通信源ホストの分類を利用したダークネット通信解析

笹生 憲 †　　森 達哉 †　　後藤 滋樹 †

† 早稲田大学
169-8555　東京都新宿区大久保 3-4-1
{saso,mori}@nsl.cs.waseda.ac.jp, goto@goto.info.waseda.ac.jp

ダークネットで観測される片方向通信のパケットはペイロードを含まない．このため，通信解析時には主としてパケットのヘッダに記録されたタイムスタンプ，送信元 IP アドレス，宛先ポート番号，パケットサイズ等の情報が利用される．しかし通信源ホストに関するデータとしては IP アドレスは限定的な情報しか提供しないという問題がある．例えば侵入を目的とした意図的なポートスキャンと新種のワームによるスキャンを IP アドレスによって区別する方法は自明ではない．本研究の狙いは通信源のホストを分類した上で通信データを解析することによって，ダークネットで収集される通信データからより多くの情報を獲得することにある．ホストを分類するためにホスト毎の通信パターンおよび OS フィンガープリントを利用する方法を提案する．4,096 個の IP アドレスで構成されるダークネットで 2 年間収集した通信データに提案手法を適用し，セキュリティ対策に有用な新規情報を抽出した事例を報告する．

Darknet Traffic Analysis by Using Source Host Classification

Akira Saso†　　Tatsuya Mori†　　Shigeki Goto†

†School of Fundamental Science and Engineering, Waseda University
3-4-1 Okubo, Shinjuku-ku, Tokyo 169-8555, JAPAN
{saso,mori}@nsl.cs.waseda.ac.jp,goto@goto.info.waseda.ac.jp

Abstract Since all the incoming unidirectional packets destined to Darknet do not consist of payload, information available from packet headers such as time stamp, source IP addresses, destination port numbers, and packet size are commonly used for Darknet traffic analysis. However, information obtained through IP address is limited. For instance, it is not an easy task to differenciate systematic port scans that arrive intermittently from the ones generated by new worm outbreaks. Based on the observation, this work aims to extend the information of source hosts by using two techniques: traffic pattern extraction and OS finger printing. Throughe the analysis of Darknet traffic data that is collected from /20 size Darknet for two years, we report several case studies that sucessfully demonstrate the usefulness of our approach.

1　はじめに

インターネット上には様々な脅威が日々発生している．脅威は時として甚大な被害をもたらすため，脅威が起こる事前の備えが肝要である．脅威に備えるための一つの有効なアプローチはネットワークを定常的に監視し，通常の状態では観測されない異常な状態や振る舞いをいち早く検知・検出し，早期に原因特定や対策の開発に着手することである．そのような目的を実現するためのネットワーク監視手法としてダークネット (darknet) が広く活用されている [1, 2, 3, 4]．ダークネットとは通常のユーザに割り当てられていないが，インターネット上で到達可能な IP アドレス空間を監視するためのシステムを総称したものである．通常のユーザが利用しないアドレスを監視することにより，ダークネットに届く

パケットは大多数が悪意のある通信によるものとみなすことができる．

ダークネットを有効に運用するためには敵にその存在を知られないことが重要である．なぜならマルウェアの開発者にダークネットの IP アドレス空間を知られた場合，ダークネットへの通信を意図的に避けるようにプログラムを開発する可能性が生じるからである．このため，一般にダークネットは敵からのパケットを受信するものの，自らはパケットを応答しない運用がなされる．このような片方向の通信にはペイロードが含まれていないため，通信の解析時に利用できる情報には制約がある．解析に利用される主要な情報はパケットの送信元 IP アドレスや宛先ポート番号である．例えばポート番号の情報を使うことにより，特定のワームやマルウェアが大流行する予兆を捉えることが可能である [1, 2]．また IP アドレスを分析することで，どこから攻撃がなされているかを把握することが可能である [1, 2]．

一方で送信元 IP アドレスは敵に関する限定的な情報しか提供しない．例えば IP アドレスの割り当て元の RIR が提供するデータベースや Geo IP サービスを利用することでホストのロケーションを推定することができるが，あるホストが発生したパケットが侵入を目的とした意図的なアクセスによるものなのか，あるいは新種のワームやマルウェアによる感染活動であるかは IP アドレスのみからでは判別が困難である．また一般にそのような区別をする方法は自明ではない．

通信源のホストを分類できた場合，以下の利点を期待出来る．

- パケット量としては少量であるが，脅威の予兆を観測するのに有用なホストの通信を個別に分析することにより，気がついていなかった脅威を発見できる．
- 通常の状態では規則的な挙動を示すホスト群の通信の変化に着目することでグローバルに生じる変化を素早く察知できる．
- 通常の監視では見逃しているホスト種別の発生を検知することで，異常やトレンドの変化を検出できる．

上記のような効果を実現する事を狙いとして，本研究では，通信パターンおよび TCP フィンガープリントにもとづき，通信源ホストを分類する方法を提案する．4,096 個の IP アドレスで構成されるダークネットを 2 年間に渡って計測した通信データ (nicter darknet 2013 [5]) に提案手法を適用し，通信の解析を行った．この結果，新たに獲得した知見のハイライトは次のとおりである．

(1) ボットネットである可能性が高いホスト群が規則的な週変動を示す．大規模なマルウェア感染等の事象発生時にその規則性が崩れる．

(2) 2011 年に発生した 3389/TCP を経由したワーム感染の流行時，3389/TCP パケットの約半数は感染ホストとは無関係のホストが生成していた．

(3) 2012 年の 23/TCP に対する通信の急増は 1 パケットをランダムに発生するパターンを持つ Linux ホストによるものであり，急増が観測される少し前から事象が生起していた．

(4) iOS 端末の通信を解析した結果，/20 空間に対してフルスキャンを行う端末が存在した．iOS 端末は全体数は少ないものの 2012 年の秋以降，1 日に観測される端末数は増加傾向にある．

本論文の構成は下記のとおりである．2 章は関連研究を示す．3 章はデータ収集環境およびデータの基礎的な統計を示す．ダークネット監視データから通信源ホストを分類する方法を 4 章で述べ，5 章で通信解析の実例を，6 章にケーススタディを示す．最後に 7 章でまとめと今後の課題を述べる．

2 関連研究

本章では，ダークネットに関連するいくつかの研究を述べる．Moore らは文献 [1] で 2003 年に猛威を振るった Slammer について詳細な分析を報告している．彼らがデータ収集に用いた Network Telescope はダークネットに相当するシステムである．Network Telescope を用いた分析の結果，Slammer の感染範囲や速度，ワーム感染の成長モデルなどが明らかになり，ダークネット解析の有用性が広く知られることとなった．

井上らが開発した nicter [2] は主としてワーム，ウィルスなどのマルウェアの流行を検知することを目的として開発されたダークネット監視システムであり，ダークネットで観測したデータをインタラク

表 1: ポート毎のパケット数および通信先宛先数.

ポート番号	パケット数	ホスト数
3389	15,667,825	2,604,647
23	5,575,737	1,288,656
445	11,189,234	504,207
210	755,173	500,115
1433	28,796,095	108,609
80	6,562,386	60,963
22	9,905,674	56,308
合計	113,010,088	7,564,109

ティブに可視化するツールや統計値が公開されている [6].

下田らはダークネットを拡張することで観測可能なデータを収集する方法を提案した [3]. 主要なアイディアは完全に未使用な連続 IP アドレス空間ではなく，利用中の IP アドレスを含む空間からダークネットとして利用可能なアドレスを動的に発見し，ソフトウェア制御によってアクティブにすることである. これにより敵に発見されにくく，かつローカルスキャンなどの多くの情報を取得可能なダークネットを構成することでできる.

最近報告された Dainotti らの論文 [4] ではダークネットで観測される情報からインターネット上の社会的イベントの分析に利用できることを示している. 例えばある国における通信の検閲状況や，東日本大震災がインターネットインフラに与えた影響分析などをケーススタディで明らかにしている. またこの仕事ではユニークな IP アドレス数が分析上有用であることを示唆している.

3 分析データの概要

本研究は MWS 2013 の研究用データセット [7] の一部として情報通信研究機構が提供する nicter darknet dataset 2013 [5] を用いる. nicter darknet dataset は nicter [2] でダークネットを計測したトラヒックデータであり，2011 年 1 月 1 日から 2013 年 3 月 31 日にかけて pcap フォーマットで計測したパケットキャプチャデータである. 本研究では 2011 年 1 月 1 日から 2012 年 12 月 31 日までの 2 年間のデータを分析対象とする. 表 1 に TCP ポート番号別のパケット数とホスト数を示す. パケット数としてはポート番号 1433 と 3389 が支配的であるが，これらはそれぞれ SQL および Remote Desktop Protocol (RDP) に使われるポートであり，近年攻撃対象になりやすいポートの一つである. 特に後者は 2011 年に発生した大規模なワーム (Win32/Morto) の影響でパケット数，ホスト数ともに数値が高い. Win32/Morto については 6.1 節でより詳細な分析を行う.

表 2: 通信パターンの定義. 宛先 IP アドレスによる分類 (上)，および Point visitor のさらなる分類 (下).

条件	パターン名
$d(h) = 1, p(h) = 1$	Single-shot (SS)
$d(h) = 1, p(h) \geq 2$	Multi-shot (MS)
$2 \leq d(h) \leq 10$	Low scanner (LS)
$11 \leq d(h) \leq 4085$	Middle scanner (MS)
$4086 \leq d(h) < 4096$	High scanner (HS)
$d(h) = 4096$	Full scanner (FS)

表 3: 通信パターン毎のパケット数およびホスト数.

パターン名	パケット数	ホスト数
SS	3,764,871	3,764,871
MS	1,381,474	433,356
LS	9,428,829	2,267,450
MS	42,503,252	352,448
HS	8,335,668	1,737
FS	47,595,994	8,323

4 通信源ホストの分類手法

本章では通信パターンおよび TCP フィンガープリントを用いて通信源ホストを分類する方法を示す.

4.1 通信パターンによる分類

ダークネットへの通信を試みたホスト h 毎に通信宛先 IP アドレス数 $d(h)$ および送信パケット数 $p(h)$ を用い，通信のパターンを定義する. ここで $d(h)$, $p(h)$ ともに 24 時間で観測した数とし，1 日毎に更新する数値である. なお本研究では 24 時間以内に同一の IP アドレスが観測された場合，それらはユニークなホストであると仮定した. 表 2 に本研究で提案するパターンの定義を示す. また，2 年間のデータすべてに対してパターン毎の統計を集計した結果を表 3 に示す.

表より，とくに FS と SS に特徴があることがわかる. FS は数としては全観測ホストの約 0.1 パーセントにすぎないが，約半分のパケットはこれらのホストから発生したものである. これらのホストの

実体は例えばNmap [8] 等のスキャニングツールや，侵入を目的としたネットワークスキャン，シーケンシャルにパブリック IP アドレスをスキャンするアルゴリズムを実装したワームなどが該当すると考えられる．一方 SS はホストの数は非常に多いが，パケット数としては全体の約 4 パーセントにすぎない．SS は Internet Background Radiation (IBR) [9] の一つの例であり，例えばIP アドレス空間をランダムにスキャンするメカニズムを実装したワームの通信が確率的にダークネットに届くケースを含む．SS に着目することにより，そのような性質を持つワームの感染活動を捉えるためのヒントとして利用できる．

4.2 ホスト種別による分類

ホストに関してさらなる情報を得るために OS フィンガープリント [10] を利用する．OS フィンガープリントとは，TCP/IP スタックの実装が OS 毎に異なる事を利用して TCP パケットに記録されたヘッダ情報の特徴から通信源の OS を推定する技術であり，IDS，トラヒックモニタリング，スパム判定などの分野で利用される技術である．本研究では OS フィンガープリントの実装として広く使われている p0f [11] をダークネットの通信データに適用する．

表 3 に 2 年間のデータすべてに対して OS 毎の統計を集計した結果を示す．観測されるホストとしては，Windows と Linux 2.4.x が支配的であることがわかる．しかしながら受信パケット数としては ”UNKNOWN” とラベルがついたホストからのものが多いことがわかる．またこれらはホスト数としては全体の数パーセントにすぎない．”UNKNOWN” は p0f で検知できなかったホストであり，p0f が持つデータベースに登録されている既存 OS と微妙にパラメタが異なるだけものから，まったく新規の TCP/IP スタックを持つと考えられるものまで様々である．後述するように特定の ”UNKNOWN” ホストが大量のパケットを送信することが明らかになっている．その他の通信元ホストとして Mac OS X や iOS が少なからず存在することがわかる．これらの OS はセキュリティの観点では歴史的にそれほど大きな被害を受けてこなかったが，最近のシェア率の高まりやモバイル端末の普及状況を鑑みると着目に値する．これらのホストに着目した通信解析の結果は 6.3 節に示す．

表 4: OS 種別毎のパケット数および通信先宛先数．

OS (TCP/IP stack)	パケット数	ホスト数
Windows XP	24,688,827	2,989,658
Linux 2.4.x	9,500,473	2,159,861
Windows 7 or 8	2,096,792	455,100
Linux 2.6.x	6,993,572	442,625
UNKNOWN	58,946,615	278,020
Windows NT kernel	3,056,833	232,856
Linux 2.2.x-3.x	793,613	121,938
Linux 2.4.x-2.6.x	1,212,701	54,999
Nmap	2,485,664	45,332
Windows NT kernel 5.x	172,189	35,612
Linux 2.2.x-3.x (barebone)	940,342	33,439
Mac OS X 10.x	100,988	15,825
Linux 3.x	877,535	5,025
Linux 2.2.x-3.x (no timestamps)	212,287	2,965
iOS iPhone or iPad	99,892	973
Others	831,765	4,691

5 ホスト分類を用いた通信解析

本章では前章で示した 2 つのホスト分類方法を用いて通信データを解析した結果を示す．

5.1 通信パターンによる解析

図 1 にホストを通信パターン別に分類し，トラヒックを解析した結果を示す．いずれも 24 時間単位で集計した数値である．全般的にパケット数の変動は比較的単調であるのに対し，ホスト数の変動は特徴的であることがみてとれる．まずパケット数を見ると FS，NS によるパケットが割合として高いことがわかる．つまり，パケット数を通じて得られる時系列の挙動はネットワークプレフィックスに対する水平スキャンをしかけている可能性が高いホストによって大きく左右される．

次に，ホスト数を見ると時系列上にいくつかの特徴的なトレンドを発見することが出来る．例えば 2011 年 8 月頃からホスト数が急増したのは 6.1 節で解析する Morto の流行によるものであるが，その増加は主として SS によるものであることがわかる．また全般的にホスト数の増減は主として SS や LS などパケット送信数が少ないホストの寄与が大きいことがわかる．これらのホストは大量のパケットに埋もれてしまう可能性があるので，モニタリング時にはそれらのホストの情報を逃さないような注意が必要である．例えば主要なルーターで実装されているパケットサンプリングを適用したモニタリングはダークネットにおける観測には向かない．

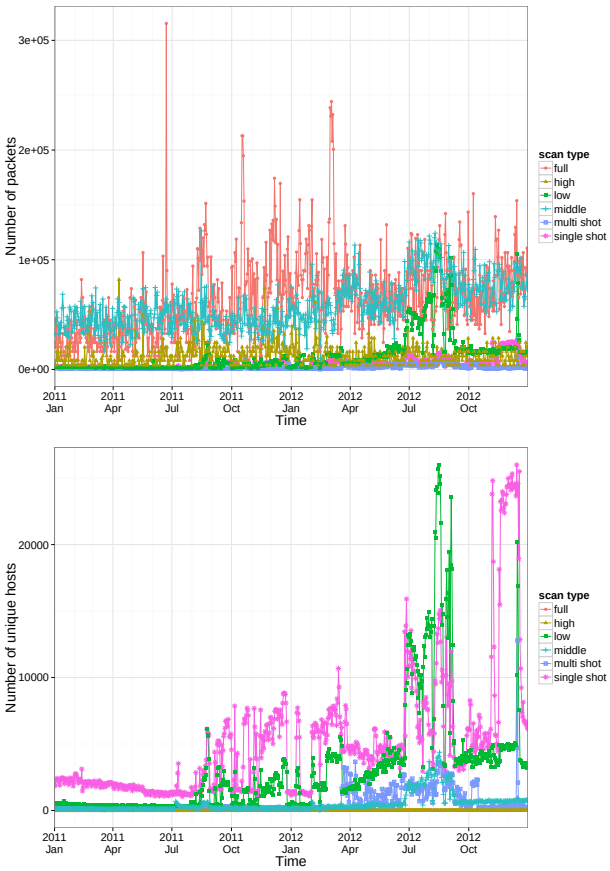

図 1: 通信パターンによるトラヒック解析．パケット数 (上) およびユニークホスト数 (下)．

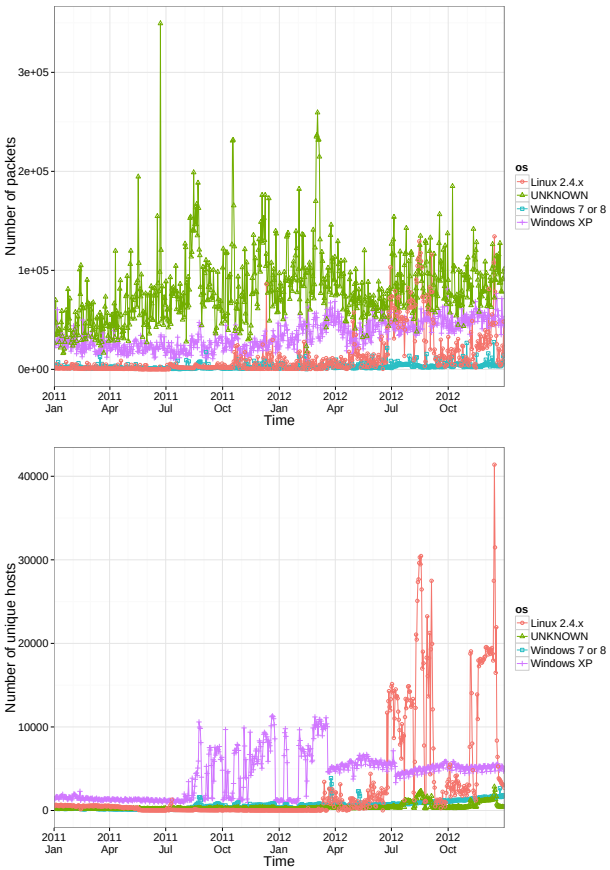

図 3: ホスト種別によるトラヒック解析．パケット数 (上) およびユニークホスト数 (下)．

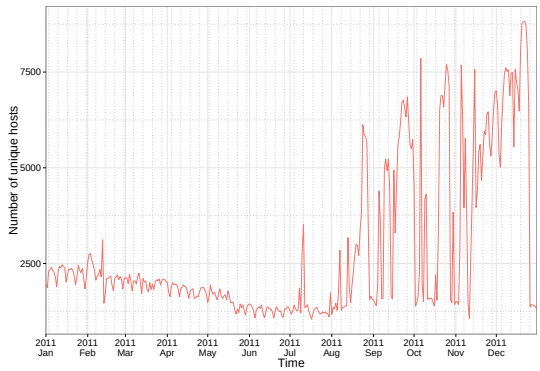

図 2: SS が発生する通信の解析．

特に SS についてトラヒック変動パターンを示したものが図 2 である．ここで興味深いのは 2011 年の前半では 1 週間を単位とした規則的な変動パターンが見受けられることである．これは安定的にインターネット上に存在するボットネット等のホストが発生するランダムなパケットが確率的に観測されている現象と予想される．ボットの活動に生じる規則性は人間の行動パターンによると推論出来る．例えば企業や大学のパソコンで感染したボットは週末は人が不在であるためパソコンの電源がオフとなり活動を休止する．このような行動様式は世界的に共通であるため，週末に一斉にホスト数が減少するグローバルな同期が観測される．一方，2011 年の後半にかけては Morto が発生した 8 月頃を境に規則性が崩れることがわかる．このように，SS の規則性の破れに着目することでグローバルに活動する大規模ワームの発生を感知することが可能である．

5.2 ホスト種別による解析

図 3 にホストを OS 種別に分類し，トラヒックを解析した結果を示す．前節と同様にパケット数の変

動から 2012 年 7 月から 10 月における Linux のパケット数増加を除いて特徴を発見しにくい．一方，ホスト数のデータはよりトレンドがクリアである．前述した Morto が Windows 系 OS の増加として観測される他，Linux の動向や UNKNOWN の増加傾向などがみてとれる．

この図から読み取れる主要なメッセージは，通信を OS 種別に分類することでワーム等のターゲットが一目瞭然になることである．さらに文献 [12, 13] などで報告されているように独自の TCP/IP スタックを持つフルカーネルマルウェアは独自の OS フィンガープリントを有するケースがある．そのようなホストの発生や流行を把握するためにはホスト種別による解析が必須である．ホスト種別に基づく通信解析によって新たに獲得できる情報の例は次章で示す．

6　ケーススタディ

本章では前章で示したフレームワークを使い，様々な観点でダークネットを解析した事例を紹介する．

6.1　3389/TCP の通信解析

2011 年には 3389/TCP を感染経路とし，Windows 系 OS に感染するワームである Morto が流行した．Morto はリモートデスクトップへの接続を試みるワームであるため，ワームが流行することによって RDP のポート番号である 3389/TCP を利用した通信パケットが急激に増加する．nicter で観測するダークネットにおいても Morto に感染したホストが発生したと考えられる TCP SYN パケットが観測された．

図 4 に 3389/TCP への通信をホスト別に分析した結果を示す．図の下段より宛先アドレス数が 2011 年 8 月より急激にスパイク状に増加していることがわかる．この観察は Win32/Morto に関するレポートで報告されている事実と一致している．ここで注目に値するのはそのスパイクの発生に寄与したのが Windows 系 OS であることが発生の瞬間から一目瞭然であることである．さらにこれらのホストの大半が SS の通信パターンを有していたことから，Windows 系 OS で動作するランダムスキャンの機能を有するワームであることがダークネットの観測情報のみを使って推察できる．実際，Morto は感染を拡大させる際にランダムに選択した IP アドレス

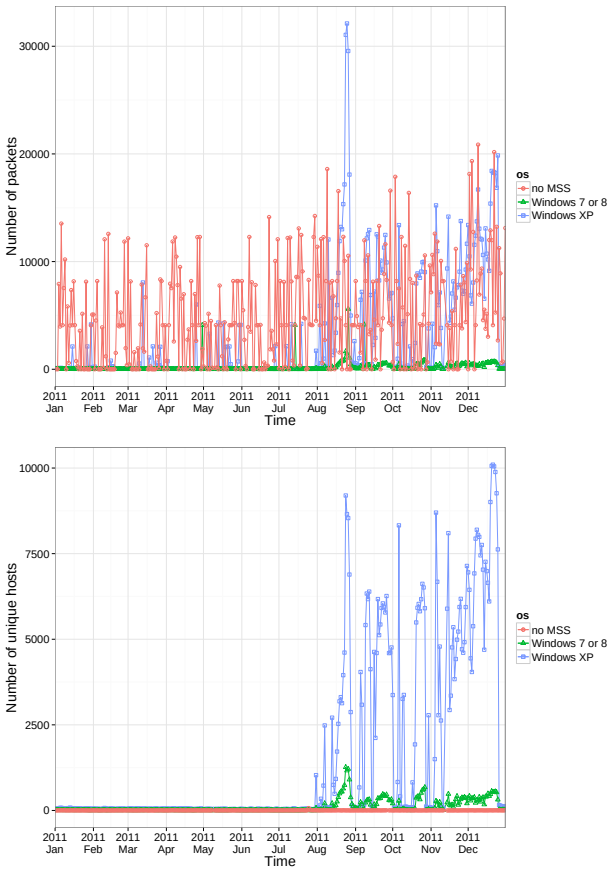

図 4: 3389/TCP への通信 (ホスト種別)．パケット数 (上) および宛先アドレス数 (下)．

に通信を試みることが報告されている [14]．このように，通信パターンとホスト種別の情報を用いてダークネット解析で得られる情報量を増やすことができた．

一方，上段の 3389/TCP のパケット数は全体的には Morto の発生とは無関係な挙動を示している．これはホスト種別でパケットを分離して解析することによって明らかになる．すなわち，図中にある ”no MSS” というホストが定期的に 3389/TCP に対して FS のパターンで通信をする影響があり，Morto のパケットが埋もれてしまっている．Windows 系のパケットのみに着目すれば宛先アドレス数の挙動と類似していることがわかる．この ”no MSS” は p0f では判定できなかったホスト種別の一つであり，SYN パケットに MSS が設定されていない特徴を持つ．現在，一般的に使われるモダンな OS で MSS を設定しないものは存在しないため，特殊な方法で生

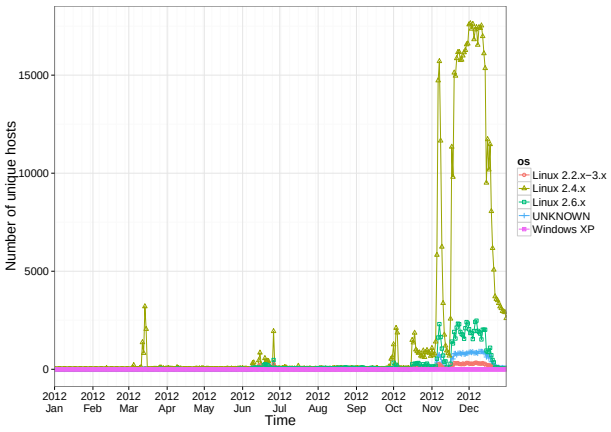

図 5: 23/TCP に対する SS ホストの通信解析.

成されたパケットであることが予想される．そのような事例のひとつはスキャン活動を行うために開発されたパケット生成ツールである．そのようなツールは MSS を適切に設定することで通信効率を向上する必要性が低いことが一要因であろう．現在広く使われているスキャンツールのひとつである Nmap はかつて MSS をつけていない時期があったが，現状のバージョンでは正しく MSS を設定している．

以上で示したような通常の OS とは異なる種別のホストから発生したパケットを分離して分析することによって事象のトレンド把握や異常検出の精度が向上することが期待できる．

6.2 23/TCP の通信解析

図 3 において，2012 年の年末にかけて Linux 系端末の数が急増した現象がみてとれる．さらに通信パターン解析を適用した結果，この増加は主として 23/TCP への通信パターン SS によるものであることが判明した．図 5 にパターン SS を持つホストによる 23/TCP への通信解析結果を示す．グラフより，Linux が主たるホストであること，およびスパイクが生じる少し前から同様のパターンを有する通信が存在していることがわかる．

この時期における 23/TCP への通信ホストの増加は SANS のサイトでも確認できるが [15]，著者らの知る限りその事象を説明したレポートは現時点で報告されてない．したがって現時点でこの現象を引き起こした要因に関する確証はまったく無い．以下では我々の解析によって得られた状況証拠のみを使って現象の要因を推察した結果を示す．まず通信元ホストが一律に Linux であること，および IP アドレスが多岐に渡っていることから，一般家庭に存在する Linux 系デバイスの可能性がある．また通信先のポートが 23/TCP (telnet) であることから，自らも 23/TCP を使うデバイスである可能性が高い．以上の 2 点を総合するとファームウェアが Linux OS で実装された家庭用ブロードバンドルーターをターゲットとしたワームである可能性があると推察できる．そのような性質を持つワームは過去に存在し，その一例は Psyb0t [16] である．

上記の仮説を検証するためには，Honeypot 等，実ネットワークで同様の性質を持つパケットを分析する手法が有効であると考えられる．今回の解析ではそのようなアクティブな分析をする際にとっかかりとなる情報として，OS 情報や通信パターンの情報をダークネット通信データから獲得することが出来た．

6.3 Apple 系端末の通信解析

最後にセキュリティ対策上は現在あまりフォーカスされていない Apple 系端末の通信解析を行った結果を示す．図 6 は Mac OS X および iOS の通信解析結果である．Mac OS X に関しては特筆すべき点は見受けられないが，iOS に関しては面白い観察結果を得た．

まず驚くことに，図の上段より iOS デバイスが 2012 年 10 月から 1 月にかけて何度かにわたったフルスキャンを行った形跡がある (4,096 パケットは /20 空間に対して 1 アドレスにつき 1 パケットを送信したパターン)．この事象の可能性として (1) iOS に実装されたスキャンアプリ，(2) iOS で動作するアプリの誤動作，(3) iOS を偽装したスキャンツール，などが考えられる．少なくとも iOS に関連するアクティビティがダークネットにまで届くようになってきた．

iOS のアクティビティの増加は図の下段からもわかる．2011 年時点では 1 日に観測される iOS 端末数はほぼ 0 か存在しても 1 であったが，2012 年 9 月以降，1 日あたり 10 前後の端末が観測されるようになった．依然として全体からすると完全に埋もれてしまう信号であるが，2013 年 6 月時点で販売台数累計が全世界で 6 億台を越える [17] iOS デバイスが持つインパクトは大きいので，今後継続した監視を行うに値する観測対象であろう．

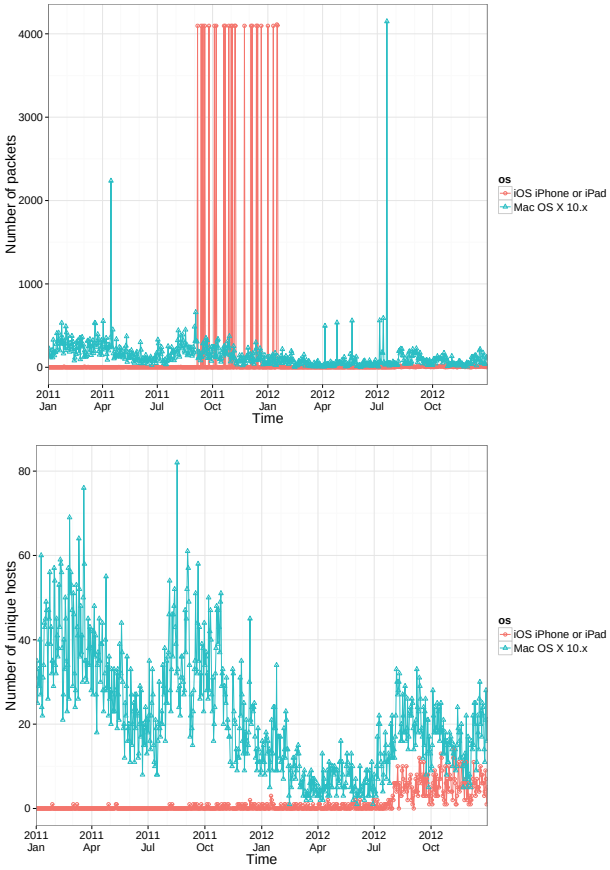

図 6: Apple 系端末の通信解析．パケット数 (上) および宛先アドレス数 (下)．

7　まとめ

本研究はダークネットにパケットを送信するホストを通信パターンおよびホスト種別で分類することでダークネットのトラヒックデータからより多くの情報を獲得する方法を提案した．4,096 個のアドレスで構成されるダークネットを 2 年間に渡って計測した通信データを用いて提案手法の有効性を確認した．通信パターンのより詳細な分類，通信パターン同定のオンライン化，未知のシグネチャを持つホストの解明は今後の課題である．

謝辞　貴重なデータセットを研究コミュニティに貢献頂いた情報通信研究機構　ネットワークセキュリティ研究所　サイバーセキュリティ研究室の諸氏に感謝します．

参考文献

[1] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, “Inside the slammer worm,” *Security & Privacy, IEEE*, vol. 1, no. 4, pp. 33–39, 2003.

[2] D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, and K. Nakao, “nicter: An incident analysis system toward binding network monitoring with malware analysis,” in *WOMBAT Workshop on Information Security Threats Data Collection and Sharing*, pp. 58–66, IEEE, 2008.

[3] A. Shimoda, T. Mori, and S. Goto, “Extended darknet: Multi-dimensional internet threat monitoring system.,” *IEICE Transactions*, vol. 95-B, no. 6, pp. 1915–1923, 2012.

[4] A. Dainotti, R. Amman, E. Aben, and K. Claffy, “Extracting benefit from harm: using malware pollution to analyze the impact of political and geophysical events on the Internet,” *ACM SIGCOMM Computer Communication Review (CCR)*, vol. 42, pp. 31–39, Jan 2012.

[5] “nicter darknet 2013.” `http://www.iwsec.org/mws/2013/files/nicterdarknet_Dataset_2013.pdf`.

[6] “nicterWeb.” `http://www.nicter.jp`.

[7] 神薗雅紀他，“マルウェア対策のための研究用データセット ～MWS Datasets 2013～.” MWS 2013 `http://www.iwsec.org/mws/2013/`, Oct 2013.

[8] G. F. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. USA: Insecure, 2009.

[9] E. Wustrow, M. Karir, M. Bailey, F. Jahanian, and G. Huston, “Internet background radiation revisited,” in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, IMC ’10, (New York, NY, USA), pp. 62–74, ACM, 2010.

[10] G. Taleck, “Ambiguity Resolution via Passive OS Fingerprinting,” in *Recent Advances in Intrusion Detection*, vol. 2820, ch. 11, pp. 192–206, 2003.

[11] “p0f.” `http://lcamtuf.coredump.cx/p0f.shtml`.

[12] 木佐森幸太, 下田晃弘, 森達哉, and 後藤滋樹, “TCP フィンガープリントによる悪意のある通信の分析,” **情報処理学会論文誌**, vol. 52, pp. 2009–2018, jun 2011.

[13] T. Mori, H. Esquivel, A. Akella, A. Shimoda, and S. Goto, “Understanding large-scale spamming botnets from internet edge sites,” in *Proc. of CEAS 2010*, 2010.

[14] G. Keizer, “New Windows worm spreads by attacking weak passwords.” `http://www.computerworld.com/s/article/9219555/New_Windows_worm_spreads_by_attacking_weak_passwords`, Aug 2011.

[15] SANS Internet Storm Center, “Port details: Port 23.” `https://isc.sans.edu/port.html?port=23`.

[16] Baume, Terry, “Netcomm NB5 Botnet — PSYB0T 2.5L.” `http://www.baume.id.au/psyb0t/PSYB0T.pdf?info=EXLINK`.

[17] Zack Whittaker, “WWDC ’13: Apple keynote, by the numbers.” `http://www.zdnet.com/wwdc-13-apple-keynote-by-the-numbers-7000016583/`.