平成 26 年2月 17 日

Topic

発信元 IP アドレスを偽装したオープン・リゾルバ[1]の探索行為の増加について

偽装された発信元 IP アドレスからのオープン・リゾルバの探索行為に起因すると考えられるパケットを多数検知しています。DNS リフレクター攻撃の踏み台とならないように、管理する DNS サーバ等の設定を確認することを推奨します。

1 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について

警察庁の定点観測システムにおいては、2月4日以降、53/UDP を発信元ポートとするパケットを多数観測しています（図1）。

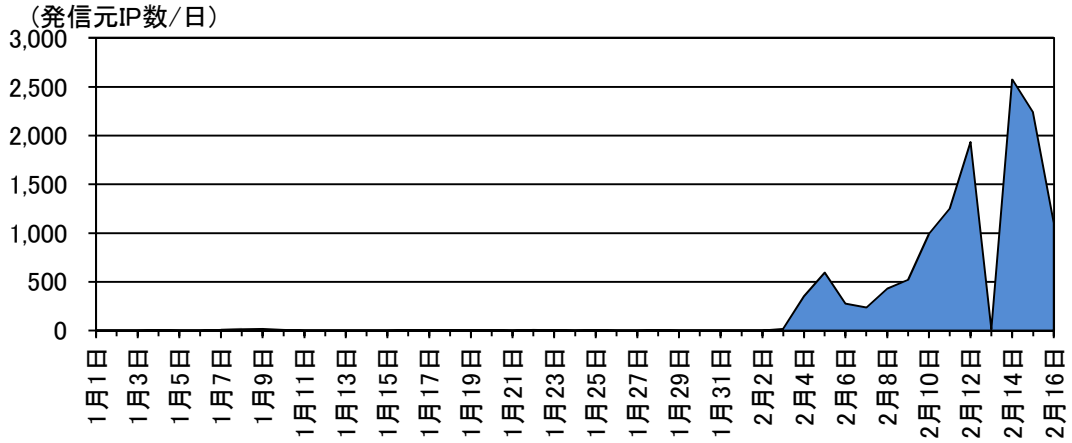

図1 53/UDP を発信元ポートとするパケットの1日当たりの発信元 IP アドレス数の推移（H26.1.1～H26.2.16）

同パケットの内容を確認すると、多くのものは DNS 問い合わせに対する応答パケットでした。また、発信元となっている IP アドレスの多くが、DNS サーバとして外部に公開されているものであることが判明しています。このことから、何者かが発信元 IP アドレスを偽装した上で、当該 DNS サーバに対して DNS 問い合わせを実施しているものと考えられます。

発信元 IP アドレスが偽装されているため、DNS サーバに対して問い合わせを実施した者は、その応答を受信することはできません。しかしながら、問い合わせを行った対象サーバが、自らで再帰問い合わせ[2]を行うオープン・リゾルバであった場合には、図2のとおり対象サーバがオープン・リゾルバであることを判別することが可能であると考えられます。

---

[1] 外部ネットワークから任意のドメインについて問い合わせが可能な DNS サーバもしくは同様の機能が有効となっているコンピュータ等のこと。DNS リフレクター攻撃の踏み台となる。DNS リフレクター攻撃（DNS リフレクション攻撃）については、次の資料を参照のこと。
「DNS リフレクション攻撃に対する注意喚起について」（平成 25 年4月 11 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130411.pdf

[2] 問い合わせを受けたドメインに関する情報を自らが持っていない場合に、必要な情報を入手するまで他の DNS サーバに問い合わせを行い、その結果を問い合わせ元に回答する動作のこと。

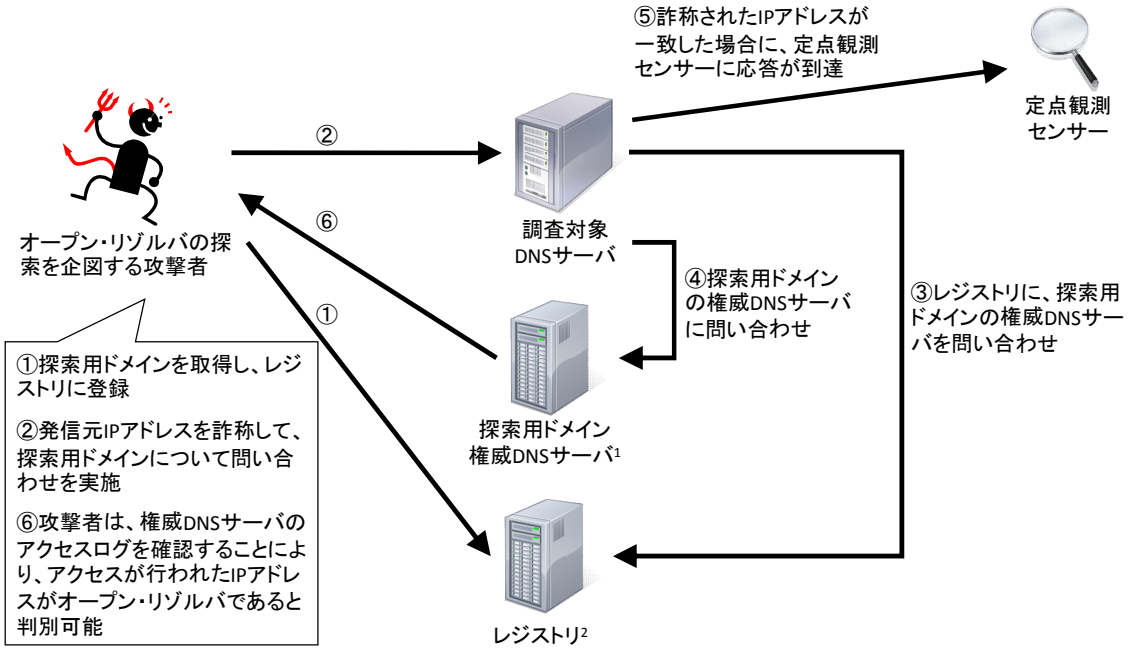

図2　発信元 IP アドレスを詐称した DNS 問い合わせによるオープン・リゾルバの探索手法

なお、発信元 IP アドレスを偽装したうえで、オープン・リゾルバの探索を実施する意図ははっきりとしませんが、身元の隠蔽や、発信元 IP アドレスが不審なアクセスの発信元としてセキュリティ対策企業等が作成するアクセス拒否リストに登録されることを防ぐためであると考えられます。

[1] 特定のドメインに関する情報を管理する DNS サーバ。「コンテンツ DNS サーバ」とも呼称される。
[2] 特定の単位に属するドメイン全体の情報を管理する組織。

2 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

管理する機器が、DNSリフレクター攻撃の踏み台として悪用されないために、過去の注意喚起と一部重複しますが、次の対策を実施することを推奨します。

(1) DNSサーバの適切な運用

ア 権威DNSサーバとキャッシュDNSサーバ[1]を分離する。

イ 権威DNSサーバにおいては、再帰問い合わせの機能を無効とする。

ウ キャッシュDNSサーバについては、適切なアクセス制限を実施する。

(2) ブロードバンドルータの適切な運用

家庭や小規模な組織のネットワークをインターネットに接続する際に使用されるブロードバンドルータについても、本来は拒否するべき外部のネットワークからの問い合わせを受け付けて、オープン・リゾルバとして動作する物が存在することが判明[2]しており、確認及び対策が必要です。

ア 確認用のウェブサイト[3]等を利用して、管理するブロードバンドルータがオープン・リゾルバとして動作していないか確認を実施する。

イ 管理するブロードバンドルータがオープン・リゾルバとして動作していることが判明した場合には、ファームウェアのアップデートや、適切な設定変更を実施して、オープン・リゾルバとして動作している状態を解消する。

以 上

[1] 組織内のネットワークからの全ての問い合わせを受け付けて、再帰問い合わせや他のキャッシュDNSサーバへ転送することにより得られた結果を応答として返すDNSサーバ。

[2] 「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/

[3] 「オープンリゾルバ確認サイト公開のお知らせ」
http://www.jpcert.or.jp/pr/2013/pr130002.html