減らない脆弱性 - 隠れオープンリゾルバ -

鈴木 常彦[1,a)]

概要：送信元 IP アドレスが詐称された DNS クエリが到達してしまう隠れオープンリゾルバを多く発見した。これは未対策のネットワークが各種の送信元 IP アドレス詐称攻撃に脆弱であることを意味しており早急な対策が必要と考えられるが、継続調査において対策があまり進んでいないことが明らかになっている。調査対象 10 万の IP アドレスのうち全体では約 7%、PTR が JP のものでは約 24%が現在も脆弱なままである。本論文をもって脆弱性が放置されている現状に対しての議論と啓発・対策の進展に寄与したい。

Unreduced Vulnerabilities - Hidden Openresolvers -

Tsunehiko Suzuki[1,a)]

Abstract: I found many hidden openresolvers which are caused by reachablity of source IP address spoofing packets. This means that those networks are vulnerable for many kind of spoofing attacks. Measures to address those vulnerable sites are not very not much progress has been made. Of the 100,000 IP addresses surveyed, about 7% overall, and about 24% of those whose PTR is JP, remain vulnerable. We hope that this paper will lead to further discussion, awareness-raising, and countermeasures.

1. はじめに

ここ 10 年くらいで DNS のオープンリゾルバの対策が進んだが、その対策において同時に行うべき送信元 IP アドレス詐称対策はあまり進んでいない。ネットワーク境界で送信元 IP アドレス詐称パケットの流入を許すと、許可された内部からのアクセスも偽装した攻撃が可能となり、サーバでのアクセス制限が意味を失う。このことの理解があまり周知されていないようにみえる。

内向きの送信元 IP アドレス詐称対策が行われていないということは、DNS のみならず ICMP や NTP, SNMP, QUIC, SSDP, Memcached, LDAP 等々の UDP サービスへの攻撃や TCP への SYN flood 攻撃などに対しても、非公開のつもりのサーバが実は無防備であることを意味する。

筆者は送信元 IP アドレスが詐称された DNS クエリが到達可能なリゾルバを隠れオープンリゾルバと名づけて 2021 年 3 月からその実態調査を行ってきた。その結果、調査対象の JP ドメインのリゾルバの約 1/4 が未だに隠れオープンリゾルバであることが判明した。

本論ではその経緯をもって脆弱性が減らない現状を示し、議論と対策を促したい。

2. オープンリゾルバの状況

まずは従来問題にされてきた一般的なオープンリゾルバについて述べる。オープンリゾルバとはアクセス制限がされておらず世界のどこからでも DNS クエリを送り込めるものを指す。これらは DNS キャッシュポイズニングに脆弱であったり、DDoS 攻撃の手法である DNS リフレクター攻撃 (増幅率が高い場合 DNS Amp 攻撃)[1] あるいは DNS 水責め攻撃 [2] の踏み台となるリスクがある。

2.1 過去の調査

オープンリゾルバについては本論文の 14 年前 2008 年 3 月の筆者による調査 [3] がある。独自に収集した 48,594 の JP ドメインの 18,190 の権威サーバを調べた結果、77%にあたる 23,609 がキャッシュ兼用のオープンリゾルバとなっていた。

2013 年の Yuuki Takano らの調査 [4] では網羅的なスキャンで発見された約 3,000 万の DNS サーバ (port 53 が応答

[1] 中京大学
Chukyo University, Toyota, Aichi, 470-9393, Japan
[a)] tss@suzuki.sist.chukyo-u.ac.jp

するもの) のうち 82.5%がオープンリゾルバだったと報告されている。

また 2018 年には 54.6%〜79.4% (調査手法による差がある) という大井らの報告?, ooi ある。

2.2 今回の調査

筆者は 2021 年 3 月頃から 104,980 の DNS リゾルバについて調査を開始した。リゾルバのリストは筆者の管理するいくつかの権威サーバ (e-ontap.com 等) へのクエリ元を収集したものである。このリストに対して以下のクエリを送りその応答による調査を行った。

dig . ns +timeout=1 +retry=1 +rec

その結果、オープンリゾルバは 2022 年 8 月 31 日現在で全体の 1.3%にあたる 1,372 であった。ここでのオープンリゾルバの定義は 1 つ以上の ANSWER セクションもしくは AUTHORITY セクションを RA フラグ付で応答したものである。なお RA フラグがつかないものも含めると 1,513 で 1.4%となる。

次にリストの IP アドレスのうち PTR(DNS 逆引き) の末尾が ".JP." となっているリゾルバを調べた。その数は 2,462 であった。そのうちオープンリゾルバと判定されたものは 59 であり 5.3%であった。JP は全体 (世界) に対して 4 倍ほど多い。

これらの数値は過去の調査と比較すると格段に少なくなっているが、これは 2008 年のいわゆる Kaminsky 攻撃 (Kaminisy の発表は間違いで B.Mueler の論文"Improved DNS Spoofing Using Node Re-delegation"[5] にあたるのが適切) による騒ぎや、DNS を用いた DDoS 攻撃の増加に対する注意喚起 [6] が広く行われて対策が進んだ結果と考えられる。また、権威とキャッシュが兼用できない実装の普及も寄与しているだろう。

3. 隠れオープンリゾルバの状況

オープンリゾルバに対してはそのサーバにアクセス制限を施す対策が推奨されてきたが、ネットワークでの送信元詐称対策が必要であることはあまり周知されていない。そのため通常はオープンリゾルバには見えなくとも送信元詐称クエリは受け入れる隠れオープンリゾルバと筆者が呼ぶものが多く存在しているのではないかと考えて本調査を開始した。詳しい調査方法については後述する。

リゾルバに詐称クエリが到達するネットワークでは DNS 以外の各種サーバも詐称攻撃に対して脆弱である可能性が高く、この調査結果は DNS のみならずネットワークの脆弱性を示している。本調査により 2022 年 8 月 31 日時点での隠れオープンリゾルバは 104,980 のリゾルバリストのうち、6.9%の 7,228 であることが判明した。通常のオープンリゾルバが 1.3%であるのに対して、その 5 倍が隠れていたことになる。

3.1 日本の隠れオープンリゾルバの状況

調査開始時点の 2021 年 3 月 7 日に PTR の末尾が.JP. であるものを抽出して JPCERT/CC へ届けた。この時点での隠れオープンリゾルバは 300 ドメイン 736 IP アドレスであった。調査対象の JP の IP アドレス数 2,462 の 3 割に相当する。その後、追加で発見されたものを加えた 774 IP アドレスを初期値として 2021 年 4 月 24 日から日毎の追跡調査を開始した。対策の推移状況を以下の図 1 と表 1 で示す。表には脆弱なリゾルバの数とその 90 日毎の削減率と調査開始時点からの削減率を掲載する。

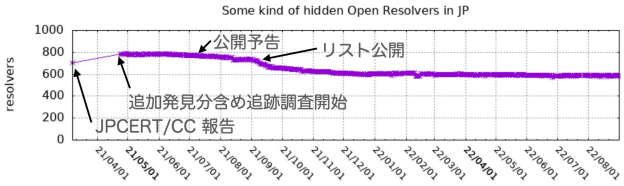

図 1 対策の推移 (JP)

表 1 対策の推移 (JP)

日付	脆弱数	90 日削減率	削減率	イベント
'21/04/24	783			追跡開始
'21/07/12	774			公開予告
'21/07/22	763	-2.6%	-3.4%	90 日後
'21/09/07	713			リスト公開
'21/10/20	628	-18%	-20%	180 日後
'22/01/16	609	-3%	-22%	270 日後
'22/04/16	595	-2.2%	-24%	360 日後
'22/07/15	586	-1.5%	-25%	450 日後

本調査には通常のオープンリゾルバも 1 割程度含まれている (2022 年 8 月 29 日時点で 40/588=7%) が少なくともソース IP アドレス詐称パケットが到達するものの数である。

この調査で注目したい点は、脆弱サイトのリスト公開の効果である。調査の途中 2021 年 9 月 7 日に筆者のサイトにおいて脆弱なドメインの公開 [7] を行った。またその 2 カ月程前からは各方面 (ブログ, Twitter, JPCERT/CC 等) への公開予告も行った。JPCERT/CC からは各方面へその旨の連絡が行われたものと思われ、一部の組織からは公開を控えられないかとの問い合わせも受け取った。しかし公開までに対策すれば良いだけであるし、そもそも攻撃者は私のリストに頼らなくとも簡単に調査可能であるという判断から注意喚起の効果に期待して公開に踏み切った。ただし最低限の考慮としてリゾルバは特定せずゾーン頂点のドメイン名だけを公開した。

そしてリスト公開の結果、それまでは数%しか解消されなかったものが、公開をまたぐ 3 カ月の間に 18%減少したのは期待通りであった。その後はまた減少率が数%程度と

なり最近はほとんど解消が進まなくなっている。2022 年 9 月 2 日時点で 590 IP アドレス。初期の 783 の 3/4 に留まっている。これは調査対象の JP の IP アドレス数 2,462 の 24%である。

なお JPCERT/CC からの情報によれば、本論文執筆の 2022 年 8 月末時点までにリストの半数程度の組織には連絡を行った他、早期警戒情報共有の枠組み、通信事業者、ホスティング事業者等々、また GO.JP、LG.JP ドメインについては政府関連の各対応機関を介した情報提供も行ったとのことであり、その上でのこの状況である。

この公開リストに対してある ISP からは「検出されているのは ISP が提供しているリゾルバではなく利用者のリゾルバであるからリストから ISP のドメイン名を消して欲しい」との声もあった。しかしこれはネットワークの脆弱性であり、詐称パケットに脆弱なネットワークを利用者へ提供しているのは ISP なのだからリストは正当である旨の回答をした。DNS の逆引き (PTR) ドメイン名はそのネットワークに責任を持つドメインを示していると筆者は考えてリストを作成している。

3.2 文科省への報告

2021 年 4 月からの継続調査のリストとは別に、 2021 年 9 月に 1,667 ドメインの AC.JP から AC.JP のホスト名のついた DNS 権威サーバを 1,132 台抽出して調査を行った。その結果、224 の AC.JP ドメインに 323 の隠れオープンリゾルバを発見した。これらのサーバは権威とキャッシュが同居していることも意味する。調査結果は 2021 年 9 月 17 日に文部科学省の CSIRT (大臣官房政策課サイバーセキュリティ・情報化推進室) へ情報提供して対策への協力を求めた。その後、継続調査を行っているが公開リスト [11] に示すようにおよそ 1 年後の 2022 年 9 月 3 日現在、約 9 割 (207 ドメイン、291 IP アドレス) が未対策で残存している。JP 全体が 1/4 減ったのと比べると大学の対応は非常に鈍い。

4. 隠れオープンリゾルバの調査方法

本調査の方法を説明する。筆者の大学や国内のホスティング事業者の多くでは BCP38[8] 等の詐称防止対策が施されていて送信元詐称ができないため、欧州のホスティング業者のサーバ (VPS) を契約して送信元詐称クエリ送出プログラム (以降 spoofer) を動作させている。この spoofer は多様な詐称が可能なものであるが、日毎の継続調査においては対象のリゾルバに隣接する IP アドレスを送信元として詐称したクエリを用いている。他の詳細な調査では必要に応じて調査対象と同じ IP アドレスやルートサーバを詐称したクエリも用いている。調査用クエリの問い合わせドメイン名は筆者の管理するドメイン名 reflec.to をサフィックスとした以下の様式のドメイン名である。

IP アドレス+"."+詐称形式+日付+".scan.reflec.to"
例: 221.7.138.30.shift0901.scan.reflec.to

これにより詐称クエリが調査対象のリゾルバに届いて受け入れられると、当該リゾルバはその名前解決のためのクエリ (非再帰の反復問い合わせ) を筆者の管理する reflec.to の権威サーバへ送ってくる。その時点で当該のリゾルバは送信元詐称対策がなされていないネットワークで運用されている隠れオープンリゾルバであることが判明する。継続調査ではそのクエリログを毎日自動解析してデータの蓄積と公開 [9] を行っている。

5. 謎の装置

本調査の中で謎の振る舞いが観測されている。クエリを送り込むとなぜか数秒以上の時間をおいて 8.8.8.8 で知られる Google Public DNS のリゾルバから権威サーバへクエリがやってくる。フォワーディングの可能性もあるが問題のリゾルバは REFUSED を応答してくる。そして応答を拒否しておきながらクエリ内容の検索は行われるのである。同じ奇妙な動作が mofa.go.jp (外務省) や nict.go.jp(情報通信研究機構)、その他いくつかの大学等の権威サーバへのスキャンで観測されている。[10]

推測やいくつかの対象組織への問い合わせでわかったのは、あるセキュリティアプライアンスがベンダーのサーバへクエリを転送し、そこでパブリック DNS キャッシュサーバをリゾルバとしてクエリをリプレイしてレピュテーションを行っているらしいということだった。そのアプライアンスが何であるかは現時点で不明なままである。

6. 対策

すでに述べたようにサーバ (リゾルバ) でアクセス制限するだけでは不十分である。境界ルータ (あるいはファイアウォール) の外側インターフェイスで内部 IP アドレスを詐称したパケットの流入を止める必要がある。

例えば内部のアドレスが 192.0.2.0/24 だった場合、FreeBSD の標準ファイアーウォール ipfw では

deny all from 192.0.2.0/24 to any in via ${ 外側 IF}

というルールで止められる。

また自組織が外部への攻撃元にならないよう境界ルータの内側インターフェイスから内部 IP アドレス以外の流出を止めること [8] も重要である。

deny all from not 192.0.2.0/24 to any in via ${ 内側 IF}

基本はネットワークでの対策になるが、ネットワーク管理者の協力が得られないサーバ管理者の自衛策として筆者は以下の対策を行っている。

deny all from 192.0.2.0/24 to me not ipttl 64,128,255

これはルータを越えてくるパケットは IP TTL がカウントダウンしているが同一セグメントからのパケットは IP TTL が初期値のままであることを利用したものである。しばらくパケットを観察しそのネットワークで使用されている機器の IP TTL を収集すると良い。

扱う IP アドレスブロックの多い大きなネットワークでの対策は難しくなるかもしれないがネットワークの分割やトポロジーの再設計、そして利用ポリシーの確立で対策は進められるはずである。

なお、自分の利用しているリゾルバが隠れオープンリゾルバかどうかは筆者が提供している Hidden Open Resolver Tester [12] で判定可能である。このテスターの詳細については本調査の詳細と併せて別な機会に論文にまとめたい。

7. 先行研究

Maciej Korczyński らの 2020 年の論文 "Don't Forget to Lock the Front Door! Inferring the Deployment of Source Address Validation of Inbound Traffic"[13] が世界の状況に詳しい。この研究も DNS のクエリ到達に着目して送信元 IP アドレス詐称に脆弱なネットワークを探索したものである。この報告では日本には詐称に弱いネットワークが/24 換算で 28,660 あることが示されている。筆者の研究はその一部を追跡調査したものと位置づけられるだろう。

8. まとめと脆弱性の取扱いに関する考察

本研究は独自収集した約 10 万ドメインによる調査ではあるが以下のことが判明した。

(1) オープンリゾルバは全体が 1.4%に対して JP は 5.3%と高い
(2) 通常のオープンリゾルバの約 5 倍の 6.9%の隠れオープンリゾルバを発見 (JP は 30%)
(3) 脆弱ドメインの公開の効果は大きい (18%減少)
(4) 調査開始からの約 1 年半で対策されたのは 24%のみ
(5) AC.JP では約 1 割しか対策が進んでいない

現時点ではまだまだ危険なサイトが多く残存しており、その中には GO.JP や重要インフラ企業など社会へ影響の大きなドメインも含まれている。これらを解消していくことは急務でありさらなる有効性の高い活動が必要である。

従来から脆弱性情報開示に関して常にフルディスクロージャ派と慎重派が常に議論を重ねてきており、日本においては経済産業省の「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」[14] や IPA 他の「情報セキュリティ早期警戒パートナーシップガイドライン」[15]、JPCERT/CC の「脆弱性関連情報取扱いガイドライン」[16] などを元にかなり慎重な取扱いが行われている。しかしこれらは主として製品の未公開の脆弱性を念頭においたものであり、現場で運用上発生している既知の脆弱性にこれらを適用するのが適切かどうかは疑問のあるところである。

日夜ありとあらゆる攻撃が行われている予測不能なネット社会において、すでに攻撃者にも知られている (知られうる) 状態にある脆弱性を社会としてどう扱っていくべきかは従来の慎重な態度とは別な議論が必要であろう。

本論文を発表する 2022 年 11 月の経営情報学会全国大会では東海支部セッションにおいて「VUCA をどう生き抜けば良いかを考える」というテーマの議論が行われる予定である。VUCA は Volatility(変動性)、Uncertainty(不確実性)、Complexity(複雑性)、Ambiguity(曖昧性) を指す軍事用語から転じた現代社会の様相を表すビジネス用語として知られている。このテーマに沿って本研究のような問題へのアプローチも議論の俎上に上げたいと考えている。

参考文献

[1] DNS リフレクター攻撃（DNS アンプ攻撃）, https://jprs.jp/glossary/index.php?ID=0156
[2] ランダムサブドメイン攻撃（DNS 水責め攻撃）, https://jprs.jp/glossary/index.php?ID=0137
[3] オープンリゾルバの状況, 鈴木常彦, 情報処理学会研究報告 (IPSJ SIG technical reports) 2008 (37), 89-91, 2008-05
[4] The Ecology of DNS Open Resolvers, Yuuki Takano and Ruo Ando and Satoshi Uda andc Takeshi Takahashi and Tomoya Inoue, ICECE Transaction B, Vol. J97-B, pp. 873-889, 2014.
[5] Improved DNS Spoofing Using Node Re-delegation,https://www.cin.ufpe.br/~vtc/Whitepaper-DNS-node-redelegation.pdf
[6] DNS の再帰的な問い合わせを使った DDoS 攻撃に関する注意喚起, https://www.jpcert.or.jp/at/2013/at130022.html
[7] 隠れオープンリゾルバを放置している日本のドメイン,https://snoopy.e-ontap.com/vulnerables.html
[8] BCP38 (RFC2827) Ingress Filtering, https://www.rfc-editor.org/rfc/rfc2827.html
[9] 隠れオープンリゾルバ, http://www.e-ontap.com/dns/hidden-openresolver/
[10] （隠れ）オープンリゾルバとなっていた謎のアプライアンスが機能停止, http://www.e-ontap.com/blog/?date=20220521
[11] 隠れオープンリゾルバを放置している AC.JP, http://www.e-ontap.com/dns/hidden-openresolver/
[12] Hidden Open Resolver Tester, https://snoopy.e-ontap.com/
[13] Don't Forget to Lock the Front Door! Inferring the Deployment of Source Address Validation of Inbound Traffic, Maciej Korczyński, et al.., International Conference on Passive and Active Network Measurement, Mar 2020, Eugene, United States.
[14] 脆弱性関連情報に関する取扱規程」, 経済産業省, https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf
[15] 情報セキュリティ早期警戒パートナーシップガイドライン,IPA,https://www.ipa.go.jp/files/000098799.pdf
[16] 脆弱性関連情報取扱いガイドライン,JPCERT/CC, https://www.jpcert.or.jp/vh/vul-guideline2017.pdf
[17] オープン DNS リゾルバの現状把握手法の提案と評価, 大井, 落合, 江崎, マルチメディア, 分散協調とモバイルシンポジウム 2018 論文集, 2018, 1126-1133, 2018-06-27