複数国ダークネット観測による攻撃の局地性分析

鈴木 将吾[†] 小出 駿[†] 牧田 大佑[†‡] 村上 洸介[*] 笠間 貴弘[‡]
島村 隼平[§] 衛藤 将史[‡] 吉岡 克成[†‡] 松本 勉[†] 井上 大介[‡]

† 横浜国立大学 240-8501 神奈川県横浜市 保土ケ谷区常盤台 79-1
{suzuki-shogo-mb, koide-takashi-mx}@ynu.jp
{yoshioka, tsutomu}@ynu.ac.jp
‡ 情報通信研究機構 184-8795 東京都小金井市貫井北町 4-2-1
{d.makita, kasama, eto, dai}@nict.go.jp
* KDDI 株式会社 163-8003 東京都新宿区 西新宿 2-3-2KDDI ビル
ko-murakami@kddi.com
§ 株式会社クルウィット 181-0013 東京都三鷹市下連雀 3-34-8 三鷹ハイデンス 509 号
shimamura@clwit.co.jp

あらまし. ダークネットに届くパケットを観測することで, インターネット上の不正活動を把握する試みが広く行われている. しかしながら, 様々な国に割り当てられた異なるアドレスブロックに届く攻撃の比較や特定の国に対する攻撃の有無について分析を行った例は少ない. 本稿では, 4 か国のダークネットで観測される攻撃の傾向の比較を行い, 特定国においてのみ観測されたり特定国からのみ届くなど局地性のある攻撃について分析を行う. 分析の結果, 実際に特定国から当該国に対してのみ観測される特徴的な攻撃が確認された. このような攻撃の情報を当該国に提供することで, 各国の事情に合った, より効果的な対策が期待できる.

Analysis on Local Characteristics of Cyber Attacks from International Darknet Monitoring

Shogo Suzuki[†] Takashi Koide[†] Daisuke Makita[†‡] Kosuke Murakami*
Takahiro Kasama[‡] Jumpei Shimamura[§] Masashi Eto[‡] Katsunari Yoshioka[†‡]
Tsutomu Matsumoto[†] Daisuke Inoue[‡]

†Yokohama National University
79-7 Tokiwadai, Hodogaya-ku, Yokohama-shi, Kanagawa, 240-8501 Japan
{suzuki-shogo-mb, koide-takashi-mx }@ynu.jp
{yoshioka, tsutomu}@ynu.ac.jp
‡National Institute of Information and Communications Technology
4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo 184-8795, Japan
{d.makita, kasama, eto, dai}@nict.go.jp
*KDDI Corporation
KDDI Bldg. 2-3-2 Nishishinjuku-ku, Tokyo, 163-8003, Japan
ko-murakami@kddi.com
§ clwit Inc.
3−34−8 Shimorenjaku, Mitaka, Tokyo, 181-0013, Japan
shimamura@clwit.co.jp

Abstract A great number of researches on the analyses of Darknet traffic have been done to observe malicious activities on the Internet. However, comparison between different countries and analysis on the local characteristics of the observed attacks are not well-studied. In this paper, we analyze attacks on certain countries as well as those from certain countries with the Darknet traffic captured in 4 countries. As a result, we have confirmed an attack that is strictly contained in a particular country, namely all attacking hosts and targeted hosts are both in the same country. Such information may be useful for the country to recognize and prepare for the risk unique to it.

1 はじめに

ダークネットに届くパケットを観測することで，インターネット上の不正活動を把握する試みが広く行われている．しかしながら，様々な国に割り当てられた異なるアドレスブロックに届く攻撃の比較や特定の国に対する攻撃の有無について分析を行った例は少ない．本稿では，4 か国のダークネットで観測される攻撃の傾向の比較を行い，特定国においてのみ観測される攻撃や特定国からのみ届く攻撃など局地性のある攻撃の分析を行う．

まず 2014 年 4 月以降増加傾向にある 10073/TCP 宛の攻撃の送信元国の分布を上記 4 か国のダークネットに関して比較したところ，A 国のみ大きく異なることが確認された．具体的には，A 国のダークネットでは，A 国内からの攻撃が多数観測されており，これらの攻撃ホストからは他の国に対して攻撃が行われていないことが分かった．すなわち，A 国内の 10073/TCP 宛ての攻撃ホスト群は他の攻撃ホスト群と異なり，自国のホストのみを対象に攻撃を行っていることが確認された．

次に同一の攻撃ツールやマルウェアからの通信を抽出するため，TCP SYN パケット内の TCP ヘッダや IP ヘッダの複数のフィールドにおいて特定の固定値をもつ攻撃に着目し，これらの攻撃が各国のダークネットでどのように観測されるかを分析したところ，TCP SYN パケットの初期シーケンス番号，IP ヘッダ ID，ウィンドウサイズの値が全て特定の固定値となる攻撃ホスト群が 7 ヶ月間継続して D 国のダークネットのみで観測され，他の国のダークネットには同様の攻撃を行っていないことを確認した．さらに上記のヘッダフィールドの固定値のうち，初期シーケンス番号を除く IP ヘッダ ID，ウィンドウサイズの値が共通する攻撃ホスト群を抽出したところ，A 国，B 国，C 国のみを継続的に攻撃するホスト群がそれぞれ確認された．ヘッダフィールドのうち，IP ヘッダ ID とウィンドウサイズ，送信元ポート番号が共通の固定値をもつことから，これらの攻撃ホスト群は何らかの関係がある可能性があり，全体で1つのボットネットを構成している可能性もある．実際，ルータ等の機器に感染して 2012 年にインターネット全体に大規模なスキャン活動を行った Carna Botnet は，各ボットにスキャン対象のアドレスレンジを割り当てており，分担してスキャンを行っていたことが報告されている[22]．このように分担された大規模スキャンは，その全体規模に対して各国のダークネットで観測される攻撃の規模が小さいため，複数国での観測により全体像を把握することが重要といえる．

本論文の構成は以下のとおりである．まず，2 章で関連研究について述べ，3 章で分析に用いた各センサの観測情報を述べ，4 章でそれらの観測情報を用いた分析について述べ，5 章でまとめと今後の課題について記す．

2 関連研究

本章では関連研究として，ダークネット観測およびダークネット分析に関する研究について述べる．

2.1 ダークネット観測

ダークネット観測に関しては，情報通信研究機構（以下 NICT）が研究開発を行っているインシデント分析センタ NICTER（Network Incident analysis Center for Tactical Emergency Response）を始め，その他国内外で多数の研究が行われている[1,2,3,5,7,8,9,10]．NICT では，インターネット上におけるセキュリティインシデントの早期検知，原因究明，対策手法の確立を目的として，NICTER [11,12]の研究開発を行っており，約 24 万の IPv4 アドレスからなるダークネットの観測・分析を行っている．JPCERT/CC による TSUBAME プロジェクト[4]では，ダークネットセンサを国内外の多数地点に分散配置し，収集したトラフィックデータの共有，分析を行っている．各地域のマルウェア感染活動や脆弱性のあるサービスを狙ったスキャンの動向など，国内外のダークネット分析をもとに，脆弱性対策情報や注意喚起情報の発信を行っている．米

国の CAIDA（Cooperative Association for Internet Data Analysis）による Network Telescope[6]では，1600 万アドレス以上の大規模なダークネットを観測し，データの一部はデータセットとして公開されている．

2.2 ダークネット分析

NICTER によるネットワーク観測および分析[13,14,15]では，2010年後半と2011年初旬にボットネットの規模に変化がみられた事例や，Win32/Conficker や Win32/Morto と呼ばれるマルウェアの感染が拡大する予兆がダークネットによって観測されていた事例を報告している．

論文[16]では，単位時間あたりにダークネットに到達する通信を，パケット数や宛先ポート・アドレスの種類数，送信元ポート・アドレスの種類数などによってクラスタリングすることでスキャンの挙動を分析している．論文[17]では，DNS ハニーポットとダークネットデータの突合分析を行っている．DNS アンプ攻撃が観測される前に，攻撃に悪用したドメイン名と同一のドメイン名を用いたスキャンがダークネットで観測される可能性が高いことを示し，ダークネット分析によって DNS アンプ攻撃に利用されるドメイン名を事前に特定できる可能性を示唆している．

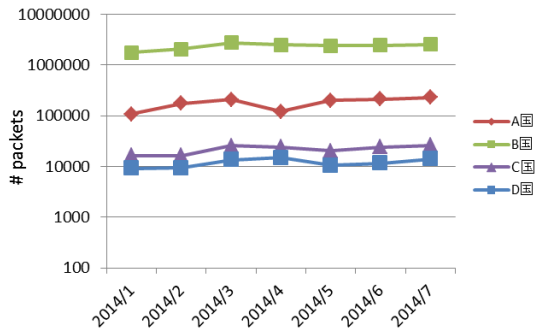

図1 各センサで観測された1アドレスあたりのパケット数推移（月毎）

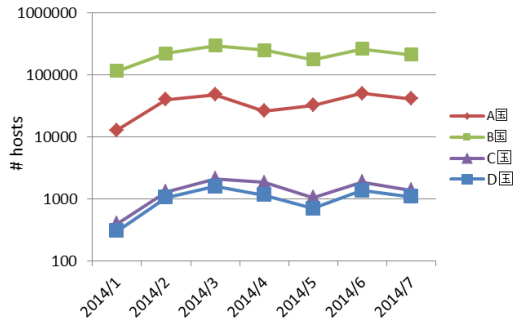

図2 各センサで観測された1アドレスあたりのユニークホスト数推移（月毎）

本研究では複数国のダークネットで観測された攻撃の傾向の比較を行い，特定国においてのみ観測される攻撃や特定国からのみ届く攻撃など局地性のある攻撃の分析を分析する．

3 分析に用いた各種センサの観測状況

本稿では，総務省の PRACTICE プロジェクトより提供された 2014 年 1 月 1 日から 2014 年 7 月 31 日の期間に，A 国/24*8，B 国/24，C 国/25，D 国/25 の 4 か国に設置されたセンサを用いて収集したダークネットデータを用いた．センサは，パケットの送信元に対して全く応答を返さないブラックホールセンサを用いた．各センサにおいて 1 ヶ月間で観測されたパケット数およびユニークホスト数の統計量を図 1，2 に示す．ここで，図 1，図 2 は，各センサの規模を考慮し，1 アドレスあたりに対して観測された数に正規化している．

図1，図2よりトラフィックを収集する国・アドレスレンジによって，1ヶ月間に1アドレスあたりに観測されるパケット数およびユニークホスト数には100倍近くの差があることが分かる．同期間に4か国のダークネットで観測したスキャンの宛先ポート番号を集計したものを表1に示す．

表1より，A国とB国では，445/TCP宛の通信の割合が高く，これは2008年に大流行した445/TCPの脆弱性を利用して感染拡大するワームconfickerによる影響を強く受けている可能性がある．論文[18]では，confickerが攻撃先を決定する際，第2オクテットまたは第4オクテットが128より大きいアドレスに対してはスキャンが行われないことが報告されている．今回用いたC国とD国のダークネットセンサIPアドレスは，第2または第4オクテットが128より大きいブロックに設置されているため，conficker感染ホストからのスキャンが到達していないと予想される．445/TCP宛を除外した通信量の推移は図4，5に示す．

表1 センサ別宛先ポート番号上(2014/1/1-7/31)

A国		B国		C国		D国	
ポート番号	割合	ポート番号	割合	ポート番号	割合	ポート番号	割合
445	19.47	445	18.96	1433	28.81	1433	19.01
23	16.46	1433	12.59	1998	9.53	22	13.31
3389	4.27	22	11.90	22	8.23	23	12.27
80	4.21	23	7.60	3306	6.66	3389	5.77
10073	3.96	8080	7.44	23	6.63	80	4.72
22	3.36	1998	4.62	3128	5.04	5000	4.64
443	2.89	80	3.43	8080	4.08	8080	4.45
8080	2.14	8585	2.69	5000	3.14	3306	3.66
21320	1.82	3389	2.56	3389	3.00	445	3.34
21	1.39	5000	2.49	8585	2.52	3128	2.97
他	40.03	他	25.72	他	22.36	他	25.86

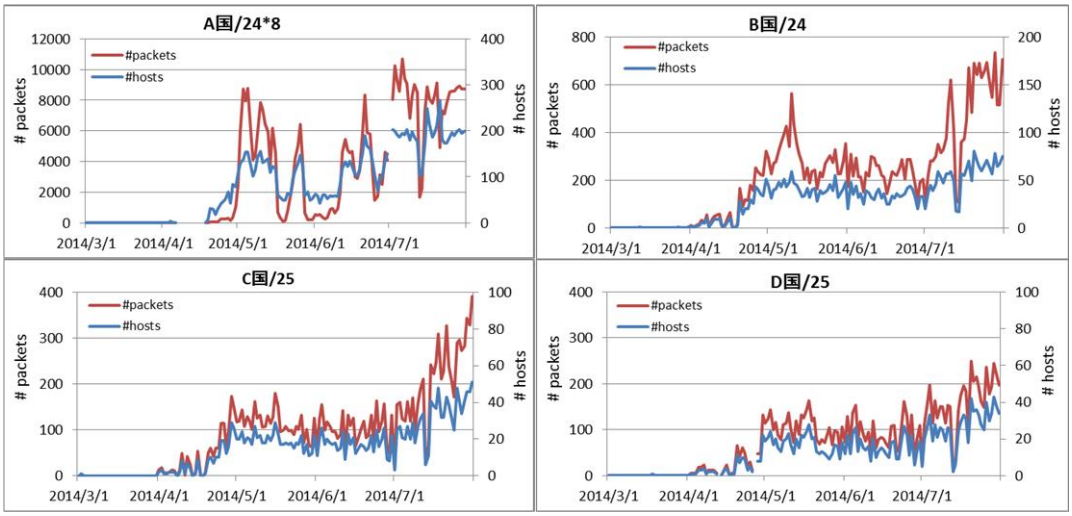

図 3　10073/TCP 宛通信のパケット数とユニークホスト数の推移（日毎）

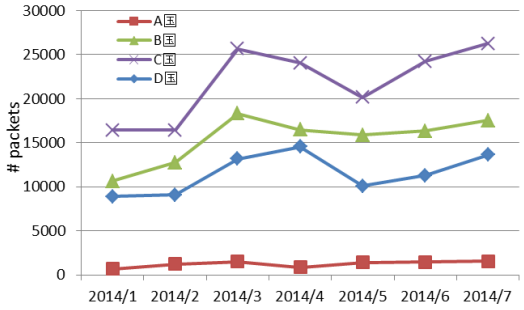

図4　445/TCP宛を除く1アドレスあたりのパケット数推移（月毎）

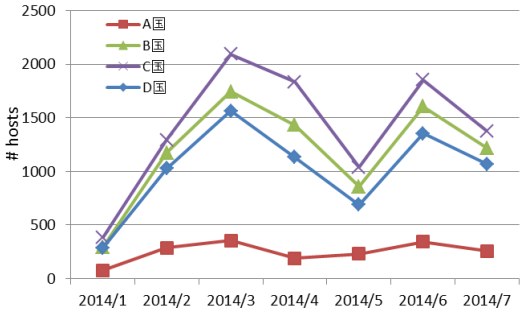

図5　445/TCP宛を除く1アドレスあたりのユニークホスト数移（月毎）

4　局地性分析結果

本章では，4か国のダークネットで観測される攻撃の傾向の比較することで，特定の国においてのみ観測される攻撃や，特定国からのみ届く攻撃など局地性のある攻撃の分析を行う．

今回の分析では，観測された各 IP アドレスは常に同じホストに対応していると仮定する．以下，それぞれの分析について詳細な説明を行う．

4.1　10073/TCP への攻撃

2014 年 4 月初旬より 10073/TCP 宛通信が増加していることを 4 か国すべてのダークネットにおいて確認している．これらの攻撃を行っているホストにホームルータやウェブカメラなどの組み込み系機器が含まれることを確認しているが，この通信の原因となっているマルウェアおよび攻撃対象機器・サービスは現在調査中である．2014 年 3 月 1 日から 2014 年 7 月 31 日の期間に観測された，10073/TCP を宛先とする SYN パケット数およびユニークホスト数の日毎の推移を図 3 に示す．

2014 年 4 月 1 日から 6 月 30 日までの 3 ヶ月の期間に，10073/TCP 宛の TCP SYN パケットを送信したホストを上記 4 か国のダークネットから抽出し，GeoIP[21]を用いてそれらホスト群の送信元国を調査した結果を表 2 に示す．

この期間に 10073/TCP 宛のスキャンを行ったホストは全体で 9,603 ホスト観測された．表 2 から，送信元が A 国であるホストのみ他とは大きく特徴が異なり，これらは A 国のダークネットで集中して観測されていることが分かる．送信元が A 国であるホストに着目したところ，4 センサで 1,068 ホスト観測され，そのうち 1,067 ホストが A 国のダークネットにおいて，残り 1 ホストが D 国のダークネットにて観測される結果となった．また，1,068 ホストのうち 1,024 ホストにおいて，送信元ホストの IP アドレス第 1 第 2 オクテットと A 国のダークネットが設置されているアドレスレンジの第 1 第 2 オクテットとが一致する結果となった．一方，各国のダークネットで観測されている 10073/TCP への攻撃については，送信元と宛先のアドレスにそのような関係は認められなか

表 2 センサごとの 10073/TCP 宛 SYN パケットの送信元ホスト国 (2014/4/1-6/30)

A国/24*8			B国/24			C国/25			D国/25		
国・地域	ホスト数	割合	国・地域	ホスト数	割合	国・地域	ホスト数	割合	国・地域	ホスト数	割合
A国	1067	23.81	ベトナム	545	20.12	ベトナム	273	20.53	ベトナム	254	22.70
ベトナム	701	15.64	マレーシア	348	12.85	マレーシア	170	12.78	マレーシア	143	12.78
マレーシア	441	9.84	タイ	303	11.18	タイ	145	10.90	タイ	101	9.03
タイ	345	7.70	モルドバ	251	9.27	モルドバ	126	9.47	モルドバ	101	9.03
モルドバ	309	6.90	ロシア	224	8.27	ロシア	93	6.99	ロシア	99	8.85
ロシア	268	5.98	インド	202	7.46	インド	90	6.77	インド	85	7.60
インド	228	5.09	アメリカ	159	5.87	アメリカ	86	6.47	アメリカ	61	5.45
アメリカ	219	4.89	トルコ	114	4.21	トルコ	73	5.49	トルコ	58	5.18
その他	903	20.16	その他	563	20.78	その他	274	20.60	その他	217	19.39
計	4479	100.01	計	2709	100.00	計	1330	100.00	計	1119	100.00

表 3 10073/TCP 通信に関するセンサ別の送信元ホスト観測状況

2014/4/1- 2014/4/30			2014/4/1- 2014/6/31		
センサ数※1	ホスト数	割合	センサ数※1	ホスト数	割合
1ヶ国	1259	99.92	1ヶ国	9569	99.65
2ヶ国	1	0.08	2ヶ国	34	0.35
3ヶ国	0	0.00	3ヶ国	0	0.00
4ヶ国	0	0.00	4ヶ国	0	0.00
合計	1260	100.00	合計	9603	100.00

※1 特定のホストが何ヶ国のダークネットで観測されたのかを表す

った. このことから, A 国内には他の 3 か国とは異なる宛先決定方法で 10073/TCP にスキャンを行うホスト群が存在することがわかる. この理由として, これらの A 国の攻撃ホスト群が 4 か国で観測されているものとは異なる種類のマルウェアに感染していることや, 何らかの理由で A 国のホストに対してのみ周辺アドレスレンジへの攻撃が指示されていたことが考えられるが, 実際に攻撃を行っているマルウェアやツールが未確認であるため, 推測の域を出ない. これらのホスト群の情報は A 国のダークネット提供元に提供予定である.

2014 年 4 月の 31 日間と 4 月 1 日から 6 月 30 日の 2 期間に, 10073/TCP 宛に TCP SYN パケットを送信したホストがいくつの国のダークネットセンサで重複して観測されたのかを表 3 に示す.

表 3 より, 2 つの期間のいずれにおいても観測されたホストの 99%以上が 1 つのセンサのみで観測されており, センサ間における観測ホストの重複が極めて少ないことが分かる. 一方, 4 か国のいずれにおいても同様の攻撃を同時期に観測していることから, 当該攻撃は IPv4 アドレス空間の広範囲に行われていることが予想されるため, 攻撃ホスト群の全体規模は各ダークネットで観測されているホスト群と比較して非常に大きいことが予想される. PRACTICE プロジェクトでは, 今後もセンサ設置国の拡大を計画しており, 多数国の情報を元に攻撃ホスト群の規模推定を実施する予定である.

表 4 ヘッダフィールドの特徴的な固有値

送信元ポート	初期シーケンス番号	IPヘッダID	ウィンドウサイズ
6000	1098121216	256	16384

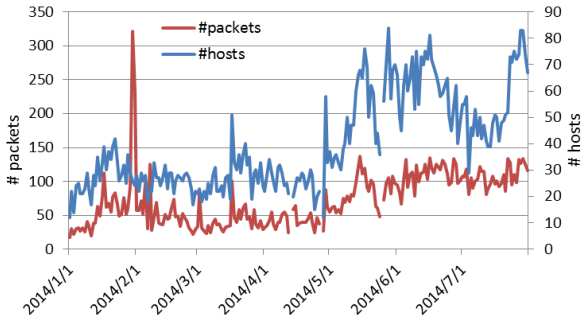

図 6 D 国のみに継続的に攻撃を行うホスト群の観測状況 (2014/1/1-7/31)

表 5 D 国のみで継続的に観測される攻撃の観測状況 (2014/1/1-7/31)

初期シーケンス番号 1098121216		
観測センサ	パケット数	ユニークホスト数
A国/24*8	1	1
B国/24	18	18
C国/25	2	2
D国/25	15237	2829

4.2 ヘッダフィールドに特徴的な値をもつ攻撃

TCP SYN パケットの TCP ヘッダや IP ヘッダの複数のフィールドに, 表 4 に示す特定の固定値をもつ攻撃ホスト群が確認されている. これらのホスト群は 2014 年 1 月 1 日から 7 月 31 日の期間で継続して D 国のダークネットで大量に観測されている. D 国のセンサで日毎に観測されたパケット数, ユニークホスト数を集計したものを図 6 に, また 4 か国のダークネットにおける同様の攻撃の観測状況を表 5 に示す.

表 6 各ダークネットで継続的に観測される攻撃ホスト群の観測状況

観測期間:2014/1/1- 2014/7/31								
送信元ポート番号 6000								
IPヘッダID 256								
ウィンドウサイズ 16384								
初期シーケンス番号 1920532480			初期シーケンス番号 1610350592			初期シーケンス番号 185073664		
観測センサ	パケット数	ユニークホスト数	観測センサ	パケット数	ユニークホスト数	観測センサ	パケット数	ユニークホスト数
A国/24*8	0	0	A国/24*8	1	1	A国/24*8	3359	794
B国/24	7	5	B国/24	24554	4839	B国/24	4	4
C国/25	16054	3509	C国/25	1	1	C国/25	7	5
D国/25	0	0	D国/25	4	4	D国/25	1	1

表 7 各ダークネットで継続的に観測される攻撃の宛先ポート番号(2014/1/1-7/31)

A国/24*8			B国/24			C国/25			D国/25		
宛先ポート	パケット数	割合	宛先ポート	パケット数	割合	宛先ポート	パケット数	割合	宛先ポート	パケット数	割合
22	2379	70.82	1433	10966	44.66	1433	9064	56.46	1433	7017	46.05
1433	565	16.82	22	9338	38.03	22	3952	24.62	22	4615	30.29
3306	186	5.54	3306	1721	7.01	3306	2383	14.84	3306	1554	10.20
3389	67	1.99	8080	585	2.38	3389	126	0.78	3389	570	3.74
8118	56	1.67	3389	479	1.95	18186	101	0.63	8088	209	1.37
8080	21	0.63	808	376	1.53	1521	97	0.60	8080	156	1.02
1998	12	0.36	8088	209	0.85	8080	50	0.31	135	147	0.96
その他	73	2.17	その他	880	3.58	その他	281	1.75	その他	969	6.36
計	3359	100	計	24554	100.00	計	16054	100.00	計	15237	100.00

図 6, 表 5 からこれらのホスト群は D 国のみを継続的に攻撃しており, 他の国のダークネットには攻撃をほとんど行っていないことが確認できる. さらに表 4 のヘッダフィールドの固定値のうち, 初期シーケンス番号を除く送信元ポート番号, IP ヘッダ ID, ウィンドウサイズの値が共通する攻撃ホスト群を抽出したところ, 初期シーケンス番号の値によって A 国, B 国, C 国のみを継続的に攻撃するホスト群がそれぞれ確認された. それぞれの国で継続的に観測されるホスト群について表6に示す. また, 表6と同期間に断続的に行われている攻撃の宛先ポート番号について集計したものを表 7 に示す.

表 6, 7 より観測国によってパケット数, ユニークホスト数に差があり, また宛先ポート番号の傾向も異なることが分かる. このように特定の国またはアドレスレンジに対してのみ行われる攻撃を認識することで, 当該国固有のリスクを認識できる可能性がある.

4.3 5000/TCP への攻撃

5000/TCP 宛のスキャンが 2014 年 2 月 12 日より急増していたことを, 4 か国のダークネットすべてにおいて観測している. 5000/TCP は Synology 社製 NAS のウェブ管理画面に使用されているポート番号で, 攻撃者はアクセス制御不備の脆弱性を悪用することにより任意のプログラムを実行される危険性が報告されている[19]. また, 米国セキュリティ機関の SANS Internet Storm Center[9]の調査によると, 防犯カメラの映像記録に使用される中国 Hikvision 製のデジタルビデオレコーダがマルウェア感染し, Synology 社製 NAS を探索するスキャンを行っていたことが報告されている[20]. 5000/TCP 宛に TCP SYN パケットを送信したホストに関して, 2014 年 2 月 1 日から 2014 年 3 月 31 日の 2 ヶ月間に, 4 か国のダークネットで 1,382,721 パケット, ユニークホストが 10,346 ホスト観測された. また, 観測されたホストがいくつのセンサで重複して観測されたのかを表 8 に示す.

表 8 5000/TCP 通信に関するセンサ別の送信元ホスト観測状況(2014/2/1-3/31)

センサ数※1	ホスト数	割合
1センサ	9955	96.22
2センサ	371	3.59
3センサ	14	0.14
4センサ	6	0.06
合計	10346	100.00

※1 特定のホストが何ヶ国のダークネットで観測されたかを表す

2 ヶ月間で観測された攻撃は 1 ホストあたり 100 パケット以上であるが, 96%以上のホストが単一のセンサで観測されており, 10073/TCP への攻撃と同様に複数国センサで観測されたホストの割合は非常に小さいということが表 8 から分かる.

4.4 考察

10073/TCP宛に攻撃を行うホスト群において，送信元国がA国であるホスト群は1ホストを除いてA国のダークネットで観測されており，A 国内の攻撃ホスト群は自国のホストのみを対象に攻撃を行っていることが確認された．さらに，これら攻撃ホストの95%以上において，ダークネットが設置されているアドレスレンジと第1第2オクテットが一致しているという結果から，送信元ホストの周辺アドレスレンジを対象に攻撃が行われていることが予想される．また，10073/TCP宛にスキャンを行うホストのうち，複数国のダークネットで重複して観測されたホストが非常に少ないことから，今回観測したホストは同様の攻撃を行うホスト全体のごく一部であったことが推察される．今回観測された通信に関して，動的 TCP フィンガープリントのツールであるp0f[23]を適用したところ，9 割以上にあたる 8,803 ホストがLinux と判定されている．さらに，これらのホストに対してTelnet(23/TCP)接続を試みると，図 7 に示すように login プロンプトが表示され，インターネット上からログイン可能な機器であることが確認できたことから，組み込み機器に感染する Linux マルウェアに関連する攻撃であることが予想される．

4.2 節で説明したホスト群から各国ダークネットへの攻撃は，スキャン対象のアドレスレンジに対応した初期シーケンス番号を有しており，何らかの分担の仕組みによりスキャンを行っている可能性がある．これらのホスト群の動向に注目することで今まで観測されなかったポートに対する攻撃の急増などを認識できると思われる．分担された大規模スキャンは，その全体規模に対して各国のダークネットで観測される攻撃の規模が小さいため，小規模かつ特定のアドレスブロックに設置されたダークネットでは全体像を把握することは困難であり，複数国での観測により全体像を分析することが重要といえる．

5000/TCP 宛にスキャンを行うホスト群は，センサ間における送信元アドレスの重複が小さいことから，今回ダークネットで観測した攻撃ホスト群は全体のごく一部であることが予想される．

最後に，今回行った分析では観測された各 IP アドレスは常に同じホストに対応していると仮定したが，実際にはIP アドレスの割り当ては時間と共に変動するため，この影響を考慮する必要がある．

図 7 Telnet 接続時の画面キャプチャ

5 まとめと今後の課題

本稿では，4 か国のダークネットで観測される攻撃の傾向の比較を行い，特定国においてのみ観測される攻撃や特定国からのみ届く攻撃など局地性のある攻撃の分析を行った．

分析の結果，実際に特定国から当該国に対してのみ観測される特徴的な攻撃やスキャン対象のアドレスレンジの割当により，分担して継続的にスキャンを行っている攻撃ホスト群が確認された．

本稿の分析結果は，マルウェアが流行している国・地域の特定や流行の予兆を早期に認知すること，攻撃ホスト群の規模推定に応用できる可能性を示唆していると考える．

今後は，マルウェア動的解析によって得られたトラフィックとダークネットトラフィックの相関分析を行うことに加え，分析に用いるダークネットを増やすことによって特定の国のみを狙った攻撃の有無についても分析を進めたい．

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] @police, "インターネット定点観測," http://www.cyberpolice.go.jp/detect/observation.html (最終閲覧日:2014/08/16)

[2] JPCERT/CC, "Internet Scan Data Acquisition System(ISDAS)," http://www.jpcert.or.jp/isdas/ (最終閲覧日:2014/08/10)

[3] 情報処理推進機構(IPA),"Multi Sensor Traffic Analysis (MUSTAN)," http://mustan.ipa.go.jp/mustan_web/

[4] JPCERT/CC, "TSUBAME(インターネット定点観測システム)," https://www.jpcert.or.jp/tsubame/ (最終閲覧日:2014/08/16)

[5] 三菱総合研究所ほか, "インターネット早期広域攻撃警戒システム WCLSCAN,"
http://www.wclscan.org/ (最終閲覧日:2014/08/16)
[6] D. Moore, "Network Telescopes: Tracking Denial-of-Service Attacks and Internet Worms around the Globe," The 17th Large Installation Systems Administration Conference (LISA '03), USENIX,2003.
[7] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson, "The Internet Motion Sensor: A Distributed Blackhole Monitoring System," The 12th Annual Network and Distributed System Security Symposium (NDSS05), 2005.
[8] EURECOM, "EURECOM,"
http://www.eurecom.fr/en (最終閲覧日:2014/08/10)
[9] Internet Storm Center, "SANS,"
https://isc.sans.edu/ (最終閲覧日:2014/08/16)
[10] TEAM CYMRU CPMMUNITY SERVICES, "The Darknet Project,"
http://www.team-cymru.org/Services/darknets.html (最終閲覧日:2014/08/10)
[11] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, "A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities," Proc. of the 2nd Joint Workshop on Information Security (JWIS2007), pp.267-279, 2007
[12] D. Inoue, M. Eto, K. Yoshioka, S. Baba, K. Suzuki, J. Nakazato, K. Ohtaka, K. Nakao, "nicter : An incident analysis system toward binding network monitoring with malware analysis," WOMBAT Workshop on Information Security Threats Data Collection and Sharing(WISTDCS2008), pp.58-66, 2008.
[13] 中里純二,大高一弘,島村隼平,中尾康二, "nicter によるネットワーク観測および分析レポート-Conficker の経過観測およマクロとミクロの相関分析の一例-," 2009 年コンピュータセキュリティ研究会,2009-CSEC-46(18), pp.1-8, 2009.
[14] 中里純二,島村隼平,衛藤将史,井上大介,中尾康二, "nicter によるネットワーク観測および分析レポート-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-," 電子情報通信学会技術研究報告.ICSS,情報通信システムセキュリティ: IEICE technical report 110(475), pp53-58, 2011.
[15] 中里純二,島村隼平,衛藤将史,井上大介,中尾康二, "nicter によるネットワーク観測および分析レポート -ネットワークインシデントの前兆-," 信学技報,Vol.113, No. 95, pp. 79-84, 2013.
[16] 土性文哉,笠間貴弘,島村隼平,中里純二,井上大介, 佐々木良一, "攻撃元ホストの振る舞い分類を用いたダークネットトラフィックの分析," 2014 年暗号と情報セキュリティシンポジウム CD-ROM 論文集, セッション 2C2-2,2014.
[17] 牧田大佑,吉岡克成,松本勉,中里純二,島村隼平, 井上大介, "DNS アンプ攻撃の早期対策を目的とした DNS ハニーポットとダークネットの突合分析," 2014 年暗号と情報セキュリティシンポジウム CD-ROM 論文集, セッション 3A5-3,2014.
[18] B. Irwin,"A SOURCE ANALYSIS OF THE CONFICKER OUTBREAK FROM A NETWORK TELESCOPE," SOUTH AFRICAN INSTITUTE OF ELECTRICAL ENGINEERS,Vol.104(2),June 2013
[19] Japan Vulnerability Note(JVN),
"JVN#95919136 Synology Disk Station Manager にアクセス制御不備の脆弱性, "
https://jvn.jp/vu/JVNVU95919136/index.html (最終閲覧日:2014/08/10)
[20] SANS Internet Storm Center, "More Device Malware: This is why your DVR attacked my Synology Disk Station (and now with Bitcoin Miner!),"
https://isc.sans.edu/diary/More+Device+Malware%3A+This+is+why+your+DVR+attacked+my+Synology+Disk+Station+(and+now+with+Bitcoin+Miner!)/17879 (最終閲覧日:2014/08/10)
[21] MaxMind, "IP 地理位置情報およびオンライン詐欺防止,"
https://www.maxmind.com/ja/home (最終閲覧日:2014/8/21)
[22] "Internet Census 2012,"
http://internetcensus2012.bitbucket.org/paper.html (最終閲覧日:2014/08/19)
[23] M. Zalewski, "p0f v3 (version 3.07b),"
http://lcamtuf.coredump.cx/p0f3/ (最終閲覧日:2014/8/21)