

Take Immediate Action Against VeriSign Sitefinder

Lydia Leong

VeriSign now directs lookups of unregistered .com and .net domain names to its Sitefinder search portal. This change introduces a host of serious problems. Enterprises, service providers — and VeriSign — should react quickly.

NEWS ANALYSIS

Event

On 15 September 2003, VeriSign changed a fundamental behavior of the Internet. Domain Name System (DNS) lookups of unregistered .com and .net domain names now return the 64.94.110.11 IP address rather than an error message for a hostname lookup failure. VeriSign launched a free and paid-search portal, called Sitefinder, at that address. VeriSign also has an e-mail responder there.

Analysis

VeriSign intended to make the Web friendlier to users by providing more useful error messages when they tried to reach a nonexistent domain. However, DNS lookups are not specific to an application, so VeriSign could not redirect Web browsing errors without also redirecting all other .com and .net domain name errors. This change affects enterprises, service providers and consumers:

- When users are taken to Sitefinder rather than the browser's branded search page, service providers lose control of the user experience as well as a small amount of revenue.
- The "connection refused" or timed-out errors that will be returned instead of domain name errors will create network troubleshooting difficulties.
- DNS resolvers that cache negative results will experience an increased ratio of positive to negative results in the cache. The few that do not cache negative results will suffer cache pollution.
- Users may accidentally disclose sensitive information to VeriSign if URLs contain it. VeriSign believes that its privacy policy protects this data from unaggregated disclosure, but the policy doesn't state that explicitly.
- Spam filters that use domain-name lookup to detect nonexistent (forged) domains fail entirely. Errors in primary mail exchange records may cause all mail delivery to a domain to fail rather than rolling over to the secondary mail exchange.
- Sitefinder becomes a single point of failure for .com and .net lookup error messages. A compromise of the site could have widespread effects, particularly if used to spread a Visual Basic- or JavaScript-based Trojan horse.
- Potentially, this change could create a new form of domain hijacking. Enterprises may have to buy search placements on Sitefinder to protect the integrity of their brand.

Given the size and importance of the .com and .net domains, Gartner believes that VeriSign should not have made this change. To be sure, VeriSign did research all the issues first. It does not seem to have violated any laws or the rules of the Internet Corporation for Assigned Names and Numbers (ICANN), the global body that governs the Internet. The implementation complies with DNS standards, and some small top-level domains (such as .cc) also use "wildcarding." Nevertheless, VeriSign did not consult with Internet service providers (ISPs), enterprises or Internet standards bodies. The move surprised everyone and affects applications and tools that depended upon the previous behavior. Because ISPs, enterprises and software vendors will likely handle this change differently, users will experience inconsistent behaviors.

Gartner urges VeriSign to restore the Internet's previous DNS behavior for .com and .net. If VeriSign does not do so, we urge Internet governing bodies and the U.S. government, which granted the company its monopoly over the world's most important top-level domains, to pressure VeriSign.

Gartner recommends the following:

Everyone:

- Alert help desk staff, particularly about network troubleshooting issues.
- Review DNS resolver cache configurations. Check that primary message exchange records are correct and that all registered domains have a nameserver.
- Protest VeriSign's behavior to ICANN.

Enterprises:

- If you do not run your own DNS servers, notify your ISP that you support blocking the VeriSign behavior. Press the ISP to upgrade its DNS infrastructure when possible. If you do run your own DNS server, upgrade your software when a fix becomes available.
- Until the issue is fixed at the DNS server level, block traffic to 64.94.110.11 at the firewall or, if you use Border Gateway Protocol, drop traffic to AS 30060.

Service Providers:

- Consider the technical implications for your network infrastructure. Implement whatever temporary fix is appropriate, and plan out a long-term fix. Incorporate a fix into your next release of client software.

Analytical Source: Lydia Leong, Gartner Research

Recommended Reading and Related Research

- "Global Internet Offers Big Opportunities for Growth" — The most-promising growth opportunities are the new markets — new regions, new technologies, new business models and new partnerships. **By Lydia Leong**
- "Regulators Combat E-Mail Spam" — Though the legislation increases the recourse that ISPs have against spammers, it also increases the burden on legitimate businesses engaged in direct marketing. **By Lydia Leong and Ron Cowles**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509