

ISC Services at PLIX

Paul Vixie, *President*
Internet Systems Consortium
Warsaw, March 4, 2010

About ISC

- Founded in 1993 to maintain BIND (then V4)
- Produced many RFC's to clarify/extend DNS
- Created BIND8 in 1996, BIND9 in 2000
- Operates F-root and a regional network
- Currently:
 - 39 employees in six countries
 - 45 F-root instances in ~30 countries
 - ~6M USD annual budget

ISC Services at PLIX

- Since 2009 there has been an ISC SIE relay node
- Since yesterday there has been an F-root node

F-Root Introduction

- Service context:
 - F is one of 13 servers for the DNS *root zone*
 - Was once NS.ISC.ORG before the A-M renumbering
 - Root zone is parent of all TLD's (including .PL)
- Capacity growth:
 - Was once a single Intel 486DX2 running BSD/OS
 - Then a cluster of DEC Alphas using OSPF ECMP
 - Now 45 clusters of Intel EM64T, independent BGP

F-Root Anycast

- Threat model:
 - DDoS is unpreventable but is manageable
 - Risk management means massive overprovisioning
- Delivery model:
 - Every F-Root anycast node has a local peering ASN
 - Offers IPv4 and IPv6 BGP announcements (AS3557)
- Benefits to PLIX members:
 - Shorter round trip times (faster service) every day
 - Service continuity during DDoS
 - Something to use IPv6 for

ISC Security Information Exchange

- Security generally depends on awareness
 - Internet is very large/complex
 - So, there is no general awareness
- Security vendors operate sensor networks
 - Information from these sensors is privately held
- ISC's interests and qualifications
 - Nonprofit public benefit corporation (no equity)
 - Strong in software, protocols, operations, business
 - Several key employees are from PAIX and LINX

ISC SIE Technology

- Looks like an IX: private DC for member equipment
 - But: equipment is analysis servers, not BGP routers
- We use VLAN tags like television channels
 - E.g., “the passive DNS channel”
- Worldwide network of sensors
 - Passive DNS, netflow, spam traps, link pairs, *+more*
- Based on software/protocols developed at ISC
 - NCAP was our attempt to replace PCAP (tcpdump)
 - Eventually replaced NCAP with NMSG

SIE Wins

- HTTP data from CONFICKER appears in realtime
 - (other botnets to come as we instrument sinkholes)
- Cross-correlation of passive DNS, spamtraps
 - Spam body URL can be reverse-indexed
 - So, a domain used in spam can be associated in real time with all other domains having same A or NS
 - Result: near-instantaneous SURBL entries
- SIE makes raw sensor data available to participating researchers (including academic, L.E., commercial)
 - So, new forms of analysis or correlation can be developed continuously

SIE Participation

- Sensor operators:
 - You can run our NMSG tools inside your networks
 - Passive DNS, netflow, darknet, spamtrap, etc
 - Upload that data to the relay server at PLIX
 - We will backhaul it to SIE nodes (California, Ottawa)
 - Result: more global awareness of Internet events
- Analysis:
 - Send us a server, we'll plug you in, you can develop your own methods of processing this realtime data
 - Or use our lookup tools from your own abuse desk

Conclusion

- ISC and PLIX both want to do what's best for the Internet and for the world
- We're working together today on root name service and Internet security
- Both parties are open to other kinds of cooperation in the future
- Any questions/discussion?