DNSの評価と計測の話
- JP DNSへのRRLの導入

2013年11月28日
Internet Week 2013　DNS DAY

株式会社日本レジストリサービス（JPRS）

あはれん　よしたか
阿波連　良尚

本発表の内容

- おさらい: DNSリフレクター攻撃の概要と対策
- 評価と計測の実例: JP DNSサーバーへのDNS RRLの導入

DNSリフレクター攻撃とは

- DDoS攻撃の一つ
  - 攻撃先の帯域幅を消費させる
- DNSサーバーを踏み台として利用
  - 主に用いられる通信プロトコルがUDPであるため、送信元IPアドレスを詐称した攻撃が成立しやすい
  - 応答のサイズがクエリのサイズよりも大きくなる
- 攻撃に利用可能なサーバーが多数存在
  - 攻撃の規模を大きくすることが容易

DNSリフレクター攻撃への対策

- 根本的対策：BCP38の適用
  - インターネット全体での対策が必要
- キャッシュDNSサーバーにおける対策
  - 送信元IPアドレスに基づいてクエリの受付を制限
- 権威DNSサーバーにおける対策
  - キャッシュDNSサーバーとは異なり、送信元IPアドレスによる制限が困難
  - 有効な対策：DNS Response Rate Limiting（DNS RRL）

JP DNSへの導入

- DNS RRLは、権威DNSサーバーにおける DNSリフレクター攻撃への対策として有効
  - JP DNSにも導入したい
- JP DNSサーバーへの導入にあたっては、 影響を与えないよう慎重な評価が必要
- 評価のステップを定め、導入への検討を実施 （次スライドで説明）

評価のステップ

- 机上評価
  - パラメータの調査と設定
- 社内評価
  - 機能面・性能面・運用面の評価
- フィールド評価
  - 影響を与えない状態での試験的な導入
- 実運用への投入

机上評価（1）概要

- RRLの機能について調査
  - 挙動の理解
  - 調整が必要なパラメータの洗い出し
- 各種パラメータの調整方針を決定
  - JP DNSの平常クエリが引っかからない（＝false positiveがないこと）
  - 過去に観測した異常クエリが引っかかる（＝false negativeがないこと）
- パラメータの調整

机上評価(2) 調整するパラメータ

RRLの応答を制限するパラメータ

項目	機能	デフォルト
`responses-per-second` *`number`*`;`	基本的な応答の制限	0 (制限無し)
`referrals-per-second` *`number`*`;`	委任応答の制限	`responses-per-second`の値
`nodata-per-second` *`number`*`;`	nodataとなる応答の制限	`responses-per-second`の値
`nxdomains-per-second` *`number`*`;`	NXDomainとなる応答の制限	`responses-per-second`の値
`errors-per-second` *`number`*`;`	エラーとなる応答の制限	`responses-per-second`の値
`all-per-second` *`number`*`;`	すべての応答を制限	0 (制限無し)

- 上記パラメータのうち、responses-per-secondを調整
  - ネットワーク単位で、同じ名前に対するクエリへの応答頻度を制限

机上評価(3)
パラメータ調整のステップ

- JP DNSの過去のクエリを解析
  - DSC†1を利用してクエリの傾向を記録
  - JP DNSサーバーの一部では、受信パケットのtcpdumpを記録
- 通常クエリに影響を与えないよう閾値を決定
  - 過去に観測した異常な頻度のクエリに対しては、応答頻度を制限することも併せて確認

†1 http://dns.measurement-factory.com/tools/dsc/

社内評価（1）機能評価

- 応答差異確認
  - JP DNSへのクエリと同様のクエリパターンを生成し、その応答をRRLの有無で比較
  - 応答内容にJP DNSとして問題となる変化がないことを確認
- 機能動作確認
  - マニュアルに基づいて、各設定項目が動作することを確認
  - 制限時のログ出力が多すぎると判明（次スライドで説明）

社内評価(1) 機能評価
多量のログ出力

- 応答を制限したクエリをログに出力
  - 高頻度のクエリを受けるとログが増大
- 当初は“querylog”カテゴリに出力
  - ログ出力レベルは“info”
  - カテゴリ・レベルが同じクエリログとの分離が困難
- ratelimitsメーリングリストに相談
  - 開発者がカテゴリとログレベルの変更を提案
  - “query-errors”カテゴリに変更

社内評価(2) 性能評価

- 性能試験
  - DNSPerf†2を利用し、DNS応答性能を計測
  - 定められた処理性能を満たすことを確認
- リソース確認
  - CPU使用率やメモリ消費の増加が、あらかじめ定めた基準値以下であることを確認
  - 応答を制限している状態では、RRLありの方がCPU負荷が低いと判明
  - 応答制限よりも、応答生成の方が負荷が高い

†2 http://nominum.com/support/measurement-tools/

社内評価(3)運用評価

- ランニング試験
  - 隔離された環境で、JP DNSと同じゾーン転送を受けるよう設定
  - 長期間の動作でも問題が発生しないことを確認
- パラメータ評価
  - tcpreplay†3を利用して、実クエリを再現
  - 通常クエリに対する応答が制限されないことを確認

†3 http://tcpreplay.synfin.net/

フィールド評価（1）概要

- JP DNSサーバーの1台に試験導入
  - JPRSが運用するサーバーに導入
  - 机上評価で定めたパラメータを設定
  - 閾値を越えた場合でも制限をかけず、ログに出力するモード（log-onlyモード）を設定
- 評価期間（1カ月）で8件のイベントを検出
  - クエリログを調査し、そのすべてが応答頻度を制限しても問題ないクエリであることを確認

フィールド評価（2）
検出したクエリの内訳

- REFUSEDになるクエリ
  - JP DNSが持っていない逆引きゾーンへの高頻度のクエリ
- NXDOMAINになるクエリ
  - 総当たり（スキャン）と思われる高頻度のクエリ（.jpゾーン・逆引きゾーン）
  - 同じ名前（qname）の高頻度のクエリ
- 委任情報を返すクエリ
  - 同じ名前（qname）の高頻度のクエリ

実運用への投入

- 評価の結果、すべてのJP DNSサーバーに導入しても問題は発生しないと判断
- 現在、各セカンダリ組織と協力し、JP DNSに順次導入を進めている
  - log-onlyモードで導入して経過観察（1カ月）
  - 問題なければ制限するモードに変更
- 2014年1月に導入完了予定

Q and A