2010年大規模DDoS体験談

NTTコミュニケーションズ
グローバル事業本部
宮田　祐雄

2010年の事例

- ntt.net(AS2914)では、2度大きなDosアタック事例がありました。
  - 尖閣諸島問題 （2010年9月）
  - ミャンマー総選挙 （2010年11月）

攻撃は複雑化、大規模化してきています。
実際に体験した攻撃の様子と、とった対策を報告します。

※AS2914はVerioではありません。☺

尖閣諸島問題(2010年9月)

- 概要
  - 尖閣諸島での漁船の衝突問題に関連して、中国最大組織のハッカー組織が日本政府機関サイト等へ攻撃すると予告あり
    - 一般への参加呼びかけ(tool/練習期間/指導?)
  - 攻撃予告日： 2010年9月18日(土)　21時
    (9月18日は満州事変勃発日)
- 攻撃の様子
  - 練習期間？に複数の攻撃を観測　(数10Mbps程度)
  - 9/18日以降も25日頃まで継続(数10Mbps程度)
  - 主に中国との接続点から流入
  - SourceIPをランダムに偽装
    - SYN flood/ UDP NULL/ ICMP/ TCP Reset
    - Portは80番、その他
- 対策:中国との接続点でtargetIP宛のパケットをフィルタリング

ミャンマー総選挙(2010年11月)

- 概要
  - ASIA　POPに収容されているミャンマーのISP宛に大規模なDDoS攻撃が長期間断続的に発生した。(10月-11月)
  - ミャンマーの総選挙(11月7日)への抗議?
  - こちらにも詳しいレポートがあります
    - http://asert.arbornetworks.com/2010/11/attac-severs-myanmar-internet/
- 攻撃の特徴
  - 最大15Gbpsのアタック　(顧客のアクセスラインは輻輳)
  - 最長継続時間　:1 day 08:56:48
  - 攻撃パターンが徐々に変化
    - 初期　TCP/ICMP flood
    - 中期　UDP
    - 後期　細かくフロー分け(source/dest)されたUDP

ミャンマー総選挙(2010年11月)

- 対策
  - TASサービス(Dos検知・緩和サービス)をお客様が利用
  - Mitigation機能
    - 初期　TCP/ICMP　flood　：非常によく機能した
      (anti　spoof対応機能)
    - 中期　UDP　flood:　destあたりの閾値を調整して対応
    - 後期　細かくフロー分けされたUDP（source/dest）
      ：　対応が困難。　通信にUDP通信に　rate　limitをかけて対応

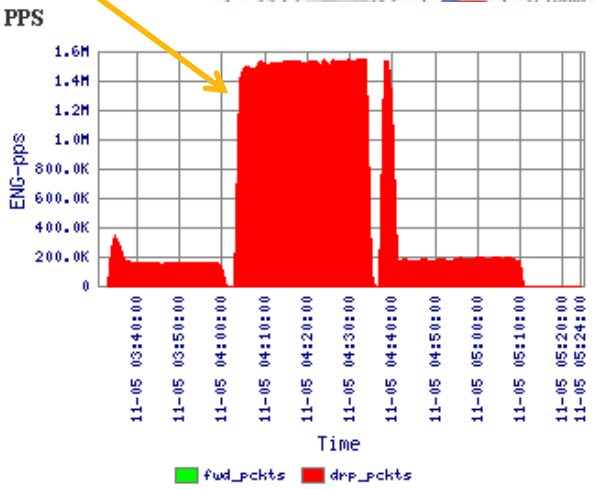
Example for a complex

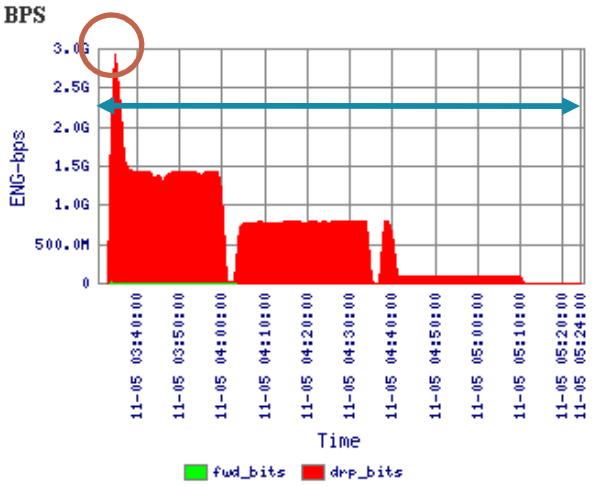
Policy	00_TAS_IPTel
Severity	MEDIUM
Attack Type	big traffic
Start Time	2010-11-05 12:31:00+9.0
Stop Time	2010-11-05 12:34:00+9.0
Duration	00:03:00
Status	Finished
Traffic Volume	851,418,664 bps
Direction	In
Src Address *	218.83.[redacted]32 200.69[redacted]32 218.83.[redacted]32
Dst Address *	203.81[redacted]32
Protocol	udp
TCP Flag	NULL
Src Port *	udp 1153 udp 58153 udp 58884
Dst Port *	udp 1024 udp 6502 udp 6308

Src Address

Address	Traffic Volume		Avg		Max		Cur	
	bytes	packets	bps	pps	bps	pps	bps	pps
218.83[redacted]/32	31.56M	30.00K	526.00K	62.50	4.21M	500.00	0.00	0.00
200.69[redacted]/32	31.56M	30.00K	526.00K	62.50	4.21M	500.00	0.00	0.00
218.83[redacted]/32	31.56M	30.00K	526.00K	62.50	4.21M	500.00	0.00	0.00
218.83[redacted]/32	31.56M	30.00K	526.00K	62.50	4.21M	500.00	0.00	0.00
218.83[redacted]/32	31.56M	30.00K	526.00K	62.50	4.21M	500.00	0.00	0.00
218.83[redacted]/32	21.04M	20.00K	350.67K	41.67	2.81M	333.33	0.00	0.00
218.83[redacted]/32	21.04M	20.00K	350.67K	41.67	2.81M	333.33	0.00	0.00
195.56[redacted]/32	21.04M	20.00K	350.67K	41.67	2.81M	333.33	0.00	0.00
218.83[redacted]/32	21.04M	20.00K	350.67K	41.67	2.81M	333.33	0.00	0.00
218.83[redacted]/32	21.04M	20.00K	350.67K	41.67	2.81M	333.33	0.00	0.00

dropped packets





Mitigation result

- Very small UDP attack came from multi source
- Attack pattern changed inside one attack
- This attack last for 01:51:22 with 2.9Gbps

まとめ

- 規模は増大
- 攻撃パターンを変えて攻めてくる

- 対策サービスは有効
  - お客様にも好評だった
  - でも、限界はある
    - チューニングしてもパターンがころころ変わると。。。。

- フィルタリング、ブラックホールも必要
- 他のお客様に影響を与えないように頑張る