VeriSign Site Finder

Scott Hollenbeck <shollenbeck@verisign.com>
SECSAC Open Meeting
7 October 2003
Overview

- What is VeriSign Site Finder?
- Site Finder Implementation
- Technical Questions Raised
- DNS Wildcard Guidelines
- Questions?
What is VeriSign Site Finder

- Uses DNS wildcard “A” record in the .com and .net zones (specifics on next slide)

- Provides web search assistance
  - Attempts to match a requested web site with a known web site
  - Offers other search alternatives

- Provides other protocol-defined responses

- Web and mail examples:
  - http://sitefinder.verisign.com
  - http://www.bookstoore.com
  - mailto:user@bookstoore.com
What is Site Finder? DNS Perspective

Before Site Finder
> dig @a.gtld-servers.net. bookstoore.com.

; <<< DiG 8.1 <<< @a.gtld-servers.net. bookstoore.com.
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 10
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUERY SECTION:
;;;;      bookstoore.com, type = A, class = IN

;; AUTHORITY SECTION:
// More dig output...

After Site Finder
> dig @a.gtld-servers.net. bookstoore.com.

; <<< DiG 8.1 <<< @a.gtld-servers.net. bookstoore.com.
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 13
;; QUERY SECTION:
;;;;      bookstoore.com, type = A, class = IN

;;;; ANSWER SECTION:
bookstoore.com. 15M IN A 64.94.110.11
// More dig output...
Site Finder Implementation

- Service is based on considered analysis of requests
  - Provides web search assistance
  - Provides other protocol-defined responses
- Details described in a public white paper
  - http://www.verisign.com/nds/naming/sitefinder/
- Extensive testing prior to launch
- Formation of Technical Review Panel
- Ongoing monitoring program
Site Finder Protocol Connection Statistics

- 85%+ of all connection attempts are for HTTP or SMTP
- TCP reset returned for other TCP protocols
- ICMP port unreachable returned for UDP protocols
- Many different protocols make up the remaining 2.51%

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>%</th>
<th>Cumulative %</th>
</tr>
</thead>
<tbody>
<tr>
<td>80/tcp</td>
<td>HTTP</td>
<td>68.81%</td>
<td>68.81%</td>
</tr>
<tr>
<td>25/tcp</td>
<td>SMTP</td>
<td>17.06%</td>
<td>85.87%</td>
</tr>
<tr>
<td>6667/tcp</td>
<td>IRC</td>
<td>4.33%</td>
<td>90.21%</td>
</tr>
<tr>
<td>53/udp</td>
<td>DNS</td>
<td>3.25%</td>
<td>93.46%</td>
</tr>
<tr>
<td>135/tcp</td>
<td>epmap</td>
<td>1.14%</td>
<td>94.60%</td>
</tr>
<tr>
<td>110/tcp</td>
<td>pop3</td>
<td>0.56%</td>
<td>95.16%</td>
</tr>
<tr>
<td>445/tcp</td>
<td>microsoft-ds</td>
<td>0.44%</td>
<td>95.60%</td>
</tr>
<tr>
<td>137/udp</td>
<td>netbios-ns</td>
<td>0.28%</td>
<td>95.88%</td>
</tr>
<tr>
<td>139/tcp</td>
<td>netbios-ssn</td>
<td>0.26%</td>
<td>96.14%</td>
</tr>
<tr>
<td>21/tcp</td>
<td>ftp</td>
<td>0.25%</td>
<td>96.39%</td>
</tr>
<tr>
<td>3531/tcp</td>
<td>joltid</td>
<td>0.16%</td>
<td>96.55%</td>
</tr>
<tr>
<td>56498/tcp</td>
<td></td>
<td>0.15%</td>
<td>96.70%</td>
</tr>
<tr>
<td>22555/tcp</td>
<td>vocaltec-wconf</td>
<td>0.14%</td>
<td>96.84%</td>
</tr>
<tr>
<td>54510/tcp</td>
<td></td>
<td>0.14%</td>
<td>96.99%</td>
</tr>
<tr>
<td>3473/tcp</td>
<td>jaugsremotec-2</td>
<td>0.14%</td>
<td>97.12%</td>
</tr>
<tr>
<td>17027/tcp</td>
<td></td>
<td>0.13%</td>
<td>97.25%</td>
</tr>
<tr>
<td>119/tcp</td>
<td>nntp</td>
<td>0.13%</td>
<td>97.38%</td>
</tr>
<tr>
<td>8080/tcp</td>
<td>http-alt</td>
<td>0.11%</td>
<td>97.49%</td>
</tr>
</tbody>
</table>
VeriSign is listening to the issues raised by the technical community
  - IAB commentary
  - SECSAC message
  - Technical discussion venues
  - Input to VeriSign support lines

VeriSign is maintaining and updating a technical FAQ

VeriSign has prepared an extensive response to the issues raised by the IAB and SECSAC
  - http://www.verisign.com/nds/naming/sitefinder/

Will speak to a few of those issues today
Email

- Improved stub mail server to bounce messages using a non-existent domain in the recipient address

- Considering a wildcard MX record to provide a “name error” response instead of Site Finder address
  - SMTP server can be eliminated if this works well
Spam

▶ Dead RBLs
  – Dorkslayers.com – issue was resolved on 16 September

▶ Forward DNS lookup of sender domain
  – Many spam services have given up on this technique – spammers have moved on
  – Our empirical analysis shows this technique catches 3% of spam. We are looking for more empirically-based statistics
Misconfigurations

✈ Misconfiguring software with a non-existent domain name

- Used to return RCODE=3, which would provoke some terminal failure in whatever program
  - Not if the misconfiguration used a wrong, but existing domain or the non-existent domain was later registered
- It’s hard to size this issue definitively
  - MX misconfiguration is very rare in practice
    - Of more than 20 million MX records for .com and .net, less than one tenth of one percent of these records (only 0.077% to be precise) are misconfigured
Privacy

- Not collecting or retaining data per these statements
  http://sitefinder.verisign.com/privacy.jsp

Single point of failure, attack

- VeriSign has a proven track record for providing reliable, high-volume services
  - VeriSign has operated the .com and .net name servers with 100% uptime over the past six years
- VeriSign performs regular daily monitoring
- Service outage produces timeout or other error message
Anything else?

- Will be happy to take questions at end
- Questions also answered via email
  - sitefinder@verisign-grs.com
Moving forward: DNS Wildcard Guidelines

Wildcards exist in TLD zones, and we believe it is appropriate to document good technical practice

- Deployed or tested prior to Site Finder: .biz, .bz, .cc, .cn, .cx, .mp, .museum, .nu, .ph, .pw, .pd, .tk, .tv, .tw, .us, .va, .ws

- Public draft guidelines now available
  - http://www.verisign.com/nds/naming/sitefinder/
  - Guidelines describe strategies derived from extensive analysis
  - Incorporate ideas gleaned from comments received over the last year
    - IAB, CENTR, public input
  - Further work anticipated; comments welcome

- Consistent behavior would be a “Good Thing”
Questions?

► Email follow-up
  - sitefinder@verisign-grs.com