宛先アドレス順序とペイロードに着目したネットワーク走査活動の分析

中村 康弘[1]　梶川 慶太[2]　芦野 佑樹[3]　鮫島 礼佳[3]　須尭 一志[3]　矢野 由紀子[3]

概要：これまでのダークネット観測結果の分析手法では，送信元アドレスや宛先ポート番号及びそれらの頻度などの統計量に着目したものが多数であった．これは，観測がステルス型でそのアドレス範囲が限定されることから，得られる特徴量が限られていることに起因するものと考えられる．しかしながら，ダークネットアドレスへの接続要求に対して応答することで，走査活動の初期ペイロードが得られるとともに，多数の連続アドレスの同時観測により，送信元からの走査の連続性などの挙動をさらに詳しく観測することができる．この研究では，同一送信元からの接続要求を着信するセンサアドレスの相互距離と着信時間差を計測することにより，送信元がどのような順序で走査しているかを推定する．また，その一連の走査活動を，既存の走査ツールの挙動や実際に送信されたペイロードの種類と照合することで走査目的の推定に役立つ情報を得ることができる．実験では，未使用の連続アドレスへ着信した接続要求パケットへ応答し，そのペイロードを観測した結果に本手法を適用し，ネットワーク走査の順序とそのペイロードに基づく特徴の分析結果を示し，その有効性を明らかにする．

キーワード：ダークネット観測，走査活動，初期ペイロード，走査順序

An Analysis of Network Scanning Activity Based on Destination Address Order And Payload

Yasuhiro Nakamura[1]　keita Kajikawa[2]　Yuki Ashino[3]　Ayaka Samejima[3]　Kazushi Sugyo[3]
Yukiko Yano[3]

Abstract: In the previous analysis method for darknet observation, most methods perform statistical processing such as source address, destination port number and their frequency. because of the stealth observation and its limited address range, obtained features will be limited. However, by responding to the connection request of the darknet address, an initial payload of the scanning activity can be acquired, and simultaneous observation of a large number of consecutive addresses enables observation of detail behaviors such as continuous scanning. In this study, by measuring the mutual distance of the target sensor addresses and the arrival time difference, it will be estimated in what order the scanner wants to scan. It is also possible to obtain useful information for estimating the scanning purpose by comparing the series of scanning activities with the behavior of the existing scanning tool and the type of payload actually transmitted. Experimental results willl indicate that this analysis method is effective for observing the scan activity and estimate an intention of the scanner.

Keywords: Darknet Observation, Scanning Activity, Initial Payloads, Scanning Order

[1] 防衛大学校情報工学科
Computer Science, National Defense Academy
[2] 防衛大学校理工学研究科
Graduate School of Science and Engineering, National Defense Academy
[3] 日本電気株式会社 ナショナルセキュリティ・ソリューション事業部 サイバーセキュリティ・ファクトリ
Cyber Security Factory, National Security Solution Division, NEC Corporation

1. はじめに

2003 年から 2010 年頃には，脆弱性のあるシステムをインターネットに接続すると短時間でボットなどのマルウェアに感染すると言われてきた [1-5]．その後，家庭用のインターネット接続も NAT ルータを経由するようになったため，脆弱なパソコンが無防備なまま，直接インターネットに接続される機会は少なくなったが，近年では，パスワードがデフォルトのままの IoT 機器やアプライアンス製品が不正アクセスの対象となり，問題視されている [6-9]．すなわち，ネットワーク上には不特定多数のアドレスに宛てて恒常的に不審なパケットを送付してくる機器が多数存在することを意味している．

このような現状を分析することを目的として，ダークネット観測に関する研究やハニーポットの研究がこれまでに数多く行われてきた．主に，分析手法に関する研究，可視化に関する研究，分散型走査活動検出に関する研究などがある．また，長期観測に着目した研究や複数センサーの情報を統合する研究なども行われている．

しかしながら，ダークネット観測とその分析には，いくつかの困難な問題がある．近年のインターネット接続ノード数の増大やトラフックの増大に対して，観測用センサーの数と設置場所に制限がある．また，ダークネットへ着信する多数の目的不明の通信から，その意図を推定することの困難さである．

そこでこの研究では，不特定多数のホストアドレスを走査する宛先アドレスの出現パターンを類型化することを目的として，長期間かつ多数のセンサーから得られた情報を分析した結果を示す．分析の結果から，送信元あるいは宛先アドレスごとの着信頻度をあまり増大させない走査方法の実態が明らかとなり，今後のダークネット観測およびその分析に資するものと考える．

2. ダークネット観測に関する既存研究

ダークネット観測に関する様々な既存研究においては，元々，IPv4 空間内で予約されているなどの理由で未定義となっているアドレスを対象としている場合と，すでに AS に属しており BGP で広告されているにも関わらず，DNS に FQDN が登録されておらず，第三者に対して用途が明示されていない IP アドレスを対象としている場合とがある．いずれにしても，これらは通常のネットワーク利用において接続するはずのないアドレスであり，このアドレスへの偶発的でない接続要求は，何らかの意図を持っているものと考えられる．

2.1 既存研究

これまでに，未定義アドレスや未使用アドレスへ着信するパケットを分析する，ダークネット観測やハニーポットに関する研究が数多く行われてきている．

分析手法に関する研究には，攻撃挙動の特徴抽出 [10]，踏み台の検出 [12]，攻撃ロジックの観測 [13]，攻撃プログラムの分類 [14]，ハニーポットによる分析 [11]，攻撃目的と推定される通信の抽出 [15] などがある．

可視化に関する研究には NICTER の可視化 [21]，可視化とハニーポットの併用 [22]，データベースを併用した長期間データの可視化 [23] などがある．

また，分散型走査活動検出に関する研究には，頻度分析による検知手法 [16]，その学習アルゴリズムの提案 [17]，ペイロードの同一性を利用する手法 [18]，着信日時とペイロードを用いる手法 [19]，宛先アドレスの変化回数を用いる手法 [20] などがある．

さらに，長期観測に着目した研究 [24], [25], [26] や複数センサーの情報を統合する研究 [27], [28], [29] なども行われている．

これらの研究においては，いずれも，通常ではパケットが着信するはずのないアドレスへ着信したパケットの意図を推定し，その実態を明らかにすることが究極の目的であると言える．そのようなアドレスへ着信する偶発的ない接続要求は，主に (1) 情報収集などの調査活動，(2) 既知の脆弱性の不正利用のいずれかが目的であろうと推測できる．

2.2 情報収集などの調査活動目的

ネットワークにどれほどのサービスが存在し，どれほどの脆弱性が放置されているか，あるいはそれらのアドレスへの疎通状況などを調査，公表するために，不特定多数のアドレスを恒常的に走査する活動が行われている．

SHODAN[30] や Censys[31] などでは走査活動の結果をデータベース化し，ウェブインターフェースを介して一般に公開するサービスを行っており，走査を行う送信元アドレス帯が公表されている．ミシガン大学では全アドレス空間を走査する研究を行っており，調査パケットの送信元となるアドレスを公表している [32]．いずれも放置されている脆弱性への注意喚起を目的としているが，その情報を利用した不正通信の増大も懸念されてきている．この他にも，不特定多数が利用可能な DNS サービスやプロキシを検索し，その結果をウェブ上に公表するなどの活動もある．

これらのサービスでは，常に最新の情報を入手する必要があるため，走査は定期的に行われるが，不正な目的の通信と解釈されることが無いよう，実稼働中の機器やサービス及びそれらの接続されたネットワークに悪影響を与えないよう配慮されている場合が多い．

また，特定のアドレス範囲を走査するためのツールとして nmap[33] や zmap[34] が知られており，全 IPv4 空間を誰でも容易に走査することができる．

2.3 既知の脆弱性の不正利用目的

既知の脆弱性を利用可能なアドレスやサービスを検索する不正利用目的の通信がある．脆弱性が利用できた場合は，機器へ侵入，権限の昇格，コードの実行，情報の取得の他，BitCoin の Miner の実行，RAT 経由の DoS 攻撃など，様々な用途に利用される可能性がある．

とくに近年では，脆弱性対策のためのアップデートを，ネットワークに接続して行うという本末転倒な対応を強いられる場面が想定される．脆弱性対策を行うべく，脆弱性対策前の機器をネットワークに接続するようなことがあれば，攻撃者はその機を逸することがないよう，可能な限り多くのアドレスへ可能な限り高速かつ継続的に攻撃コードを送付し続ける必要がある．

しかしながら，攻撃側のアドレス数や帯域幅などのリソースも限られているであろうし，昨今ではそのような意図不明で高速な走査活動はその着信頻度から容易に検知，排除できるようになってきているため，送信側はこれを検知されないように様々な工夫を行なってきている．

2.4 分析対象

現状，未使用アドレス空間へは多種多様かつ多数の通信が到達しており，その全容を明らかにすることは容易ではない．ここで，それらの通信の目的が上記の 2 通りに大別できるものと考えると，いずれの目的であろうとも，できる限り多くのアドレスを，できる限り高速に走査しようとするであろう．しかしながら，前者の場合はその通信が実通信に悪影響を及ぼさないように，後者の場合は検知を逃れるようにするために，対象アドレスの順序をランダム化するなどの工夫が行われている．

この研究では，観測中のセンサーアドレス空間を全走査するような一連の活動を抽出し，それらの走査順序等を類型化するとともに，送付されたペイロードを取得することで走査意図の推定に役立つ分析を行うことを目的とする．

3. 観測システム

観測対象のセンサーアドレスは，BGP で広告している 2048 アドレスから，実運用に使用しているアドレス帯を除いた約 1,500 アドレスである．観測システムは 1 台の PC 内に設置した 2 台のバーチャルマシンにより，図 1 のように構成した．

境界ルータにミラーポートを設置し，これをバーチャルマシン `Observer` のアドレスのないインターフェースに接続する．`tcpdump` コマンドのオプションにて実運用中のアドレスを除外して，それ以外の通信をすべてキャプチャして保存する．

もう一台のバーチャルマシン `Responder` には同じミラーポートに接続したインターフェースと，実アドレスを持つインターフェースの二つのインターフェースを用意する．

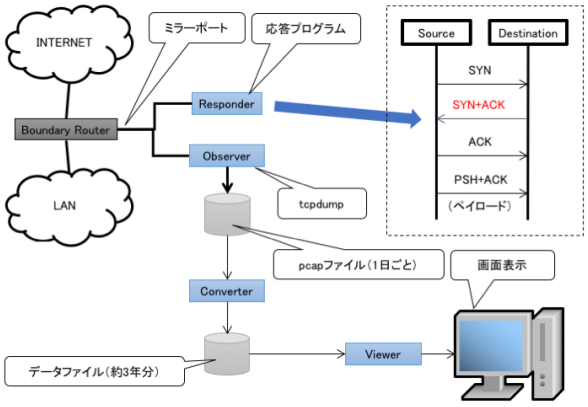

図 1 観測システム

表 1 観測パケット総量

年	送信元 IP 数	総パケット数	サイズ合計
2014	10,820,482	1,784,737,682	377 GB
2015	7,782,370	802,817,763	354 GB
2016	31,401,336	7,715,811,575	1.2 TB
2017	43,033,563	33,331,096,398	4.4 TB

ミラーポート側で未使用アドレス宛ての `SYN` パケットを着信すると，そのパケットの宛先アドレスを送信元アドレスとする `SYN+ACK` パケットを生成し，`RAW` ソケット経由で送信するとともに，セッション切断用の `RST` パケットを送信する．

本システムは 2013 年末から観測を開始しており，これまでにキャプチャしたパケットの総量を表 1 に示す．一部，施設の都合等により観測が停止していた時期を含む．また，2014 年 5 月 16 日に BGP への広告内容を一部変更したため，その前後で観測アドレス数が若干異なる．以下では 2014 年の観測データの分析結果を示す．

4. 分析結果

ここでは，2014 年の 1 年間の観測データの分析結果について示す．

4.1 走査対象アドレス数

まず，送信元アドレスごとの宛先アドレス数（センサーアドレス数）を調べた．宛先アドレス数は限られているため，宛先アドレス数が一致する送信元アドレス数を調べた．すなわち，ひとつの送信元アドレスから 1 年間に着信したパケットの宛先アドレスの種類数を横軸とし，それに合致する送信元アドレス数を縦軸（対数軸）とした．その結果を図 2 に示す．宛先アドレス数が 256 の整数倍近傍の送信元が多くなっていることから，256 アドレスを単位として走査活動を行なっているものが多いことがわかる．

図 2 内で局所的に最大となるアドレス数ののみを抽出して、表 2 に示す。宛先数 1 のアドレスは観測された全送信

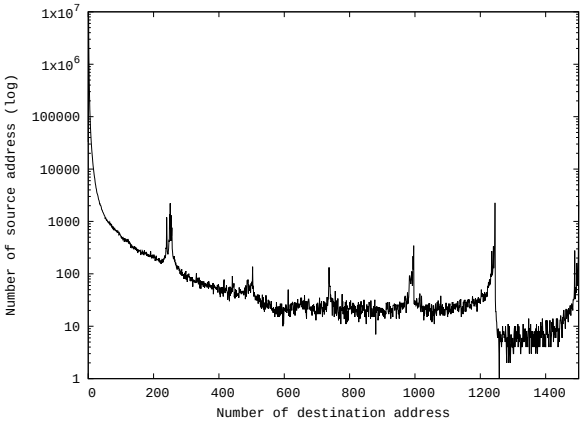

図 2 宛先アドレス数ごとの頻度

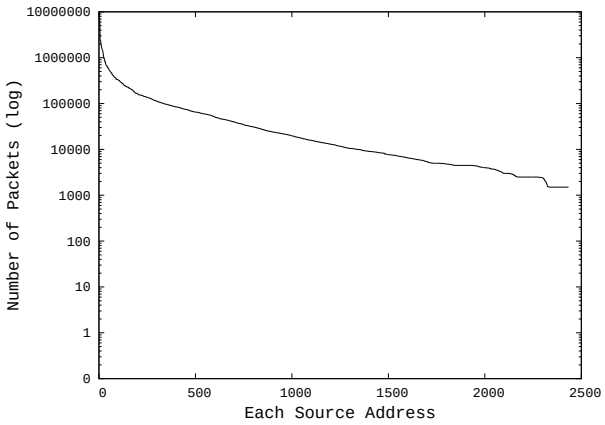

図 3 全数走査アドレスごとの送受信パケット数

表 2 宛先数別の送信元アドレス数（図 2）の局所最大値

宛先数	送信元数
1	7,990,074
240	1,194
249	1,382
251	2,225
254	1,305
503	137
737	133
994	218
996	346
1,240	335
1,244	370
1,245	2,268
1,489	278
1,501	2,434

元アドレス数の約 8 割を占めていることがわかる。

宛先数 1,245 アドレスに顕著なピークがあり，それ以後の送信元アドレス数が少ないことから 1,245 アドレスまでを走査する送信元と，1,245 アドレス以上を走査する送信元とは傾向が異なることがわかる．図 2 右端の全センサーアドレスを宛先とした送信元アドレス数は 2,434 アドレスであった．以後，この 2,434 アドレスを全数走査アドレスと呼ぶ．

4.2 全数走査アドレス

全数走査アドレスは宛先アドレスの種類数は全て 1,501 で同一であるが、それぞれのアドレスに送信したパケット数は異なる。全数走査アドレスを送受信パケット数の多い順に並べた結果を図 3 に示す．右端の 66 アドレスはそのパケット数が宛先センサーアドレス数 (1,501) に一致しているため，同一アドレスへ複数回送信していない．左端の最もパケット数が多いアドレスは年間で 9,552,216 パケットを送信しており，各センサーアドレスあたり，平均約 6,000 回の接続を試みている．

送信されたパケット数がセンサーアドレス数に等しい 66 アドレスについて，パケット着信日時と宛先アドレスを調査した．66 アドレスのひとつ 37.187.198.238 から着信した日時と宛先アドレスを図 4 に示す．横軸は実時間の epochtime、縦軸はセンサーアドレスの番号である。全アドレスに 1 回ずつ，かつ実アドレスの若い方から順に，ほぼ一定時間間隔で送信してきていることがわかる．66 アドレスのほとんどはこの図 4 と同様の結果となった．

しかしながら，いくつかのアドレスからのアクセスは，全センサーアドレスへ 1 回ずつパケットを送信している点は同じでも，その宛先のアドレス順序が異なる．27.214.130.177 の場合を図 5 に，199.233.236.222 の場合を図 6 に示す．このように，1 年間を通して，各センサーアドレスへ各 1 回のみのパケットを送信した場合であっても，その宛先アドレスの順序には差異があることがわかる．これはパケットを送信するプログラムの宛先アドレス選定アルゴリズムを直接的に表しており，そのアドレスの変化のさせ方の違いを観測できていると言える．

なお，図 4 から図 6 のグラフの途中の 2 箇所の空白は，当時，アドレス範囲が広告されておらず着信できていないアドレス帯と，実運用に使用中のためにキャプチャを行なっていなかったアドレス帯である．この他にも直線に見える部分内にも運用中のために除外されて観測していないアドレスがある。

空白アドレス帯の前後が直線で補完できる場合（直線を延長したときに接続可能な場合）は，観測できていなくともそのアドレスにもパケット送信を行なっているものと推定できるが，もしそのアドレス帯を飛ばして直後に次のアドレス帯に移っていた場合（すなわち直線がつながらず段差に見える場合）は，BGP の広告を見た上で，該当のアドレス帯のみを狙って走査しているものと推定できる．手動で確認した範囲では，そのような走査を行なっているアドレスは無かったが，今後，全送信元について検証したい．

4.3 宛先アドレス変化の類型

年間最多パケット数の送信元アドレスの第 10 位までを表 3 に示す．パケット数が多いアドレスが必ずしも長期間

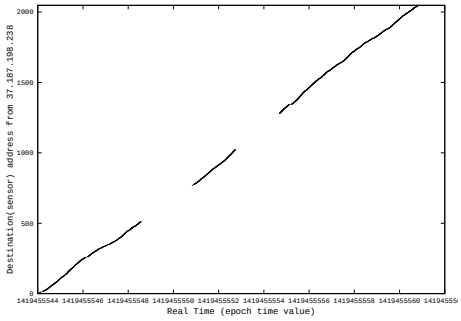

図 4 37.187.198.238 からの着信日時と宛先アドレス
AS16276 OVH SAS (FR)

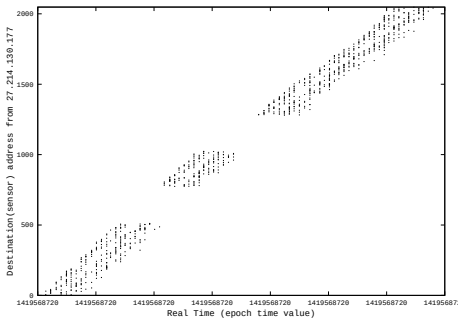

図 5 27.214.130.177 からの着信日時と宛先アドレス
AS4837 CNCGROUP China169 Backbone (CN)

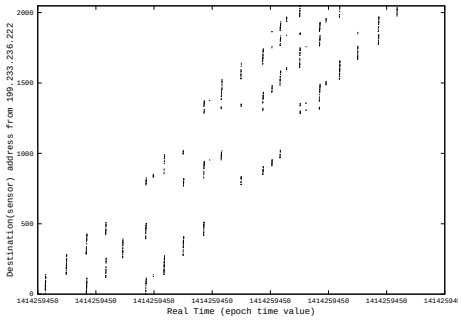

図 6 199.233.236.222 からの着信日時と宛先アドレス
AS46261 QuickPacket, LLC (US)

送信し続けているとは言えない．第 1 位のアドレスからのパケットは 2 月 3 日から 4 月 10 日の間にのみ着信している．なお、第 9 位はゲートウェイアドレスのキャプチャ除外漏れである．

第 2,5,7,10 位のアドレスは TTL の値が表示範囲内でランダムに変化していた。とくに中国からの着信では TTL の値が ±1 程度変化することはあるが、定常的にこれだけ大きく変化するのは意図的なものと推測できる。

第 6 位と第 8 位は TTL 及び宛先ポート番号が頻繁に変化していた。これは一定時間特定のポートを走査し、その後、別のポートを走査することを繰り返していた。

第 10 位の宛先ポート番号は、それぞれの宛先アドレスに対して、表下に示すポート番号を順に走査していた。既知のポート番号リストを元に順に走査する挙動は nmap で使用される nmap-services と同一である。

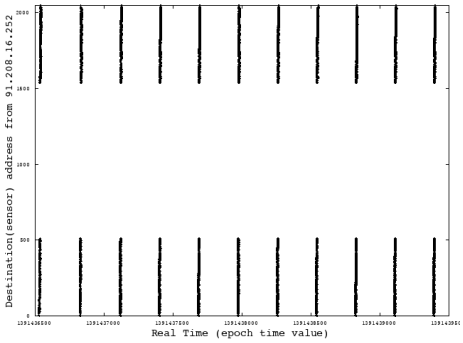

図 7 91.208.16.252 からの宛先アドレスの推移

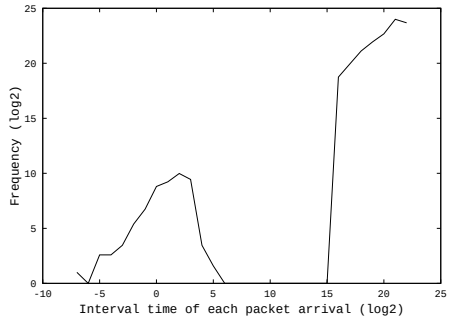

図 8 図 7 の着信時間間隔の頻度

パケット数が第 1 位のアドレスからの数時間にわたる着信の様子を図 7 に示す．図 4 から図 6 の全数走査アドレスの場合と異なり、センサーアドレスの上位と下位のセグメントのみが走査されており、一定量の送信を行なった後，一定間隔を開けて同様の送信を繰り返しているように見える．

そこで，着信時間間隔のヒストグラムを求めた。その結果を図 8 に示す．横軸は着信時間間隔（秒）の 2 の対数値であり，0 のとき 1 秒間隔，10 のとき 2^{10} 秒間隔でパケットが到着した回数を 2 の対数で縦軸に表している．2^6 から 2^{15} 秒間隔の出現数はゼロであり，その前後に度数があることから，約 1 秒前後の間隔で連続してパケットを着信した後，2^{16} 以上の時間を開けて，再度，約 1 秒間隔で着信していることがわかる．

したがって，2^{10} 秒間隔をしきい値として，それ以下の着信時間間隔が連続する時間帯をひとつのブロックとして切り出すことにより，繰り返し送信される一連のパケット群を抽出することができる．そのうちの 1 ブロックのみに着目し，宛先アドレスの時間変化を表示した結果を図**??**に示す．すなわち，これは図 7 の垂直方向の 1 本の直線を時間軸方向に引き伸ばしたものになる．さらに，同一ブロック中で同一アドレスへの複数回の接続を削除し，初回接続のみをプロットすると図 10 になる．

このようにして得られた各送信元からの宛先アドレスの変化をさらに詳細に調べる．図 9 は 1 ブロックを切り出したため，全体でも 30 秒程度である．このため，横軸を実時間ではなく，データの並び順に置き換え，各点を線で結

表 3 年間最多パケット数の送信元アドレス（第 10 位まで）

順位	IP アドレス	パケット数	CC	AS 番号	TTL	Port	着信日
1	91.208.16.252	44,604,863	RU	AS57430	57	5900	2/3∼4/10
2	186.2.161.103	17,820,852	BZ	AS262254	76∼115	21,22	3/26 6/15∼17
3	208.87.34.30	17,076,421	BS	AS18635	52	22	11/11∼12/31
4	114.202.2.12	16,621,119	KR	AS9318	53	22	8/22,23
5	84.22.47.94	10,074,780	RS	AS33983	109∼112	445	1/3∼12/3
6	93.174.93.51	9,552,216	SC	AS29073	多数	多数	1/12∼12/31
7	89.45.14.31	8,953,072	FR	AS39855	76∼116	21,22	3/9∼4/5 6/28,29 7/2
8	69.163.40.28	8,761,449	US	AS46816	多数	多数	6/24∼7/3
9	150.99.**.**	8,285,807	JP	AS2907	-	-	(SINET gateway)
10	218.77.79.43	7,462,991	CN	AS4134	239∼243	†1	6/12∼12/31

†1 : 21,22,23,25,53,80,443,3389,8080

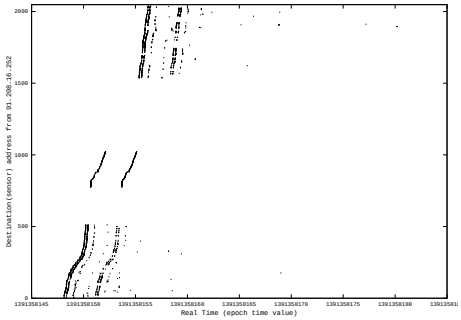

図 9 図 7 の最初の 1 ブロックの拡大

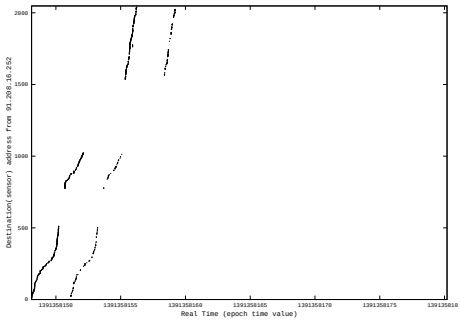

図 10 図 9 の初出アドレスのみ

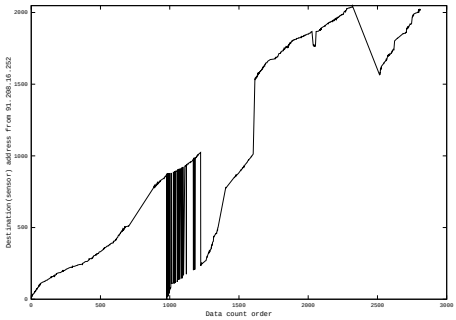

図 11 図 10 のデータの並び順

んだ結果を図 11 に示す．これは図 9 をさらに横方向へ引き伸ばした形となる．途中，セグメントをまたいだ付近で乱れているように見えるのは，アドレスの並び順を意図的に乱すために乗算合同法のような，乱数を加えて剰余を取る演算が行われているものと推測できる．

5. まとめ

ここでは，(1) 多数の連続したダークネットアドレスを監視するセンサー，(2) 接続要求に擬似応答することによるペイロードの取得，(3) 長期間の連続観測，の 3 つの特徴を持つ観測システムで得られた観測データの分析結果について述べた．全センサーアドレスを走査した複数の送信元アドレスごとに，一連の走査の繰り返し間隔を求めた上で，宛先アドレスの変化の様子を調査した．この結果，以下のいくつかの知見を得ることができた．

- センサーのアドレス数に対し，特定の送信元が走査するアドレス数は少ないものが多く，全アドレスを走査する送信元は一部である．
- 宛先アドレス数が多いものが長期間走査を行なっているとは限らず，短時間に多くのアドレスを走査するものもある．
- 走査パケットの密度を上げないように走査パケットの時間間隔を長めにした上で，隣り合う宛先アドレスの差分が一定にならないように順序を変更しているものが多い．
- 遅延等により着信パケットの順序が入れ替わったと推測できる場合があるが，着信したパケットの宛先アドレスの変化の様子から，宛先アドレスの概ねの変化順序を取得することができる．

今後，この分析結果を踏まえてアドレス変化のアルゴリズムの推定，類似の走査方法を行うアドレスのグループ化，ペイロード情報を加味した上で走査意図の推定を行いたい．とくに長期間の蓄積データ処理ではなく，一定時間間隔内のアドレス変化の様子を連続的に観測することで，不正な意図を持つ通信を実時間で観測できるシステムへと発展させたい．

参考文献

[1] パッチ未適用の Windows システム，「生存時間」は約 20 分–米調査, http://japan.cnet.com/news/sec/story/0,2000056024,20070526,00.htm (2004/8/18).

[2] 「国内ユーザーの 40 人に 1 人がボットに感染」—Telecom-ISAC などが調査, https://tech.nikkeibp.co.jp/it/free/ITPro/NEWS/20050727/165402/ (2005/07/27).

[3] ネットで検証, パッチなしの Windows 2000 は 1 時間強で侵入される, http://www.atmarkit.co.jp/news/200603/21/symantec.html (2006/3/21).

[4] 深く静かに広まる「ボットネット」の恐怖 — 第 4 回　面倒でも地道なウイルス対策こそが重要，パッチなしではたった 5 時間で感染, https://tech.nikkeibp.co.jp/it/article/COLUMN/20071022/285119/ (2007/11/01).

[5] 脆弱な PC の生存時間はネット接続から約 4 分, https://it.srad.jp/story/08/07/19/1959205/ (2008/7/20).

[6] 脆弱性の公開から攻撃までが短期化–侵入前提の対策を：IBM 東京 SOC 分析, https://japan.zdnet.com/article/35053019/ (2014.8.28).

[7] Kovah,Kallenberg - CanSecWest 2015: ハッカーが 2 分以内にマルウェアを埋め込める BIOS の脆弱性が発見される https://gigazine.net/news/20150330-bios-hack/ (2015.3.30).

[8] モバイル Wi-Fi ルーターがマルウェアの感染経路になっていた！日本を狙った「XXMM」亜種の特徴的な感染経路, https://internet.watch.impress.co.jp/docs/news/1099223.html (2017.12.27).

[9] 不正侵入やデータ流出にかかる実際の時間とは？　ハッカー調査で判明 (1/2), http://techtarget.itmedia.co.jp/tt/news/1806/14/news03.html (2018.6.14).

[10] 福島 祥郎, 堀 良彰, 堀 良彰, “ダークネット観測データに基づく攻撃挙動の特徴抽出に関する考察”, 電子情報通信学会技術研究報告, 情報通信システムセキュリティ (ICSS), IEICE technical report Vol.109, No.285, pp.37-42, 2009.

[11] 池部実, 宮崎桐果, 吉田和幸, “ハニーポットによる大分大学におけるダークネット宛通信の分析”, 情報処理学会 CSEC Vol.69, No.17, pp.1-8, 2015.

[12] 後藤洋一, 中村康弘, “ダークネット観測結果とアクティブスキャンを用いた踏み台検出手法の提案”, コンピュータセキュリティシンポジウム (MWS2014), 2A1-2, pp.308-313, 2014-10-22.

[13] 小堀 佳和子, 稲村 勝樹, “状態変化型リアクティブセンサーを用いた攻撃ロジック観測手法の提案”, コンピュータセキュリティシンポジウム (CSS 2017), Vol.2017, No.2, 2017-10-16.

[14] 芦野佑樹, 中村康弘, 矢野由紀子, 島成佳, “サイバー攻撃の初期段階と推定される活動で使用されるプログラムの分類手法の提案と評価”, コンピュータセキュリティシンポジウム (CSS 2017), 3B3-1, pp.1238-1245, 2017.

[15] 鮫島礼佳, 芦野佑樹, 矢野由紀子, 須尭一志, 矢野由紀子, 中村康弘, “サイバー攻撃の有無が不明な通信データからサイバー攻撃目的と推定される通信を抽出する手法の提案”, 第 82 回コンピュータセキュリティ (CSEC) 研究発表会, Vol. 2018-CSEC-82, No.41, 2018.

[16] Yaokai Feng , Yoshiaki Hori , Kouichi Sakurai , Jun'ichi Takeuchi “A Behavior-based Method for Detecting Distributed Scan Attacks in Darknets”, Journal of information processing, Vol.21, No.3, pp.527-538, 2013-07-15.

[17] 王 サン, フォン ヤオカイ, 川本 淳平, 堀 良彰, 櫻井 幸一, “挙動に基づくポートスキャン検知の自動化に向けた学習アルゴリズムの提案とその性能評価”, 情報処理学会論文誌, Vol.56, No.9, pp.1770-1781, 2015.

[18] 中村康弘, “初期ペイロードに着目したネットワーク走査活動の分析”, 情報処理学会 第 79 回全国大会, 5D-2, Vol.3, pp.523-524, 2017/3/17.

[19] 梶川慶太, 中村康弘, “分散型走査グループの検知と攻撃ペイロードの分類”, 第 16 回情報科学技術フォーラム (FIT2017), 講演論文集 第 4 分冊, pp.181-182, 2017.9.12-14.

[20] 梶川慶太, 中村康弘, “宛先変化数に着目した分散走査活動の検出”, 2018 年電子情報通信学会総合大会, D-19-2, 2018.3.21.

[21] 中尾康二, 松本文子, 井上大介, 馬場俊輔, 鈴木和也, 衛藤将史, 吉岡克成, 力武健次, 堀良彰, “インシデント分析センタ nicter の可視化技術”, 信学技報 ISEC Vol.106, No.176, pp.83-89, 2006.

[22] 曽根直人, 正力達也, 鳥居明久, 村尾岳人, 森井昌克, “可視化によるダークネットの不正パケット解析：ハニーポットとの併用による相関分析”, 信学技報 ICSS Vol.111, No.495, pp.43-48, 2012.

[23] 芦野佑樹, 鮫島礼佳, 矢野由紀子, 島成佳, 中村康弘, “センサーが捕捉した通信データの解析を支援する可視化手法の提案”, 2018 年暗号と情報セキュリティシンポジウム (SCIS 2018), 1E1-2, 2018.

[24] 水谷 正慶, 渡邊 裕治, “調査対象の IP アドレス属性を考慮した長期的な攻撃元ホストの振る舞いの分析”, コンピュータセキュリティシンポジウム (CSS 2017), 3B4-3, Vol.2017, No.2, 2017-10-16.

[25] 芦野佑樹, 山根匡人, 矢野由紀子, 島成佳, “長期間に渡るインターネットノイズの観測に基づいたサイバー攻撃の初期活動と推定される通信の発信源を分類する手法の提案”, 第 78 回コンピュータセキュリティ (CSEC) 研究発表会, Vol.2017-CSEC-78, No.6, p.1-8, 2017.

[26] 鮫島礼佳, 芦野佑樹, 矢野由紀子, 島成佳, 中村康弘, “長期間の観測データを用いたサイバー攻撃と推定される通信を分析する手法の提案”, 2018 年暗号と情報セキュリティシンポジウム (SCIS 2018), 1E1-1, 2018.

[27] 村上 洸介, 蒲谷 武正, 千賀 渉, 鈴木 将吾, 小出 駿, 島村 隼平, 牧田 大佑, 笠間 貴弘, 衛藤 将史, 吉岡 克成, 井上 大介, 中尾 康二, “複数のダークネット観測拠点で同時期に急増する攻撃を検知する手法の提案”, コンピュータセキュリティシンポジウム (CSS 2014), Vol.2014, No.2, pp.32-39, 2014-10-15.

[28] 村井 健祥, 古本 啓祐, 村上 洸介, 中尾 康二, 森井 昌克: “複数のダークネットに対するトラフィックデータ解析とそこからの情報漏洩について”, 第 14 回情報科学技術フォーラム (FIT2015), 講演論文集 Vol.14, No.4, pp.165-170, 2015/08/24.

[29] 芦野佑樹, 鮫島礼佳, 矢野由紀子, 須尭一志, 矢野由紀子, 中村康弘, “インターネットに接続されたサイバー攻撃観測用センサーの環境に関する考察”, 第 82 回コンピュータセキュリティ (CSEC) 研究発表会, Vol. 2018-CSEC-82, No.40, 2018.

[30] SHODAN, https://www.shodan.io (2018/7/10 参照).

[31] censys, https://www.censys.io (2018/7/10 参照).

[32] Computer Science & Engineering, University of Michigan, http://researchscan273.eecs.umich.edu (2018/7/10 参照).

[33] Nmap: the Network Mapper - Free Security Scanner, https://nmap.org (2018/7/10 参照).

[34] The ZMap Project, https://zmap.io (2018/7/10 参照).