平成 26 年 7 月 23 日

Topic

日本国内のオープン・リゾルバを踏み台とした DDoS 攻撃発生に起因すると考えられるパケットの増加について

日本国内のオープン・リゾルバを踏み台とした新たな攻撃手法に起因すると考えられるパケットを観測しています。管理する機器がオープン・リゾルバとなっていないか改めて確認することを推奨します。

1 発信元ポートを 53/UDP とするパケットの観測状況の変化について

警察庁においては、平成 26 年2月3日以降、発信元ポートが 53/UDP である DNS 問い合わせに対する応答パケットを観測しています。同パケットについては、発信元を偽装したオープン・リゾルバの探索行為に起因[i]するものであると考えられていたところです。しかしながら、6月から同パケットの観測状況に次に示す3点の変化が生じています。

(1) 使用実態が確認できるドメインの問い合わせに対する応答が増加

同パケットが観測され始めた2月当初の段階では、観測された応答パケットにおける問い合わせ対象のドメインは、探索行為を実施するためだけに取得されたと考えられる使用実態が確認できないドメインが多数を占めていました。しかしながら、6月からは、ウェブサイト運用等の使用実態が確認できるドメインの問い合わせに対する応答パケットが多数観測されるようになっています。このことから、単なるオープン・リゾルバの探索行為だけではなく、別の目的を持った活動に起因するパケットが増加しているものと考えられます。

(2) 日本国内の発信元 IP アドレスの割合が増加

観測されたパケットの発信元 IP アドレスのうち、日本に割り当てられている IP アドレス（以下「日本国内の IP アドレス」という。）が占める割合が大きくなっています。おおむね3～5%前後で推移していた日本国内の IP アドレスの割合が、6月 29 日からは同割合が 10%以上になる日が多数となっています（図1）。これは、全 IPv4 アドレスのうち日本国内のアドレス数が占める割合[ii]と比較すると大きな値となっています。日本国内の IP アドレスを多数含む何らかのリストに基づいた活動に変化している可能性が考えられます。

[i] 「発信元 IP アドレスを偽装したオープン・リゾルバの探索行為の増加について」（平成 26 年2月 17 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140217.pdf
[ii] 約 4.7%（平成 26 年7月 22 日現在）

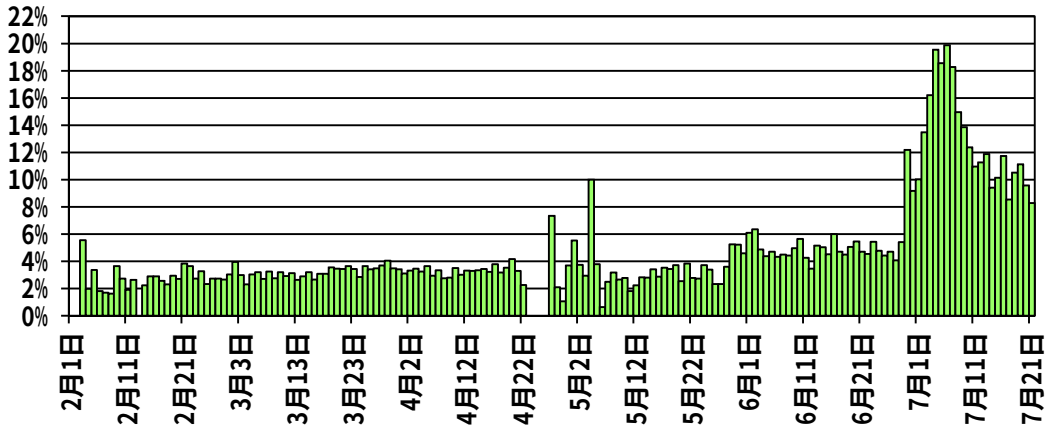

図1　発信元ポートを 53/UDP とするパケットの発信元 IP アドレスのうち、日本国内の IP アドレスが占める割合の推移（H26.2.1～7.21）

(3) 発信元 IP アドレス当たりの観測パケット数が増加

同パケットの日本国内の発信元 IP アドレスに着目すると、1個の発信元 IP アドレス当たりの観測パケット数が増加しています。これまでは1個の発信元IPアドレスから観測されるパケット数は基本的には1件でした。しかしながら、6月 29 日からは、1個の発信元 IP アドレスから観測されるパケット数が2件以上となる状況が見られるようになりました（図2）。発信元を偽装したオープン・リゾルバの探索行為が行われている場合には、1個の IP アドレスに対して2件以上の DNS 問い合わせを送信する必要はありません。このため、1個の IP アドレスに対して DNS 問い合わせが繰り返し送信されている現状から、何らかの攻撃活動が実施されている可能性が考えられます。

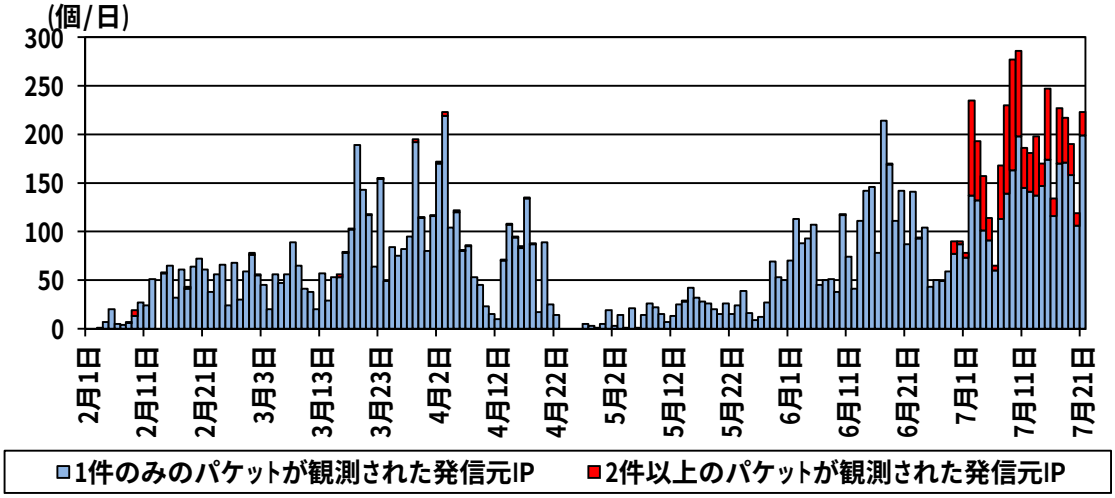

図2　発信元ポートを 53/UDP とするパケットの日本国内の発信元 IP アドレス数の推移（H26.2.1～7.21）

2 想定される攻撃手法について

(1) 想定される攻撃手法

日本国内の複数の ISP 事業者から、深刻な通信障害が発生しているとの広報が複数回行われています。また一部の事業者においては、管理するキャッシュ DNS サーバに大量のアクセスが発生しているとの広報も行われています。

これらの情報と、警察庁における観測状況から推測すると、あらかじめ把握しているオープン・リゾルバを踏み台とした大量の DNS 問い合わせを行うことにより、攻撃対象となった DNS サーバの正常な運用を妨害する DDoS 攻撃が実施されている可能性が考えられます。

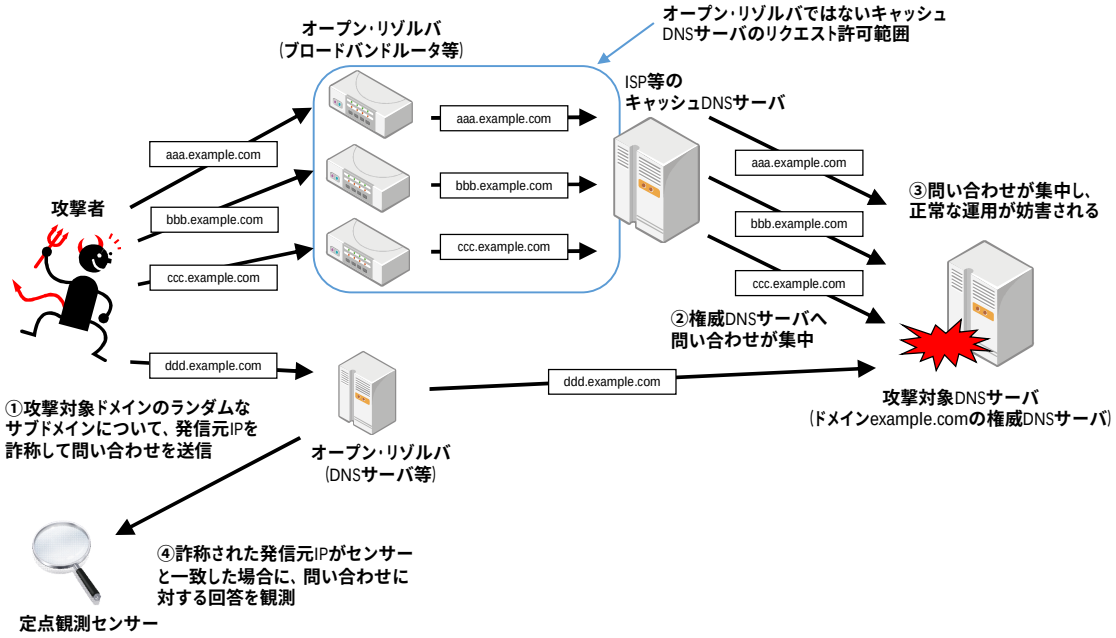

図3 想定される攻撃手法

同手法は DNS リフレクター攻撃とは異なり、オープン・リゾルバからの回答パケットを攻撃対象 DNS サーバに送信するものではありません。このため、オープン・リゾルバによるパケットサイズの増幅は行われません。しかしながら、攻撃対象 DNS サーバで受信する DNS 問い合わせの発信元 IP アドレスが、ISP 事業者が運用する正規のキャッシュ DNS サーバであった場合には、単純に IP アドレス単位でのアクセス拒否を実施できない等の点で、攻撃者に利点がある手法であると考えられます。

なお、JPCERT/CC からは、同様な攻撃手法とみられる具体的な観測事例が報告[i]されています。

[i] 「インターネット定点観測レポート(2014 年 4～6 月)」(平成 26 年 7 月 17 日)
https://www.jpcert.or.jp/tsubame/report/report201404-06.html

(2) 攻撃の踏み台となった場合の影響

同手法による攻撃が実行された場合、攻撃対象 DNS サーバだけではなく、踏み台となるオープン・リゾルバ等においても、以下の影響を受ける可能性があります。

- オープン・リゾルバにおける運用妨害

  踏み台となるオープン・リゾルバに、大量の DNS 問い合わせが行われた場合、回線帯域や機器の処理能力がひっ迫し、正常に動作しなくなる可能性が考えられます。一般家庭等に利用されているブロードバンドルータ等の場合には、インターネットに接続できなくなるといった影響が考えられます。

- キャッシュ DNS サーバにおける運用妨害

  一般家庭等で運用されているブロードバンドルータ等は、多くの場合、契約している ISP のキャッシュ DNS サーバを参照しています。この様な多数の機器が参照するキャッシュ DNS サーバには、参照する機器が踏み台となった場合に大量の DNS 問い合わせが集中し、正常な運用が妨害される可能性が考えられます。

  また、ランダムなサブドメインについて問い合わせをされた場合には、キャッシュが短時間であふれるとともに、問い合わせを受ける都度、自らも権威 DNS サーバに対して問い合わせを行う必要があるため、負荷がより大きくなる可能性が考えられます。

  ISP のネットワーク内からのみ問い合わせを許可する等、オープン・リゾルバとはならない適切な運用が行われている場合でも、本攻撃手法に対する有効な対策とはならないことにも留意する必要があります。

(3) 同攻撃手法の発生を防ぐ対策について

攻撃対象となった DNS サーバや、ISP 事業者が管理するキャッシュ DNS サーバ等で実施できる対策は限定されます。このため、DNS リフレクター攻撃の対策と同様に、オープン・リゾルバを根絶し、攻撃発生の機会を低減させることが最も重要となります。

警察庁においても、オープン・リゾルバに対する対策については、既に注意喚起[i]を実施しているところです。インターネットの全ての利用者は、利用している機器がオープン・リゾルバとなっていないかを改めて確認するとともに、同状態となっている機器を発見した場合には的確な対処を実施することが推奨されます。

---

[i] 「情報技術解析平成 25 年報」の「6.4 DNS リフレクター攻撃の踏み台とならないために推奨する対策」を参照のこと。
http://www.npa.go.jp/cyberpolice/detect/pdf/H25_nenpo.pdf