Feb 6/7 2007 DNS Attack Recap*
*public archival version

DNS-Operations Meeting
July 27, 2007

John Kristoff
jtk@ultradns.net
While many of us were here...
Events interpreted as...

- “According to information from experts, all 13 root servers were attacked […].”
- “Three of the world's 13 root servers […] were victims of […].”
- “The attackers targeted five of the Internet's DNS root name servers […].”
- “They did this by flooding two of the top level DNS servers with requests.”
- “At least six root servers were attacked […].”
And my personal favorite

Tech News

UltraDNS attack targeted G and L root servers (1st Update)

By Steve Ragan Feb 7, 2007, 21:40 GMT
But they were all wrong

- Four root servers (F, G, L and M)
- Three .info servers
- And a set no one's probably heard of
  - Fast flux DNS spammy something-or-other
Early, imperfect advice

From: John Kristoff <jtk@ultradns.net>
Date: Tue, 6 Feb 2007 12:05:50 +0000 (GMT)

[...] Protocol UDP, destination port 53. High rate senders are sending bogus DNS payloads. If you can, one thing that can help is to filter packets of size > 300 bytes. Since these should all be queries, you should not be seeing large packets destined to those addresses.

[...]
Gotta love the media
Secrets of the DoS Root Server Attack Revealed
February 7, 2007

• “Security experts say possibly millions of zombie computers were used [...]”
  • Uhm, not quite.
Web Host Industry Review
RIPE Protects Against DDoS Attack
February 8, 2007

• “[...] it was able to prevent overnight attempts to disrupt global computer traffic thanks to its managed K-root server.”
  • Hehe, K-Root wasn't even attacked
Network World
Defending Against Global Information War
February 7, 2007

• “More than likely the Chinese government, engaged in a form of Class III Information Warfare [...]”

• Pffftttt... *plonk*
Korea Times
Korea Becomes Haven for Hackers
February 19, 2007

• “We learned a host server in Coburg, Germany ordered a flurry of Korean computers to stage DOS assaults on the root servers,” said Lee Doo-won, a director at the ministry.

  • Germany: Sprechen sie WTF?!?!
Accurate story hard to find

- Even the ICANN “fact sheet” was imprecise on:
  - Who exactly got hit
  - The attack duration and start/stop times
  - The packet-level details

- [http://www.icann.org/announcements/announcement-08mar07.htm](http://www.icann.org/announcements/announcement-08mar07.htm)
Here is what we now know
The Botnet

• About 4500-5000 bots on Microsoft Windows boxes
• About 65% from South Korea
• About 19% from the United States
• About 3.5% from Canada
• About 2.5% from China
• The rest from various places
• Note: these are bot numbers, bps distribution differs
The Controller

- HTTP-based, located in the USA
- Bots located it via DNS (there was a backup name)
- Was still doing DDoS attacks up until late May
The Attack Profile

- Bot performed one DNS query per victim
- Set up three “threads” per victim
- Unique, but stable source port per thread
- Each thread had it's own 1023-byte payload “seed”
- UDP packets blasted to each victim on port 53
- Source addresses not spoofed
- Each UDP packet of random 0-1023 seed payload
- Each thread set to last for 24 hours
Filtering and mitigation

• Packet filter by source, but a bit unwieldy
• Packet size filter > 300-512 bytes helped some
• Better regex possible if gear can handle it
• TCP switch-over gear
Motivation

• I really don't know, I can only speculate
• Probably a test of strength or a demonstration?
• Other targets this botnet later hit may provide clues
  • Almost all .ru hosts
And finally...

- People pay more attention when it's the root servers
- Anycast helps a great deal
- The so-called experts rarely are, they're not involved
- Kudos to F-Root for making data available to OARC