Topic

平成 25 年9月 11 日

中国を発信元とする再帰問い合わせ可能な DNS サーバの探索行為の増加について

DNS リフレクション攻撃の準備行為が行われている可能性があります。各組織や個人で管理する DNS サーバが攻撃に悪用されないように注意してください。

1 再帰問い合わせ可能な DNS サーバの探索行為の増加について

警察庁では、9月 10 日から中国を発信元とする宛先ポート 53/UDP に対するアクセスの増加を検知しています(図1)。

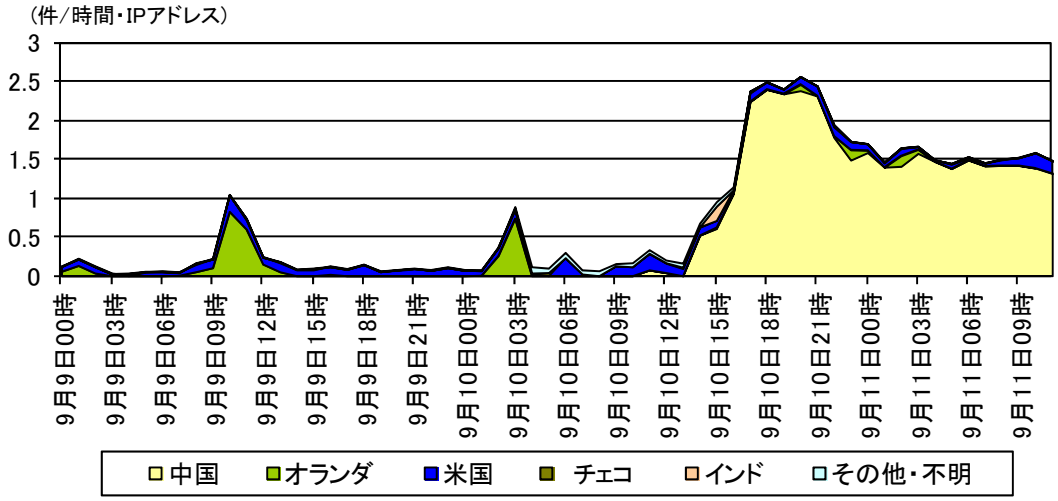

図1 宛先ポート 53/UDP に対するアクセス件数の推移(9/9 00:00～9/11 12:00)

同アクセスの内容を分析した結果、外部から再帰問い合わせ可能であるとともに、DNS の拡張機能「EDNS0」[1]に対応している DNS サーバの探索を実施していることが判明しました。

このことから、同アクセスは、効率的な DNS リフレクション攻撃に悪用可能である再帰問い合わせ可能な DNS サーバ(オープンリゾルバ)の探索を実施しているものと考えられます。

警察庁では、DNS リフレクション攻撃(DNS アンプ攻撃)及び同攻撃の準備行為と考えられる再帰問い合わせ可能な DNS サーバの探索の増加について、注意喚起を実施してきたところです。[2,3,4]

2 DNS サーバが DNS リフレクション攻撃に悪用されないために

9月 18 日が満州事変の契機となった柳条湖事件が発生した日であることから、昨年の9月 18 日前後には、中国語の掲示板等において国内の行政機関や重要インフラ事業者等に対するサイバー攻撃の呼びかけが行われました。幾つかの事業者に対しては実際にサイバー攻撃が実施されたことも確認しています。このため、本年の9月 18 日前後にも、DNS リフレクション攻撃を含め、サイバー攻撃が敢行されることが懸念されます

各組織や個人においては、管理する DNS サーバが DNS リフレクション攻撃に悪用されないように、次の事項を再度確認することを推奨します。

- キャッシュ DNS サーバと権威(コンテンツ)DNS サーバが分離されているか。
- キャッシュ DNS サーバについては、外部からの不要なアクセスを制限しているか。
- 外部へ公開している権威(コンテンツ)DNS サーバにおいては、再帰問い合わせを無効としているか。
- 外部へ再帰問い合わせ可能な DNS サーバを公開する必要がある場合には、応答頻度の制限や、不要な IP アドレスからのアクセス制限などを実施しているか。

---

[1] 「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」(平成 18 年7月 11 日)
http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/20060711_DNS-DDoS.pdf

[2] 「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

[3] 「インターネット観測結果等(平成 25 年6月期) 」(平成 25 年7月 26 日)
http://www.npa.go.jp/cyberpolice/detect/pdf/20130726_1.pdf

[4] 「インターネット観測結果等(平成 25 年度第 1／四半期(4月～6月))」(平成 25 年8月1日)
http://www.npa.go.jp/cyberpolice/detect/pdf/20130801.pdf