

オープンリゾルバの状況

鈴木 常彦[†]

[†] 中京大学情報理工学部 〒470-0393 豊田市貝津町床立 101

E-mail: †tss@sist.chukyo-u.ac.jp

あらまし アクセス制限のない DNS キャッシュサーバ (オープンリゾルバ) は、IP アドレス詐称と応答の増幅により DNS amp と呼ばれる DDoS 攻撃の踏み台となる。本論文では、独自に開発したオープンリゾルバの検査ツール DNS Amp Checker を紹介する。また、DNS Amp Checker による調査結果として、日本国内の DNS コンテンツサーバの約 8 割がオープンリゾルバであり、DNS amp の踏み台となるオープンリゾルバを大量かつ容易にリストアップできる危険な状態のまま改善が進んでいない状況にあることを報告する。

キーワード DNS amp, オープンキャッシュ, オープンリゾルバ

Status of Open Resolvers

Tsunehiko SUZUKI[†]

[†] School of Information Science and Technology, Chukyo University 191 Tokodachi, Kaizu-cho, Toyota, 470-0393 Japan

E-mail: †tss@sist.chukyo-u.ac.jp

Abstract DNS cache servers (DNS open resolvers) without access controll could be misused for DDoS attack. This paper introduces the original tool 'DNS Amp Checker' for finding open resolvers. And using the tool, it's made clear that about 80% of DNS authoritative servers are open resolvers. So anyone can find many open resolvers. And the state is not improved in these years.

Key words DNS amp, open cache, open resolver

1. ま え が き

DNS amplifier attack(以下 DNS amp) とは、数十 byte の DNS query に対し、その応答が数百 byte から最大 4kbyte(EDNS0) にまで増幅されることを利用した DDoS 攻撃手法である。攻撃のシナリオは、

(1) 再帰検索要求をアクセス制限なく受け付ける多くの DNS キャッシュサーバ(以下 open resolver) にあらかじめ query を送って大きなサイズのキャッシュを用意しておく

(2) タイミングを見計らってソース IP アドレスを攻撃対象の IP アドレスに詐称した query をボットなどから同時に送信すると

(3) 攻撃対象は多くの DNS キャッシュサーバからの大量の応答パケットに襲われる

というものである。DNS amp について US-CERT が注意喚起文書 [2] を出したのは 2005 年 12 月、JPCERT の注意喚起文書 [3] が 2006 年 3 月、それから 2 年経過した現在でも、筆者の調査では対策は数%程度しか進んでおらず、JP ドメインの約 8 割は未対策のままである。この調査には独自に作成した検査プ

ログラムを用いている。プログラムは学術的あるいはオープンソースの精神からは公開すべきであるが、対策が進んでいない現在、危険性を鑑みて公開は見送っている。本論文ではツールの概要と調査結果を公表し、広く対策を呼びかけるものである。

2. 問題の対象

2.1 非再帰と再帰

本研究で問題とするのは DNS トラフィックのうち再帰検索 (recursive query) とその応答である。そもそも DNS はその仕組み自体が原理的に危険な存在である。DDoS 攻撃として有名な ICMP による smurf 攻撃では、ICMP ブロードキャストの転送 (redirect) による ICMP パケットの増幅効果が武器として用いられた。そのため 1999 年の RFC2644 [1] でそれまでルータの機能として必須 (MUST) であった ICMP ブロードキャストの転送が禁止 (MUST NOT) され、インターネットは深刻な問題の一つから開放されつつある。しかし、DNS はその基本動作が増幅 (query:answer) を伴うものであり、また UDP を用いているために ICMP と同様に送信元を容易に偽装でき、応答のトラフィックを攻撃対象に誘導できる。そして、DNS トラ

フィックにおいて、非再帰検索要求とその応答は一般的に DNS コンテンツサーバがゾーンデータを世界に公開するためのものであるから、アクセス制限を行うこともできない。DNS の代替品の普及を図るか、詐称 UDP データグラムをインターネットから一掃していく努力だけが現在のところ唯一行える対策である。従って、現状において対策の術がなく、どうしても必要とされる DNS 応答については本論では問題の対象外とする。一方で、再帰検索を提供するサーバは一般的に世界に公開する必要はなく、アクセス制限が可能である。再帰検索を行うフルリゾルバは一般にキャッシュ機能を兼ね備えているため、攻撃者は予め大きなサイズのデータをキャッシュに入れて攻撃に用いることができる。攻撃者は大きなサイズのデータを持った DNS コンテンツサーバを探し回るより、はるかに容易に効率の良い攻撃が行える。従って、オープンリゾルバを無くしていくこと、つまり、アクセス制限によって攻撃者に DNS キャッシュサーバを使わせないようにしていくことは、十分意味のある行為であるといえる。この観点から特に本論で問題とするのは、オープンリゾルバになってしまっている DNS コンテンツサーバである。もし DNS コンテンツサーバの多くがオープンリゾルバの機能も兼ね備えていると仮定すると、大量のドメインのリストさえ入手できれば、攻撃者はそのドメインの権威サーバを検索することで、容易に大量の踏み台サーバを手に入れることができ、インターネットは大きな脅威にさらされることとなる。本論は、その仮定が真であることを裏付けを提供し、対策の必要性を訴えるためのものである。

2.2 オープンリゾルバの定義

筆者が問題とするオープンリゾルバとは、以前は外部ネットワークから任意なゾーンの再帰検索を受け付ける DNS キャッシュサーバを意味していた。例 1 はある社団法人のドメインの権威サーバに、外部 (筆者の利用する ISP) から筆者が管理するドメインの MX を検索要求した結果であり、従前の意味におけるオープンリゾルバになっている。

例 1. オープンリゾルバ

```
% dig @ns.*****.or.jp -t mx e-ontap.com +sh
50 mx.e-ontap.com.
```

しかし、これまでの調査によって、外部からの再帰検索要求に対して正しくアクセス制限が行われているように見えても、許可された内部ネットワークから入れられたキャッシュを、外部に対して応答してしまうサーバが多く存在することが判明した。こうしたキャッシュサーバに対して、内部のメールサーバやウェブサーバ等の逆引きをトリガーとして、キャッシュを取り入れさせることは容易であろう。また、否定応答としてルートキャッシュや上位ドメインに関するヒント情報 (referral) をキャッシュで答えてくるものもある。最近ではルートキャッシュやトップレベルドメインも AAAA レコード等で肥大化しており、十分脅威となりうることから、こうした応答をするものについても、広義なオープンリゾルバとして問題にすることにした。

3. 調査ツール

オープンリゾルバの判定を行うため、DNS Amp Checker というプログラムを作成した。作成には Ruby 1.8 と、net-dns 0.3 [4] を用いた。Net-dns は Perl の DNS ライブラリである Net::DNS モジュールが Ruby に移植されたものである。DNS Amp Checker は以下の動作をするものである。

- (1) 検査対象ドメイン名を入力
- (2) 検査対象ドメイン名の権威サーバを検索
- (3) 各権威サーバに対し以下の応答をチェック
 - (a) . の NS レコードを検索
 - (b) com の NS レコードを検索
 - (c) ある有名ドメインの NS レコードを検索
- (4) Answer Section にキャッシュ応答結果出力
- (5) Authority Section にキャッシュ応答結果出力

また、このプログラムで多くのドメインを走査するためのパッチスクリプトと、Web インターフェイスを持たせた CGI 版も作成した。CGI 版は <http://www.e-ontap.com/internet/check/> で 2007 年 6 月から公開している。公開に際しては、最初 HTTP 接続元の IP アドレスから得られる PTR のドメインだけを対象としていたが、公開 3 日後には任意のドメインについて検査できるようにした。ただし、検索結果を画像出力することにより、ロボットを用いて大量のオープンリゾルバを探し出すような悪用を避ける工夫を盛り込んだ。攻略はさほど困難ではないだろうが、それをするくらいならば自分で DNS スキャナーを作った方が早いと思われる。

4. スキャンによる調査

筆者はコンテンツサーバがキャッシュサーバを兼用していて、それがオープンリゾルバになっていないかを継続的に調査している。100 万ドメインを越える JP ドメインのうち、筆者の手元にリストされている 5 万ドメインについて、2008 年 3 月 10 日に約 6 時間かけてゆっくり走査した結果を表 1 に示す。上記のように、調査対象の 77% にあたる 18,190 台の権威サーバ (コンテンツサーバ) が再帰検索に対しキャッシュ応答を返すという結果となった。また、そのようなサーバを放置しているドメインは調査対象の 80% を占める。この数字は、絶対値としても深刻な状況を示すものであるが、さらに問題が深刻なのは、1 年前の 2007 年 4 月 22 日の調査 [5], [6] から 6% 程度しか改善が進んでいないということである。1 年前は 24,214 台の権威サーバ中、キャッシュ応答のあったのは 83% にあたる 20,091 台であった。

5. Web による公開結果

2007 年 6 月 10 日に任意ドメインを検索できる版を Web で公開してから、2008 年 4 月 9 日までの約 10 ヶ月の DNS Amp Checker の利用状況を表 2 に示す。1 台でもオープンリゾルバがあったドメインを不合格とすると 68% のドメインが不合格である。これが 5 万件の調査の 80% より 12% 低いのは、DNS amp に対する関心の差が考えられる。それでも 68% が不合格

表 1 JP ドメイン走査結果
Table 1 open resolvers in JP domains

検査したドメイン総数	48,594	
その権威サーバ総数	23,609	
再帰検索に応答した権威サーバ	18,190	77%
問題ある権威サーバを持つドメイン	38,727	80%

表 2 Web 版利用状況
Table 2 Web visitors status

訪問者のべ総数	10177	
訪問者 IP アドレス	4146	
検査ドメイン総数	4279	
合格ドメイン	1378	32%
不合格ドメイン	2901	68%
0 点ドメイン	1724	40%

表 3 検査結果の変化
Table 3 Change log of results

複数回検査ドメイン	658	
向上を確認したドメイン	162	40%
悪化したドメイン	66	10%

というのはやはり憂慮すべき状態に変わりはない。さらに、日を開けて複数回の検査がなされたドメインについて経過を見たものが表 3 である。複数回の検査がなされ、そのうち向上が確認されたドメインは 40%、うち全てのオープンリゾルバを解消したものが 6%あった。多少なりとも検査サイトが役に立った可能性がある。なお、公表は差し控えるが、ブロードバンドルータの検査においてキャッシュ応答のあったものが僅かながら存在する。設定ミスでなければ脆弱性を抱えた製品が存在する可能性を示唆している。これについては現在調査を進めているところである。

6. ま と め

約 5 万ドメインを調査しただけで、2 万台近いオープンリゾルバが見つかった。2 万台のオープンリゾルバがあれば 1 台あたり実効 10Mbps としても単純計算で 180Gbps の DDoS 攻撃が行えることになる。100 万ドメインの JP 全体に同率のオープンリゾルバがあれば、3.6Tbps である。そして、JPCERT/CC や JPRS、警察庁など関係団体が注意喚起 [3], [7], [8] を行っているにも関わらず、その改善がなかなか進まない状況をどうすれば良いのであろうか。ネットワーク技術の研究よりも、むしろ、危機管理工学など多方面からのアプローチが必要かもしれない。

文 献

- [1] RFC2644, <http://www.ipa.go.jp/security/rfc/RFC2644JA.html>
- [2] The Continuing Denial of Service Threat Posed by DNS Recursion, http://www.us-cert.gov/reading_room/DNS-recursion121605.pdf
- [3] DNS の再帰的な問合せを使った DDoS 攻撃に関する注意喚起,

<http://www.jpCERT.or.jp/at/2006/at060004.txt>

- [4] net-dns, <http://net-dns.rubyforge.org/>
- [5] DNS の危機的状況, FIT2007 (第 6 回情報科学技術フォーラム) 一般講演論文集, 第 4 分冊, pp.29-31, 2007.
- [6] DNS Security: Now and The Future, Rikitake, K., Suzuki, T. and Nakao, K. IEICE Technical Report ICSS2007-01, pp.3-8 (2007).
- [7] DNS の再帰的な問合せを使った DDoS 攻撃の対策について, <http://jprs.jp/tech/notice/2006-03-29-dns-cache-server.html>
- [8] DNS の再帰的な問い合わせを悪用した DDoS 攻撃手法の検証について, http://www.cyberpolice.go.jp/detect/pdf/20060711_DNS-DDoS.pdf