DNS Changer

NANOG55 - June 4, 2012
Lightning Talk

Merike Kaeo (merike@isc.org)

(Presented by Tony Tauber – ttauber@1-4-5.net)

Agenda

- What Is DNS Changer
- Takedown/Replacement of seized servers
- Are your customers infected?
- Remediation Statistics
- ISP Remediation Efforts
- What Happens July 9, 2012?
  - Court Order end date for running DNS Redirection

DNS Changer (aka 'Ghost Click')

- Installs malware on PCs and MACs, changes the DNS, and tries to reconfigure the home gateway's DNS.
- Points the DNS configurations to DNS resolvers in specific address blocks and use it for their criminal enterprise.
- Law Enforcement Details:
  - http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911



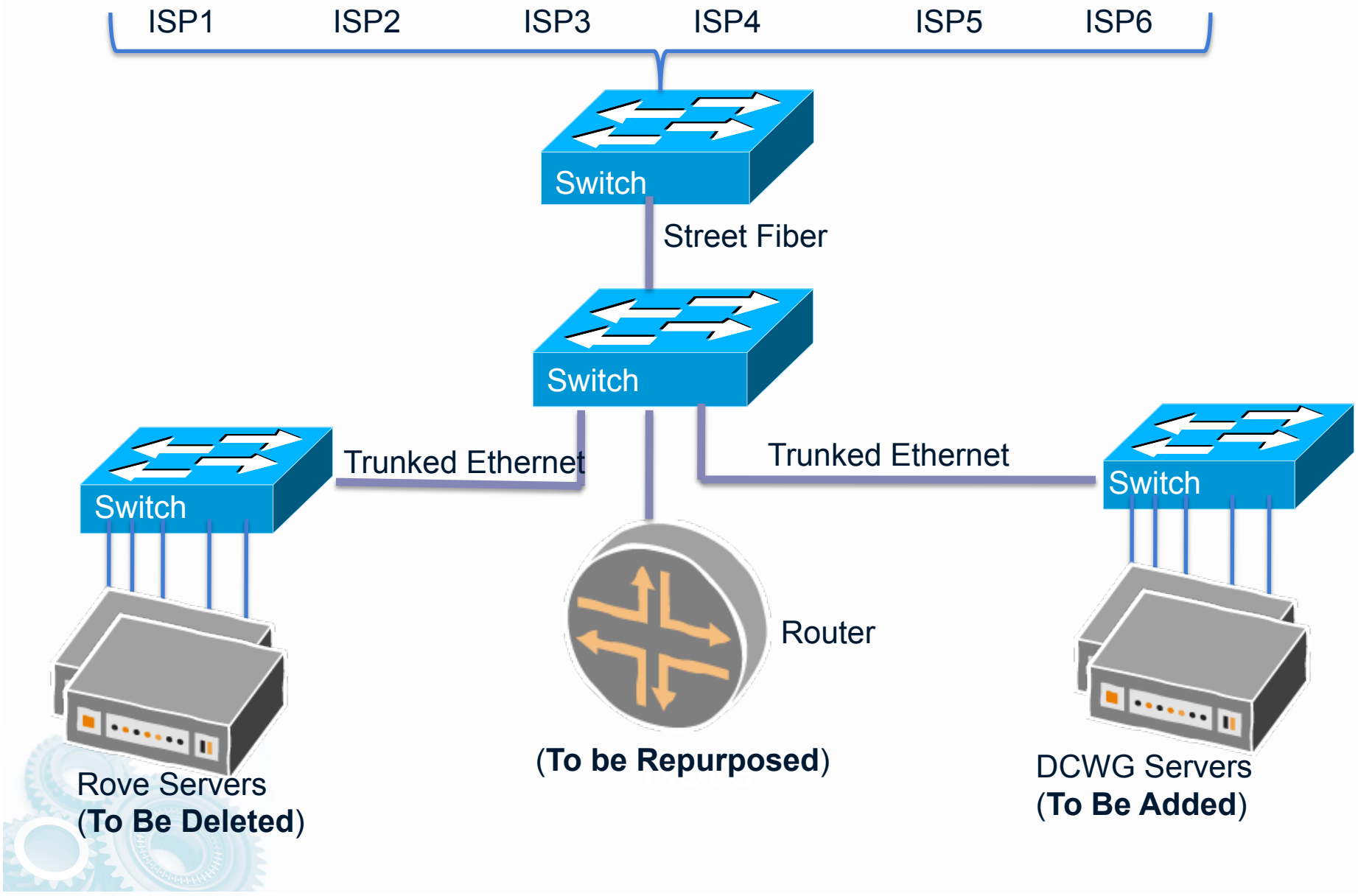
Netblocks Involved

- IP Address Blocks:
  - 85.255.112.0/20
    - (85.255.112.0 through 85.255.127.255 /20)
  - 67.210.0.0/20
    - (67.210.0.0 through 67.210.15.255)
  - 93.188.160.0/21
    - (93.188.160.0 through 93.188.167.255)
  - 77.67.83.0/24
    - (77.67.83.0 through 77.67.83.255)
  - 213.109.64.0/20
    - (213.109.64.0 through 213.109.79.255)
  - 64.28.176.0/20
    - (64.28.176.0 through 64.28.191.255)

Initial Takedown Remediation

- Trusted DNS resolvers under the control of the investigative team have replaced the criminal's DNS resolvers.
  - All users who might be infected are now going to trusted DNS resolvers.
  - Users might still be infected, but at least they are not going to rogue DNS server or having their DNS service stopped.
  - This "DNS resolver replacement" was done to prevent customer DNS from breaking and having a surge of help desk calls.
- All involved netblocks are advertised as /24s to minimize risk of hijacking by the bad guys.

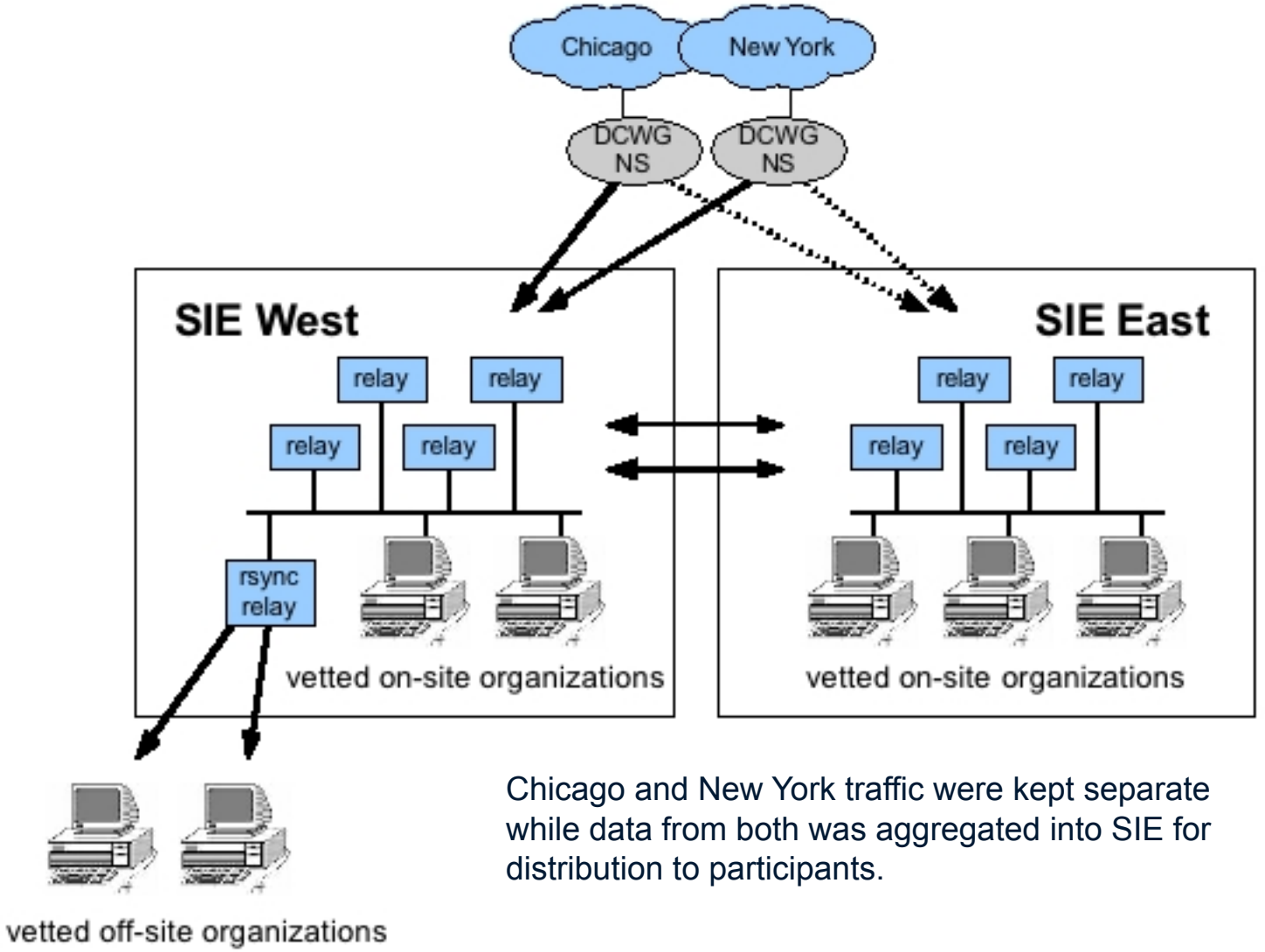
Re-routing Architecture



Remediation Information

- Logs from the trusted DNS resolvers with the SRC/DST IP addresses, ports, and time stamps are being fed to remediation groups
  - http://www.dcwg.org/cleanup.html
  - ISPs should work with these groups to get feeds to see who in their ASes are infected and help remediate.
- Main site for remediation information is at **http://dcwg.org**
  - Updated news
  - Cleanup details
  - Ongoing efforts

Remediation Architecture



Chicago and New York traffic were kept separate while data from both was aggregated into SIE for distribution to participants.

Are You Infected?

- Global 'are you infected' websites to help in local languages can be found here:
  - http://www.dcwg.org/detect/
- Clearing up some misinformation
  - No software is downloaded
  - No changes are performed on your computer
  - No scanning is done on your computer
- Beware possible "false negatives"
  - Some ISPs re-routing those prefixes internally
- Some websites and ISPs are also notifying in the browser

Tools to Clean Up Infections

- Analysis of the infected computers show that they have multiple infections with boot sector infections.
  - The infections varied over the past five years ranging from the “codex” infections (Zlob) to today’s Alureon.
- Unfortunately, this is not an easy "just use this tool to clean it up."
- The anti-malware community is working on tools.
- http://www.dcwg.org/fix/

Home Routers

- Initial analysis show the following router types might be violated:
  - UTSTARCOM routers from BNSL (India)
  - D-Link
  - Linksys
  - OpenWRT/DD-WRT
  - A-Link
  - Netgear
  - ASUS ZVMODELVZ Web Manager
  - SMC
- No evidence of "changing code," only config
- No evidence of changing the existing password.

Home Network Infections

- Service provider automatically configures DNS Servers using automated mechanisms
  OR
- Service provider provides you with DNS Server IP addresses that get statically configured

DNS Server is:
203.0.113.231

Home router automatically configures DNS Servers over wireless network

DNS Server is:
203.0.113.231

Computer
192.168.1.101

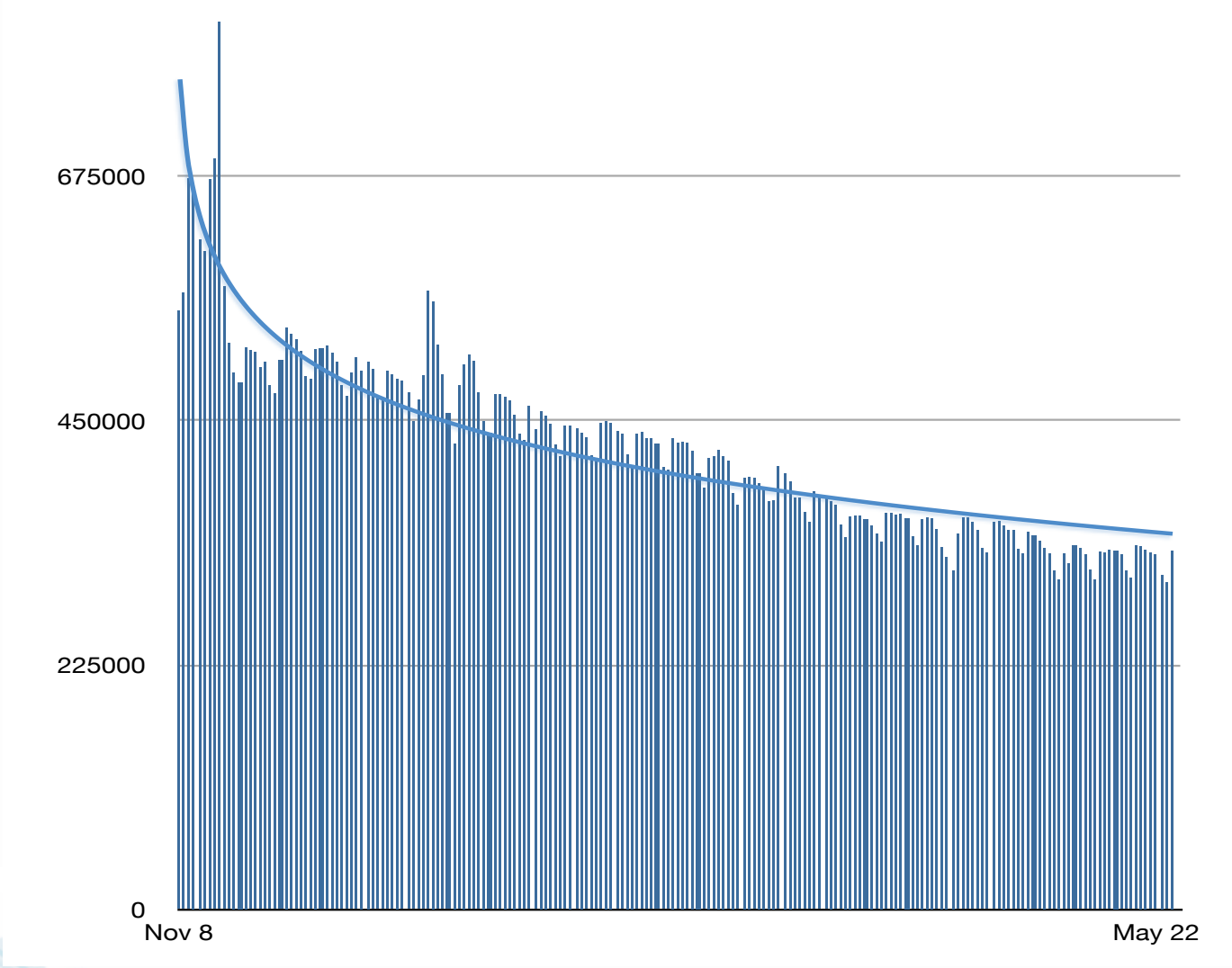
Home Router
WAN: 204.0.113.66
LAN: 192.168.1.1

DNS Server is:
203.0.113.231

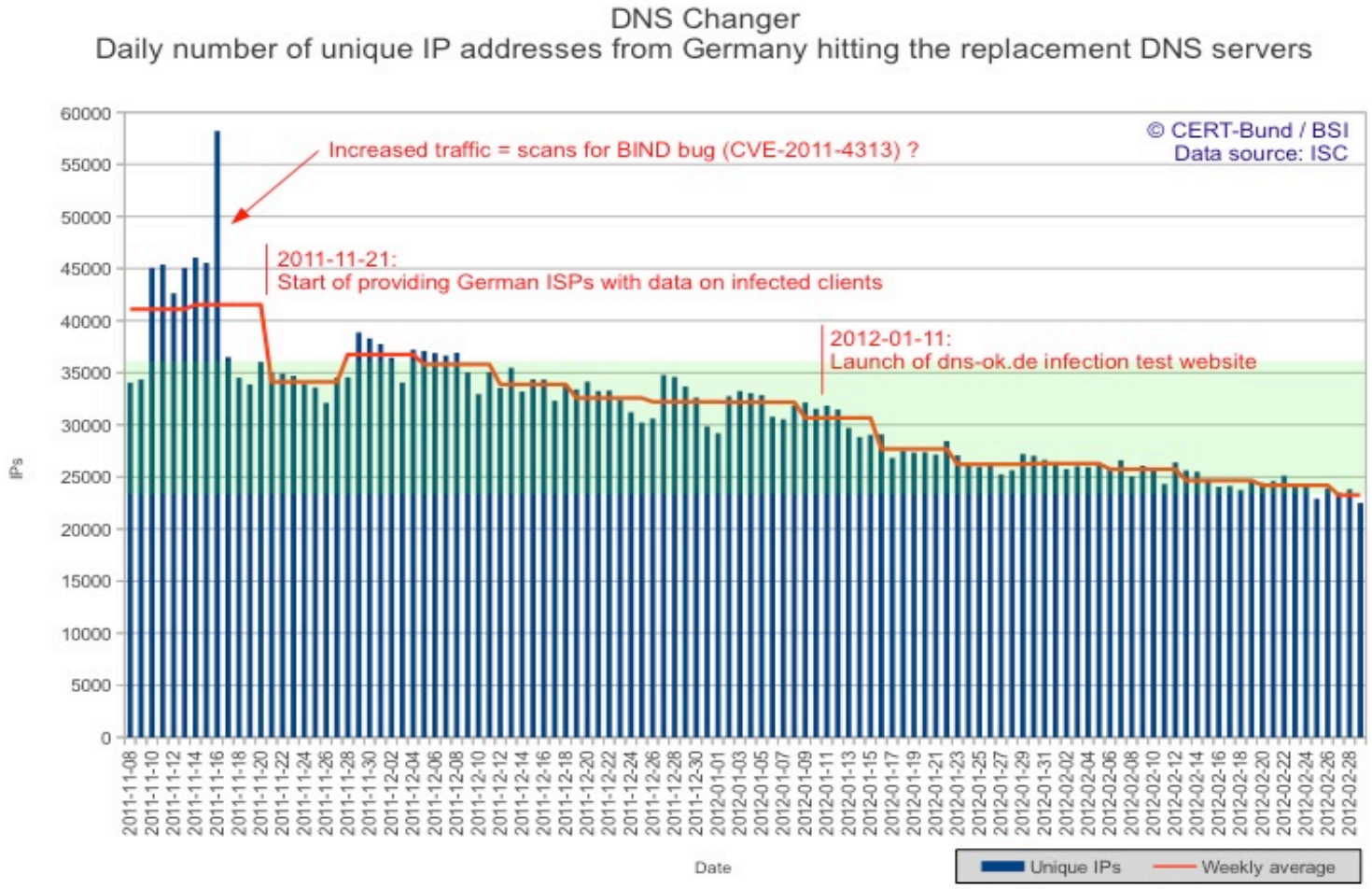
Home router automatically configures DNS Servers over wired network

Smartphone
192.168.1.102

Daily Unique Hits on Replacement Servers



Statistics for .de



Positive ISP Lessons Learned

- Some ISPs have gone through learning curve and next time the processes are in place
  - Do you have a process in place?
- Why haven't folks been doing this before?
  - No one to force issue
- Recent trends are to participate in self-regulation efforts
- Senior management type people who need to approve remediation resources are more cognizant of criticality for business
  - Reputation
  - Avoiding down time and user calls

Still To Figure Out

- What happens after the court order extension for ISC to run the trusted DNS servers?
  - The initial court order had the trusted DNS servers enabled until March 8, 2012
  - This has now been extended to July 9, 2012 to give the industry more time for effective global remediation.
- What happens to non remediated devices after this?
- What are YOUR next steps?

Whose Move Is It?

Questions