Feb 6/7 2007 DNS Attack Recap

NANOG 40 nsp-security BoF

John Kristoff
jtk@ultradns.net
Previously on NANOG...
This was 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

- F-Root, G-Root, L-Root and M-Root
- A9.INFO.AFILIAS-NST.info
- B9.INFO.AFILIAS-NST.ORG
- C9.INFO-AFILIAS-NST.info
- And a set no one's probably heard of...
  - ns[2-5].opihhkj.com
  - And I suspect ns1.opihhkj.com, but I'm not sure
  - 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 being seeing large packets destined to those addresses.

[...]
Gotta love the media
“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 [...]”

• Pfffttt... *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
Here is what I found out
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 Dallas, TX, USA
- Bots located it via DNS (there was a backup name)
- Russian-affiliated reseller
- Was still doing DDoS attacks up until 2007-05-23
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 its 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
- If available, could have done something like this:
  - 10:2 dns flags
  - 12:2 qdcount
  - 14:2 ancount
- Packet size filter > 300-512 bytes helped some
- 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:
  
  – 1kalyan.ru, 85.249.132.19,
    allpills.net, brute.ru, calyan.ru,
    clubaccord.ru, generic365.com, irr.ru,
    kalian-shop.narod.ru, kalyan-optom.ru,
    kalyan4you.ru, kuban.ru, mdfc.info,
    ohvatim.ru, vkontakte.ru, wmirk.ru,
    www.1kalyan.ru, www.allpills.net,
    www.analisi.ru, www.calyan.ru,
    www.irr.ru, www.kalyanopt.ru,
And finally...

- People pay more attention when it's the root servers
- A well-formed attack would have made it worse
- This was not that bad
- Anycast helps (and peer with your DNS providers :-)"
- The so-called experts rarely are, they're not involved
- F-Root data available through OARC invaluable
- Looking for more pro-active ops people in the "@home" ISPs and Asia-Pac region, wanna t-shirt?