Janog34 BoF
我慢する？あきらめる？工夫する？
大量攻撃トラフィック対応

ビッグローブ株式会社　クラウドサービス本部
熊木 美世子

概要

- タイトル:
  我慢する？あきらめる？工夫する？大量攻撃トラフィック対応
  - http://www.janog.gr.jp/meeting/janog34/tutorial/bkdos.html

- Abstract
  - 年々、件数も攻撃力もupするDoS/DDoS、あなたのネットワークではどのように対処していますか？
  - 5月末に各ISPで発生した DNSへの大量アタックの話を中心に現在の対応方法の情報交換および今後の対応方法について各種技術的解決方法やIP*b(53,123, 他port) の是非を議論します。

- 目的:
  - 今後の攻撃対策も兼ねた解決案を模索・議論する
  - 今回以外のDNSむけ攻撃、他プロトコルむけ攻撃などの対策も考えたい

最近発生した顕著なDoS/DDoS

- DNSへの攻撃は5月末～まだまだ続いてます
  - 攻撃きた？
  - 耐えた？
  - 対策した？

- もっと大規模な攻撃がきたらどうしよう？
- 他サーバ（特定プロトコル）への攻撃がきたらどうしよう？

BIGLOBEでの対策の試行錯誤

- 普段からのDoS/DDoS対策を強化
  - Mitigation
  - NWの出入り口でトラフィック量の異常を検知し対策
  - DNSむけトラフィックをセキュリティ装置へ誘導
- DNSのBlacklist準備
- DNS usage監視の強化

これらの方法、アリ？ナシ？

1. 増設して耐える
2. 網内のオープンリゾルバをつぶしていく
3. Bind改修
4. DNS用WAF
5. 網全体でのMitigation
6. DNS でのblocking list
7. 有事はrequest packetを間引く
8. IP53B
9. 8.8.8.8 など他社DNSをユーザに通知

セキュリティ仕事（沼）に陥らないベストな対応について議論していきましょう