VeriSign®
The Value of Trust℠

VeriSign Site Finder

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

VeriSign®
The Value of Trust℠

Overview

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

VeriSign®
The Value of Trust℠

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...
```

VeriSign®
The Value of Trust℠

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**
  - http://www.verisign.com/nds/naming/sitefinder/trp.html
- **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%

Port	Protocol	%	Cumulative %
80/tcp	HTTP	68.81%	68.81%
25/tcp	SMTP	17.06%	85.87%
6667/tcp	IRC	4.33%	90.21%
53/udp	DNS	3.25%	93.46%
135/tcp	epmap	1.14%	94.60%
110/tcp	pop3	0.56%	95.16%
445/tcp	microsoft-ds	0.44%	95.60%
137/udp	netbios-ns	0.28%	95.88%
139/tcp	netbios-ssn	0.26%	96.14%
21/tcp	ftp	0.25%	96.39%
3531/tcp	joltid	0.16%	96.55%
56498/tcp		0.15%	96.70%
22555/tcp	vocaltec-wconf	0.14%	96.84%
54510/tcp		0.14%	96.99%
3473/tcp	jaugsremotec-2	0.14%	97.12%
17027/tcp		0.13%	97.25%
119/tcp	nntp	0.13%	97.38%
8080/tcp	http-alt	0.11%	97.49%

VeriSign® The Value of Trust℠

Technical Questions Raised

- **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**
  - http://www.verisign.com/nds/naming/sitefinder/info.html
- **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**

VeriSign®
The Value of Trust℠

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

VeriSign®
The Value of Trust℠

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

VeriSign® The Value of Trust℠

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

VeriSign®
The Value of Trust℠

Privacy

- **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

VeriSign®
The Value of Trust℠

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