Consequences I
What was affected

David Schairer
XO Communications

Some things that didn't break

- Root server wildcards not usable for a caching server denial of service attack
- No direct impact to DNS within already-delegated .com/.net zones
- No direct impact to reverse DNS

Web Systems Impact – Missing Functionality

- Wildcard IP only handles port 80
  - No HTTPS/SSL
  - No support for other URI schemes – ftp, rtsp, etc, as well as proprietary browser extensions, or alternate ports for any service
- No support for HEAD/POST or other HTTP extensions
- These both lead to considerably less functional error handling for any request that's not a port 80 HTTP GET

Web Systems Impact – Accessibility

- Sitefinder web site only responds in English, ignoring Accept-language HTTP header
- Overrides alternate error handling for handicapped users
- Replaces more appropriate/readable error handling for handheld/ embedded/non-traditional devices

Web Systems Impact – Network Cost

- Transfer of Sitefinder page is ~17k, roughly 100x that of DNS response
- ...which equates to an average sized email transfer per hit
- End users who pay by the packet or by session time pay directly for this increase in traffic
- This can also cause more network sessions to be initiated if DNS cache is local to user
- Size is entirely dependent on future changes in Sitefinder

Web Systems Impact – Stability Risks

- Resolution of no-domain requests moves from multi-address distributed infrastructure to single-address centralized one
- There has been no open peer review on the new components as there has been on the root server architecture
- Customer experience depends on response time on this centralized infrastructure
- The Sitefinder service (wildcard address and Sitefinder servers) is extremely likely to be a denial of service attack by rogue elements

Mail Systems Impact – SMTP interactions

- Initially deployed SMTP server on wildcard IP was badly non-compliant and was replaced soon after launch
- New server speaks valid SMTP but interaction problems at the SMTP layer remain:
  - Initial EHLO negotiation limits size of messages to 10MB, which causes some senders of larger messages to bounce with a 'message too large' error rather than the more appropriate 'domain not found' error
  - Very low timeout value on client response may cause slow senders to time out and frequently retry

Mail Systems Impact – DNS/MX interactions

- MX records pointing to non-existent A records are skipped. With the wildcard, some of those records become valid and point to the Sitefinder SMTP rejector:
  - An MX configuration where the lower-priority non-existent A is available only internally via private DNS or non-DNS means
  - The case where a lower-priority A record domain expires and mail flowed unnoticed to the higher-priority server

Mail Systems Impact – Network and Operational Cost

- Increased traffic and cost for messages that bounce
- Increased operational cost for mail server farms to handle increased effort in bouncing undeliverable mail
- Any slowdown or unavailability of the wildcard SMTP rejector will cause mail to queue at all server farms, causing a chain-reaction effect on performance

Mail System Impact – Spam filtering

- Wildcard SMTP trap breaks very commonly used spam filtering rule that rejects messages with envelope sender addresses that do not resolve
  - This rule alone blocks 10%+ of inbound mail before it goes to heavier filtering logic
- Wildcard record also impacts both spammers and legitimate mailing list operators

Mail System Impact -- User Experience

- Customer server DNS error replaced by wildcard SMTP error
- Wildcard forces SMTP relays to attempt delivery, which prevents them from giving in-session errors to customer clients sending to incorrect addresses, thus changing common end-user behavior
- Common end user configuration errors in email clients can lead to clients sending messages directly to the wildcard SMTP server, which also bounces legitimate mail

DNS Systems Impact

- Breaks alarms and other monitoring that expect negative response from caching servers
- Similarly breaks some monitoring systems which alarm on domains expiring from the .com/.net roots
- Causes some tests on domain non-existence (e.g. for checks on domain availability) to fail

Impact on Other Protocols

- Wildcard IP only handles SMTP and HTTP – other protocol requests are rejected or dropped
- The bulk of Internet traffic – those not coming from an HTTP browser or an SMTP system – come from systems whose behavior with the wildcard is unpredictable
- Problems resulting from the wildcard will often be slow to be found and diagnosed
- Many of these systems are embedded applications, firmware agents, non-traditional computational platforms, or legacy applications that cannot be readily updated

Client Configurations

- Client configuration UIs that check for valid DNS on input will now fail to detect mistyped domain names and replace a useful error to the end-user with a much less useful one later on
- These later errors will often lead to frustrated users and support calls, which cannot easily be resolved over the phone when due to subtle typing errors

Conclusions

- Wildcard deployment did not cause network-shattering and readily understandable failures that would be reported in the popular media
- Instead, it caused a plethora of smaller problems affecting numerous systems, protocols, and technology areas
- These have required an ongoing cleanup effort similar in concept although smaller in scope to Y2K preparations

Conclusions

- No technology system before the Internet has been both so complex and so ubiquitous, and with so many involved components
- DNS is both central to Internet functionality and the most centralized portion of it
- The effects of the wildcard on .com/.net root illustrate the extreme sensitivity to infrastructure change
- RFC compliance alone is insufficient to judge the impact of infrastructure change – best common practices must also be evaluated