較を図 6 に示す．P2P 通信については，時間の経過に伴い宛先数に関して 2 つの環境の解析結果に大きな差が見られた．すなわち，ポート開放環境において宛先数が劇的に増加したのに対してポート非開放環境では大きな変化はなかった．このことについて考察する．ZeroAccess の P2P ネットワークには一般ノードとスーパーノードが存在している[6]．スーパーノードの役割は重要であり，ZeroAccess 感染ホスト群の IP アドレスリストの情報をスーパーノード間でシェアしつつ，一般ノードからの IP アドレスリスト取得要求に応じて最新の情報を送信する．そのため，外部からの接続要求に応じられる感染ホストがスーパーノードとして機能することとなる．ポート開放環境では外部からの接続要求を受信できるため，実行環境がスーパーノードとして機能しており，そのために多数の感染ホスト群と通信を行っているものと推測される．なお，実行環境とこれらの外部ホスト群は相互に P2P 通信のパケットを送受信していることから，これらの外部ホスト群は ZeroAccess 感染ホストである疑いが濃厚である．図 7 に本実験により観測された通信先ホスト数の累計を示す．2013/08/23 までの解析により約 136 万ホストが観測された．なお，実行環境と同じように 16471/udp へのアクセスに対して応答し，スーパーノードとして動作していると推測されるホスト数は約 28 万である．

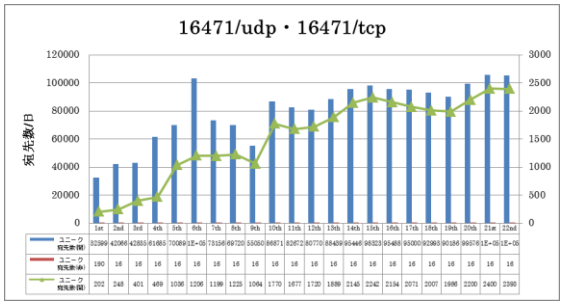

図 6. ZeroAccess の P2P 通信の宛先ホスト数の推移

また，今回の評価実験とは独立して，提案方式を用いて同一のマルウェアを 1 ヶ月半(2013/05/23~2013/07/08)に渡り解析した先行実験の結果を図 8 に示す．上記と同様の判定基準に基づく感染疑いホスト数は累計約 480 万台観測され，そのうちスーパーノードとして機能していると思われるホスト数は約 70 万台となった．

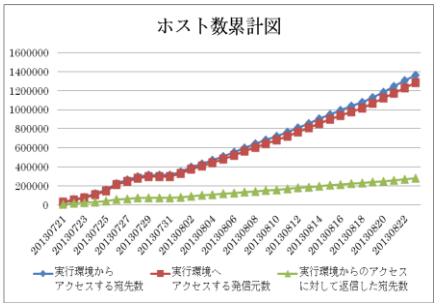

図 7. ZeroAccess の P2P 通信の宛先ホスト数累計

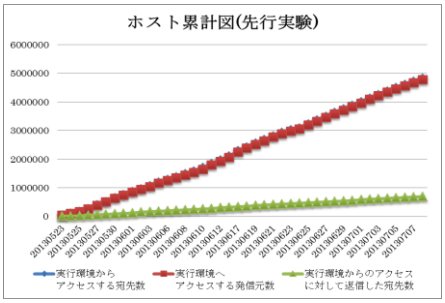

図 8. ZeroAccess の P2P 通信の宛先ホスト数累計（先行実験）

Pramro は，感染ホスト上でプロキシサーバとして動作し，攻撃者によって悪用されることが知られている[10]．解析した Pramro 検体の情報を表 4 に示す．

表 4. Pramro 検体情報

検体名	Trojan.Pramro(Symantec[9])
MD5 値	422f9bee95ca41ca31efdc77b6557f02
解析期間	2013/08/09 ~23(15days)
待ち受けポート	(開)6593/tcp, 15423/tcp, 15421/udp (閉)1570/tcp, 11353/tcp, 11351/udp

当該検体を実行すると 3 種類のポートで待ち受けを始める．待ち受けポート番号は実行の度に異なる．解析時の待ち受けポートは，ポート開放環境では，6593/tcp，15423/tcp，15421/udp，ポート非開放環境では，1570/tcp，11353/tcp，11351/udp であった．また，解析期間は 2013/08/09~23 の 15 日間である．ポート開放環境は，08/16~17 の間，約 15 時間，シャットダウンしたため，この間，観測されたデータが少なくなった．

Pramro 検体を二つの実験環境上で解析して得られた通信先のホスト数及び名前解決を行ったドメイン数を表 5 に示す．表 5 から，TCP の通信に対して，二つの実験環境の解析結果が大きく異なっている．ポート開放環境では，SMTP(25/tcp)，HTTPS(443/tcp)の通信があり，また HTTP(80/tcp)の通信量がポート非開放環境より遥かに大きい．加えて，その他の TCP ポート(多くはハイポート)に対し，通信先ホスト数はポート開放環境がポート非開放環境の約 2 倍となっている．

次に開放したポートのうち，どのポートへのアクセスがあったかについて図 9 に示す．開放した 6593/tcp，15423/tcp，15421/udp のうち 15423/tcp と 15421/udp へのアクセスは全くなく，08/11 にポート待ち受け状態でなくなった．一方，6593/tcp へのアクセスは定常的に発生しており，一日当たり，約 1000 台の外部ホストがアクセスしており，プロキシサーバとして動作していた可能性が高い．毎日，アクセスしたホストは約 5%の 50 台で，約 95%は新たなホストからのアクセスであった．攻撃者は何らかの方法で実行環境のグローバル IP アドレスをプロキシが動作しているアドレスとして情報共有しているものと思われる．また，毎日，80/tcp でアクセスするホストは一つであり，一日当たり，約 2000 パケットを通信している．通信内容は暗号化されており，詳細は不明である．

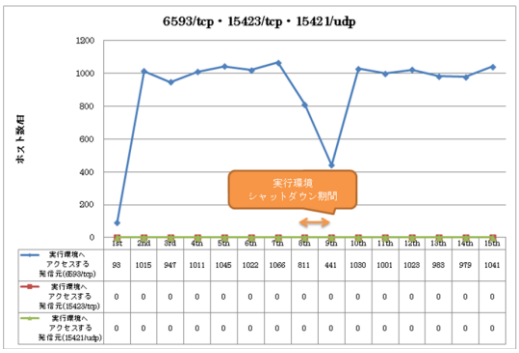

図 9. Pramro 検体の待ち受けポートへアクセスしたホスト数の推移

表 5. Pramro 検体:宛先ホスト数及び問い合わせたドメイン数

	TCP								UDP			
	SMTP		HTTP		HTTPS		OTHER		DNS		OTHER	
日付	(開)	(非)	(開)	(非)	(開)	(非)	(開)	(非)	(開)	(非)	(開)	(非)
20130809	106	0	5	4	8	0	139	236	4	5	1	2
20130810	1092	0	200	1	55	0	1647	765	0	0	1	1
20130811	651	0	110	1	14	0	1552	743	1	0	1	1
20130812	1047	0	121	1	13	0	1723	729	0	0	0	0
20130813	1187	0	124	1	52	0	1714	745	0	0	0	0
20130814	1407	0	112	1	54	0	1687	734	0	0	0	0
20130815	1617	0	172	1	26	0	1770	678	0	0	0	0
20130816	1057	0	70	1	4	0	1520	762	0	0	0	1
20130817	547	0	25	1	0	0	712	733	0	0	0	0
20130818	1221	0	146	1	5	0	1722	758	0	0	0	0
20130819	1136	0	112	1	0	0	1613	752	0	0	0	0
20130820	1164	0	157	1	2	0	1747	745	0	0	0	0
20130821	1045	0	49	1	1	0	1689	730	0	0	0	0
20130822	638	0	138	1	6	0	1712	751	0	0	0	0
20130823	1166	0	78	1	2	0	1775	741	0	0	0	1

Zeus はブラックマーケットで入手可能なツールキットを使って作成される場合が多く，主にスパム送信とドライブバイダウンロードを介して配布される[11]．今回解析した Zeus 検体は P2P らしい通信を行っていることから，ZeuS-P2P[7]の可能性が高い．

表 6. Zeus 検体情報

検体名	Trojan.Zbot(Symantec)
MD5 値	b3fa77fe874f86ec7f7dd09151f39460
解析期間	2013/08/02~07(6days)
待ち受けポート	(開)12360/tcp, 13558/udp (閉)24514/tcp, 13699/udp

解析した Zeus のマルウェア検体の情報を表 6 に示す．当該検体の待ち受けポートも検体を実行する度に変わる．解析時の待ち受けポートは，ポート開放環境では，12360/tcp, 13558/udp，ポート非開放環境では，24514/tcp, 13699/udp である．解析期間は 2013/08/02~07 の 6 日間である．

表 7. 開放するポートへのアクセスするホスト数

日付	20130802~07
実行環境へ接続する発信元数(15423/tcp)	0
実行環境へ接続する発信元数(15421/udp)	0

ポート開放環境では，検体が待ち受け状態にあるポートを開放したが，当該ポートへの外部ホストからのアクセスはなかった(表 7)．また当該検体からアクセスした外部ホスト数および名前解決を行ったドメイン数についても，二つの環境で差異は見られなかった(表 8)．

表 8. Zeus 検体がアクセスした宛先ホスト数及び名前解決したドメイン数

	TCP		UDP			
	HTTP		DNS		OTHER	
日付	(開)	(閉)	(開)	(閉)	(開)	(閉)
20130802	7	10	1004	1002	16	17
20130803	34	36	1002	1002	17	17
20130804	30	33	1002	1002	17	17
20130805	26	34	1002	1002	16	17
20130806	31	35	1002	1002	17	17
20130807	26	37	1167	2002	17	17

5 考察

4 章の評価実験の結果から，ZeroAccess 及び Pramro 検体については提案手法であるポート開放環境の有効性が確認できた．一方，Zeus 検体については，ポート待ち受け状態となるものの，ポート開放環境とポート非開放環境で観測結果に大きな差異は見られなかった．なお，実験環境の準備の都合上，ポート開放環境とポート非開放環境では API フック機能の有無の点で異なっており，これが解析結果に影響したことは否定できないが，通信観測結果からポート開放が解析結果に与えた影響が大きいと考える．また，Pramro 検体は解析期間内で，ポート待ち受け状態が変わったことが確認された．このようなケースに対応するために，継続

的にポートの待ち受け状態を監視することが必要といえる.

なお, 提案手法は, 実行環境が待ち受け状態にあるポートの情報を取得し, 当該ポートをルータ上で開放するが, マルウェアの中にはUPnP(Universal Plug and Play)[13]を利用し, ルータなどゲートウェイ機器のルーティング設定を変更し, 外部ホストからの接続要求を受信できるようにする場合がある. このようなマルウェアに対応するため, ルータの設定自体も常時監視し, マルウェアによる設定変更に対しても適切に対処する必要がある.

6 まとめと今後の課題

本稿では, 実行環境のポート待ち受け状態を監視し, その状況に応じてNATを実現しているルータのルーティングを自動変更する解析手法を提案した. また, 外部からの接続要求に応えて動作するマルウェアの挙動を観測できることを確認した. 特にZeroAccessの解析実験では, 当該マルウェアへの感染が強く疑われる500万近いホストを発見した.

今後の課題は, 同時に複数の実行環境が同一のポート番号で待ち受け状態となった場合の対応や, 同一グローバルアドレスの継続使用によるIPクローキング等の影響の調査である.

謝辞 本研究の一部は, 総務省情報通信分野における研究開発委託／国際連携によるサイバー攻撃の予知技術の研究開発／サイバー攻撃情報とマルウェア実体の突合分析技術／類似判定に関する研究開発により行われた.

参考文献

[1] K. Yoshioka and T. Matsumoto, "Multi-pass Malware Sandbox Analysis with Controlled Internet Connection,"IEICE Trans. Vol. E93-A, no.1, pp. 210-218, 2010.
[2] 青木一史, 川古谷裕平, 岩村誠, 伊藤光恭, "半透性仮想インターネットによるマルウェアの動的解析", コンピュータセキュリティシンポジウム論文集, pp.1-6, 2009.
[3] D.Inoue, K.Yoshioka, M.Eto, Y.Hoshizawa, K.Nakao, "Automated Malware Analysis System and Its Sandbox for Revealing Malware's Internal and External Activities", IEICE Trans. Vol. 92-D, pp.945-954, 2009.
[4] 鉄穎, 田辺瑠偉, 水戸慎, 神薗雅紀, 星澤裕二, 吉岡克成, 松本勉, "多数のマルウェア検体を並列解析可能な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 2012 論文集, Vol.3, pp.728-735, 2012.
[5] 田辺瑠偉, 鉄穎, 水戸慎, 牧田 大佑, 神薗雅紀, 星澤裕二, 吉岡克成, 松本勉, "長期動的解析によるマルウェアの特徴的な DNS 通信の抽出",コンピュータセキュリティシンポジウム 2012 論文集, Vol.3, pp.712-719, 2012.
[6] James Wyke, " The ZeroAccess Botnet: Mining and Fraud for Massive Financial Gain", Sophos Technical Paper, 2012.
[7] Cert POLSKA Technical report, "Zeus-P2P monitoring and analysis", 2013.
[8] McAfee, http://www.mcafee.com/japan/.
[9] Symantec, http://www.symantec.com/.
[10] Win32/Pramro, http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32/Pramro.
[11] Trojan.Zbot, http://www.symantec.com/ja/jp/security_response/writeup.jsp?docid=2010-011016-3514-99.
[12] VirusTotal, http://www.virustotal.com/jp/
[13]UPnP, http://www.upnp.org/.
[14] Daniel Garcia, "Universal plug and play (UPnP) mapping attacks", http://toor.do/DEFCON-19-Garcia-UPnP-Mapping-WP.pdf.
[15] IPTABLES, http://linuxjm.sourceforge.jp/html/iptables/man8/iptables.8.html