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

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†

†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

{tanabe-rui-nv, tie-ying-fc, mito-makoto-xy, makita-daisuke-jk, yoshioka, tsutomu}@ynu.ac.jp

‡セキュアブレイン

102-0083 東京都千代田区麹町 2-6-7

{masaki_kamizono, yuji_hoshizawa}@securebrain.co.jp

あらまし 我々は，広域ネットワークモニタリングと長期的なマルウェア動的解析を融合することで，マルウェアの活動を大域的かつ詳細に追跡する技術の研究開発を進めている．本稿では，マルウェアの特徴的なDNS通信を動的解析により抽出し，観測対象ネットワークのキャッシュDNSサーバのトラヒックと比較することでマルウェア感染ホストを検出する方法を検討する．具体的には，動的解析環境内でマルウェア検体を数日から数か月間継続的に動作させたり，同一検体を独立な実行環境で並列に動作させたり，同一検体を数十回連続して短期間実行した際のDNS通信をそれぞれ観測し，感染ホスト検出を行う上で有効な検知用シグネチャを導出するための基礎データを取得した．前述の実験の結果，(1)同一の検体が数週間の観測期間で継続的かつ定期的に名前解決する固定ドメイン群 (2)実行環境や実行時刻が異なる場合でも同一検体が必ず名前解決を行う固定ドメイン群 (3)スパムメール送信先アドレスのドメインに関する大量の名前解決 (4)スパム送信時にオープンリレーサーバ等にアクセスするための名前解決 (5)大量かつ継続的な名前解決失敗など，検知用シグネチャとして利用できる可能性があるDNS通信が多数観測できた．

Extracting Signatures from Malware DNS Traffic by Long-Term Sandbox Analysis

Rui Tanabe† Ying Tie† Makoto Mito† Makita Daisuke†

Masaki Kamizono‡ Yuzi Hoshizawa‡ Katsunari Yoshioka† Tsutomu Matsumoto†

†Yokohama National University

79-7 Tokiwadai, Hodogaya-ku, Yokohama-shi, Kanagawa, 240-8501 Japan

{tanabe-rui-nv ,tie-ying-fc ,mito-makoto-xy ,makita-daisuke-jk, yoshioka, tsutomu}@ynu.ac.jp

‡Secure Brain

2-6-7 Koujimati, Tiyoda, Tokyo 102-0083, Japan

{masaki_kamizono ,yuji_hoshizawa}@securebrain.co.jp

Abstract In this paper we investigate DNS traffic from long-term malware sandbox analysis to

derive signatures to detect infected hosts from traffic at cache DNS server. In order to decide what characteristics we should focus in order to detect malware infected hosts, we observed DNS traffic of malware samples executed in the sandbox in various settings such as monitoring the same sample for days and months, monitoring the same sample executed in several independent sandboxes at the same time, and monitoring the same sample for tens of times for a short period. As a result, we noticed many characteristic DNS traffic that can be used as a signature to detect infected hosts such as: (1) a fixed set of domains that are resolved by the same sample every several hours for months (2) a fixed set of domains that the same malware always resolves in every instance of its execution (3) very frequent and constant queries to resolve domains of spam mail targets (4) queries for open relay mail servers, and (5) very frequent and constant name resolution failure.

1　はじめに

情報漏洩，スパムメール，フィッシング，サービス妨害攻撃などのセキュリティ脅威の多くは，攻撃者によって遠隔から操作されるマルウェア感染ホスト群によってもたらされていると言われている．我々は，こうしたマルウェア感染ホスト群と攻撃者の不正活動を，国際的な連携により広域的かつ詳細に把握し，攻撃の予知を目指す PRACTICE（Proactive Response Against Cyber-attacks Through International Collaborative Exchange）プロジェクトを推進している．PRACTICE では，ダークネット，ハニーポット，クライアントハニーポットによるモニタリング，連携先組織における DNS サーバトラヒックの分析，スパムメール分析，ライブネットワーク観測といった多角的なネットワーク観測により攻撃者の動向を広域的に把握する「マクロ観測」を検討している．同時に，これらの攻撃の原因となっているマルウェアの検体を取得し，外部ネットワークに接続した動的解析環境内で長期間動作させることで，攻撃者に制御されるマルウェア感染ホスト群の一員として不正活動を観測する「ミクロ観測」の技術開発を進めている．さらに，マクロ観測とミクロ観測の両アプローチで得られた情報の突合を行うことで，脅威のメカニズムをより正確に把握することを目指している．

本研究では，特にマクロ観測データとして，連携先組織内キャッシュ DNS サーバのトラヒックを想定し，この中からマルウェア感染ホストを検出するため，ミクロ観測において得られるマルウェアの特徴的な DNS 通信をシグネチャとして利用する方法について検討した．

具体的には，マルウェア動的解析環境内で同一検体を数日から数か月間継続的に動作させたり，同一検体を独立した実行環境で長期間並列に動作させたり，同一検体を同一環境で数十回連続して短期間実行し，それぞれの環境で検体が行う DNS 通信を観測・比較した．その結果，(1) 同一検体が数週間の観測期間で継続的かつ定期的に名前解決する固定のドメイン群 (2)実行環境や実行時刻が異なる場合でも同一検体が必ず名前解決を行う固定ドメイン群 (3)スパムメール送信先アドレスのドメインに関する大量の名前解決 (4)スパム送信時にオープンリレーサーバ等にアクセスするための名前解決 (5)継続的かつ大量の名前解決失敗など，シグネチャとして利用可能と思われる特徴的な DNS 通信が多数確認できた．

以降，2 章で関連技術を紹介し，3 章では実験に用いたマルウェア動的解析環境について述べる．4 章では観測された特徴的な DNS 通信について考察を行う．最後に，5 章でまとめと今後の課題を述べる．

2　関連技術

マルウェアを解析する技術の 1 つに，解析環境内でマルウェアを実際に動作させ，その挙動を観測するマルウェア動的解析が存在する．マルウェア動的解析の代表的なものとして NORMAN Sandbox[14], GFI Sandbox[12], Anubis[13]など

が挙げられる．論文[19]では攻撃者が操作するC&C サーバなどの応答の変化に応じたマルウェア検体の挙動の変化を観測するため，マルウェアが行う通信をダミークライアントにより模擬し，効率的に長期的な挙動観測を行う手法が提案されている．

また，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．論文[15,17]ではボットに感染したホスト群が C&C サーバから命令をうけ協調して動作する特徴を用いて検知する手法が提案されている．さらに，ボット感染ホストの多くがC&C サーバのドメイン名を共通して名前解決する挙動を用いた検知手法[4]やボット感染ホストが送信する DNS クエリの順番やシーケンスを用いた検知手法[8]，ボット感染ホストの DNS トラフィックからその挙動に類似した挙動を示すホストを検出する手法[10]が提案されている．このように多くの先行研究が存在するが，インターネット上で流通するマルウェアの変遷は著しく，既存研究において感染ホスト検知に用いられている手法が現在も十分に有効性をもつかを検証する価値がある．また，既存研究では注目されていない特徴的な通信が存在する可能性がある．そこで本研究では，実際に攻撃者から指令を受けて不正活動を行う検体の動作を解析して特徴的なDNS 通信を抽出する．

3　マルウェア動的解析システム

本章では DNS 通信の観測のために用いたマルウェア動的解析システムについて説明する．当該システムの全体図を図 1 に示す． システムは CentOS v5.5 が動作する 1 台のハードウェアマシン上に実装した．

第一犠牲ホスト: 第一犠牲ホストはマルウェア検体を実行し，感染時に発生するマルウェア検体による様々な通信や内部挙動を観測するためのホストである．第一犠牲ホストには VMware Server v1.0.1 のゲスト OS (WindowsXP Professional SP1)を用いた．

アクセスコントローラ: アクセスコントローラは，第一犠牲ホスト上でマルウェアが行う通信を擬似インターネットまたは実インターネットへと転送する役割を持つ．事前に設定されたフィルタリングルールに従い，マルウェアが行う通信のうち，リモートエクスプロイトなど危険性の高い通信については擬似インターネットへ転送し，それ以外の通信は実インターネットへと転送する．アクセスコントローラは Linux のパケットフィルタリングツールである iptables を用いて実装した．

擬似インターネット: 擬似インターネットは，実インターネット上のサーバを模擬することでマルウェアに対してネットワークサービスを提供する．疑似インターネット上では様々なダミーサーバを動作させることが可能だが，本動的解析システムでは，低対話型ハニーポット Nepenthes[11]と echo サーバを動作させ，Nepenthes が待ち受けを行うポートへの通信は，Nepenthes に転送し，それ以外のポートへの通信は echo サーバに転送する設定とした．

解析マネージャ: 解析マネージャは，動的解析システムの中核として第一犠牲ホストの OS のイメージの管理，解析対象マルウェアの管理，アクセスコントローラの設定，擬似インターネット中の各種サービスの管理，通信ログのキャプチャ，解析結果の出力を行う．

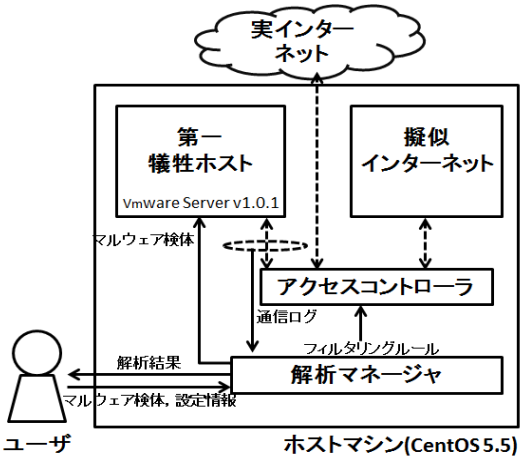

図 1. 実験に用いたマルウェア動的解析システム

4　動的解析による特徴的な DNS 通信の観測

本章では，3 章で説明した実験環境を用いて様々な状況でマルウェア検体を動的解析し，観測された特徴的な DNS 通信について説明する．4.1 節で実験目的について説明し，4.2 節で具体的な実験方法，4.3 節で実験結果として得られた特徴的な DNS 通

信について，検知用シグネチャとしての利用可能性の考察を行う．

4.1 実験目的

本研究の目的はキャッシュ DNS サーバのトラヒックからマルウェア感染ホストを検知することであるが，近年のマルウェアはステルス性が高いものがあり，感染から長期間が経過しても駆除されずに動作を続けていることが想定される．そこで今回の実験では数週間から数か月に渡り，マルウェア検体を解析環境内で継続的に動作させることで，上記のような長期間感染状態のホストの挙動を推測する．

しかしながら，ある検体について単一の実行環境で長期間挙動解析を行ったとしても，観測された挙動の一般性は明確でなく，したがって検知用シグネチャとしての有用性も不明である．そこで，同一検体を独立した複数の実行環境で実行・観測し，そのいずれにおいても観測される特徴を抽出することで，一般性の高い特徴を明らかにする．理想的には，同一の検体を様々な設定や状態の実行環境で様々な時刻に実行し，いずれの状況においても観測される共通の特徴を抽出することが望ましいが，実験に利用できる実行環境の数は限られているため，本実験では，同一検体を 2～3 の独立した実行環境で長期間動作させる実験と，同一検体を短時間実行・観測する試行を数十回繰り返す実験を行った．具体的な実験方法は次節にて説明する．

4.2 実験方法

検体 低対話型ハニーポット dionaea[18]と Nepenthes で 2007 年 8 月から 2010 年 7 月の間に収集した 491 検体と Virus Total[7]から提供を受けた 10 検体，合計 501 検体に対して，事前実験として 60 秒間の動的解析を行い，名前解決や通信量が多く，80/tcp や 65520/tcp 番ポート等でインターネット上のホストと通信を行った 3 検体を選定して実験対象とした．表 1 に検体一覧を示す．以下では簡単のため 3 検体をそれぞれ Spybot, Zbot, Virut と呼ぶこととする．なお，これらの検体の収集時期は解析実験実施時期の 2 年以上前であるが，実際には，実行後に攻撃者のマルウェア配布サイトから新たな実行可能ファイルをダウンロードして実行しており，攻撃者からの命令に基づき様々な不正活動を行っていることから，本実験結果は最近のマルウェアの動向を反映していると考える．

実験方法 数日から数週間に及ぶ長期動的解析を，各検体について独立に 3 回行った(表 2)．以降では，各検体について n 回目の長期動的解析実験を長期解析実験 n と呼ぶこととする．例えば，Spybot の長期解析実験 1 の期間は表 2 の通り，2012/5/17 から 2012/7/15 である．なお，以降の年月の記載では特に断らない限り西暦は 2012 年とする．また，各検体に対して 15 分間の短時間の動的解析を 50 回独立して行った．この実験を以降では短期解析実験と呼ぶこととする．なお，解析環境のアクセスコントローラの設定は，リモートエクスプロイト攻撃に利用される 135/tcp, 139/tcp, 445/tcp, 1025/tcp, 5000/tcp 番ポートへの通信についてはダミーサーバへ転送し，上記以外のポートへの通信は全て実インターネットへ接続を許可するようにした．また，インターネット接続用に 2 つの異なる ISP のブロードバンド回線 ISP1, ISP2 を用意した．

表 1. 実験で使用した検体の一覧

McAfee/Symantec	MD5ハッシュ値
W32/Bobax.worm.gen W32.Spybot.Worm	3b7eb30a8309d9ec39ce22f07c958f15
PWS-Zbot.gen.aac Trojan Horse	65dc0682604e08c4bb2201ea67204181
W32/Virut.gen.a W32.Virut.W	017f3b27048857ffd08495fb6d58da4e

表 2. 長期動的解析の実施期間

	長期解析実験1	長期解析実験2	長期解析実験3
Spybot	5/17～7/15 8週間 ISP 1	6/9～6/14 5日間 ISP 1	6/9～6/14 5日間 ISP 1
Zbot	7/24～7/31 1週間 ISP 2	7/18～7/19 1日 ISP 2	8/22～8/23 1日 ISP 2
Virut	6/9～6/18 1日 ISP 2	8/15～8/16 1日 ISP 1	8/24～8/25 1日 ISP 2

表 3. 短期動的解析の実施期間

	Spybot	Zbot	Virut
解析期間	6/27～7/6	8/16	8/17
解析環境	ISP1	ISP1	ISP1

4.3 実験結果

4.1 節の実験の結果，3 検体から観測された特徴的な DNS 通信についてそれぞれ説明する．

(1) 継続的かつ定期的に名前解決する固定ドメイン群

長期動的解析実験の結果，Spybot，Zbot，Virut のいずれからも観測期間中，継続的かつ定期的に名前解決を行う，各検体に固有のドメイン群が確認された(表 4，5，6)．これらのドメインから得られる接続先へは HTTP または SMTP による通信を行っていた．HTTP については，通信の内容から C&C サーバかマルウェア配布サイトと考えられる．また，mxs.mail.ru や alt4.gmail-smtp-in.l.google.com は，マルウェアがスパムメールや感染ホスト情報をメール送信する際に利用するメールサーバのドメインである．これらのドメイン群には正規ドメインも含まれているが数時間毎に定期的なアクセスを繰り返すという特徴を考慮することで，高い精度で当該マルウェアに感染したホストを検出できると思われる．

次に，これらのドメイン群の名前解決の同期性を調べるため，Spybot が定期的に名前解決するドメインの 1 つ kukutrustnet.info に注目し，長期解析実験 1，2，3 でそれぞれ当該ドメインを名前解決した時刻を図 2 に示す．図 2 からわかる通り，いずれの実験においても，同じ時間間隔で名前解決を行うものの，名前解決を行う時刻にはずれがあることがわかる．したがって，このドメインが名前解決される時刻に基づく感染ホスト検知は難しいといえる．

表 4. Spybot が定期的に名前解決するドメイン群

ドメイン名	名前解決の頻度
mxs.mail.ru	1時間おき
www.supinator1.com.	4時間おき
www.informat1onupd.info	4時間おき
www.bpfq02.com	4時間おき
www.kukutrustnet.com	4時間おき
www.g1ikdcvns3sdsal.info	4時間おき
www.kukutrustnet.info	4時間おき
www.h7smcnrwlsdn34fgv.info	4時間おき
www.hkukud123ncs.info	4時間おき
www.lukki6nd2kdnc.info	4時間おき
smtp.loaadss.pl	12時間おき
pop.loaadss.pl	12時間おき
mail.loaadss.pl	12時間おき

表 5. Zbot が定期的に名前解決するドメイン群

ドメイン名	名前解決の頻度
mail.loaadss.pl.	12時間おき
mx2.finansgroups.com.	12時間おき
mx3.finansgroups.com.	12時間おき
mx4.finansgroups.com.	12時間おき
mx5.finansgroups.com.	12時間おき
alt4.gmail-smtp-in.l.google.com.	1時間おき
gmail-smtp-in.l.google.com.	1時間おき
mail7.digitalwaves.co.nz.	1時間おき
mxs.mail.ru.	1時間おき

表 6 Virut が定期的に名前解決するドメイン群

ドメイン名	名前解決の頻度
mxs.mail.ru.	1時間おき
alt4.gmail-smtp-in.l.google.com.	1時間おき
gmail-smtp-in.l.google.com.	1時間おき

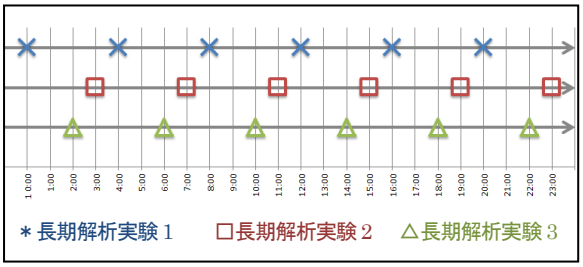

図 2. Spybot がドメイン kukutrustnet.info を名前解決した時刻の比較

(2) 同一検体が必ず名前解決を行うドメイン群

長期解析実験，短期解析実験のいずれにおいても，実行環境や実行時刻によらず，実行後に必ず名前解決を行うドメイン群が 3 つの検体それぞれに存在した(表 7，8，9)．これらのドメイン群は検体間で共通するものはほとんどなく，検体毎にユニークなドメイン群だった．表 7，8 には正規のドメイン名も含まれているため，それぞれのドメインを単一のブラックドメインとして検知に用いることはできないが，これらのドメイン群のうち一定数以上を名前解決する，といったように条件を設定することで感染ホストを検知できる可能性がある．文献[8]では，このようなドメイン群が名前解決される順序に着目し,ドメイン間の遷移をグラフとして表現することで DNS 通信の特徴を定

義している．マルウェアのコード内でリストとして保持されているドメイン群については，名前解決される順序に特徴が現れることが予想されるため，名前解決の順序に着目した感染ホスト検知は有効といえるが，名前解決の成否によってその後の挙動が変化する場合もあるため，シグネチャ作成を行う際は注意が必要である．動的解析による観測の場合，ダミーDNS サーバによりドメイン名の名前解決結果を制御することができるため，名前解決結果によってマルウェアの挙動がどのように変化するかを観測可能であることが利点といえる．また，前述の定期的に名前解決されるドメイン群と，実行後必ず名前解決を行うドメイン群には重複が多くある．これらは，感染ホスト検知用シグネチャとしても最も効果が期待できるドメイン群といえる．

表 7. Spybot が必ず名前解決を行うドメイン群

proxima.ircgalaxy.pl	www.he3ns1k.info
mxs.mail.ru	www.kukutrustnet.info
www.supinator1.com.	www.h7smcnrwlsdn34fgv.info
mail.earthlink.net	www.hkukud123ncs.info
www.informat1onupd.info	www.lukki6nd2kdnc.info
www.bpfq02.com	smtp.loaadss.pl
www.kukutrustnet.com	pop.loaadss.pl
www.f5ds1jkkk4d.info	mail.loaadss.pl
www.g1ikdcvns3sdsal.info	

表 8. Zbot が必ず名前解決を行うドメイン群

alt4.gmail-smtp-in.l.google.com.	mx2.finansgroups.com.
gmail-smtp-in.l.google.com.	mx3.finansgroups.com.
in1.smtp.messagingengine.com.	mx4.finansgroups.com.
mail.loaadss.pl.	mx5.finansgroups.com.
mail7.digitalwaves.co.nz.	mxs.mail.ru.

表 9. Virut が必ず名前解決を行うドメイン群

proxima.ircgalaxy.pl

(3) スパムメールの宛先に関する大量の名前解決

Spybot と Virut については，スパムメールを送信するために，宛先メールアドレスのドメインの名前解決を大量に行っていた．具体的には，まず宛先メールアドレスのドメインを名前解決するため MX レコードを要求する．名前解決が成功すると MX レコードに対してメールサーバのドメイン名が得られるため，そのドメインに対してさらに名前解決を行う．1 つの宛先メールアドレスに対して上記の 2 回の名前解決が発生するが，スパムメールは様々なアドレスに対して大量に送られるため，大量の名前解決が発生する．表 10 に各検体の名前解決のリクエスト数，MX レコードのリクエスト数の 1 時間当たりの平均値を示す．

表 10. DNS レコードの 1 時間当たりの平均

	Spybot 長期解析実験1	Zbot 長期解析実験1	Virut 長期解析実験1
名前解決のリクエスト数	14406	32	5218
MXレコードのリクエスト数	7268	0	2072
名前解決できなかった数	932	0.36	1177

また，Spybot の長期解析実験 1 における最初の 5 日間の DNS トラフィックを図 3 に示す．横軸は時刻，縦軸は 1 時間当たりのパケット数である．

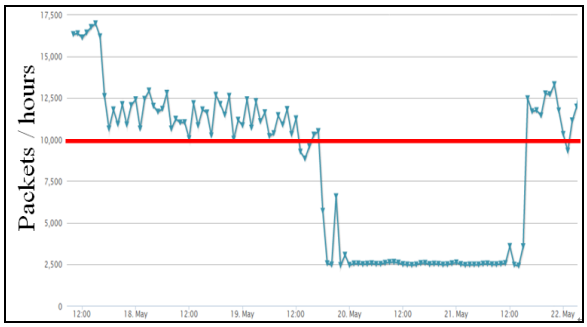

図 3. 長期解析実験 1 における Spybot の 5 日分の DNS トラフィックの時間推移

図 3 から，5 日間のうち半分以上の期間について，1 時間当たり 1 万パケット以上の大量の名前解決が定常的に発生していることが分かる(図 3 の赤線は 1 万回)．なお，名前解決回数が一時的に落ち込む期間についてはオープンリレーサーバへの接続の項で説明する．このような落ち込みは他の観測期間でも同様に観測されている．また，前述のとおり，名前解決の対象は MX レコードと A レコードがほぼ半数ずつとなっている．通常のクライアントマシンから MX レコードと A レコードについてこのような大量の名前解決が発生するとは考えにくいことから，この DNS 通信は感染ホスト検知のために有効な特徴と考えられる．

次に，長期解析実験 1 において Virut が行った名前解決数の推移を図 4 に示す．Virut の場合，1 時間当たりの名前解決数の増減幅が Spybot よりも大きいが，やはり，通常のクライアントマシンの動作とは大きく異なると思われることから，観測期間が十分であれば検出は比較的容易と思われる．

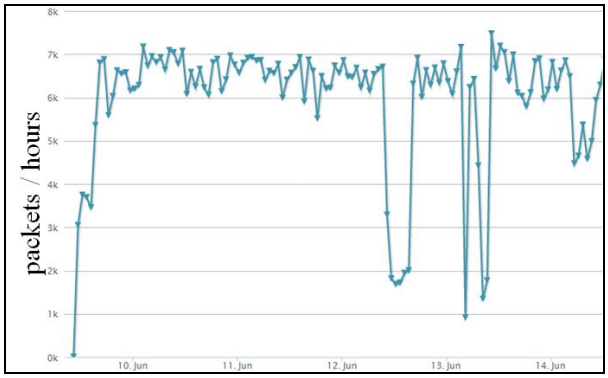

図 4. 長期解析実験 1 における Virut の DNS トラフィックの時間推移

(4) オープンリレーサーバ等の名前解決

図 3 から Spybot が行う名前解決数が急減する期間が数日間存在していることがわかる．これらの期間では MX レコードの名前解決をまったく行わなくなった．一方，25/tcp への通信は継続的に発生していることからスパムメールの送信は停止していない．この時期は，スパムメールの宛先アドレスのメールサーバに直接送信するのではなく，オープンリレーサーバや gmail などのメールサービスを用いてメールを送信していた．具体的には，まずオープンリレーサーバ等のドメインの名前解決を行い，得られた IP アドレスに対して 25/tcp で接続し，メールの送信を試みていた．これらのメールサーバへの名前解決から感染ホストを検知できる可能性があるが，正規ユーザがこれらのサーバを利用する場合も想定されることから更なる検討が必要である．

(5) 大量の名前解決失敗

表 10 から Spybot と Virut についてはドメインの名前解決が失敗し，NXDomain が返信された場合が多数確認された．名前解決に失敗したドメインを調べると Domain Generation Algorithm (DGA)[20] を用いたと思われるドメインが多数確認された．表 11 に DGA を用いて生成されたことが予想されるドメインの一部を示す．DGA を用いて生成されるドメインの多くは，対応する A レコードが存在しないため，名前解決が失敗する．図 5 は Spybot が 1 時間当たりに名前解決に失敗した回数の推移である．このように定常的に名前解決失敗が大量に発生するため，この特徴を感染ホスト検出に利用できると思われる．

表 11. Domain Generation Algorithm により生成されたことが予想されるドメイン群の例

acdgrikru.dynserv.com
ajfgffpjh.dynserv.com
anwgtctvxr.dynserv.com
bjlydbagnlu.dynserv.com
bqlevrolvaa.dynserv.com
bvqffersost.dynserv.com
celmvuqkwkn.dynserv.com
cfrntdejpqz.dynserv.com
ciwsdmi.dynserv.com

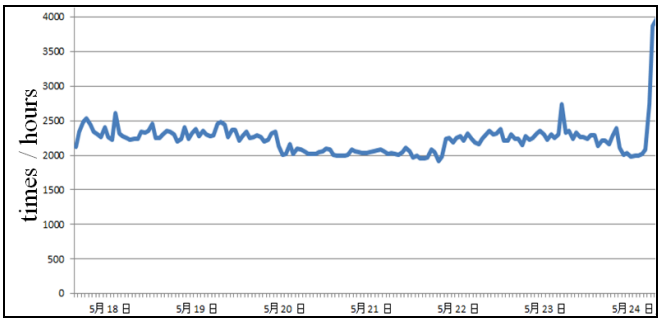

図 5. 長期解析実験 1 における Spybot の 5 日分の名前解決失敗回数の時間推移

5 まとめと今後の課題

マルウェア動的解析を同一検体に対して様々な設定や期間に実施することで特徴的な DNS 通信を観測し当該検体に感染したホストを検知するためのシグネチャとしての利用可能性を検討した．

今後は，より多くの検体で実験を行い，さらに特徴的な DNS 通信を抽出するとともに，マルウェア検知用シグネチャとして明確に定義し，実際のキャッシュ DNS トラフィックとマッチングを行うことでマルウェア感染ホストの検知を行うことである．また，動的解析中に観測された通信の内容を，より詳細に調査することで感染ホストの検知だけでなく C&C サーバの特定を行うことも検討する．また， DNS を使わずに IP アドレスを直接指定して行う不正活動の観測につい

ても本研究と並行して検討する必要がある.

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, D. Inoue, M. Eto, Y. Hoshizawa, H. Nogawa, and K. Nakao, "Malware sandbox analysis for secure observation of vulnerability exploitation," IEICE Trans. Vol. E92D, No.5, pp. 955 - 966, 2009.

[2] 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.

[3] 中里純二, 大高一弘, “nicter レポート～長期ネットワーク観測に基づく攻撃の変遷に関する分析～” 独立行政法人情報通信研究機構季報 Vol. 57, Nos. 3/4, 2011.

[4] H. Choi, H. Lee, H. Lee, and H. Kim, “Botnet detection by monitoring group activities in dns traffic,” Proc. of the 7th IEEE International Conference on Computer and Information Technology, pp. 715 - 720, 2007.

[5] McAfee, http://www.mcafee.com/japan/

[6] Symantec, http://www.symantec.com/ja/jp/

[7] VirusTotal, http://www.virustotal.com/jp/

[8] J. Lee, J. Kwon, H.J. Shin, and H. Lee, “Tracking multiple c&c botnets by analyzing dns traffic,” 2010 6th IEEE Workshop on Secure Network Protocols (NPSec), pp. 67 - 72, 2010.

[9] M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “A multifaceted approach to understanding the botnet phenomenon,” Proc. of the 6th ACM SIGCOMM conference on Internet measurement pp. 41 – 52, 2006.

[10] R. Villamarin-Salom´on and J.C. Brustoloni, “Bayesian bot detection based on dns traffic similarity,” Proc. of the 2009 ACM symposium on Applied Computing, pp.2035 - 2041, 2009.

[11] P. Baecher, M. Koetter, T. Holz, M. Dornseif, and F. C. Freiling, "The Nepenthes Platform: An efficient approach to collect malware," 9th International Symposium on Recent Advances in Intrusion Detection (RAID 2006), pp. 165 - 184, 2006.

[12] GFI Sandbox, http://www.gfi.com/malware-analysis-tool

[13] Anubis, http://analysis.seclab.tuwien.ac.at/.

[14] NORMAN Sandbox Information Center, http://www.norman.com/microsites/nsic/

[15] H. Choi, H. Lee, and H. Kim, “BotGAD: detecting botnets by capturing group activities in network traffic,” Proc. of the 4th Intl. ICST Conf. on COMmunication System software and middlewaRE, pp. 1 - 8, 2009.

[16] F. Leder, T. Werner, and P. Martini, “Proactive botnet countermeasures - an offensive approach,” Proc. of the Conf. on Cyber Warfare, CCDCoE: Cooperative Cyber Defence Centre of Excellence, 2009.

[17] G. Guofei, Z. Junjie, and W. Lee, “BotSniffer: Detecting botnet command and control channels in network traffic,” Proc. of the 15th Annual Network and Distributed System Security Symposium, (NDSS2008), 2008.

[18] dionaea – catches bugs, http://dionaea.carnivore.it/

[19] 笠間 貴弘, 吉岡 克成, 松本 勉, 山形 昌也 衛藤 将史, 中尾 康二“疑似クライアントを用いたサーバ応答蓄積型マルウェア動的解析システム”, MWS2009, A7-2, 2009.

[20] Sandeep Yadav, Ashwath K.K. Reddy, A.L. Narasimha, and Supranamaya Ranjan Reddy, “Detecting algorithmically generated malicious domain names,” Proc. of the 10th ACM SIGCOMM conference on Internet measurement , pp 48-61, 2010