RIPE-46 BoF: NSP-SEC

Hank Nussbacher
hank@mail.iucc.ac.il

RIPE46
Amsterdam, Sept 2, 2003

2002 – The Real Security Problem

- Sept 2002 – ISP/NSP Operations Security engineers could not:
  - Find their security colleagues at directly connected peers
  - Find security engineers at providers 2 hops away
  - Find any security engineers at big Asia providers
- No way to work together when under distributed attacks
- Sept 2003: security engineers now work together to mitigate attacks

NSP-SEC

- NSP-SEC – Closed security operations alias for engineers actively working with NSPs/ISPs to mitigate security incidents
- Multiple layers of sanity checking the applicability and trust levels of individuals
- Not meant to be perfect – just better than what we had before
- http://puck.nether.net/mailman/listinfo/nsp-security

NSP-SEC Membership requirements

“Membership in nsp-sec is restricted to those actively involved in mitigation of NSP Security incidents.Therefore, it will be limited to operators, vendors, researchers, and people in the FIRST community working to stop NSP Security incidents.That means no press and (hopefully) none of the "bad guys.“”

NSP-SEC membership requirements

- Being a “security guru” does not qualify
- Being from a “government” does not qualify
- You need to be someone who *touches* a router in the ISP backbone
- No lurkers – if you don’t contribute you will be removed

NSP-SEC: Daily DDOS Mitigation Work

I've been working an attack against XXX.YY.236.66/32 and XXX.YY.236.69/32. We're seeing traffic come from <ISP-A>, <ISP-B>, <IXP-East/West> and others.

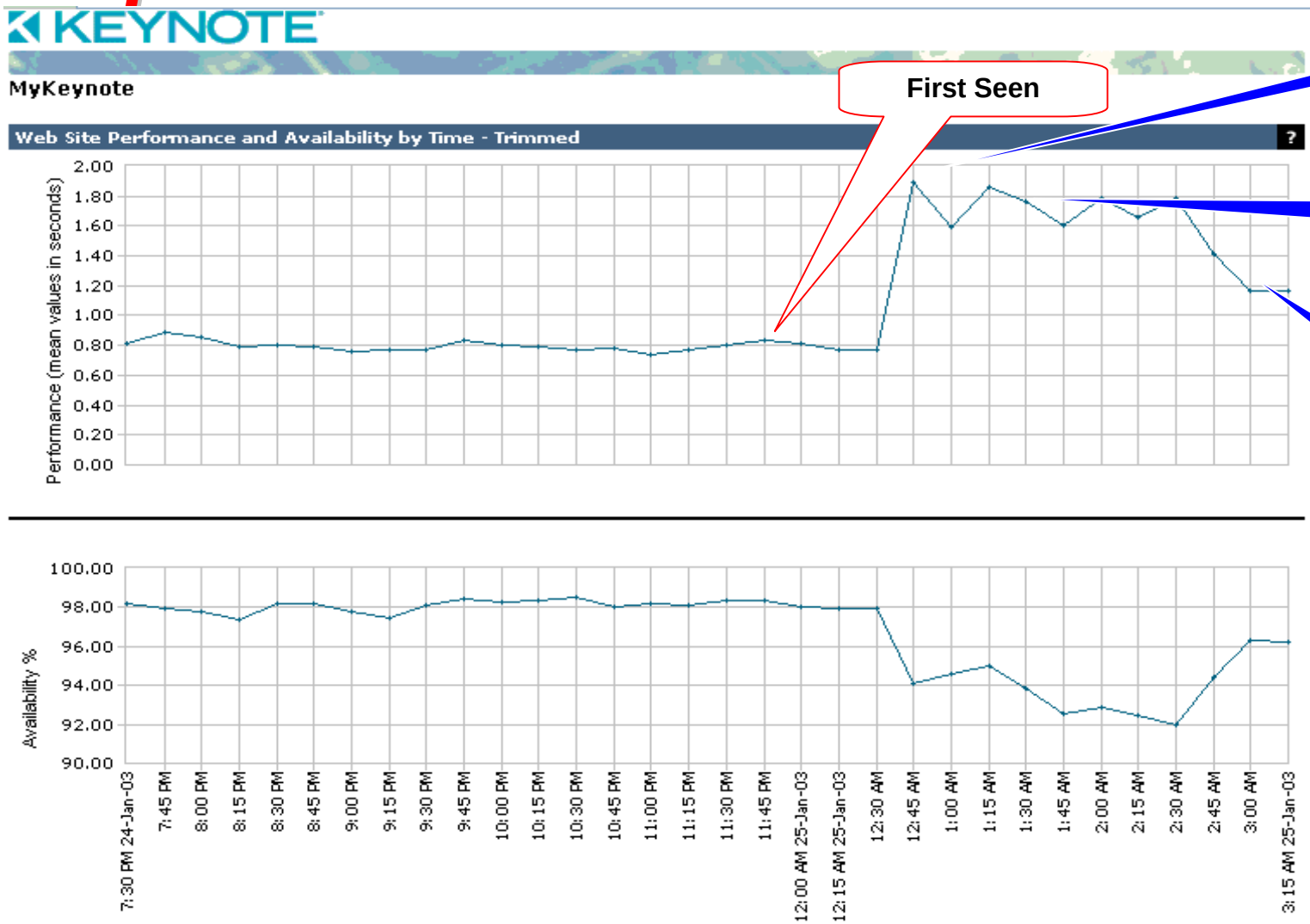
Attack is hitting both IP's on tcp 53 and sourced with x.y.0.0.

I've got it filtered so it's not a big problem, but if anyone is around I'd appreciate it if you could filter/trace on your network. I'll be up for a while :/

NSP-SEC's Role during Slammer

- The ISPs were the first to notice something was happening
  - Circuits saturated, routers spiking, BGP sessions flapped, and customers complained.
- NSP-SEC was the first reporter of the worm.
  - CERT/FIRST teams got their alert from NSP-SEC
- NSP-SEC members were the ones who dumped the packets, analyzed the worm, characterized its spread, and came up with a way to contain the worm

Impact of NSP-SEC's Containment



First Seen

Real Impact

Containment Starts

Containment Takes Effect

4:00 a.m. PST Containment

In the Skitter Core

NSP-SEC-DISCUSS

- NSP-SEC is where the mitigation takes place
  - Very operational orientated
  - You do not learn anything, you are already expected to know
- NSP-SEC-DISCUSS is the place to learn, consult, work on new mitigation techniques, and lurk (if you want to)
  - Over 190 members
  - About 5-10 postings per day
- http://puck.nether.net/mailman/listinfo/nsp-security-discuss

What can you do to help?

- If you configure routers, are in operations, and handle ISP Security for an ASN, then apply for nsp-sec membership:
  - http://puck.nether.net/mailman/listinfo/nsp-security
- NSP-SEC is looking for 2-3 engineers from each ISP who have the authority to configure routers and handle security incidents
  - Currently about 400 members
  - About 5-10 postings per day