DNS オープンリゾルバ問題

適切にアクセス制限されていないキャッシュDNSサーバをDDoS攻撃の踏み台として悪用されるケースが相次いでいます。オープンリゾルバと呼ばれるこういったキャッシュDNSサーバの問題点について解説します。

2.1 はじめに

今年3月、「史上最大のサイバー攻撃」と呼ばれた大規模なDDoS攻撃が行われたと報じられました[*1]。迷惑メール対策団体のSpamhaus及びSpamhausをホスティングしているCloudFlare社が最大300GbpsものDDoS攻撃を受けた事件[*2]で、CloudFlareが「インターネットが崩壊寸前まで追いこまれた」といささか誇張した表現を使ったせいもあってか[*3]、大きく注目を集めました。

このときに使われたのが、DNS amplification attack（DNS amp）という手法です。CloudFlare事件後も、5月にはDDoS対策サービスのProlexic社が167GbpsにのぼるDNS amp攻撃を受けたことを発表しており[*4]、他にも公表されていない多数の事例があると思われます。IIJによる観測でも、ほぼ恒常的に行われていることが分かっています。

本稿では、DNS amp攻撃、ならびにこの攻撃の踏み台として使われるオープンリゾルバの問題について考察します。

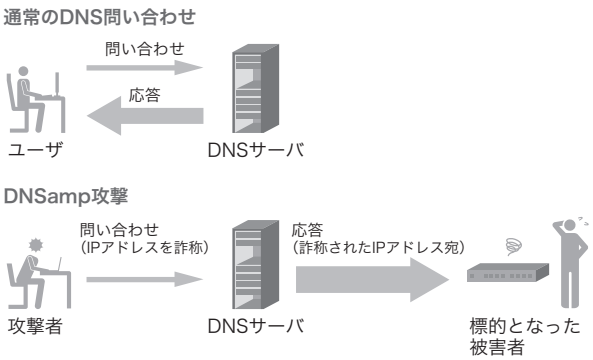


図-1 DNS amp

2.2 DNS ampとオープンリゾルバ

DNSは主にUDP上でやりとりされますが、UDPにはTCPのようなセッション確立手続きがありません。そのため、クライアントが悪意を持って自らのIPアドレスを詐称してもサーバはこれを検証できず、詐称されたIPアドレスに身に覚えのない応答が届けられることになります。これをリフレクション（反射）攻撃と呼びます。

DNSはもともと問い合わせよりも応答パケットの方がサイズが大きくなる性質があり、この比は最大で50倍以上にもなります。この増幅効果をリフレクション攻撃と組み合わせることで、攻撃者は少量の攻撃トラフィックを踏み台となるDNSサーバ（リフレクタ）に送るだけで標的のネットワークを埋めつくすことができます。これがDNS ampです（図-1）。ボットネットを利用すると更に効率的なトラフィック飽和攻撃が可能になります。

DNS ampは標的のネットワークに対する攻撃であり、ホストの特定の脆弱性を狙うものではありません。そのため対策が難しく、また、標的となった被害者からは踏み台とされたDNSサーバしか見えないため、真の攻撃者を特定するのが困難という特徴があります。

キャッシュDNSサーバは、組織ごとあるいはISPごとに用意しその内部のユーザだけにその機能を提供できれば十分で、不特定多数の用に供する必要はありません。このような外部からの不要なアクセスを制限していないキャッシュDNSサーバのことをオープンリゾルバと呼びます。

＊1 Internet Watch、「ネットを崩壊の瀬戸際に追い込んだ「史上最大のサイバー攻撃」が明るみに～早急な対策が望まれるオープンリゾルバーDNS問題」（http://internet.watch.impress.co.jp/docs/news/20130328_593523.html）。インターネットコム、「史上最大規模の DDoS 攻撃が、インターネット全体の速度低下を招く― SpamHaus と Cyberbunk 間のサイバー戦争で」（http://japan.internet.com/webtech/20130328/8.html）など。
＊2 http://www.apricot2013.net/__data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf
＊3 http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet
＊4 http://www.prolexic.com/news-events-pr-prolexic-stops-largest-ever-dns-reflection-ddos-attack-167-gbps.html

オープンリゾルバはあらゆる送信元IPアドレスからの問い合わせに答えてしまうため、外部から自由にDNS amp攻撃の踏み台に悪用できてしまいます。非常に危険ですが、世界には多数存在しており、CloudFlareは3月の事件後、およそ8万のオープンリゾルバが関与していたと発表しています(アジア太平洋地域では日本が最多という残念な数字が出ています)[*5]。Open Resolver Projectの調査では、全世界に実に2800万ものオープンリゾルバが存在するとしており[*6]、対策の遅れが窺えます。

リフレクション攻撃やamp攻撃の手法自体は古くから知られており、遅くとも1999年には注意喚起されているようです[*7]。攻撃は主にDNSが使われますが、むしろUDPであることが本質なので、DNS以外のUDP上のプロトコル、例えばSNMPやNTPなどでも同様の攻撃が成立します[*8]。特に、SNMPは増幅率が1,000倍近くになることもあり[*9]、非常に危険性の高いものとなっています。

2.3 DNSキャッシュポイズニング攻撃

オープンリゾルバのキャッシュDNSサーバは、DNS amp攻撃の踏み台とされる以外に、キャッシュポイズニング攻撃を受けやすいという側面もあります。

キャッシュポイズニングは、キャッシュDNSサーバに対して細工された応答を注入し、偽の情報をキャッシュさせようとする攻撃です。これを成功させるには、キャッシュDNSサーバが権威DNSサーバに問い合わせを送った後、応答が返ってくるまでのわずか数ミリから数十ミリ秒程の間に偽造応答を割り込ませる必要があり、適切にアクセス制限されていれば、攻撃機会は非常に限定されます。

しかし、アクセス制限されていないキャッシュDNSサーバに対しては、攻撃者がトリガーとなる問い合わせを任意に送ることができ、偽造応答を送りこむタイミングも容易に制御できます。その結果、こういったサーバを利用しているユーザは、偽造された情報を受けとる危険性が高まることになります。

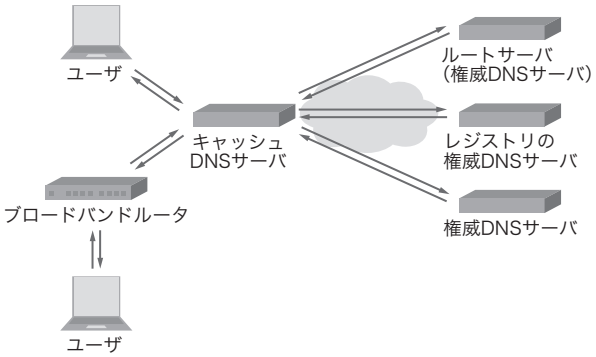
2.4 DNS ampの踏み台

リフレクション攻撃は、IPアドレスを詐称することで応答パケットの宛先を操作するものなので、DNSの応答を返すものはすべて踏み台になりえます(図-2)。

2.4.1 キャッシュ DNSサーバ

クライアントからの問い合わせを受けて、ルートサーバから順に権威サーバを探して名前解決を行うサーバです。前述のとおり、組織外からのアクセスは制限されるべきですが、現実にはそうではないものが多数存在しています。

例えば、権威DNSサーバとして運用しているつもりが、管理者の設定ミスや知識不足などの理由でキャッシュも有効になっていたなど、意図せずキャッシュDNSサーバとして動作しているものが踏み台にされるケースが多く見られるようです。



DNS応答を返すものはすべてampの踏み台になりえる。

図-2 DNSのプレーヤー

*5 前掲(http://www.apricot2013.net/__data/assets/pdf_file/0009/58878/tom-paseka_1361839564.pdf)。
*6 http://openresolverproject.org/breakdown.cgi
*7 http://www.auscert.org.au/render.html?it=80
*8 An Analysis of DrDoS SNMP/NTP/CHARGEN Reflection Attacks(http://www.prolexic.com/kcresources/white-paper/white-paper-snmp-ntp-chargen-reflection-attacks-drdos/index.html)。SNMP Reflected Amplification DDoS Attack Mitigation(http://www.bitag.org/documents/SNMP-Reflected-Amplification-DDoS-Attack-Mitigation.pdf)。
*9 http://mailman.nanog.org/pipermail/nanog/2013-July/060094.html

また、インターネット草創期にはこの攻撃手法が知られていなかったこともあり、相互扶助を意図してあえてアクセスを制限しないことも珍しくありませんでした。現在は当時と大きく事情が変化していますが、一度開放したものを後から制限するのは難しく、ISPなどでは歴史的経緯としてアクセス制限せず運用を続けているケースがあります。

2.4.2 ブロードバンドルータ

家庭用／業務用ブロードバンドルータの多くは、DNSフォワーダあるいはDNSプロキシと呼ばれる機能を持っています。宅内機器の名前解決のために使われるもので、本来LAN側からの名前解決要求にだけ答えればいいはずですが、一部に初期状態でWAN側からの問い合わせに無制限に答えてしまう製品が存在します[*10]。

ブロードバンドルータは、オープンリゾルバ以外にも外部から悪用される脆弱性を持つ製品が存在することが指摘されており、対策の必要性が議論されています。これについては、前号IIR Vol.20でも触れていますので参照ください。

2.4.3 権威DNSサーバ

DNSを構成するプレーヤーのうち、ゾーン情報を登録してキャッシュDNSサーバからの問い合わせに答える役割を担っているのが、権威DNSサーバ（コンテンツサーバ）です。

キャッシュDNSサーバやブロードバンドルータのDNSフォワーダは、外部から取得した情報のコピーを応答するので、増幅率が高くなるよう外部の攻撃者が情報を仕込むのも容易でした。しかし、権威DNSサーバは正当な管理者以外は情報を登録できないので、外部の攻撃者が意図的に増幅率の高い応答を返させるのは困難です。そのため、権威DNSサーバがDNS ampの踏み台として悪用されることはこれまでほとんどありませんでした。

しかし、DNSSECが有効になっていると、応答に電子署名が付加されるため、署名がない場合に比べて格段に応答が大きくなります。DNSSECはDNSのセキュリティ向上のための仕組みですが、見方を変えれば、攻撃者がわざわざ仕込まなくても十分に効率よく増幅できる踏み台を生み出してくれる仕組みであると考えることもできます。

権威DNSサーバの場合はオープンリゾルバとは呼ばれませんが、今後DNSSECの普及にともなってDNS ampの踏み台としての悪用事例も増えると想定され、対策が急がれています。

2.5 DNS amp対策

DNS amp攻撃に対する有効な対策手法をいくつか挙げてみます。RFC5358（BCP140）としてもまとめられていますので、そちらも参照してください[*11]。

2.5.1 アクセス制限

外部からのアクセスが適切に制限されていれば、仮にDNS ampの踏み台として狙われても、問い合わせが許可されていないとして無視するので、攻撃は成立しません。IPアドレスをアクセス許可されたものに詐称されている場合には制限が回避されてしまいますが、その場合でも応答する先は内部のネットワークになるため、少なくとも踏み台となって外部を攻撃することはなくなります。

また、LAN側インタフェースからの問い合わせのみを許可してWAN側からは無視する、といったネットワークインタフェースによる制限は、IPアドレスに頼らないため、外部からの不正な問い合わせ全般を防御できます。これはブロードバンドルータなど、複数のネットワークインタフェースを持つ機器では特に有効な対策です。

2.5.2 イングレスフィルタリング

リフレクション攻撃はパケットの送信元のIPアドレスを詐称することで行うので、ルータ側で詐称パケットの通過を許可しないように設定すると、攻撃は成立しなくなります。詐称IPアドレスによる攻撃手法は、他にもTCP SYN flood攻

＊10 JVN、「JVN#62507275 複数のブロードバンドルータがオープンリゾルバとして機能してしまう問題」（http://jvn.jp/jp/JVN62507275/）。ただし、この脆弱性レポートに記載されているもの以外にも、このような機器は広く販売されている（いた）ようなので注意が必要。
＊11 RFC5358（http://tools.ietf.org/html/rfc5358）。

撃やSmurf攻撃などいくつか知られており、これらも含めた根本対策として非常に有効です。この手法は、RFC2827(BCP38)で詳しく解説されています[*12]。

しかしながら、内部のネットワークから出ていくパケットに外部のIPアドレスが付与されている場合は比較的簡単に判別できますが、外部から流入してくるネットワークAからのパケットに、ネットワークBのIPアドレスが詐称されていても、それを判別するのは困難です。つまり、BCP38は外部からDNS ampの踏み台に悪用されないための防御策ではなく、内部のクライアントがIPアドレス詐称による不正行為を行えないようにするための対策となります。DNS amp攻撃は、自ら意図して攻撃を行うよりも、マルウェアに感染してボットとして意図せず攻撃に参加させられてしまうことが多いので、こういった攻撃がネットワーク内部から行われないようにするためにも必要な対策です。

世界中のネットワークでBCP38への対応が完了すれば、IPアドレス詐称による攻撃はなくなる理屈ですが、残念ながらほとんど対応は進んでいないのが現状です。

2.5.3 レート制限

キャッシュDNSサーバやブロードバンドルータと異なり、権威DNSサーバは不特定多数のキャッシュDNSサーバから広く問い合わせを受け付ける必要があり、アクセス制限するという手段は取れません。

キャッシュDNSサーバは、その名のとおり、受け取った応答を一定時間キャッシュするので、その間は権威DNSサーバに再度同じ問い合わせをすることはないはずです。この考えに立ち、権威DNSサーバでは、時間あたりの応答レートを制限することで大量の応答を抑止するという手法(RRL)が有望視されています[*13]。.orgや.infoなどのレジストリであるAffiliasは、amp攻撃の踏み台に使われて最大で2.3Gbpsまで増大した外向きのトラフィックが、RRLの導入により70Mbpsまで抑止されたと報告しています[*14]。

なお、アクセス制限ではなくレート制限によりamp攻撃の踏み台として悪用されにくくするというアプローチは、キャッシュDNSサーバに対しても一部で行われており、Google Public DNSは、この対策を行うことで不特定多数のユーザにオープンリゾルバを提供しています[*15]。

2.6 おわりに

DNS amp攻撃は、その手法自体は比較的古くから知られていたものの、十分な対策はこれまであまりされておらず、実質的に野放しに近い状態にあります。

国内では、今年に入ってから通信事業者各社やセキュリティ団体によって注意喚起や実態調査の動きが活発になってきましたが、実際の対策となると緒に就いたばかりというところで、道のりはまだまだ険しいと言わざるを得ません。

ここまで他人事のように筆を進めてきましたが、実はIIJにもオープンリゾルバとなっているキャッシュDNSサーバは存在しており、現在まさに対策を進めているところです[*16]。これまでの過ちを正しながら、安全なサービスを提供できるよう努めて参ります。

執筆者:

山口 崇徳(やまぐち たかのり)
IIJ プロダクト本部 プロダクト開発部 メッセージングサービス課。2006年入社。メールサービス、DNSサービスの運用に従事。

*12 RFC2827(http://tools.ietf.org/html/rfc2827)。BCP38(http://www.bcp38.info/)。
*13 http://www.redbarn.org/dns/ratelimits
*14 http://lists.redbarn.org/pipermail/ratelimits/2012-December/000144.html
*15 https://developers.google.com/speed/public-dns/docs/security#rate_limit
*16 IIJ、「オープンリゾルバ根絶に向けての取り組み」(http://www.iij.ad.jp/company/development/tech/activities/open_resolver/)。てくろぐ、「『昔IIJを使っていた人』にお願いです – オープンリゾルバ対策」(http://techlog.iij.ad.jp/archives/718)。