実はコンテンツサーバもヤヴァい

DNSOPS.JP BoF - InternetWeek 2006

2006年12月6日

民田雅人 <minmin@jprs.co.jp>

株式会社日本レジストリサービス

DNS amplification attacks

- キャッシュサーバを使った、増幅攻撃
  - 松崎さん@IIJ - 本日のDNS DAYでのお話
- キャッシュサーバに、種となる大きなレコードを仕込んで、そのキャッシュサーバ経由で、増幅したパケットで攻撃する

種となるレコードって？

もちろんコンテンツサーバのデータ

ん？

DNSプロトコル

- 問い合わせに対して、応答を返す
- 応答パケットは、回答の情報が付加される
- つまり、応答パケットは問い合わせより大きい
  - エラーをのぞく
- キャッシュサーバを使った増幅攻撃の場合、主に、偽造したレコードが使われている
  - TXT RRを山ほど記述したもの等

コンテンツサーバ

- クラックされなくても、すでに大きなレコードが登録してあるかも…
- その性格上サービス対象を絞ることはできない
  - どこからの問い合わせに対しても応答を返さないといけない

コンテンツサーバによる増幅

domain	type	authoritative server	Q	A	Mag
dnslab.jp	any	ns.dnslab.jp	55	312	5.7
wide.ad.jp	any	ns-wide.wide.ad.jp	56	356	6.4
jprs.jp	any	ns01.jprs.co.jp	53	395	7.5
jprs.co.jp	any	ns0.jprs.co.jp	56	453	8.1
.	ns	BIND 9 with hint	45	256	5.7
.	ns	BIND 9 with hint	45	464	10.3
se	ns	a.ns.se(DNSSEC)	59	>3k	>60

サイズはIPヘッダ、UDPヘッダを含む

実は随分前から知られている話

- Denial of Service (DoS) attacks using the Domain Name System (DNS)
  - AusCERTの情報(1999年8月)
  - http://www.auscert.org.au/render.html?it=80