海外におけるインターネットセキュリティインシデント概観

中国における大規模ネットワーク障害

2009.11.24

JPCERT/CC

2007 DDoS

DDoS

- 初めて攻撃者逮捕

標的

- 聯眾、完美時空等オンラインゲーム

損失

- 数千万円

攻撃者

- 上海ファイアーウォール会社

4-2. 2009年 DDoS 攻撃

JPCERT CC®

5月
- 519 事件・大規模インターネット障害

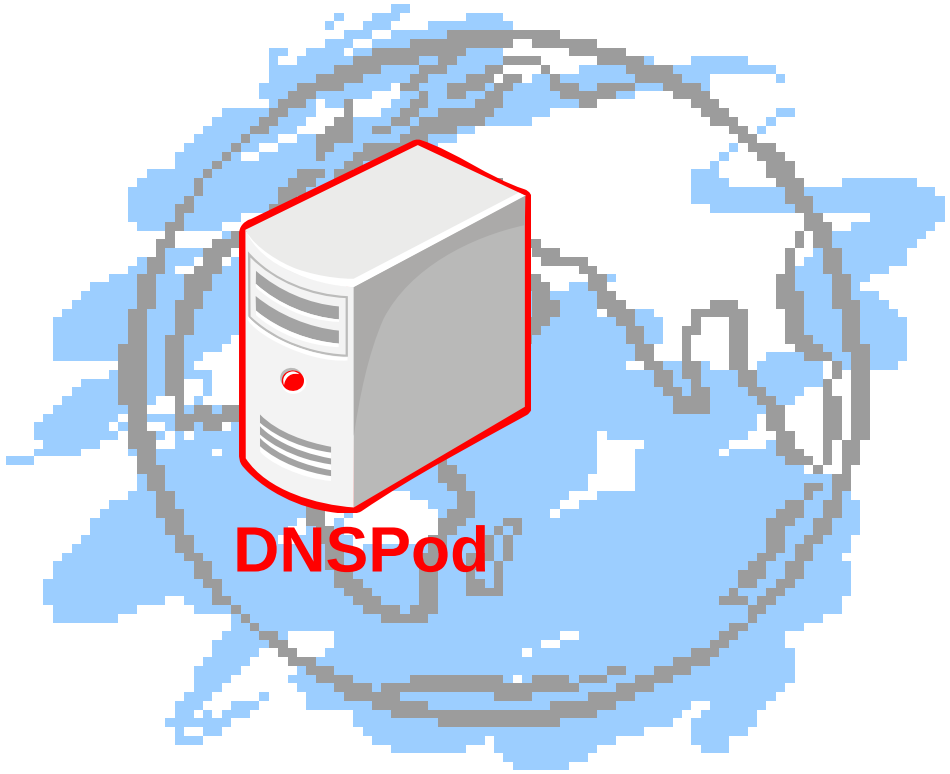
6月
- QQ 騰訊サイトへの DDoS

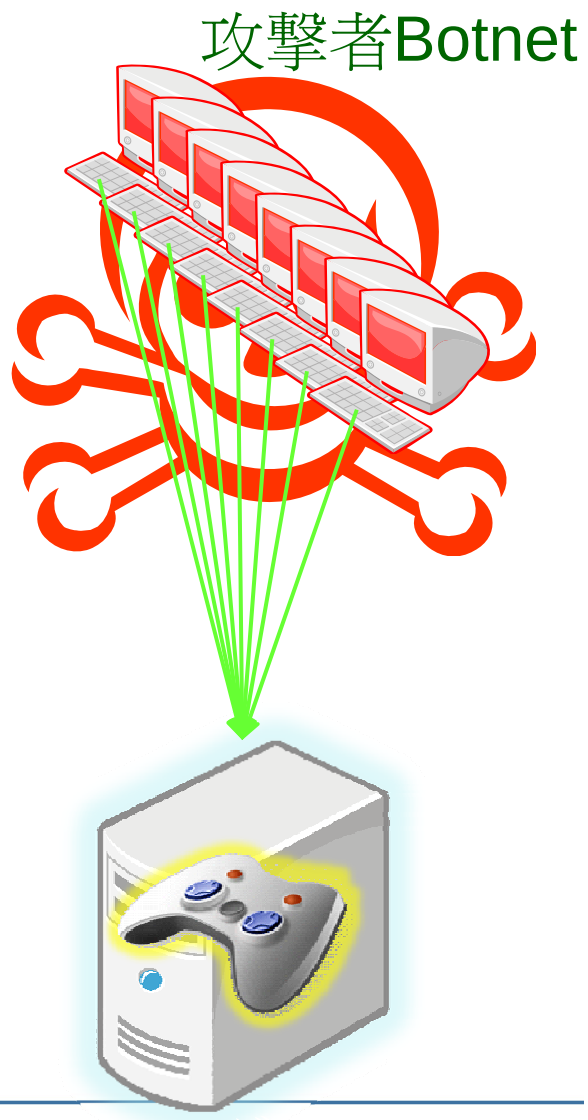
7月
- 新網互聯 www.dns.com.cn

8月
- 商務中國 www.bizcn.com
- 中資源 www.zzy.cn

中國水產養殖網、175U網頁遊戲 (175u.com)

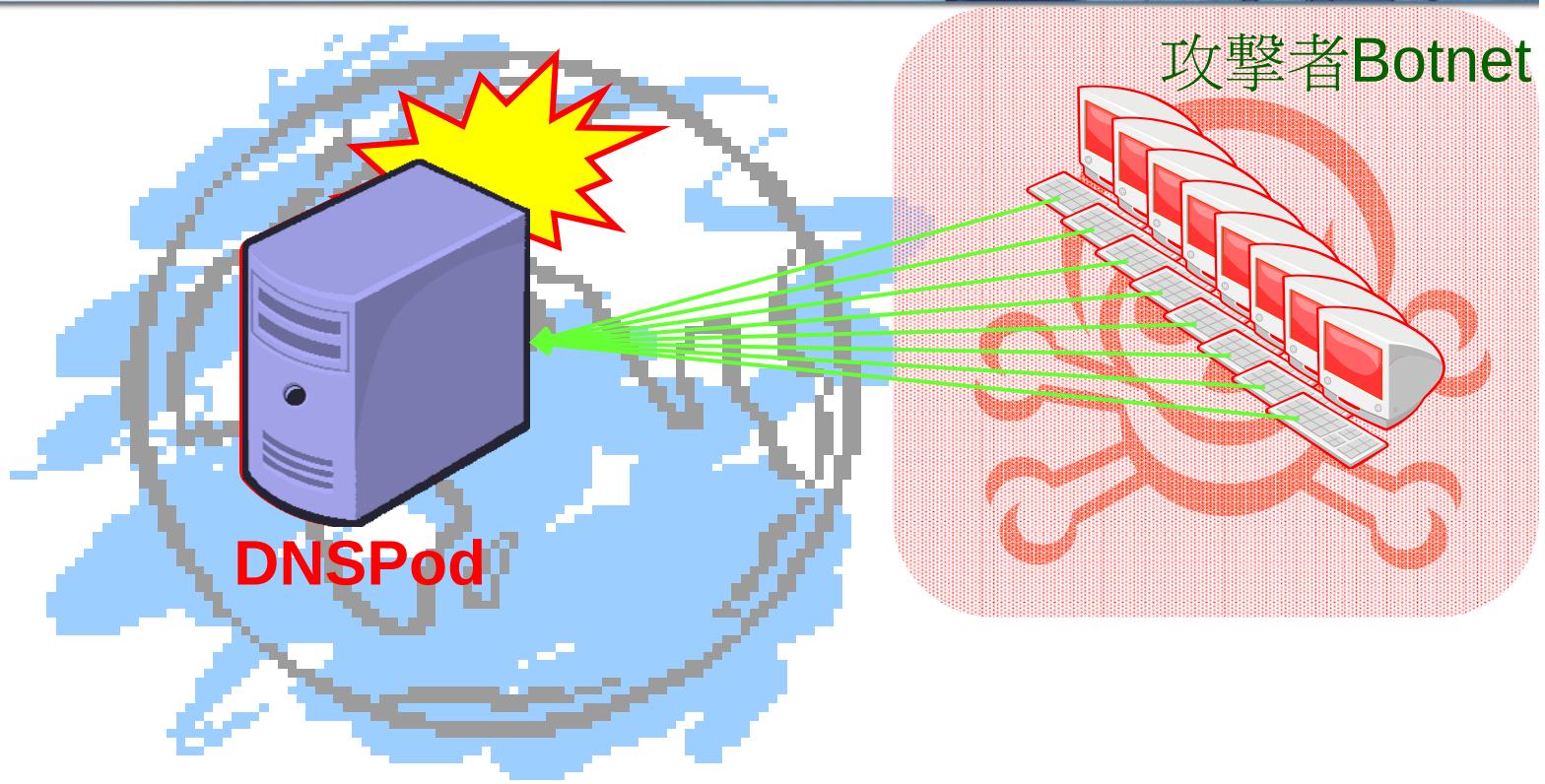
519障害事件：①野良サーバ業者の攻撃





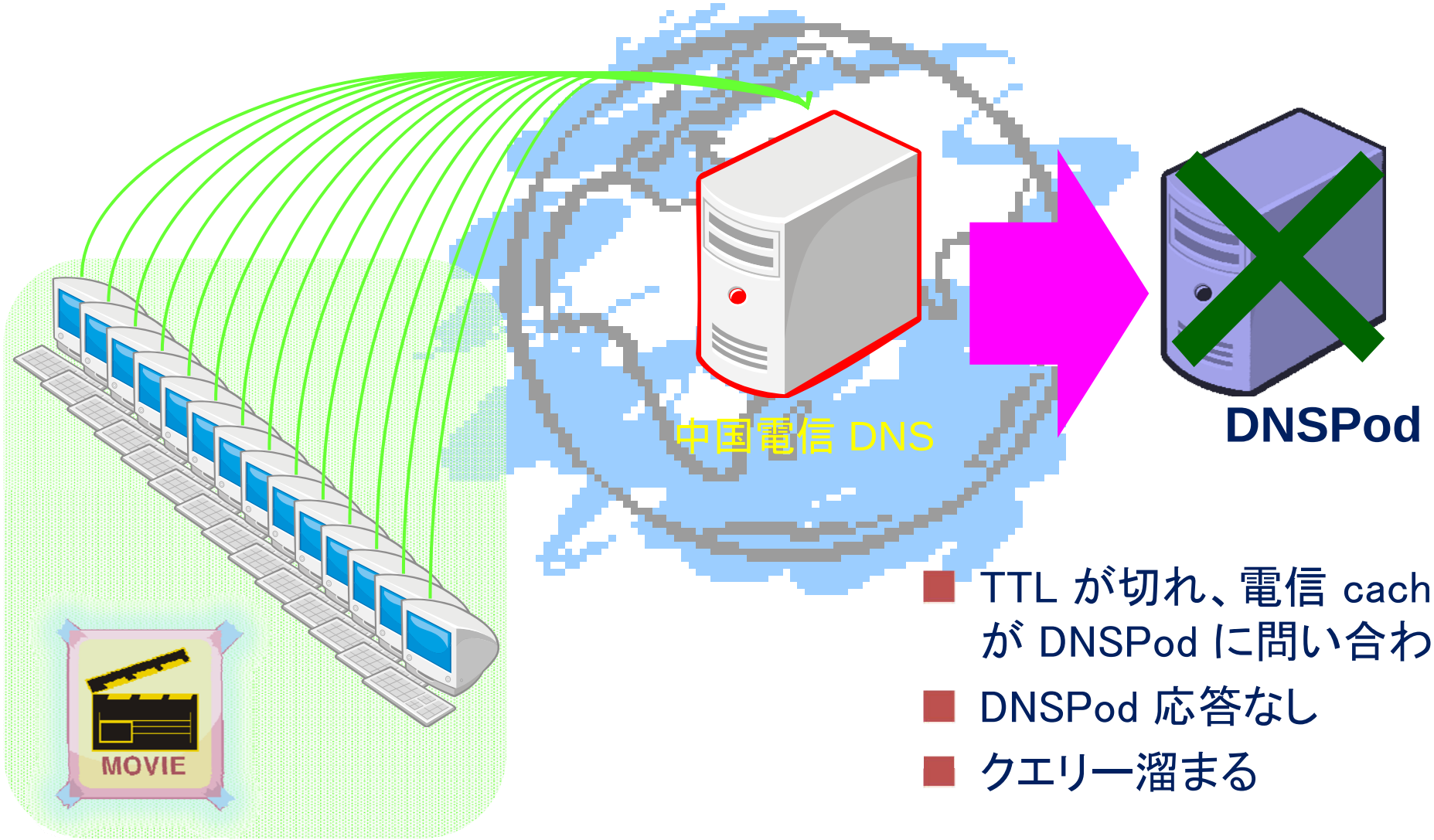
- ゲームユーザ獲得
- Botnet（=殭屍網路、Bot=肉鶏）
- 熾烈な攻防
- →利用しているDNS を攻撃

519障害事件：②05/18 DNSPodへの DoS



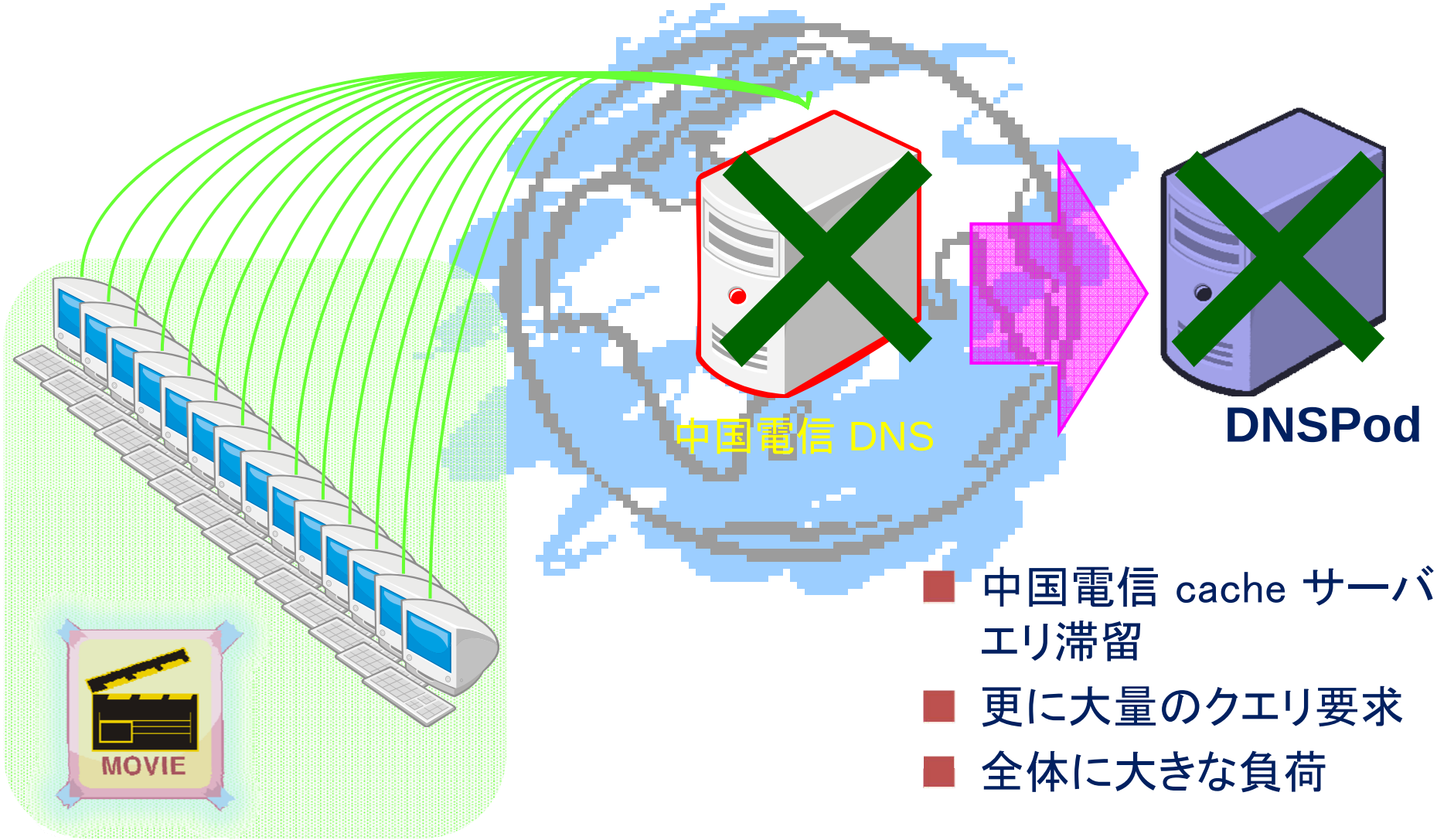
- 攻撃者 によるDNSPod への攻撃
- プライマリサーバ落ちる
- 残りサーバの TTLを1日へ変更
- 中国電信(ISP)対応 によりIP 使用停止

519障害事件：③05/19「暴風影音」大量クエリ



- TTL が切れ、電信 cache サーバが DNSPod に問い合わせ開始
- DNSPod 応答なし
- クエリー溜まる

519障害事件: ④05/19 DNS 過負荷



- 中国電信 cache サーバ大量のクエリ滞留
- 更に大量のクエリ要求
- 全体に大きな負荷

まとめ

暴風影音

- 「暴風門事件」
- ソフトウェア更新
- 238万賠償要求

攻撃者

- 逮捕
- 計算機情報システム破壊罪

DNSPod、通信事業者

- DNS フリーサービス
- 「蝶の羽ばたきが台風を生んだ」
- 20数省が影響
- 設備強化

政府

- 「519事件」
- 「6省断網」
- トロイ・ボットネット対応規則
- 中国脆弱性DBの設立

ありがとうございます

JPCERT CC®

- Contact info
  - Jack YS LIN
    - Information Security Analyst
    - Watch and Warning Group
- JPCERT Coordination Center
  - Web. https://www.jpcert.or.jp
  - Tel. +81-3-3518-4600
  - Fax. +81-3-3518-4602
  - Email. office@jpcert.or.jp