Computer Security Symposium 2021
26 - 29 October 2021

ダークネットに対する並列走査アドレスグループの推定手法

ファン・アン・ソン[1,a)]　中村　康弘[1,b)]

概要：インターネット上の不特定多数のアドレスへの不審な通信が数多く観測されており、近年では急激に増加する傾向にある。これらの通信の目的を推定するために、着信パケットヘッダに含まれる送信元アドレスや接続先ポート番号等を調査・分析する研究が行われている。攻撃者がコンピュータやネットワークアドレスなどのリソースを多数保有している場合には、それらを活用して目的を達成しようとするであろうと推定できる。そこでこの研究では、攻撃者は特定の AS 内の複数アドレスを同時に用いて、同一のペイロードを並列送信するものと仮定する。この前提に基づき、多数の着信パケットの中から、特定の意図に基づき、特定 AS 内で分散化されたアドレスから同一ペイロードを並列送信するアドレスグループを抽出することを目的とする。処理アルゴリズムを提案し、実データに適用した結果、複数の送信元アドレス群を抽出することができた。得られたアドレス群から送付されたペイロードを調査することにより、送信者の規模と意図の推定に有益な情報を得ることができた。

キーワード：ダークネット、並列走査、初期ペイロード

A Method for Estimating Parallel Scan Address Groups on Darknet

Son Pham Anh[1,a)]　Yasuhiro Nakamura[1,b)]

Abstract: A large number of unnumbered communications to unspecified addresses on the Internet have been observed, and the number has been increasing rapidly in recent years. To estimate the purpose of these communications, research has been conducted to investigate and analyze source addresses, destination port numbers, and other information contained in incoming packet headers. If an attacker has a large number of resources such as computers and network addresses, it can be assumed that he will try to utilize them to achieve his goal. Therefore, in this study, we assume that the attacker will use multiple addresses in a particular AS simultaneously to send the same payload in parallel. Based on this assumption, we aim to extract from a large number of incoming packets a group of addresses that send the same payload in parallel from distributed addresses within a specific AS, based on a specific intention. As a result of proposing a processing algorithm and applying it to real data, we were able to extract multiple source address groups. By examining the payloads sent from the obtained address groups, we were able to obtain useful information for estimating the size and intention of the senders.

Keywords: Darknet, Parallel Scan, Initial Payload

1. はじめに

インタネット上では不特定多数の宛先 IP アドレスへ大量の不審なパケットが送信されている。その活動傾向と脅威を早期に発見するために、未使用 IP アドレス空間であるダークネットで着信パケットを観測する。ダークネットへ着信するパケットはいくつかの理由で送信されると考えられる。アドレスの誤入力などの人為的誤り，マルウェアによる感染対象の探索活動，ボットネットや手動操作によるアドレススキャンやポートスキャンなどである。従来のステルスダークネット観測システムでは接続要求パケットのヘッダ情報から、送信元，送信先，ポート番号等の限られた情報しか得ることができない。また、NICTER の年間観測レポートによると、近年ではパケット量が急増する一方であり、送信者の意図を推移することが一段と困

[1] 防衛大学校理工学研究科
Graduate School of Science and Engineering, National Defense Academy of Japan
[a)] phamsonhvhc@gmail.com
[b)] yas@nda.ac.jp

難になっている [1]。送信者の意図を推定するためには、送信側の挙動を観測しつつ送受信をエミュレートするハニーポットが有効であるが、あらかじめ予測したプロトコルおよび脆弱性への攻撃観測に限られるとともに多数のアドレス空間での観測はコストが高くなる。

そこで、この研究では、最初の接続要求に対して擬似応答を行い、初期ペイロードのみを取得する観測システムを用いる。得られた初期ペイロードの内容を分析することで、パケットヘッダ情報に加えてさらに多くの情報を得ることができ、送信者の意図の推定に利用できる。また、多数アドレスを同時利用可能な送信者は、走査活動が検知されにくくするとともに走査効率を上げるため、複数の送信元アドレスを同時並行的に利用して、同一の走査プログラムを実行する場合があると仮定する。本研究はこの前提に基づき、多数の着信パケットの中から、特定の意図に基づき、特定 AS 内の複数アドレスから同一ペイロードを並列送信するアドレスグループを抽出することを目的とする。この方法で得られるアドレスグループには、(1) 上記の仮定に基づく意図的な走査活動、(2) 独自のペイロードによりネットワーク走査を実施している企業等、(3) 特定の AS 内でのみ感染流行している新種マルウェアからの並列走査活動などが含まれることが予想できる。処理アルゴリズムを提案し、実データに適用した結果、複数の送信元アドレス群を抽出することができた。得られたアドレス群から送付されたペイロードを調査することにより、送信者の規模と意図の推定に有益な情報を得ることができた。

2. 関連研究

山門ら [2] は自組織内からダークネットアドレスへ送信するパケットは不適切な通信とみなし、通信ログと擬似応答により取得できた初期ペイロードを元にその通信を発生させたアプリケーションを自動的に特定する研究を行った。

笹生ら [3] はダークネット観測結果から 24 時間毎の宛先アドレス数、パケット数による通信パターンの種別と OS フィンガープリントによる送信元を分類した。ダークネット全空間に対するスキャンを行う送信元の数は非常に少ないが、半分のパケットはこれらのホストから発生していることがわかった。また、1 回しか送信してこなかった送信元の数は非常に多かったが、着信したパケット全体の 4%にすぎないことを明らかにした。さらに、OS による分類結果は Windows と Linux2.4.x からのパケットが支配的であるとわかった。しかし、この分析法によると、24 時間以上の周期で通信するホストや時間をずらしながらスキャンを行う攻撃者の送信を捕捉することができない。

中村ら [4] 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、その走査順序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、走査活動や意図の推定を行った。これにより全アドレスを走査する送信元は一部であり、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に順序を変更しているものが多いことを明らかにした。

ソンら [5] はダークネット観測センサに着信したパケットの中から、特定の AS 内の複数のアドレスから一定時間内に同一のペイロードを送信するような走査活動に着目した。このようなアドレス群の挙動をパターン化する手法を提案した。これにより、多数のアドレスを利用しダークネットへ走査活動を行ったアドレス群の存在を確認し、それらの挙動を分類することができた。

3. 提案手法

本研究で提案される手法は次の手順で行われる。

- ステップ 1 : 観測データ内のペイロードのあるパケットから以下の情報を抽出する。
  (1) ペイロードのハッシュ値（MD5)
  (2) AS 番号
  (3) 送信元 IP アドレス
  (4) 宛先 IP アドレス
  (5) 送信時刻
- ステップ 2 : ステップ 1 で抽出した情報を用い、特定の AS のみから送信されたペイロードのハッシュ値をキーとして、送信元の AS 番号と送信元 IP アドレス数を抽出する。
- ステップ 3 : 送信元 IP アドレス数の多い順にペイロードのリストを並び替える。
- ステップ 4 : ペイロードの内容を確認し、送信者の意図推定を行う。

4. 実験と結果

4.1 実験データ

提案手法の有効性を検証するため、既存の AS に割り当てられたアドレス範囲内で 2017 年 4 月 1 日から 2017 年 4 月 31 日までの間に観測された実データを用いて分析を行なった。観測対象の未使用 IP アドレス数は約 1600 個である。

4.2 実験結果

まず、ひとつの意図に基づく走査活動に利用可能なアドレス数から、その活動の規模を推定するためペイロードごとの送信元アドレス数が多い順に並び替えた。この結果を表 1 に示す。表 1 から、特定の AS 内で同一のペイロードを並列送信したアドレスグループの存在が確認できる。送信元アドレス数が一番多いものは 245 個であった。また、観測アドレス範囲全体へ送信したアドレスグループやひとつの観測アドレスのみへ走査活動を行ったアドレスグループを発見することができた。

観測期間中のペイロードの種類数は 6,952,805 個であり、送信元アドレス数によるペイロード種類数の割合を表 2 に示す。表 2 によると、単一の IP アドレスから送信されたペイロードが 97.65%を占めており、64 から 127 個および 128 から 255 個の IP アドレスを同時利用するペイロードはそれぞれ 273 個、32 個であり、全体のわずか一部であることがわかった。

5. AS ごとの意図推定

表 1 の結果を用いて、AS 毎から送信したペイロード内容の調査を行った結果、ほとんどのペイロードは公開されたポートスキャンプロジェクトによる通信であった。その他、悪意と考えられる通信が存在したことが確認できた。

5.1 AS42570-Portscaning EU-CH-KS

AS42570 はスイスにあるネットワークスキャンをする企業で

表 1　送信元アドレス数順のペイロードハッシュ値

ハッシュ値	AS	送信元数	宛先数
2bc274feeb261a266bdb3f394f4195ef	46573	245	1429
e7eb1630e288b776e748ea197f5818a9	46573	245	1259
cdbb36c5cfb046a28414e1138684d9fe	46573	243	1263
4c37d0424c83c36b9437d79ffaab4453	46573	243	1236
...	...	...	...
f7abe0e61a39def19b9f8991de19e980	12322	171	334
33c48a66f1328e7a33caa1abfd434d3c	14061	149	654
88d62874c2ff30000830610e05371f75	14061	149	1127
6457c1ad96e91f75ea5d0481e7212f4a	14061	149	1132
...	...	...	...
ae88a181a997a3865f1c4c90dffb382a	42570	124	1028
69a1dda9d5fc454a642a09da560b6c0f	42570	123	1012
2d66a76141ee5564a0eea35f4135a721	42570	123	1028
721a7e74ced5fa6f57deb258f2b2d588	42570	99	1614
49b1d72deccce3c5a530477ce0ad93e7	53217	98	1
882bb13c6e19aff32ce19ac221728f6f	53217	93	1
11cfbece2f4b04fdda6db79ab807f1d5	53217	92	1
8f1e9eabc85d1d116d56c84fc10e77e9	53217	92	1
...	...	...	...

表 2　送信元アドレス数の割合

送信元アドレス数	数	割合
1(/32)	6789444	97.65%
2-63(/32-/26)	163056	2.34%
64-127(/26-/25)	273	0.004%
128-255(/25-/24)	32	0.0004%

ある。AS42570 の保有アドレスから送信されたペイロードの一覧を表 3 に示す。AS42570 の保有アドレスから着信したペイロードは 58,990 種類であり、その中で送信元アドレス数が多いもののみ、その内容を調査した。

その結果、ほとんどの通信は 443 番ポートへの TLSv1、SSLv2、SSLv3 の接続要求であり、https サービスを提供する Web サーバの探索という走査活動と推定される。他にポート 1883 に対して、表 4 のようなペイロードも送信された。これは MQTT プロトコル（Messege Queueing Telemetry Transport Protocol）のパケットであり、IoT 機器を調査する目的だと考えられる。さらに、送信したペイロードの送信元をまとめた結果、AS42570 は約 192 個 (3 つの/26) の連続した IP アドレスを利用し、観測センサーの全アドレス空間へ並列に走査活動を行ったことが分かった。送信元アドレスのリストを表 5 に示す。他の AS から送信されたパケット内容も確認したとこと、ほとんどの AS はこの AS42570 のようにプロキシサーバや Web サーバを探索することを目的として多数のパケットを送信していることが分かった。

5.2　AS63199-CapitalOnline Data Ser Co.LTD

AS63199 から着信したペイロードハッシュの一覧を表 6 に示す。この表によると、AS63199 は観測した期間内には全空間へ 47,858 種類のペイロードを送信したことが分かった。また、この AS から送信していたペイロード内容を確認した結果を表 8 に示す。AS63199 からは悪意な意図だと考えられるペイロードが多数確認できた。表 8 のように Cookie にユーザ名を設定して、RDP 経由で不正ログインを狙った通信 [6] や、Windows の Fox Pro に対する試行コードなどが数多く送信されていた。また、データベースを標的としたログイン試行コマンドや IoT 機器を標的とした不正な SSDP（Studidly Simple DDoS Protocol）パケットで発生する 100Gbps の DDoS 攻撃 [7] 用ペイロードも確認できた。特に、Momentum Botnet による TeamSpeak2 UDP ログインリクエストフラッド攻撃 [8][9] と MacOS X サーバに対するシリアル番号化 [8] などの通信も多数発見した。Momentum Bonet は Linux を狙う様々な攻撃を行うマルウェアであり、2018 年 12 月中旬に初めて観測され [10]、

表 3　AS42570 から着信したペイロード一覧

ペイロードのハッシュ値	送信元数	宛先数
69a1dda9d5fc454a642a09da560b6c0f	123	1012
2d66a76141ee5564a0eea35f4135a721	123	1028
179e019766ca85dee5c6ec2e9183c68f	124	1012
9ee436711151c83b1807991219505790	124	1014
...	...	...
faf1a9627065d15628329c3006e8daab	124	1048
672bd690ac48cad9251563b64bc835a8	124	1049
c11910a9905cd51faa0ca8ed6f93df44	124	1053
7f8e6e0937a1670390d8f1e4e8e6e1f9	124	1062
2f27a172d5fe35f0759c490ba67eab99	124	1064
96a325356dd0961973a5d5e73007b77b	124	1068
fa49b4636171925841940101ee1c669a0	124	1072
f23358df3c1e360ed045d52d62a96701	124	1081
a58d49bc902c735596d829435387356b	71	1602
639bd8854a0712233c6e827dda04ca11	71	1615
751ff3d9ba93b16ce7a3101df5978e79	82	1611
bbb7c8e202c820f60b2af2f4fd685f86	89	1616
721a7e74ced5fa6f57deb258f2b2d588	99	1614
...	...	...

表 4　MQTT パケットの内容

```
24 e9 b3 84 fc 41 0c 86 10 a5 fc 30 08 00 45 00   $....A.....0..E.
00 37 6b af 40 00 34 06 c4 66 b9 23 3f a6 ca 19   .7k.@.4..f.#?...
53 c8 94 65 07 5b c2 b4 eb aa 31 9f 58 48 50 18   S..e.....1.XHP.
39 08 7c 0c 00 00 10 0d 00 04 4d 51 54 54 04 02   9.|.......MQTT..
00 3c 00 01 5a                                    .<..Z
```

表 5　AS42570 が使用した IP アドレス一覧

IP アドレス
185.35.63.4
185.35.63.5
185.35.63.8
185.35.63.9
185.35.63.10
...
185.35.63.188
185.35.63.189
185.35.63.190
185.35.63.191

同月 18 日に公開された。本研究で使用した実データの観測時期は 2017 年 4 月であるため、Momentum Botnet の通信は観測されないはずであるが、Momentum Botnet 攻撃通信と全く同じペイロードが観測された。さらに、これら全てのペイロードを同時並列に送信した送信元アドレスは表 7 に示す 37 個である。Momentum の初期の感染活動において、これらの IP アドレスを利用して感染活動や攻撃の試行などを行っていたのではないかと推測できる。

6.　まとめ

本研究では多数のアドレスを利用可能な送信者は、その走査効率を上げるために、複数の送信元アドレスを同時並列的に利用して、同一の走査プログラムを実行する場合があると仮定し、これらの送信元アドレス群を抽出する手法を提案した。実データを用いて分析した結果、並列走査活動アドレスグレープの存

表 6　AS63199 から送信したペイロードの一覧

ペイロードのハッシュ値	送信元数	宛先数
06b59fa62369fc1e9815dcb505080162	37	1512
c7dd66719728d36ac0a6accd5fcfcd6b	37	1521
20a1d4a4a54e3cf08f1cd1770eb0dc66	37	1532
58113f184470d7a063aea1ffbb4bbcfa	37	1549
45fb59e6f55a684ac47f48e446ff2550	37	1562
b26d06c046f15dfec57787024d6c64f2	37	1575
a668727d917520a1bd87a15c1380cec2	37	1576
6bea85f92173b0a9ec293b123ebdf4a9	37	1577
d879ab828b597acdf4ff6328f2605ab8	37	1577
100a9e2cda856218ebc6b03070c464ec	37	1578
788c5ced29ce3e7e65ccb2cfb2b3defe	37	1578
ca66cc18bb9a8311515ed8c20dec7015	37	1581
2487e13d8a2026521511cc85404cb213	37	1582
0f8cc5d0a8b3a3d476ccab1a0f60abc4	37	1583
b160c20f62edfe2ed57a1426845b60d3	37	1583
b21daf8e2171b9a4cccfa551801cb803	37	1583
65f9e11badaceab046de8d1d59a6bb51	37	1584
81647d31e2f92f3f85bbea17b9eee2bd	37	1586
30728cacb60be862905bbfee20ef904e	37	1588
...	...	...

表 7　AS63199 が使用した送信元アドレス

IP アドレス	IP アドレス
118.193.27.8	118.193.26.34
118.193.27.9	118.193.26.35
118.193.27.10	118.193.26.36
118.193.27.11	118.193.26.37
118.193.27.12	118.193.26.38
118.193.27.13	118.193.26.39
118.193.27.14	118.193.26.40
118.193.27.26	118.193.26.41
118.193.27.27	118.193.26.42
118.193.27.28	118.193.26.43
118.193.27.29	118.193.26.44
118.193.27.30	118.193.26.45
	118.193.26.46
118.193.22.234	118.193.90.130
118.193.22.243	118.193.90.131
118.193.22.250	118.193.90.132
118.193.22.251	118.193.90.133
118.193.22.252	118.193.90.134
118.193.22.253	
118.193.22.254	

在を確認することができ、走査活動で並列に使用された送信元アドレス数の割合を求めた。この結果、1 個の IP アドレスで送信したペイロードがほとんどで、多数の IP アドレスで走査活動を行った送信者はごくの一部だと分かった。

次に、送信されたペイロードを確認することで、送信者の意図を推定することができた。スキャン会社によるプロキシサーバや Web サーバの探索するなどのものがほとんどで、それ以外に悪意を持った通信が存在することがわかった。また、AS 毎の送信元アドレスリストを列挙することができ、将来この結果により送信者の能力等を推定する根拠になると考えられる。さらに、Momentum による攻撃通信と同一の初期ペイロードが観測できたため、本手法により、多数の通信履歴の中から作成中のマルウェアの活動や新しい攻撃通信を発見できる可能性を見出すことができた。

しかしながら、実験に用いた観測データにおいては並列走査活動のほとんどは HTTP の接続要求が多数を占めた。HTTP の接続要求では、メソッドと URI が同一であっても、Host: のタグ部分は宛先の IP アドレスが格納されるため、初期ペイロードのハッシュ値が観測アドレスによって異なってしまう。この結果、同一目的で送信されたものであっても、異なるハッシュ値に分類されるため、アドレスグループの検出能力を低下させてしまう。HTTP を代表とするいくつかのプロトコルにおいては、そのプロトコルに応じた自由度を考慮した判定を行う必要がある。例えば、初期ペイロードの先頭からのバイト数を限定して判定するなどの方法が考えられる。

参考文献

[1] 情報通信研究機構 (NICT)、NICTER 観測レポート、https://www.nict.go.jp/press/2021/02/16-1.html

[2] ダークネットあて通信分析によるネットワーク管理者支援、山門 彩、佐藤聡、 新城靖 、情報処理学会研究報告 Vol.2018-IOT-40 No.31、2018/3/6.

[3] 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、Computer Security Symposium 2013、2013/10/21-23.

[4] 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簿分析中村康弘、梶川慶太、芦野佑樹、鮫島礼佳 Computer Security Symposium 2018、2018/10/22-25.

[5] ダークネット観測における特徴的な通信を持った送信元の挙動調査に関する研究、ファン・アン・ソン、中村康弘 Forum on Information Technology 2021、2021/08/25-27.

[6] サイバーセキュリティブログ：ハニーポット月次分析 9 月度 〜Ethereum と Redis〜https://sec-chick.hatenablog.com/entry/2018/10/21/233231、2018/10/21.

[7] Stupidly Simple DDoS Protocol (SSDP) generates 100 Gbps DDoS、Marek Majkowski、https://blog.cloudflare.com/ssdp-100gbps/、2017/06/29.

[8] IoT デバイスやルータを侵害し DDoS 攻撃を仕掛けるボットネット「Momentum」、トレンドマイクロセキュリティ報告、https://blog.trendmicro.co.jp/archives/23361、2019/12/27.

[9] IoT デバイスを標的とするボットネット「Momentum」の最新動向を詳細解説、トレンドマイクロセキュリティ報告、https://blog.trendmicro.co.jp/archives/23361、2020/01/15.

[10] Momentum Botnet、https://digital.nhs.uk/cyber-alerts/2019/cc-3317、Last edited: 2021/01/29.

表 8　AS63199 から送信された初期ペイロードの内容

Hex	ACII	推定目的
24 e9 b3 84 fc 41 0c 86 10 a5 fc 30 08 00 45 00 00 4a 55 26 40 00 3a 06 3d 48 76 c1 16 f3 ca 19 56 72 86 b4 07 aa e6 65 35 66 17 9b 46 50 50 18 00 e5 47 ab 00 00 03 00 00 22 1d e0 00 00 00 00 00 43 6f 6f 6b 69 65 3a 20 6d 73 74 73 68 61 73 68 3d 41 37 30 30 0d 0a	$....A.....0..E. .JU&@.:.=Hv..... Vr.....e5f..FPP. ..G.....”..... .Cookie: mstshas h=A700..	Cookie にユーザ名 をセットして、 RDP 経由で 不正ログインを 狙った通信
24 e9 b3 84 fc 41 0c 86 10 a5 fc 30 08 00 45 00 00 5c 07 0b 40 00 3b 06 8a 51 76 c1 16 f3 ca 19 56 72 85 ee 07 aa a9 36 75 67 ef 40 7c 27 50 18 00 e5 65 91 00 00 66 6f 78 20 61 20 31 20 2d 31 20 66 6f 78 20 68 65 6c 6c 6f 0a 7b 0a 66 6f 78 2e 76 65 72 73 69 6f 6e 3d 73 3a 31 2e 30 0a 69 64 3d 69 3a 32 0a 7d 3b 3b 0a	$....A.....0..E. .:@.;..Qv..... Vr.....6ug.@—’P. ..e...fox a 1 -1 fox hello.{.fox .version=s:1.0.i d=i:2.};;.	Fox Pro 試行する
24 e9 b3 84 fc 41 0c 86 10 a5 fc 30 08 00 45 00 00 d0 2c db 40 00 3b 11 68 e4 76 c1 16 f3 ca 19 51 90 d3 c9 07 aa 00 bc 24 5e f4 be 03 00 00 00 00 00 00 00 00 00 01 00 00 00 32 78 ba 85 09 54 65 61 6d 53 70 65 61 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 57 69 6e 64 6f 77 73 20 58 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 20 00 3c 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 6e 69 63 6b 6e 61 6d 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	$....A.....0..E. ..,.@.;.h.v..... Q.....$ˆ..... .....2x...T eamSpeak..... .....Win dows XP..... ..... . ¡..... .... .nickname.....	Momentum Bonet による、TeamSpeak2 UDP ログインリクエスト フラッド攻撃
24 e9 b3 84 fc 41 0c 86 10 a5 fc 30 08 00 45 00 00 3a 2c da 40 00 3b 11 69 7b 76 c1 16 f3 ca 19 51 90 b2 52 07 aa 00 26 8f 39 53 4e 51 55 45 52 59 3a 20 31 32 37 2e 30 2e 30 2e 31 3a 41 41 41 41 41 41 3a 78 73 76 72	$....A.....0..E. .:,.@.;.i{v..... Q..R...&.9SNQUER Y: 127.0.0.1:AAA AAA:xsvr	Momentum Botnet による、MacOSX サーバ シリアル番号化
24 e9 b3 84 fc 41 0c 86 10 a5 fc 30 08 00 45 00 00 59 a5 f9 40 00 3a 06 ec 65 76 c1 16 f3 ca 19 56 72 b0 65 07 aa a6 82 cc 87 4e 84 da 2a 50 18 00 e5 bb 21 00 00 55 53 45 52 20 74 65 73 74 20 2b 69 77 20 74 65 73 74 20 3a 54 65 73 74 20 57 75 7a 20 48 65 72 65 0a 4e 49 43 4b 20 76 6c 64 62 72 65 7a 79 74 0a	$....a.....0..e. .y...:..ev.... Vr.e.....N..*P. ...!..USER test +iw test :Test W uz Here.NICK vld brezyt.	ログイン試行
24 e9 b3 84 fc 41 0c 86 10 a5 fc 30 08 00 45 00 00 6b 4c f8 40 00 3a 06 45 55 76 c1 16 f3 ca 19 56 72 e4 1a 07 aa db 24 37 9b b7 70 66 41 50 18 00 e5 29 9d 00 00 43 00 00 00 03 00 00 00 ff ff ff ff d4 07 00 00 00 00 00 00 61 64 6d 69 6e 2e 24 63 6d 64 00 00 00 00 00 ff ff ff ff 1c 00 00 00 01 6c 69 73 74 44 61 74 61 62 61 73 65 73 00 00 00 00 00 00 00 f0 3f 00	$....A.....0..E. .kL.@.:.EUv..... Vr.....$7..pfAP. ..)...C..... .....admin. $cmd..... ..listDatabases. .....?.	データベースを 一覧表示
24 e9 b3 84 fc 41 0c 86 10 a5 fc 30 08 00 45 00 00 7f 72 34 40 00 3a 11 25 3d 76 c1 16 f3 ca 19 51 2f 89 74 07 aa 00 6b 80 09 4d 2d 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 32 33 39 2e 32 35 35 2e 32 35 35 2e 32 35 30 3a 31 39 30 30 0d 0a 53 54 3a 75 70 6e 70 3a 72 6f 6f 74 64 65 76 69 63 65 0d 0a 4d 61 6e 3a 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d 0a 4d 58 3a 33 0d 0a 0d 0a 0d 0a	$....A.....0..E. ..r4@.:.%=v..... Q/.t...k..M-SEAR CH * HTTP/1.1..H ost:239.255.255. 250:1900..ST:upn p:rootdevice..Ma n:”ssdp:discover ”..MX:3.....	SSDP による 生成された 100Gbps DDoS 攻撃の仕掛け
…	…	…