

JANOG 33.5 Interim Meeting

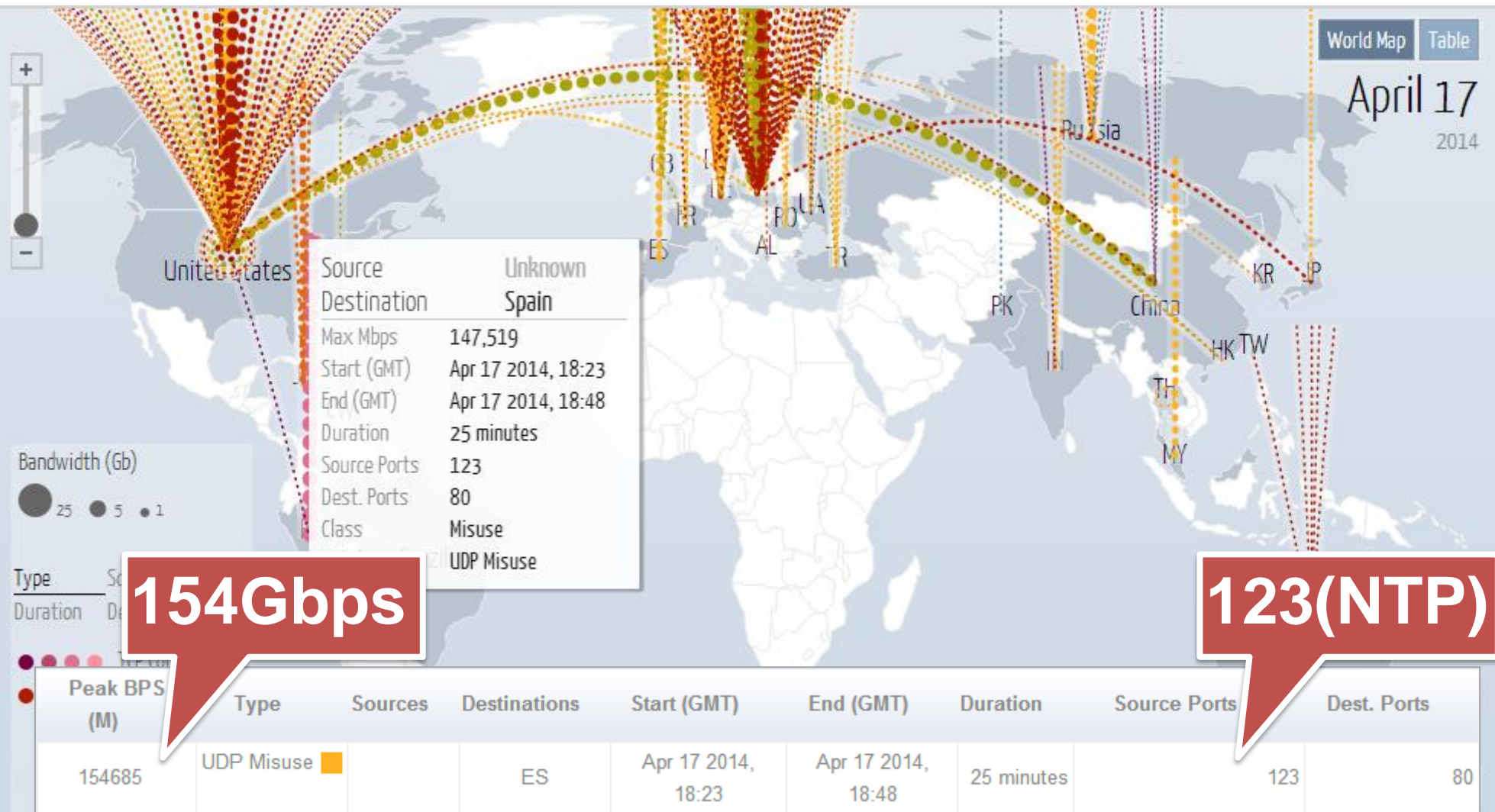
NTP 情報交換WGアップデート

2014年4月18日

JANOG NTP 情報交換WG

チェア 中島 智広
高田 美紀

はじめに (本日の世界の様子)

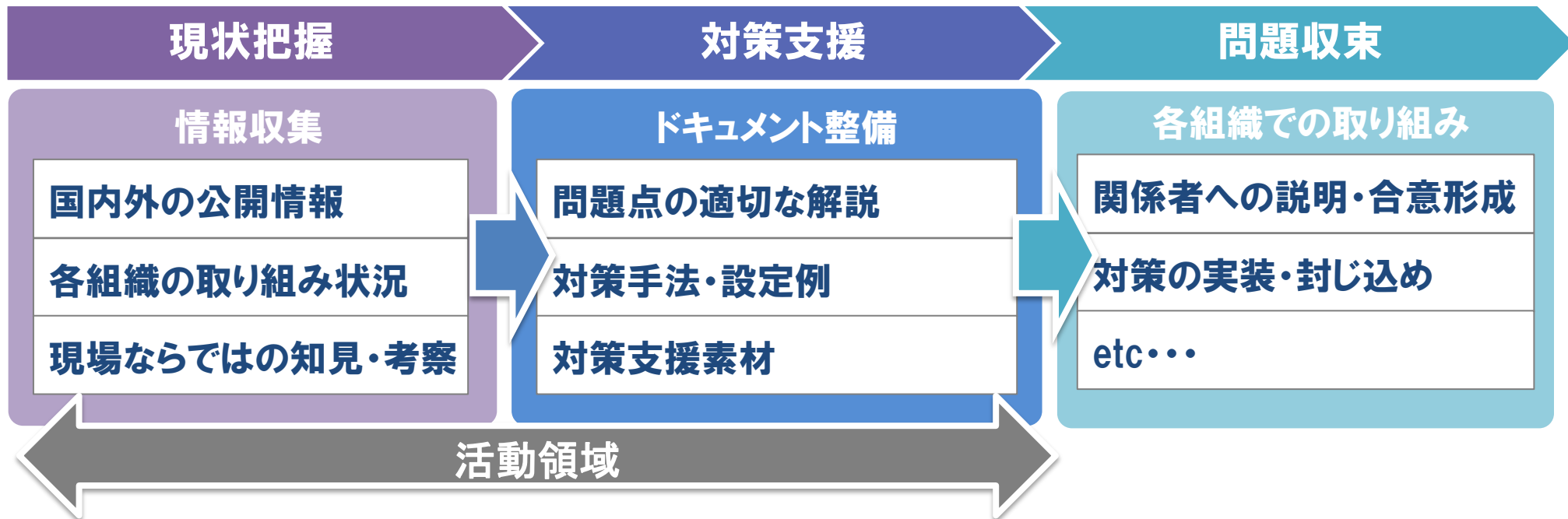


(引用元)Digital Attack Map Top daily DDoS attacks worldwide, <http://www.digitalattackmap.com/>

NTP 情報交換WG 概要

■目的

- 2013年後半より流行している、NTP を用いたDDoS攻撃(NTP Reflection DDoS)の現状把握を行い、ドキュメント整備を通じて対策を支援し、問題の収束に資する



なぜやってるの？（問題意識）

- 攻撃手法は、有効性が広く認知されることで、さらに流行する、いよいよどうにもならなくなる前に収束方向に向かわせたい
- 100Gbps級だけでなく1Gbps級も十分な脅威
 - 5Mbps→1Gbpsは容易に発生可能、しかしサーバのNICはまだまだ1Gbps
 - (そもそも100Gbps級も日常茶飯事になってきているような・・・)
- 危険性を訴えるだけでは誰も得をしない、技術的方法論だけで無く、収束に繋げていくアプローチの模索が必要
- 対策・啓蒙活動を進めていく上での、リファレンス先が不十分必要な人に、必要な情報が、伝わる記述で

活動スタンス

■ スコープ

- UDPを用いたDDoSはNTPだけの問題ではないが、まずは悪用が容易なNTPを喫緊の脅威ととらえ焦点を絞って活動

■ スケジュール

- 現在予定しているドキュメント整備はJANOG34を目処に完了させたい
- 少々時間がかかってもきちんと使えるドキュメントを整備
タイミングが遅れ、世の中に必要とされなくなったとして、それはそれで幸いなこと

活動経過

■第1回ミーティング(2014年2月14日)

- 大雪の積もる中、有志が集まって、持ち寄った情報で議論、まずは叩き台文書を作成することになる

■第2回ミーティング(2014年3月28日)

- 叩き台文書(A4×9枚)を元に議論、成果物の構成、骨子を確定
- 最初の成果物となる「詳解編」の執筆を割り当て、執筆に着手

■第3回ミーティング(2014年5月1日予定)

- 「詳解編」の進捗確認と内容レビュー、公開へ向けての議論
- 次の成果物「設定編」の進め方の議論

成果物構成

1. 詳解編

A4 10頁超の長めの文書。これさえ読めば、課題と取り組むべき内容をひと通り把握できる。対象はエンジニアや、情報システム担当者。

2. 設定編

具体的な設定例や対策例を、機器種別ごとに整理。対象は、エンジニア。





3. 簡易解説編

取り組みに理解を示してもらい、協力を得るための読みやすい資料。A4一枚。対象はITに疎い関係者及びエンドユーザ。

4. テンプレート編

関係者への説明や合意形成に利用可能なテンプレート。対象はxSP事業者。

成果物と進捗

No	成果物	進捗	課題と対応
1	詳解編	 55%	世の中インシデント続き で、執筆陣が工数を捻出できていない、第3回ミーティングで仕切り直し
2	設定編	 0%	対象機器の精査、情報収集ができてない、この場を借りてお願いしてみる
3	簡易解説編	 0%	詳解編が完成してから検討
4	テンプレート編	 0%	これから検討

ちらっと、成果物イメージ

1. 詳解編

1. 概要

2. 問題点

1. 事例からみる脅威

2. メカニズムから見る脅威

3. 対策

1. 攻撃から守る対策

2. 悪用を防ぐ対策

3. 当事者になった場合の対応

4. まとめ

5. 参考資料

次に、NTP Reflection DDoSは、その名の通りNTP(Network Time Protocol)を悪用したDDoS攻撃です。NTPもUDPを用いるサービスの一つであるため、送信元の詐称が容易であり、DDoS攻撃に悪用可能です。NTP Reflection DDoSでは、NTPの通信の中でも特にmonlistが利用されています。これは、NTPサーバの監視機能の一つであり、過剰に通信が行われることでホスト情報を取得するものです(図2参照)。NTPの通信にはmonlistというコマンドがあり、いずれもDDoS攻撃に悪用可能です。その中でもmonlistが最もレスポンスサイズが大きいため攻撃者に好んで用いられています。

Remote Address	Port	Local Address	count	m	ver	rstr	avgint	lstint
Host A	xxxx	X.Y.Z.A	xxx	x	x	0	xxxxx	xxxxx
Host B	xxxx	X.Y.Z.B	xxx	x	x	0	xxxxx	xxxxx
Host C	xxxx	X.Y.Z.C	xxx	x	x	0	xxxxx	xxxxx
Host D	xxxx	X.Y.Z.D	xxx	x	x	0	xxxxx	xxxxx

最大600件

図2 NTPの監視機能とmonlist

お願い

- 活動にご協力いただける方を引き続き募集しています。
興味をお持ちの方は第3回ミーティング(5月1日)にぜひお越し下さい。
- 設定編に盛り込んだ方が良い機器の情報提供お待ちしております。
(特にメーカーの方、民生用、エンタープライズ共に)
- 詳解編α版を近日公開予定、フィードバックお願いします。
- 各組織の観測状況、取り組みヒアリングさせてください。
(規模の大小問いません)

最後に

- 問題収束はみなさんと力をあわせて取り組んで行く必要があります。上手く収束させていくために協力して行きましょう。

現状把握

情報収集

国内外の公開情報

各組織の取り組み状況

現場ならではの知見・考察

対策支援

ドキュメント整備

適切な問題点の解説

対策手法・設定例

対策支援素材

問題収束

各組織での取り組み

関係者への説明・合意形成

対策の実装・封じ込め

etc・・・

[参考] DDoS発生の仕組み (UDP-based Amplification Attacks)

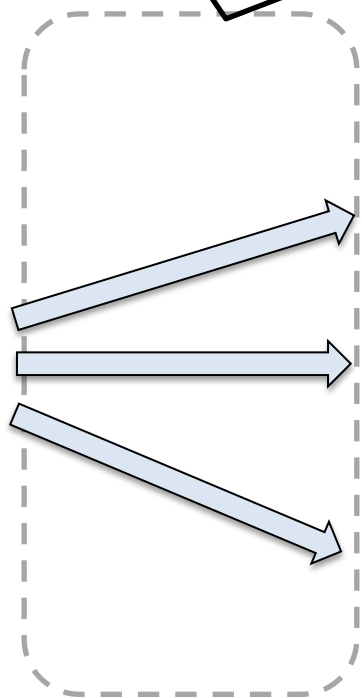
①送信元アドレスを標的に詐称したリクエストを踏み台に対し大量に送信

②サイズの増幅されたレスポンスが標的システムのアドレスに対し大量に送付

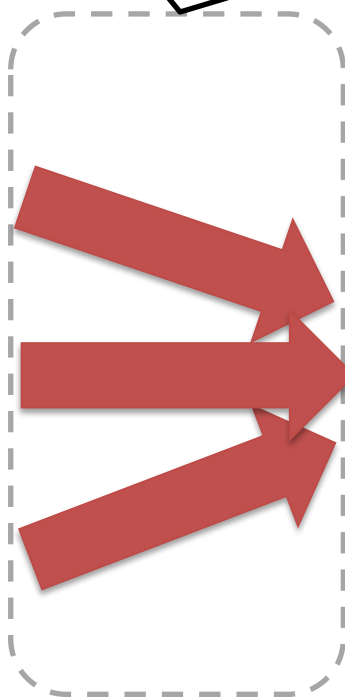
③ネットワーク帯域が占有される(DDoS状態)



攻撃者



踏み台



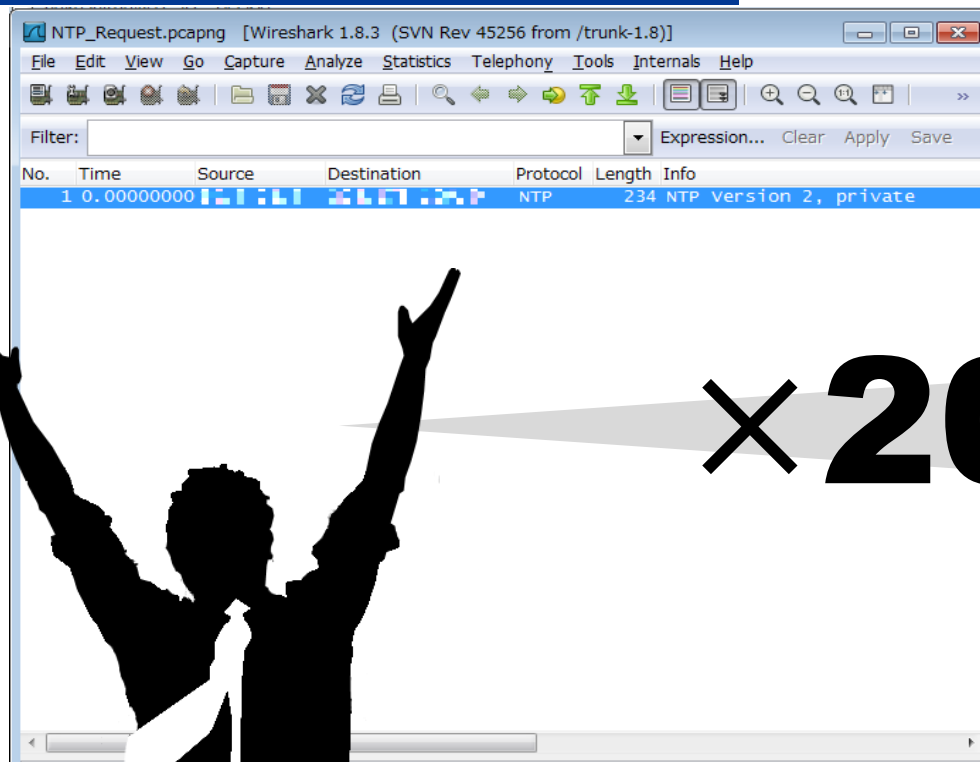
標的システム

リクエストに対するレスポンスの増幅率が高く、踏み台が多いほど効率的

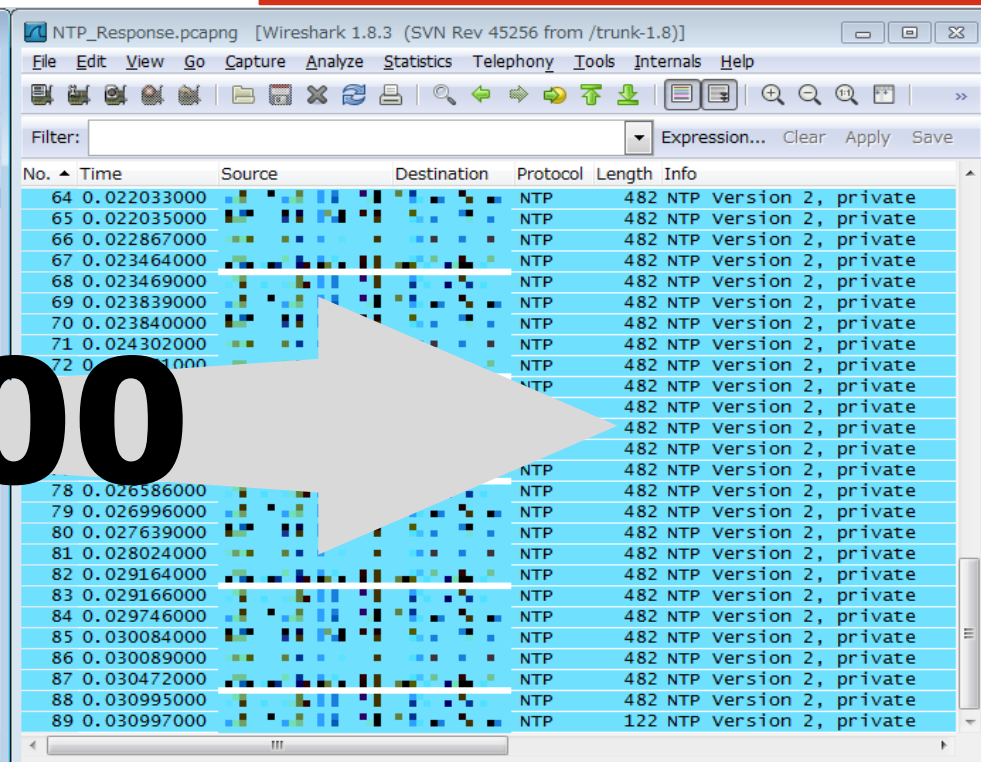
[参考] NTP (monlist) の高い増幅率 (検証例)

Request **234**Byte

Response **44000**Byte



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.1.1	192.168.1.2	NTP	234	NTP Version 2, private



No.	Time	Source	Destination	Protocol	Length	Info
64	0.022033000			NTP	482	NTP Version 2, private
65	0.022035000			NTP	482	NTP Version 2, private
66	0.022867000			NTP	482	NTP Version 2, private
67	0.023464000			NTP	482	NTP Version 2, private
68	0.023469000			NTP	482	NTP Version 2, private
69	0.023839000			NTP	482	NTP Version 2, private
70	0.023840000			NTP	482	NTP Version 2, private
71	0.024302000			NTP	482	NTP Version 2, private
72	0.024303000			NTP	482	NTP Version 2, private
73	0.024304000			NTP	482	NTP Version 2, private
74	0.024305000			NTP	482	NTP Version 2, private
75	0.024306000			NTP	482	NTP Version 2, private
76	0.024307000			NTP	482	NTP Version 2, private
77	0.024308000			NTP	482	NTP Version 2, private
78	0.026586000			NTP	482	NTP Version 2, private
79	0.026996000			NTP	482	NTP Version 2, private
80	0.027639000			NTP	482	NTP Version 2, private
81	0.028024000			NTP	482	NTP Version 2, private
82	0.029164000			NTP	482	NTP Version 2, private
83	0.029166000			NTP	482	NTP Version 2, private
84	0.029746000			NTP	482	NTP Version 2, private
85	0.030084000			NTP	482	NTP Version 2, private
86	0.030089000			NTP	482	NTP Version 2, private
87	0.030472000			NTP	482	NTP Version 2, private
88	0.030995000			NTP	482	NTP Version 2, private
89	0.030997000			NTP	122	NTP Version 2, private

x200

[参考] おびただしい数の踏み台

OpenNTPProject.org - NTP Scanning Project

Search my IP space (eg 192.0.2.0/24 - searches "larger" than /22 will be rejected):

If you are a

How can I check
monlist 192.0.2.
response, your s

How can I fix my
upgrade to NTP-
to your ntp.conf
version. Also che
- Also see [NTP](#)

The server shoul
requests as well

We test the inter
responses.

Cisco customers
[CSCum44673](#).

Recent News

02-2
DDoS

0
0

Open NTP Search Results for 192.0.2.0/22

自動アクセスの場合は、電子メールを ntp-scan@puck.nether.net へください

Data updated weekly. E-Mail the project for per-ASN reports

time	responding_ip	ntp_version	ntp_mode	response_length	ntp_data
0	192.0.2.35	2	7	44000	
0	192.0.2.36	2	7	44000	
0	192.0.2.37	2	7	44000	
0	192.0.2.38	2	7	44000	
0	192.0.2.42	2	7	44000	
0	192.0.2.43	2	7	44000	
0	192.0.2.44	2	7	44000	
0	192.0.2.45	2	7	44000	
0	192.0.2.46	2	7	44000	
0	192.0.2.48	2	7	44000	
0	192.0.2.49	2	7	44000	
0	192.0.2.51	2	7	44000	
0	192.0.2.53	2	7	44000	
0	192.0.2.54	2	7	44000	
0	192.0.2.55	2	7	44000	
0	192.0.2.57	2	7	44000	
0	192.0.2.61	2	7	44000	
0	192.0.2.64	2	7	44000	
0	192.0.2.66	2	7	44000	
0	192.0.2.67	2	7	44000	
0	192.0.2.68	2	7	44000	

レスポンスサイズが最大の44KB(600ホスト分)であることから、実際にNTP Reflection DDoSに悪用されていると考えられる。

アドレスレンジ内にほぼ隙間無くぎっしり

