

## MWS Cup 2014

### 事前課題 4 「Darknet Traffic Analysis」 解答例

#### 1 出題の意図

MWS Datasets 2014[1]で提供された NICTER Darknet 2014[2]は NICTER[3]が保有するダークネット（未使用 IP アドレス）のうち、ある特定の/20 の範囲のダークネットに届いたトラフィックデータである。本事前課題は NICTER Darknet 2014 を解析対象データとし、3つの設問から構成される。設問 1 と設問 2 では最近大きな脅威となっている二つの事象（DRDoS 攻撃、組込みシステムへの攻撃）を取り上げ、それらについての基本的な知識を確認するとともに、データセットから当該攻撃に関するトラフィックについて抽出・分析させ、得られた知見をまとめさせている。また設問 3 では、上記の攻撃に限らず各解答者の自由な発想で注目すべき事象を探し、考察する問題となっている。

サイバーセキュリティ分野の研究活動を進める上では実際の攻撃データやマルウェア検体など実データの利用が非常に重要である。そして実データを利用する上では、自らデータに触り、考え、課題を見つけ、それに取り組む力が求められる。本事前課題がそれらを身に着けるための一助になれば幸いである。

#### 2 出題内容

NICTER Darknet 2014 に含まれるダークネットトラフィックデータのうち、2014年4月1日～2014年8月31日の期間のデータ（以下データセットと呼ぶ）について、以下の設問に答えよ。

##### [設問 1]

DRDoS（Distributed Reflective Denial of Service）攻撃に関して以下の各問いに答えよ。

- (1) 上記の攻撃の概要について 200 文字以内で答えよ。(1 点)
- (2) DRDoS 攻撃に悪用されうるサービス（プロトコル）を 3 つ以上述べよ (1 点)
- (3) データセットに含まれる DRDoS に関連すると思われるトラフィックを分析し、それらの特徴について 400 文字以内で述べよ。なお回答にあたっては分析結果(図表も可)だけではなく、分析の着眼点や具体的な分析手法、利用した参考情報なども記述することで加点対象とする。(2 点)

##### [設問 2]

組込みシステム（ルータ、ウェブカメラ等）に対する攻撃に関して以下の各問いに答えよ。

- (1) ダークネットトラフィックデータから上記の攻撃に関連するトラフィックを推定す

る方法を 200 文字以内で答えよ。(1 点)

- (2) データセットに含まれる上記の攻撃に関連すると思われるトラフィックを分析し、それらの特徴について 400 文字以内で述べよ。なお回答にあたっては分析結果(図表も可)だけではなく、分析の着眼点や具体的な分析手法、利用した参考情報なども記述することで加点対象とする。(2 点)

### [設問 3]

設問 1 および設問 2 の攻撃に関連する事象以外に、データセットに含まれる注目すべき特徴的な事象(例えば、2011 年の **Morto** 出現時に観測された 3389/TCP に対するスキャンホストの急増など)を発見し、その事象に関して、注目した理由も含め 500 文字以内で説明せよ。なお、発見できなかった場合であっても、試行錯誤の課程を説明することで加点対象とする。(3 点)

## 3 解答例

MWS Cup 2014 参加チームから提出された事前課題レポートより、一部優秀であった解答内容を抜粋・要約する。【】内はチーム名を示す。

### 3.1 [設問 1]

#### 【GOTO Love with m1z0r3】

(1) DRDoS 攻撃とは、TCP、UDP、ICMP など、基本的な通信手段やアプリケーションにおいて生成される様々な応答パケットを大量に発生させて行う反射型の DoS 攻撃である。攻撃者は、ターゲットの IP アドレスを送信元に偽造し、踏み台となるホストにパケットを送信することで、ターゲットへ応答パケットを一斉に送る。また DNS や NTP などのプロトコルは要求に対して応答のデータ量が数十倍～数百倍にまで増幅される。(200 字)

(2) DRDoS 攻撃に悪用されるサービス(プロトコル)の一覧を以下に示す。

|                            |                  |            |
|----------------------------|------------------|------------|
| TCP SYN                    | IP pkt (low TTL) | BitTorrent |
| TCP ACK                    | SNMP v2          | Kad        |
| TCP DATA                   | NTP              | Quake 3    |
| TCP NULL                   | DNS              | Steam      |
| ICMP Echo Request          | NetBioS          | ZAv2       |
| ICMP Time Stamp Request    | SSDP             | Salinity   |
| ICMP Address Mask Request  | Chargen          | GameOver   |
| UDP(ICMP Port Unreachable) | QOTD             |            |

(3) DRDoS 攻撃の中でも DNS を用いた amp 攻撃に関する通信に着目する。攻撃におけ

る踏み台の探索通信とバックスキヤッタのトラフィックを図 4.1 に示す。前者は送信先ポートが、後者は送信元ポートが 53 番の通信である。数回に渡ってバックスキヤッタが急増しているが、それぞれ問い合わせドメインが同じことから、同一の攻撃者による攻撃であることがわかった。探索通信に関して、送信元のロケーションを分析した結果を図 4.2 に示す。解析期間を通してアメリカの ISP からの通信が大部分を占めているが、ある時期に中国の "Baidu"からのスキャンが急増している。また DNS 通信において、パケット数が多かった問い合わせドメインの一覧と amp 攻撃でよく用いられるドメインの BlackList[4]を比較した結果を図 4.3 に示す。ダークネットで観測される DNS の問い合わせドメインは amp 攻撃でよく用いられるものであることがわかった。(400 字)

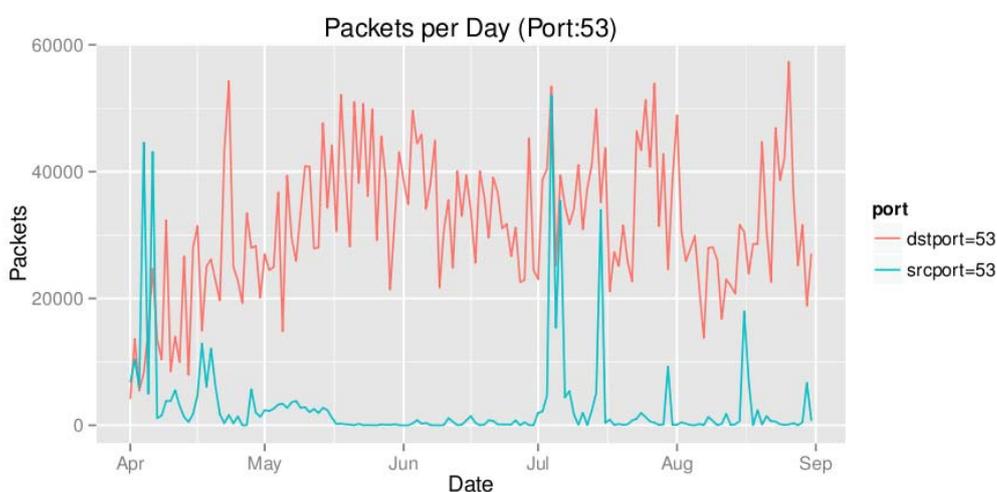


図 4.1 DNS amp 攻撃における踏み台の探索通信(赤)とバックスキヤッタ(青)のトラフィック

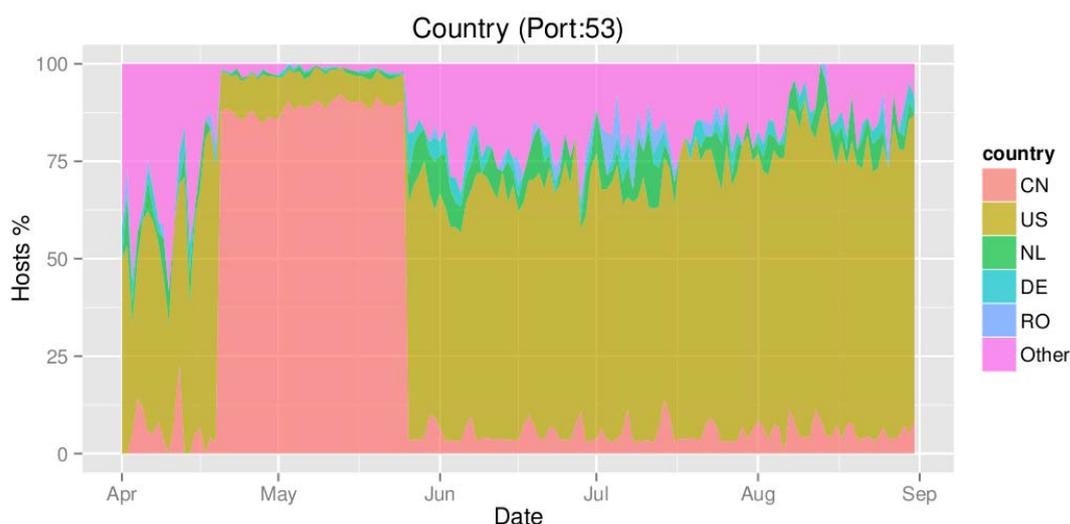


図 4.2 DNS amp 攻撃における踏み台探索通信の送信元ロケーションの内訳

| 問い合わせドメイン                                          | ドメイン数   | Black List |
|----------------------------------------------------|---------|------------|
| dnsscan.shadowserver.org                           | 637,346 | ○          |
| VERSION.BIND                                       | 449,995 | ○          |
| <a href="http://www.google.com">www.google.com</a> | 433,853 | ○          |
| <a href="http://www.google.it">www.google.it</a>   | 409,531 | ○          |
| com                                                | 637,544 | ○          |
| isc.org                                            | 154,588 | ○          |
| 1x1.cz                                             | 133,702 | ○          |
| wradish.com                                        | 125,233 | ○          |
| magas.bslrpg.com                                   | 112,063 | ○          |
| ietf.org                                           | 102,581 | ○          |

図 4.3 ダークネットにおける上位問い合わせドメインと、Black List との比較結果

#### 【人海戦術チーム】

(1) DDoS 攻撃の一種で、攻撃者は踏み台を利用して攻撃対象にサイズの大きいパケットを大量に送信することで、サービスの不能・停止に追い込む。攻撃者は送信元 IP アドレスを攻撃対象に詐称して踏み台にリクエストを送信することで、踏み台は攻撃対象にリプライを送信する。その際、ハンドシェイクが不要である UDP、リクエストに比べてリプライのサイズが大きい（増幅率が高い）プロトコルが利用される傾向にある。（189 文字）

(2) DNS(28~54), NTP(556.9), SNMPv2 (6.3), NetBIOS(3.8), SSDP(30.8), CharGEN(358.8), QOTD(140.3), BitTorrent(3.8), Kad(16.3), Quake Network Protocol (63.9), Steam Protocol (5.5)

※括弧内は増幅率（US-CERT より引用[5]）

(3) DRDoS 攻撃に利用されるプロトコルとして、DNS,NTP,SNMP について分析した。それぞれの送信量を見るために、データセットから送信先ポートが DNS(53)、NTP(123) ,SNMP(161)のパケット数を算出した。(MacDB から、日毎にポートごとのパケット数をカウントする SQL を作成)

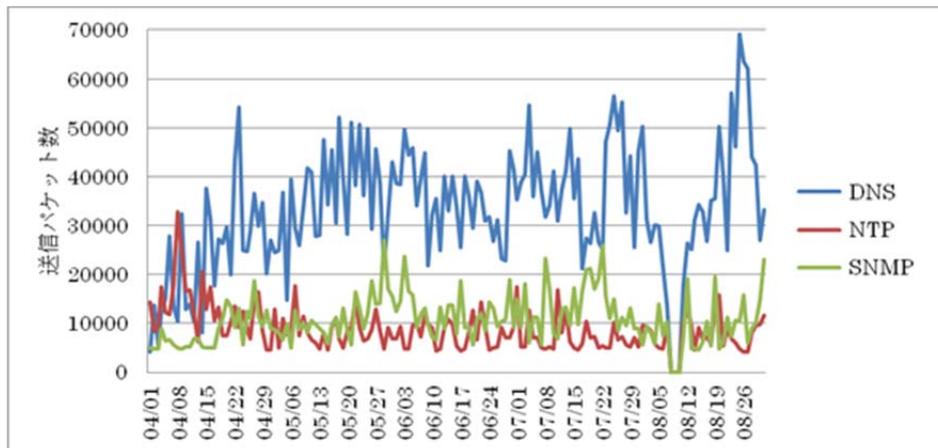


図 4-1 DNS,NTP,SNMP パケット数推移

図 4-1 より、DNS のパケット数が他と比べて多く(約 3 倍)、4~5 月にかけて増加している。NTP は 4 月に一時的に増加しているが、5 月以降は安定している。SNMP は大きな変動はない。いずれのプロトコルも 4~8 月は毎日送信されている。

DNS のクエリタイプは DNS\_TYPE\_ANY(0x00ff)がもっとも多い。これは DNS サーバの全ての情報を取得するコードで、応答パケットのサイズが大きくなる[6]。これより、増幅攻撃を目的としたパケットであると推測できる。

NTP は、monlist 機能を使用することで増幅率が高くなる[7]。パケットを確認したところ、4 月 8 日に大量の monlist のリクエストコード(MON\_GETLIST\_1(0x42))が送信されていた。これより、4 月の NTP 総パケットの増加の要因は、monlist であることが分かった。(394 文字)

## 3.2 [設問 2]

### [n00b]

(1) ブロードバンドルーターに感染し Windows ホストに対する攻撃を行う Chuck Norris と呼ばれるワームが存在する。このワームはまず Telnet 接続可能な機器を探索しデフォルトログインを試みる。ワームはログインが成功した機器に感染し攻撃対象となるファイル共有機能がオンとなっている Windows ホストの探索を行うため、23/TCP のスキャンが増加した後に 139/TCP,445/TCP のスキャンの増加が観測される。ルーターに対する攻撃には同様のトラフィックの変化が観測されるはずである。

(2) まず上記推測に基づき NONSTOP 上に存在する、TELNET の通信を行っている通信

データを探した。その結果 mws\_201407300000.dmp 中に TELET 通信を発見した。解析の結果同一 IP アドレスからポート 23 番に対して、syn パケットを投げ、ポートスキャンを行っている通信があった (図 10)。

| No. -  | Time         | Source          | Destination    | Protocol | Info                                      |
|--------|--------------|-----------------|----------------|----------|-------------------------------------------|
| 202660 | 14912.409701 | 187.153.150.176 | 172.16.217.229 | TCP      | 34337 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202661 | 14912.431387 | 187.153.150.176 | 172.16.217.108 | TCP      | 33047 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202662 | 14912.471325 | 187.153.150.176 | 172.16.217.230 | TCP      | 38247 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202663 | 14912.473666 | 187.153.150.176 | 172.16.217.231 | TCP      | 40518 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202664 | 14912.510798 | 187.153.150.176 | 172.16.217.232 | TCP      | 53038 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202665 | 14912.511735 | 187.153.150.176 | 172.16.217.233 | TCP      | 51498 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202666 | 14912.540909 | 187.153.150.176 | 172.16.217.109 | TCP      | 47239 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202667 | 14912.574295 | 187.153.150.176 | 172.16.217.234 | TCP      | 55093 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202668 | 14912.604095 | 187.153.150.176 | 172.16.217.235 | TCP      | 38115 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202669 | 14912.620165 | 187.153.150.176 | 172.16.217.236 | TCP      | 54032 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202671 | 14912.651835 | 187.153.150.176 | 172.16.217.237 | TCP      | 37569 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202672 | 14912.653864 | 187.153.150.176 | 172.16.217.238 | TCP      | 56005 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202673 | 14912.656829 | 187.153.150.176 | 172.16.217.239 | TCP      | 51596 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202674 | 14912.660575 | 187.153.150.176 | 172.16.217.240 | TCP      | 51544 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202675 | 14912.681481 | 187.153.150.176 | 172.16.217.241 | TCP      | 56596 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202676 | 14912.741388 | 187.153.150.176 | 172.16.217.242 | TCP      | 59693 > telnet [SYN] Seq=0 Win=5840 Len=0 |
| 202677 | 14912.762138 | 187.153.150.176 | 172.16.217.243 | TCP      | 37578 > telnet [SYN] Seq=0 Win=5840 Len=0 |

図 10

ChuckNorris のスキャン元 IP アドレスの多くは、家庭用ルーターや、モデムである事から [8] そのスキャン元の IP アドレス (187.153.150.176) を、IP アドレスを基にネットワークに接続された組み込み機器等が検索できる shodan で検索した。その結果認証がかかった web サイトが発見された。対象の IP アドレスが、実際に家庭用ルーターである事は確認することは出来なかったが、Login.lp という名称の認証のかかったページである事から、ルーターの設定画面への認証サイトである可能性が高い (図 11)。

Shodan Exploits Scanhub Maps Blog Membership

SHODAN 187.153.150.176 Search

Services

HTTP 1

187.153.150.176

Uninet S.A. de C.V.  
Added on 15.06.2014

HTTP/1.0 302 Moved Temporarily  
Date: Sun, 15 Jun 2014 07:07:24 GMT  
Server:  
Content-length: 0  
Connection: keep-alive  
Keep-Alive: timeout=60, max=2000  
Location: http://187.153.150.176/login.lp  
Set-Cookie: xAuth\_SESSION\_ID=q9pOMY8M0D02cplxBJpCQAA=; path=/  
Cache-control: no-cache="set-cookie"

Top Countries

Mexico 1

dsi-187-153-150-176-dyn.prod-infinity.com.mx

1

Privacy Policy | Terms of Service © SHODAN

図 11

### 【フレックス・スヴェンソンチーム】

(1) 文献 0、0 より、ルータへ感染するボット 0 は、デフォルトログイン可能なルータに感染するため、Telnet で接続できる機器を探索する。また、組込みシステムは、メーカーにより特殊なポート番号を使用する場合がある。これらのポートに着目することで、組込みシステムへの攻撃を推定できる。また、感染した組込みシステムから他の組込みシステムへ感染する攻撃の推定は、OS フィンガープリントが効果的である。

(2) 我々は、ルータ、IP 電話(SIP)、および BACnet0 への攻撃を中心にトラフィックを調査した。図 19 より、8 月末に大規模な telnet スキャンが発生したことが分かる。図 20 より、SIP の探索は、周期的に実施していることが分かる。また、図 21 より、BACnet の探索は、7 月から増加し、周期的に実施していることが分かる。これは、文献 0 より、一度に複数の機器情報を取得する ReadPropertyMultiple パケットが増加していると考えられる。また、p0f0 を使用し、telnet を探索する送信元 OS を特定し、分析した(参考 0)。表 1 より、Linux 2.4.x 系や UNKNOWN が多いことが分かる。これより、古い Linux を使用している一般家庭に存在する組込みシステムや独自の組込みシステムに感染したマルウェアから telnet を探索していると推察できる。

| OS                       | 4 月     | 5 月     | 6 月    | 7 月     | 8 月     | 割合      |
|--------------------------|---------|---------|--------|---------|---------|---------|
| Linux 2.4.x              | 1645421 | 1039423 | 653438 | 1280304 | 6077468 | 69.9    |
| Linux 2.2.x – 3.x        | 402791  | 209250  | 284318 | 142297  | 240097  | 8.37    |
| Linux 2.2.x – 3.x (nt)   | 254542  | 162233  | 231345 | 106235  | 331023  | 7.1     |
| UNKWOWN                  | 224368  | 340051  | 294814 | 349024  | 365897  | 10.3    |
| Linux 2.4.x – 2.6.x      | 79430   | 41111   | 13737  | 21082   | 41414   | 1.29    |
| Linux 2.6.x              | 58774   | 34555   | 34076  | 25080   | 29854   | 1.19    |
| Linux 3.x                | 37934   | 9943    | 17456  | 17451   | 131326  | 1.4     |
| Linux 3.11 and newer     | 4123    | 1744    | 3102   | 1010    | 166     | 0.0663  |
| Windows XP               | 4103    | 1279    | 2326   | 43      | 9       | 0.0508  |
| Solaris 10               | 2442    | 4021    | 3548   | 1777    | 2336    | 0.0924  |
| Linux 2.2.x – 3.x (bare) | 2201    | 2650    | 988    | 130     | 1065    | 0.046   |
| Windows NT kernel        | 1113    | 33      | 28     | 7       | 292     | 0.00964 |
| Windows 7 or 8           | 253     | 205     | 366    | 352     | 669     | 0.0121  |
| Linux 3.1 – 3.10         | 11      | 4421    | 290    | 9       | 9604    | 0.0121  |

表 1: telnet スキャンの送信元 OS の統計

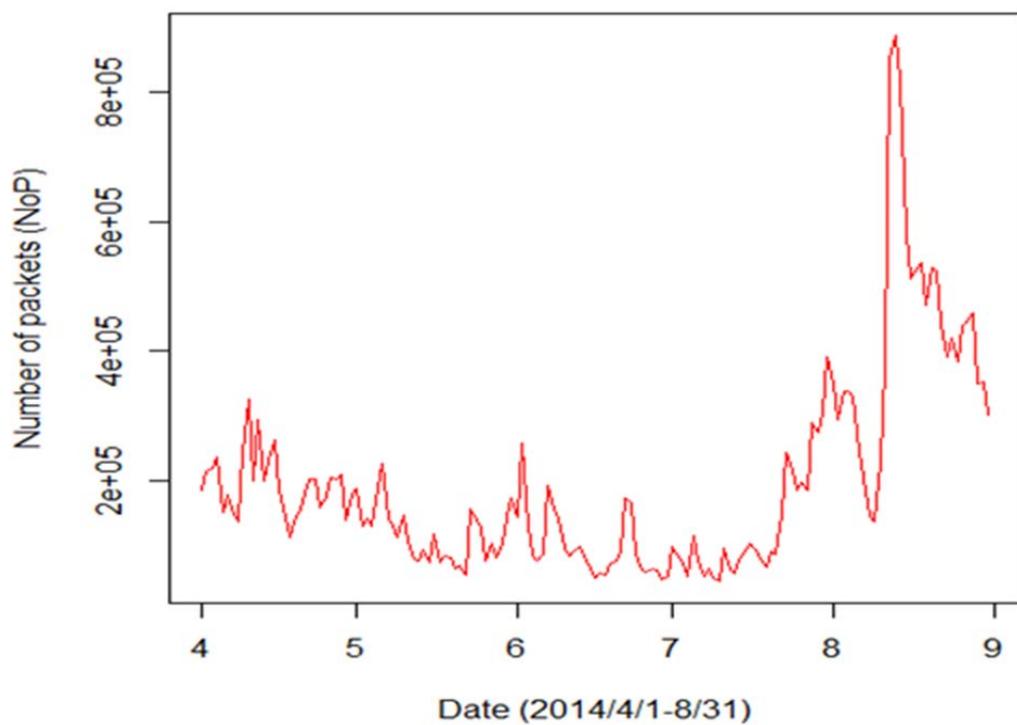


図19: telnet スキャンの統計

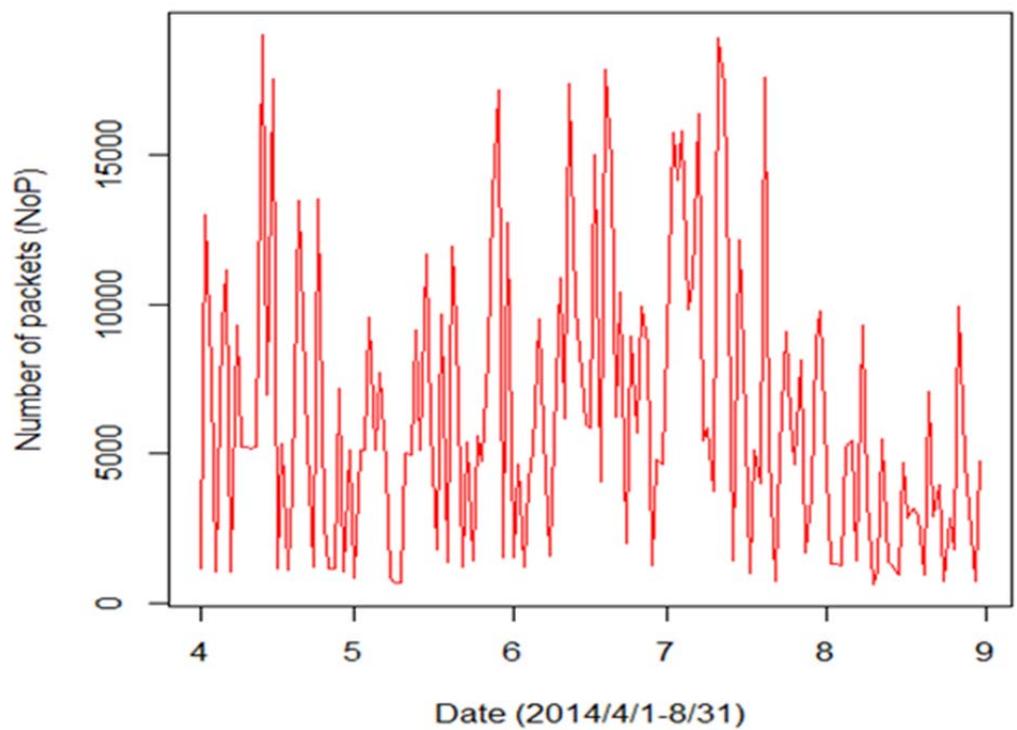


図20: SIP スキャンの統計

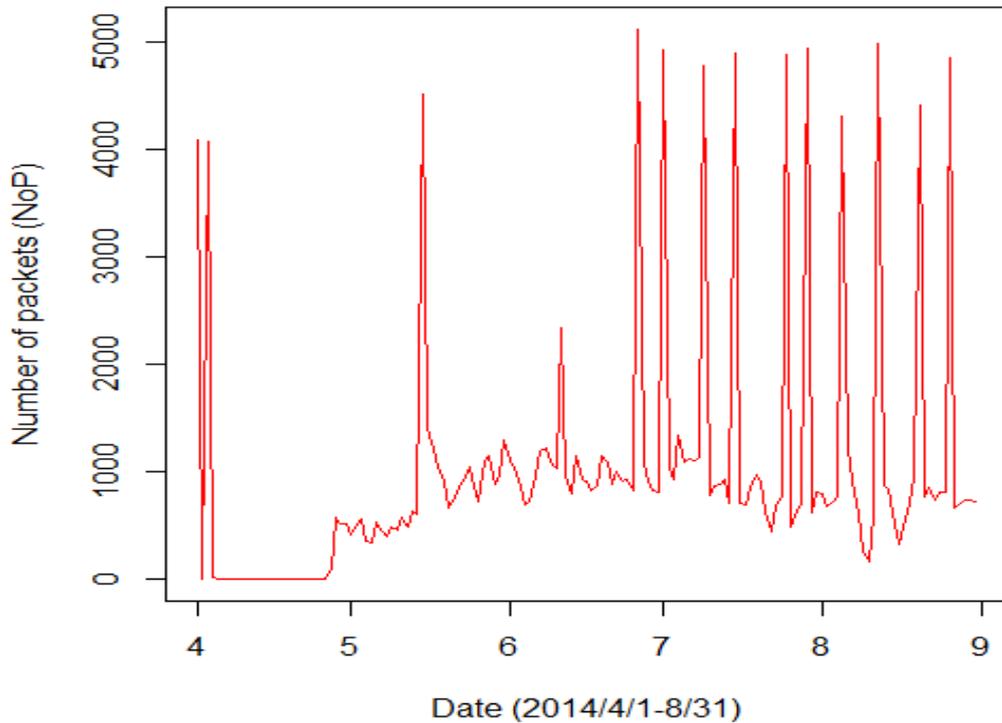


図21: BACnet スキャンの統計

### 3.3 【設問 3】

#### 【TDU ISL with 親方 リターンズ】

最初に,OpenSSL の Heartbleed の事象についての分析を行った.しかし,ポート 443/TCP からは有効なデータが見つからず,443/UDP に着目して,パケット数の推移をグラフ化した.

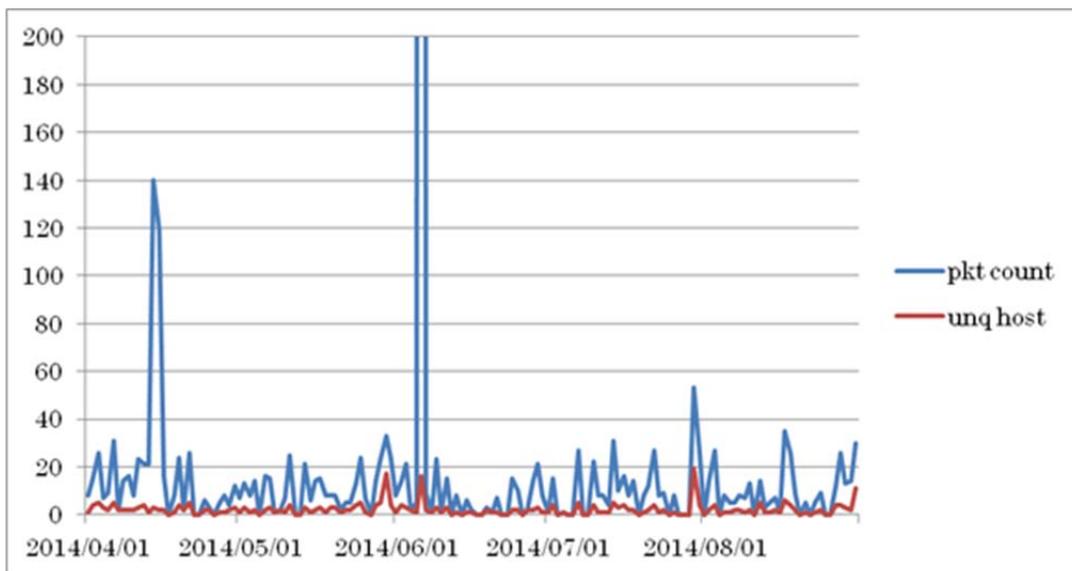


図 4.3-1. 443/UDP のパケット数

heartbleed の報告後に少し遅れてパケットが急増していることを確認できる。しかし、2014年6月6日に4月の約40倍近い増加を確認できた。調査の結果、6月の脆弱性報告の中に OpenSSL のクリティカルな脆弱性(CVE-2014-0221)を発見した。脆弱性報告とパケットの急増の時期が一致するため、この脆弱性に着目してパケット解析を行った。抽出したパケットは図2と図3の通りである。

| No.    | Time                       | Source          | Destination    | Protocol | Length | Info         |
|--------|----------------------------|-----------------|----------------|----------|--------|--------------|
| 153150 | 2014-06-06 04:44:13.275256 | 198.143.173.176 | 172.16.218.156 | DTLS     | 161    | Client Hello |
| 153155 | 2014-06-06 04:44:19.134413 | 198.143.173.176 | 172.16.218.65  | DTLS     | 161    | Client Hello |
| 153155 | 2014-06-06 04:44:28.545400 | 198.143.173.176 | 172.16.218.105 | DTLS     | 161    | Client Hello |
| 153462 | 2014-06-06 04:45:09.909922 | 198.143.173.176 | 172.16.218.118 | DTLS     | 161    | Client Hello |
| 153502 | 2014-06-06 04:45:19.342411 | 198.143.173.176 | 172.16.218.128 | DTLS     | 161    | Client Hello |
| 153520 | 2014-06-06 04:45:21.516221 | 198.143.173.176 | 172.16.219.117 | DTLS     | 161    | Client Hello |
| 153543 | 2014-06-06 04:45:25.665158 | 198.143.173.176 | 172.16.220.206 | DTLS     | 161    | Client Hello |
| 153548 | 2014-06-06 04:45:27.138784 | 198.143.173.176 | 172.16.218.133 | DTLS     | 161    | Client Hello |
| 153585 | 2014-06-06 04:45:34.274240 | 198.143.173.176 | 172.16.211.230 | DTLS     | 161    | Client Hello |
| 153939 | 2014-06-06 04:46:39.871637 | 198.143.173.176 | 172.16.212.19  | DTLS     | 161    | Client Hello |
| 154068 | 2014-06-06 04:47:06.871138 | 198.143.173.176 | 172.16.220.131 | DTLS     | 161    | Client Hello |
| 154213 | 2014-06-06 04:47:35.358155 | 198.143.173.176 | 172.16.211.140 | DTLS     | 161    | Client Hello |
| 154241 | 2014-06-06 04:47:40.537243 | 198.143.173.176 | 172.16.221.55  | DTLS     | 161    | Client Hello |
| 154769 | 2014-06-06 04:49:28.967553 | 198.143.173.176 | 172.16.216.45  | DTLS     | 161    | Client Hello |

図 4.3-2. 2014年6月6日における 443/UDP パケット抽出

```

▶ Frame 123081: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits)
▶ Ethernet II, Src: bd:0e:81:00:02:5e (bd:0e:81:00:02:5e), Dst: ca:c9:cc:4e:24:17 (ca:c9:cc:4e:24:17)
▶ Internet Protocol Version 4, Src: 198.143.173.185 (198.143.173.185), Dst: 172.16.218.218 (172.16.218.218)
▶ User Datagram Protocol, Src Port: 53308 (53308), Dst Port: https (443)
▼ Datagram Transport Layer Security
  ▶ SSL Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: DTLS 1.0 (OpenSSL pre 0.9.8f) (0x0100)
    Epoch: 0
    Sequence Number: 0
    Length: 106
  ▶ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 94
    Message Sequence: 0
    Fragment Offset: 0
    Fragment Length: 94
    Version: DTLS 1.0 (OpenSSL pre 0.9.8f) (0x0100)
    Random.gmt_unix_time: Jun 5, 2014 22:52:40.000000000 JST
    Random.bytes
    Session ID Length: 0
    Cookie Length: 0
    Cipher Suites Length: 54
    ▶ Cipher Suites (27 suites)
      Compression Methods Length: 1
    ▶ Compression Methods (1 method)

```

図 4.3-3. Client Hello パケットの内容

DTLS プロトコルの Client Hello パケットが 99%以上であり、脆弱性(CVE-2014-0221)

に対する特徴的なトラフィックであることがわかる。更にパケットから Version OpenSSL0.9.8fを確認できる。脆弱性を持つOpenSSL(0.9.8y以前の全て)に対しての攻撃であることがわかる。また、ダークネットには、Change Cipher Specメッセージは到達していないが、CVE-2014-0224にも関連があるといえる。

### 【フレックス・スヴェンソンチーム】

我々は、2014年4月～8月の月ごとに、TCPとUDPのパケットから全ポート番号ごとのパケット数を分析し、特徴的な事象を調査した。TCPパケットの統計を図22～26、UDPパケットを図27～31に示す。また、月ごとのパケット数の上位10位までのプロトコルを表2と表3に示す。表2より、6000番と12200番ポートを使用するパケットが多いことが分かる。6000番のパケットは、1433(MSSQL)、4899(Radmin)、22(ssh)、3306(MySQL)を中心に探索していた。文献0より、海外製ツールによる探索活動であると推察できる。12200番のパケットは、1080(SOCKSプロキシ)、8080、21320、3128、1998など、プロキシを探索していた。さらに、4935番のパケットは、複数のホストから3389(RDP)を探索していた。また、送信元ホストのウィンドウサイズが65535であることから、Windows XPの可能性が高い。このため、XPに感染したマルウェアがRDPを使用するシステムへ感染活動していると推察できる。UDPは、設問2に関連する通信がほとんどであった。

表2: ポート番号ごとのパケット数の上位10(TCP)

| 順位 | 4月    | 5月    | 6月    | 7月    | 8月    |
|----|-------|-------|-------|-------|-------|
| 1  | 6000  | 6000  | 6000  | 6000  | 6000  |
| 2  | 12200 | 12200 | 12200 | 12200 | 12200 |
| 3  | 80    | 80    | 80    | 80    | 80    |
| 4  | 25565 | 4445  | 7678  | 40778 | 22    |
| 5  | 6868  | 7678  | 2272  | 22    | 25565 |
| 6  | 4935  | 6868  | 35925 | 2272  | 4935  |
| 7  | 7678  | 6005  | 22    | 2816  | 2816  |
| 8  | 110   | 21303 | 4445  | 3879  | 3879  |
| 9  | 53    | 25563 | 42082 | 30564 | 23514 |
| 10 | 3339  | 4935  | 53    | 2013  | 443   |

表 3: ポート番号ごとのパケット数の上位 10 (UDP)

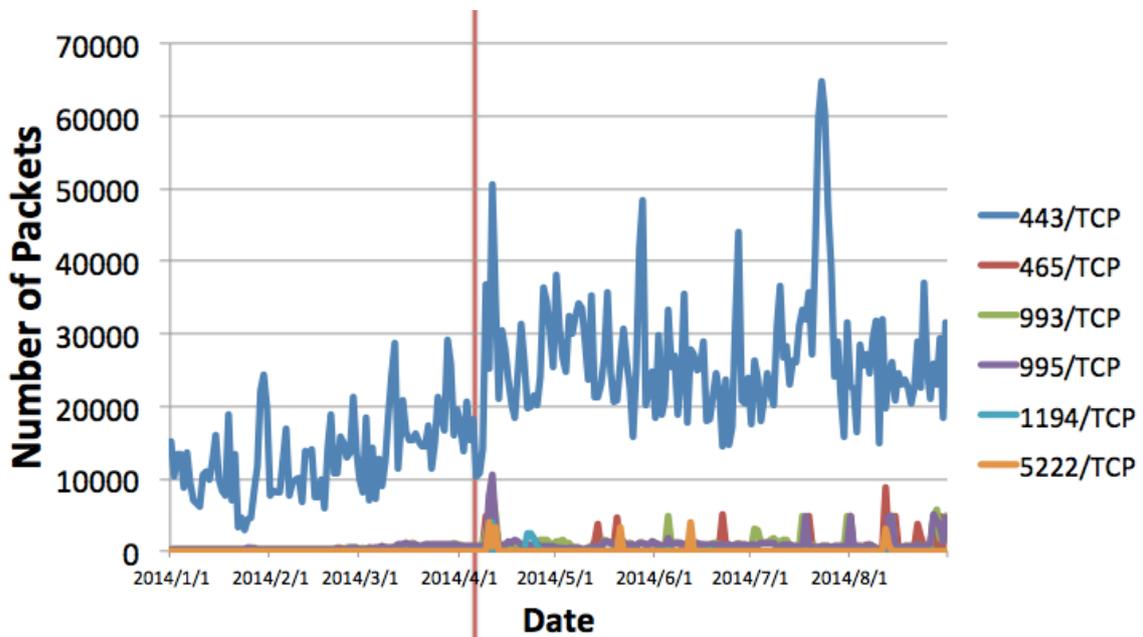
| 順位 | 4 月   | 5 月   | 6 月   | 7 月   | 8 月   |
|----|-------|-------|-------|-------|-------|
| 1  | 53    | 40000 | 40000 | 53    | 40000 |
| 2  | 7678  | 7678  | 7678  | 40000 | 53    |
| 3  | 5553  | 5131  | 39228 | 39228 | 7678  |
| 4  | 51413 | 5344  | 8090  | 51413 | 51413 |
| 5  | 8090  | 51413 | 5061  | 7678  | 35688 |
| 6  | 5072  | 53    | 51413 | 8090  | 8090  |
| 7  | 6881  | 8090  | 24583 | 5061  | 6881  |
| 8  | 24583 | 5060  | 5060  | 34731 | 39228 |
| 9  | 43105 | 6881  | 56856 | 6881  | 45682 |
| 10 | 5062  | 39228 | 41734 | 5060  | 1024  |

### 【GOTO Love with m1z0r3】

2014/4/7 に OpenSSL の脆弱性「Heartbleed」[16]が発表されたため、表 4.2 に示す OpenSSL を利用したポート[17]宛のパケットに着目し、分析した。なお、4 月以降との差異を見るため、それ以前のデータも分析した。図 4.8 と図 4.9 に 1 日ごとのパケット数とホスト数の推移を示す。両図より 4/7 以降にパケット数とホスト数の急増という事象を発見した。また、図 4.10 と図 4.11 は 4/4~4/13 の 5 分ごとのパケット数とホスト数の推移である。この 2 つの図より、4/7 以前は 443/TCP にボットからの周期的なスキャンを発見し、それ以降に Heartbleed の影響で周期性の乱れを発見した。図 4.10 から 443/TCP を除いた図 4.12 では、4/7 以降に約 6 時間かかる/24 へのスキャンを複数発見した。さらに、7 月後半の 443/TCP のスパイクの発信元国情報を分析すると大半が中国と米国だった(図 4.13 参照)。中国のホストは 110.249.\*.\*の1つであり SPAMHAUS[18]の PBL に存在した。米国のホストは 140.212.\*.\* /24 に約 60 あり、PBL に存在しなかった。(497 文字)

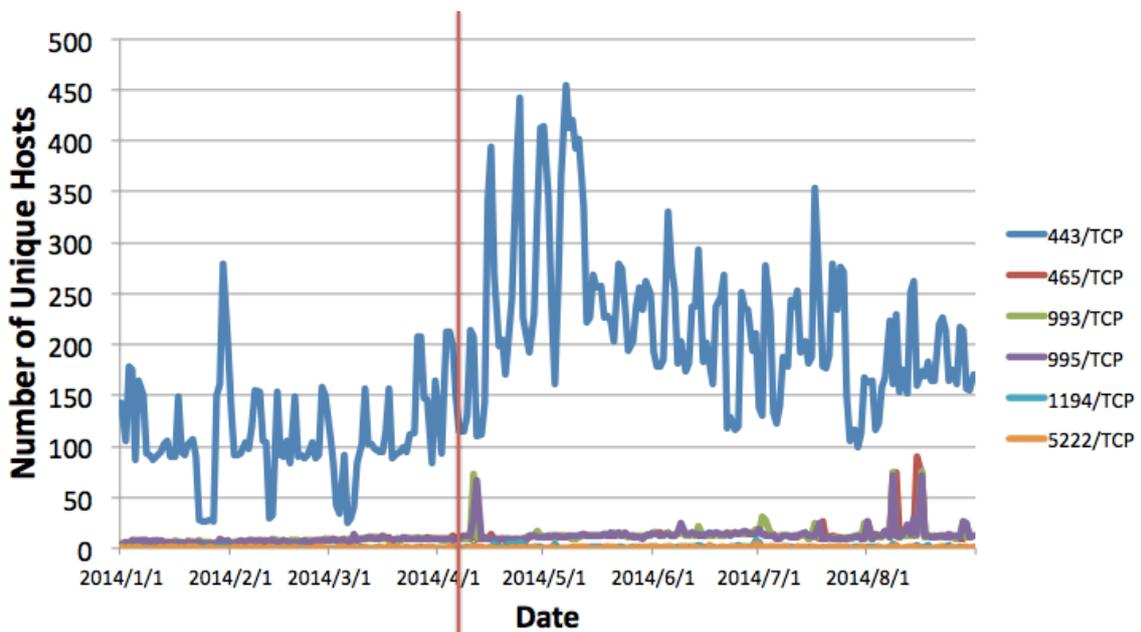
表 4.2 分析対象とした宛先ポート番号の一覧と利用されるサービス名[19]

| ポート番号 | プロトコル | サービス名       | 説明                                     |
|-------|-------|-------------|----------------------------------------|
| 443   | TCP   | https       | http protocol over TLS/SSL             |
| 465   | TCP   | urd         | URL Rendezvous Directory for SSM       |
| 993   | TCP   | imaps       | imap4 protocol over TLS/SSL            |
| 995   | TCP   | pop3s       | pop3 protocol over TLS/SSL (was spop3) |
| 1194  | TCP   | openvpn     | OpenVPN                                |
| 5222  | TCP   | xmpp-client | XMPP Client Connection                 |



2014/04/07にOpenSSLの脆弱性が発表

図 4.8 Heartbleed 関係のダークネット到達パケット数推移



2014/04/07にOpenSSLの脆弱性が発表

図 4.9 Heartbleed 関係のダークネット到達パケットのホスト数推移

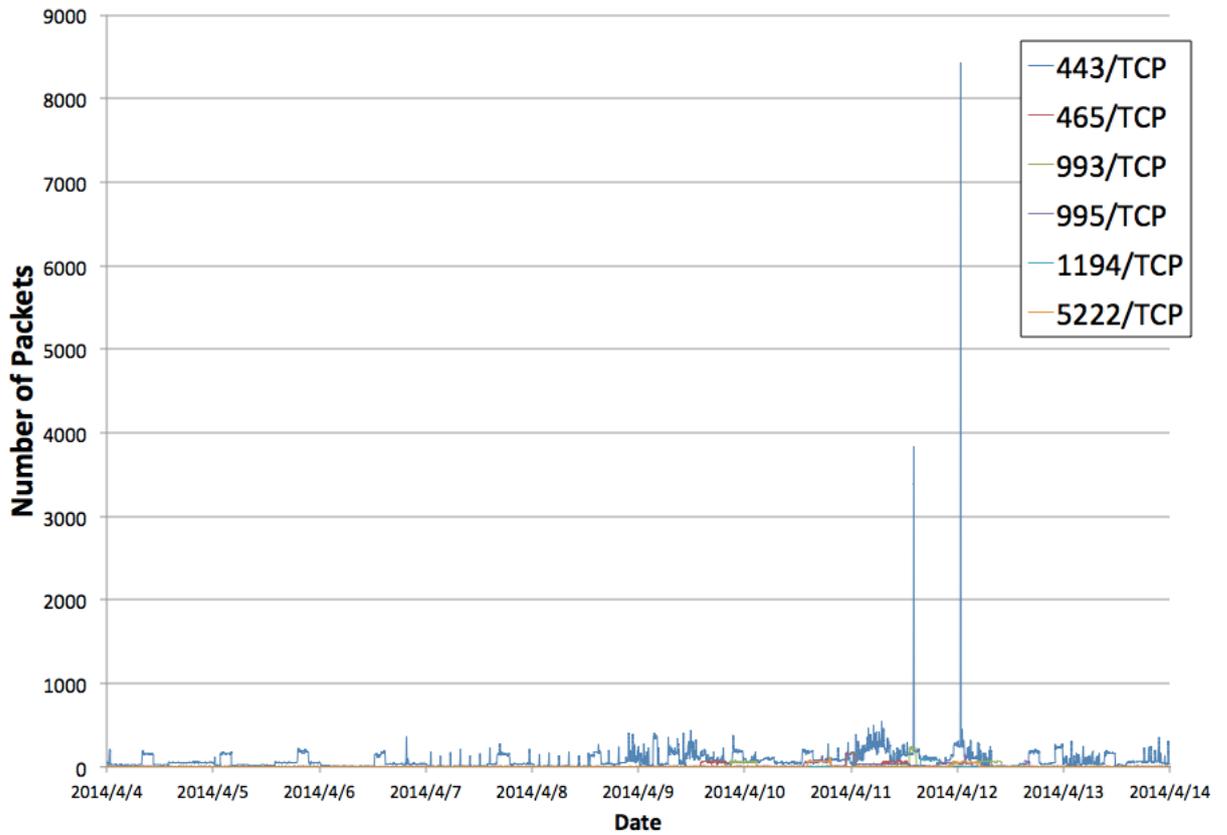


図 4.10 4/4～4/13 でダークネットに到達した Heartbleed 関係のパケット数推移

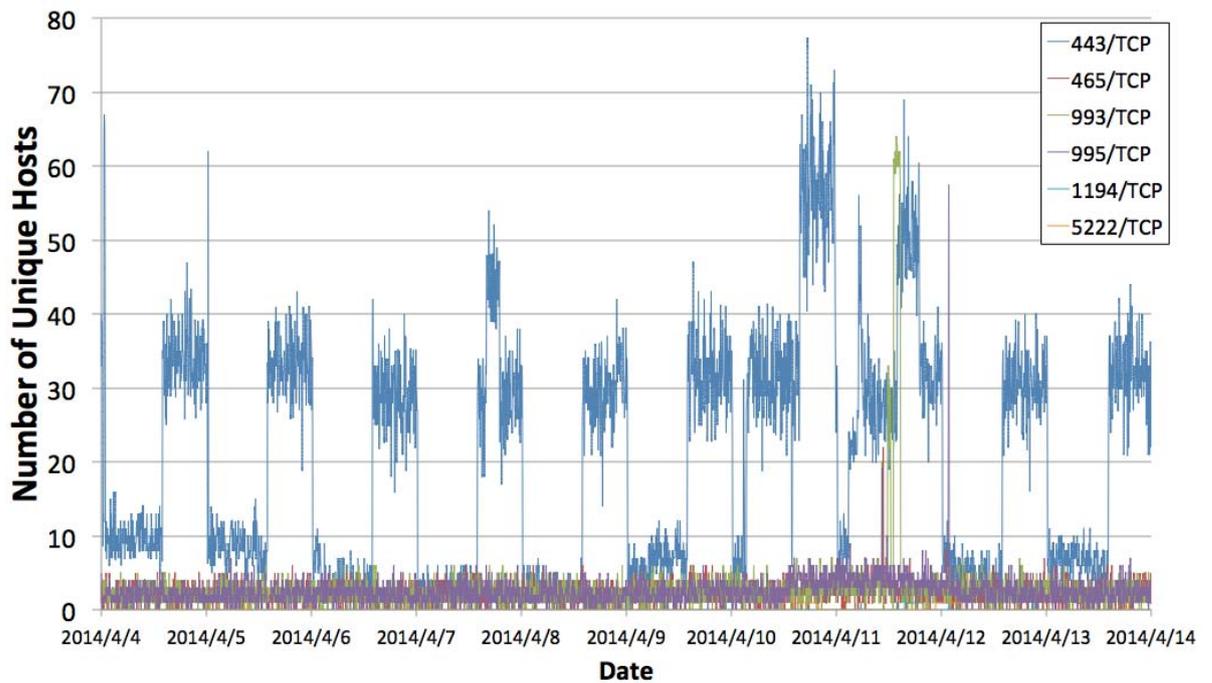


図 4.11 4/4～4/13 でダークネットに到達した Heartbleed 関係のパケットのホスト数推移

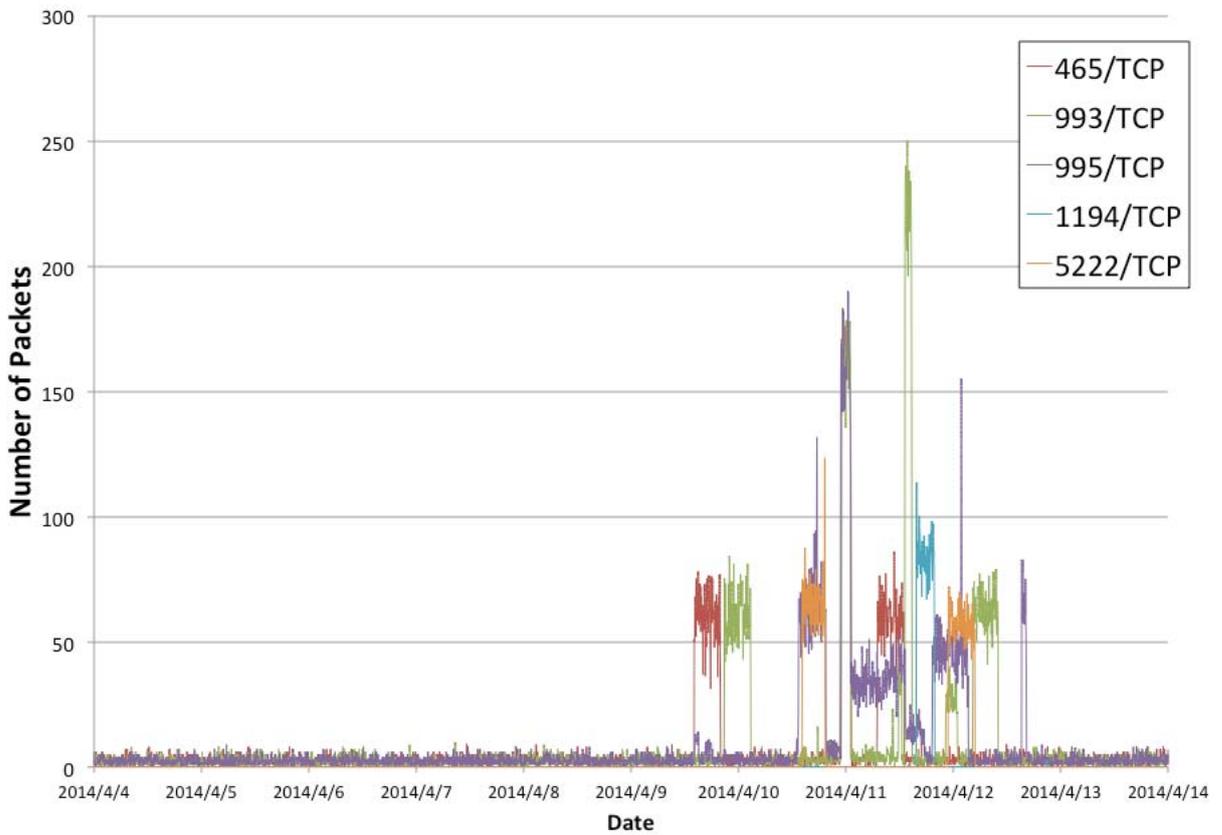


図 4.12 4/4～4/13 でダークネットに到達した Heartbleed 関係のパケット数推移(443/TCP は除外)

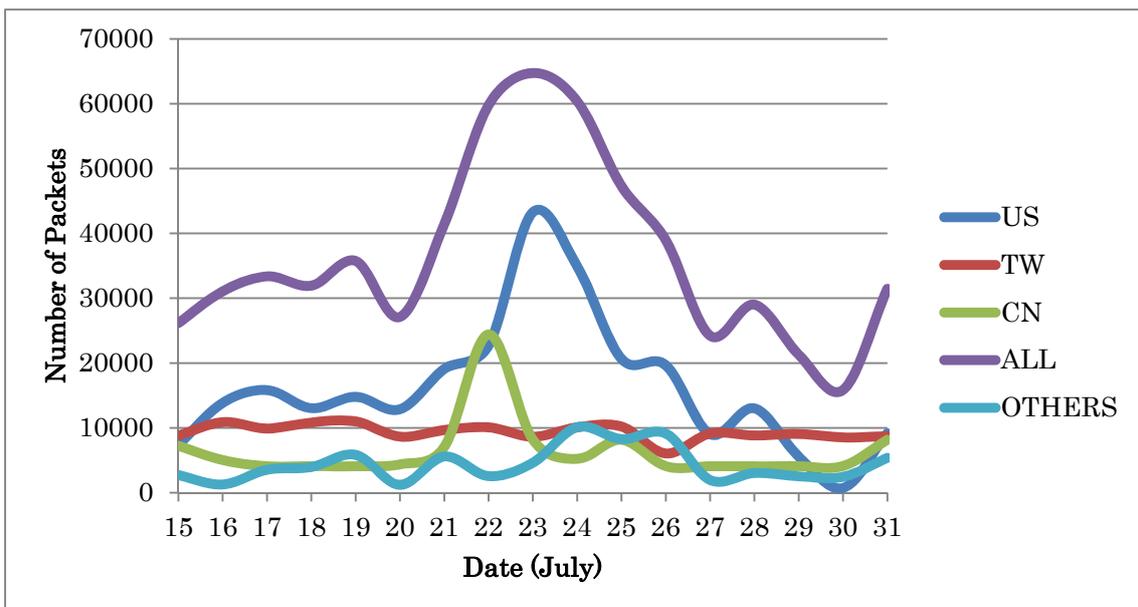


図 4.13 7/15～7/31 でダークネットに到達した 443/TCP 宛パケットの国別パケット数推移

## 参考文献

- [1] 秋山, 他, “マルウェア対策のための研究用データセット ～MWS Datasets 2014～,” 情報処理学会 研究報告コンピュータセキュリティ (CSEC) , Vol. 2014-CSEC-66, No. 19, pp. 1-7, 2014.
- [2] 笠間, 竹久, “MWS 2014 意見交換会 NICTER Darknet Dataset 2014 / NONSTOP,” [http://www.iwsec.org/mws/2014/files/NICTER\\_Darknet\\_Dataset\\_2014.pdf](http://www.iwsec.org/mws/2014/files/NICTER_Darknet_Dataset_2014.pdf)
- [3] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, and K. Rikitake, “nicter: An Incident Analysis System using Correlation between Network Monitoring and Malware Analysis,” In Proceeding of the 1st Joint Workshop on Information Security, June 2006.
- [4] “No Think!,” [http://www.nothink.org/honeypot\\_dns.php](http://www.nothink.org/honeypot_dns.php)
- [5] “Alert (TA14-017A) UDP-based Amplification Attacks,” <https://www.us-cert.gov/ncas/alerts/TA14-017A>
- [6] “ntpd の monlist 機能を使った DDoS 攻撃に関する注意喚起,” <https://www.jpccert.or.jp/at/2014/at140001.html>
- [7] “Alert (TA13-088A) DNS Amplification Attacks,” <https://www.us-cert.gov/ncas/alerts/TA13-088A>
- [8] P. Celeda, et al., “Embedded Malware – An Analysis of the Chuck Norris Botnet,” [http://is.muni.cz/th/98863/fi\\_r/botnet-chuck-norris.pdf](http://is.muni.cz/th/98863/fi_r/botnet-chuck-norris.pdf)
- [9] 笹生 憲, 森 達哉, 後藤 滋樹: 通信源ホストの分類を利用したダークネット通信解析, コンピュータセキュリティシンポジウム 2013 論文集, Vol.4, pp. 729-736 (2013).
- [10] 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～組み込みシステムに感染するマルウェア～, 研究報告コンピュータセキュリティ (CSEC), Vol.56, pp.1-5 (2013).
- [11] “旧型ボットネットの再来! ボットネット「Chuck Norris」、ルータの脆弱性を突く!,” <http://about-threats.trendmicro.com/RelatedThreats.aspx?language=jp&name=Botnet+Rises+in+the+Name+of+Chuck+Norris>
- [12] “BACnet,” <http://ja.wikipedia.org/wiki/BACnet>
- [13] “ビル管理システムに対する探索の検知について (第 3 報),” <http://www.npa.go.jp/cyberpolice/detect/pdf/20140706.pdf>
- [14] “p0f v3 (version 3.07b),” <http://lcamtuf.coredump.cx/p0f3/>
- [15] “Ops: Deep Darknet Inspection - Part 3 of 3,” <http://www.cymru.com/jtk/blog/2010/09/15/>
- [16] “The Heartbleed Bug,” <http://heartbleed.com/>
- [17] “OpenSSL の脆弱性を標的としたアクセス、最大 1 日に 12,881 件 (警察庁),” <http://scan.netsecurity.ne.jp/article/2014/05/22/34236.html>
- [18] “SPAMHAUS,” <http://www.spamhaus.org/lookup/>

[19] “Service Name and Transport Protocol Port Number Registry,”  
<http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>