VeriSign Site Finder

Mark Kosters <markk@verisign.com>
Matt Larson <mlarson@verisign.com>
NANOG
20 October 2003

Before We Begin

- **“.. verisign has not done anything strictly against spec. this is a social and business issue. ..” – Randy Bush**
  - http://www.merit.edu/mail.archives/nanog/2003-09/msg01191.html
- **Discuss the service and technical issues**
- **Other questions need to be asked in other forums**

Overview

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

What is VeriSign Site Finder

- **Used DNS wildcard “A” record in the .com and .net zones**
  - Only comes into play for nonexistent domains
  - Wildcard answer is synthesized by the server
    - Indistinguishable from a non-synthesized response
  - Matches any number of labels
  - Is RFC compliant
- **Intent is to provide a web search service**
  - Attempts to match domain name with known registered names
  - Offers other search alternatives

Precedent

- **This is not a new service**
  - Multiple TLDs have either tested or deployed wildcards since as early as 1998 (if not earlier)
  - Deployed or tested prior to Site Finder: .biz, .bz, .cc, .cn, .cx, .mp, .museum, .nu, .ph, .pw, .pd, .tk, .tv, .tw, .us, .va, .ws
  - MANY registries are interested in running this type of service
  - SECSAC – call for registries to provide data

Site Finder Implementation

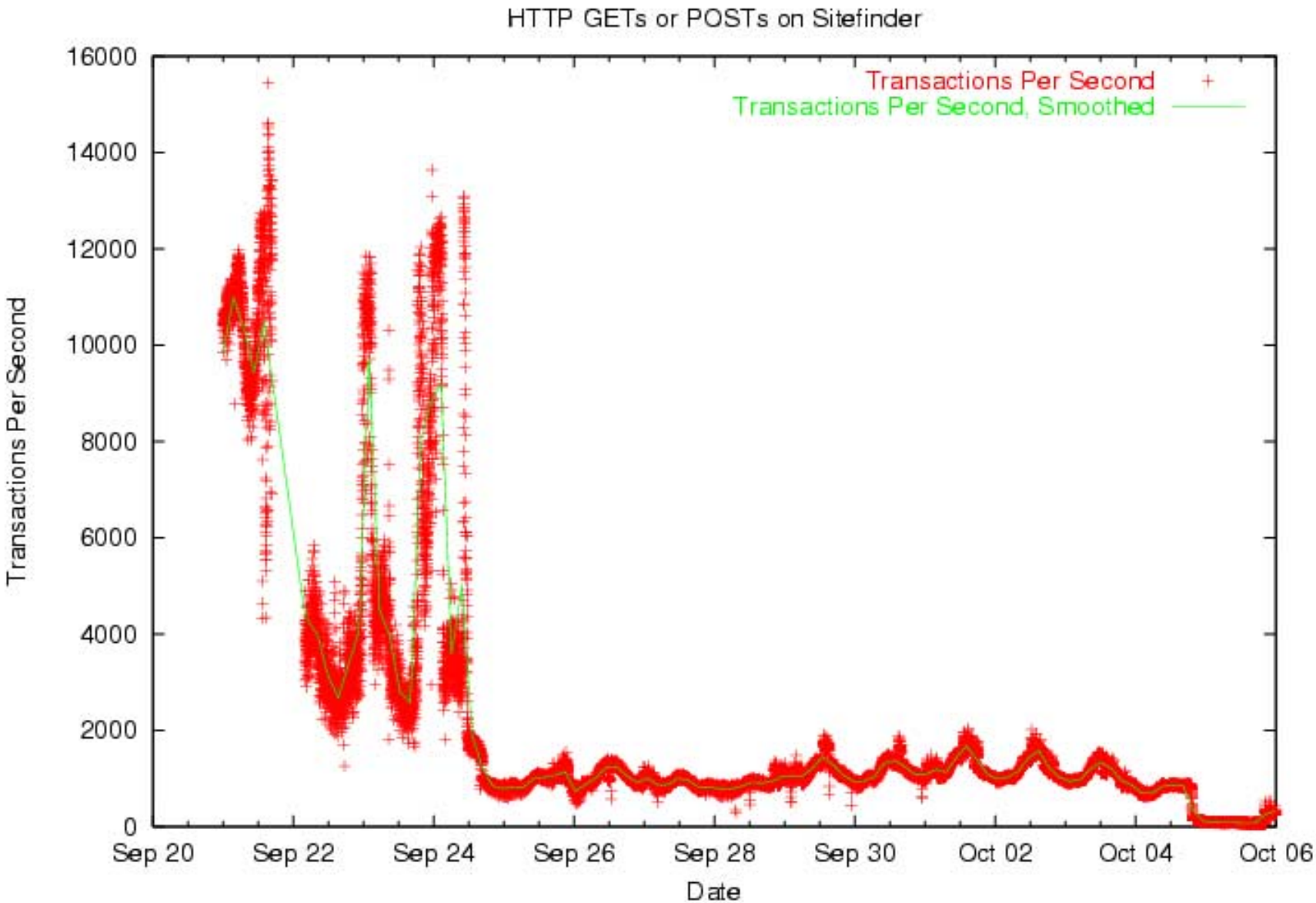
- **Details described in a public white paper**
  - http://www.verisign.com/nds/naming/sitefinder/
- **Extensive testing prior to launch**
- **Technical Review Panel**
  - http://www.verisign.com/nds/naming/sitefinder/trp.html
- **Monitoring program integral part of program**
  - DOS attacks
  - Tainted domains
    - Attack drones waiting to communicate with the mother ship
    - Originally 98.7% of all traffic on Site Finder site was HTTP
    - Did a good deal of mitigation

Site Finder Protocol Connection Statistics

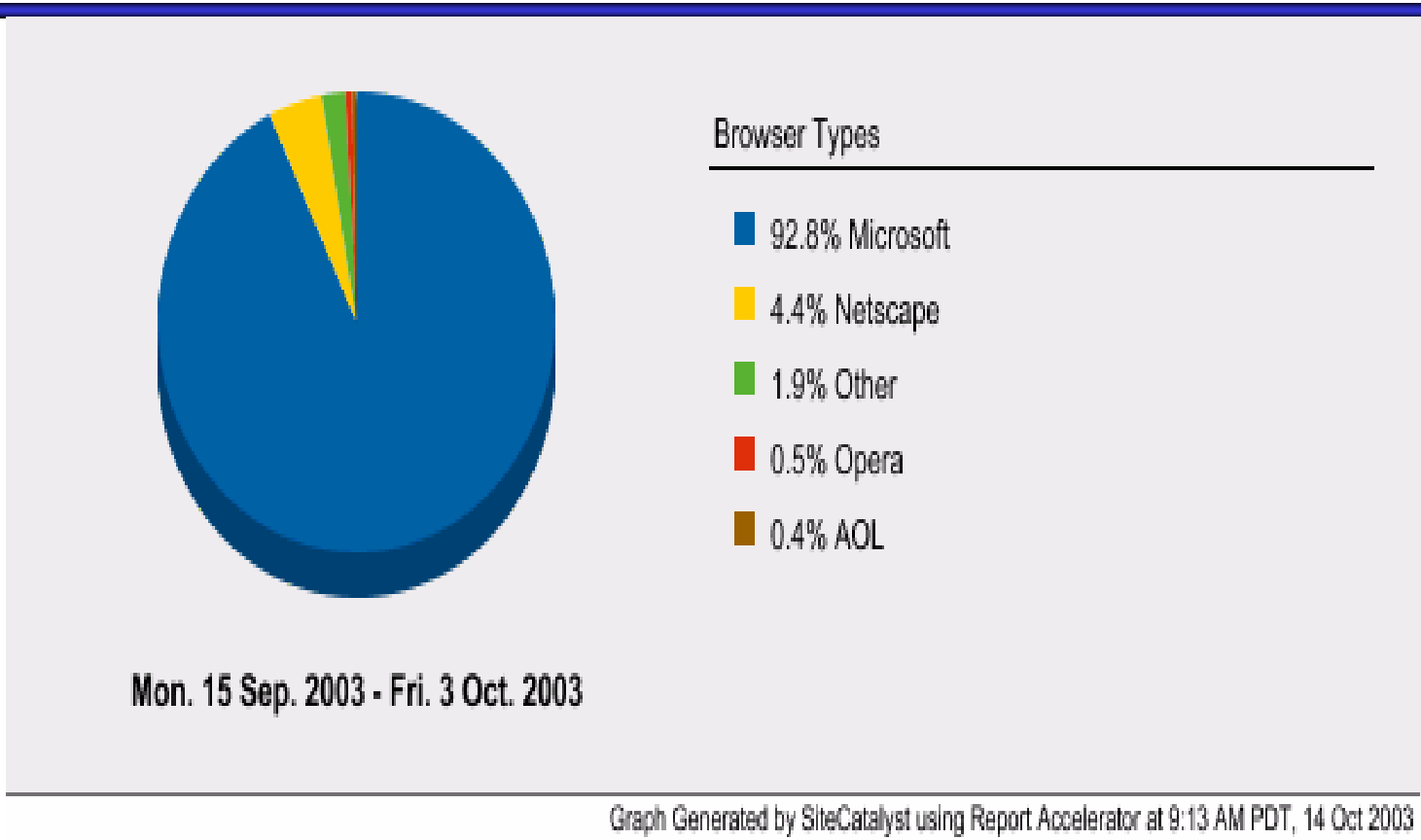
- **85%+ of all connection attempts are for HTTP or SMTP (counting SYNs on TCP only)**
- **TCP reset returned for other TCP protocols**
- **ICMP port unreachable returned for UDP protocols**
- **Many different protocols make up the remaining 2.51%**

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%

Daily Traffic at Site Finder



User Characteristics



- **Total Unique users - 90.6 M**
  - Average Unique Users/Day 6.6 M
- **Total Visits - 131.4 M**
  - Text Searches - 45.3 M
  - Did You Mean - 6.7 M

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 a response to the issues raised by the IAB and SECSAC**
  - http://www.verisign.com/nds/naming/sitefinder/
- **VeriSign technical people are active on sitefinder-tech-discuss list**
  - sitefinder-tech-discuss@lists.elistx.com

Issues Raised

- **Email**
  - SMTP bounce server was not the answer
  - Really need a wildcard MX with a nonexistent target
- **SPAM**
  - Fixed dorkslayers.com on Sept 16
  - 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

Issues Raised (cont)

- **Misconfigurations**
  - MX nonexistent target
    - Surveyed 20M com/net domains (0.077% had this issue)
    - MX's with IP addresses and invalid glue are more common errors
      - MX leading to known unroutable addresses: 6.135%
      - MX with IP address as target: 1.5%
      - MX with non-existent target: 0.077%
  - NetBIOS failover
    - Dangerous to begin with (enough said)
- **Privacy**
  - Not collecting data
    - http://sitefinder.verisign.com/privacy.jsp

Moving forward: DNS Wildcard Guidelines

- **Wildcards exist in TLD zones and we believe it is appropriate to document good technical practice**
- **Public draft guidelines 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, NANOG, public input
  - Further work anticipated; comments welcome
- **Consistent behavior would be a “Good Thing”**

Questions?

- **Email follow-up on particular Site Finder issues**
  - sitefinder@verisign-grs.com
- **Call for hard data to ICANN's Security and Stability Committee**
  - secsac-comment@icann.org
- **Technical discussion list**
  - sitefinder-tech-discuss@lists.elistx.com