

NT-Bugtraq: Re: DNS Hijacking: The largest single breach of privacy and security thus far online...

Re: DNS Hijacking: The largest single breach of privacy and security thus far online...

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-09/0085.html>

From: Tony (*ntBugTraq_at_ATTRON.COM*)

Date: 09/18/03

Date: Thu, 18 Sep 2003 11:02:01 -0500

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

I need to learn not to post at 4:30 in the morning... After reading my post following a few hours of rest on Monday I emailed Russ to ask that he not forward my message to the list, but apparently his trigger finger got the better of him. This obviously is not as significant as I make it out to be because the wildcards in the .net and .com zone files only causes lookups in undefined second-level zones (asYetUnregisteredAndUndefined.com) to be resolved to Verisign's 'Site Finder' service. In my testing I mistyped one of my queries for a zone that I control and received the Site Finder IP address. This led me to believe that all unsuccessful lookups beneath .com and .net were redirected to the Site Finder IP. This mistake was mine alone... and I thought that I caught it in time :)

Below is a corrected version of my post. Kindly destroy any copies of my previous post and use the electrons for a more useful purpose.

-----Original Message [Corrected]-----

Subject: DNS Hijacking: Or how to advertise for free if you own the zones...

While this probably isn't one of the most flagrant abuses of the public trust that I have seen in a long time, it does reflect a pattern of behavior that concerns me and many other members of the Internet community.

In a reckless fashion, Verisign has seized control of every non-existent domain in the .com and .net top-level zone around 12:00pm EDT on September 15, 2003. Their so-called 'Site Finder' service causes any DNS lookup for a non-existent second-level zone (commonly called a 'domain') beneath .com and .net to resolve to an IP address under Verisign's control. For instance, if you type asYetUnregisteredAndUndefined.com you will be directed to a Verisign web site without your prior knowledge or consent. It has been reported that registered domains without name server records are also subject to this redirection.

Re: DNS Hijacking: The largest single breach of privacy and security thus far online...

NT–Bugtraq: Re: DNS Hijacking: The largest single breach of privacy and security thus far online...

This hijacking of namespace was announced by mlarson@verisign.com on a public mailing list of network administrators many hours AFTER the change was implemented. There was little formal involvement of Internet standards and operational organizations before the change was made. From what I understand those few who were contacted suggested that wildcards in .net and .com was a Bad Idea(tm).

What this Means to Your Network

Every mistyped URL (that results in typing a non–registered domain), mistaken DNS query, email to a removed mail server, and other traffic is redirected to Verisign's network for their collection and use.

Your customers who mistype your web address (like www.companyy.net, assuming that company.net is unregistered) will be redirected to a Verisign web site containing content of their choosing.

Cookies for the intended domain WILL NOT be redirected to Verisign because the second–level zones will not match. Your site's cookies are not subject to this kind of hijack as I suggested in my previous post. URL query strings (and POST data in forms that point to an unregistered domain — probably unlikely) will be passed to the Verisign server. For instance, if my bank allows me to type in their URL like this to login: <http://notreallysecure.bank.com/login?user=myuser&pass=mypass> and I accidentally replace 'bank.com' with 'bankk.com' (which we will assume is unregistered) then the username and password is sent to Verisign. While this specific scenario is unlikely, a more common issue is for session data that is passed via query string to be accidentally redirected. Currently, there is no process listening on port 443 so SSL (https) URLs are not currently sent to their server.

Any application that expects a NXDOMAIN response to an invalid DNS lookup in .com and .net will no longer receive such a reply. This has been causing problems with spam filters, network analysis tools, intrusion detection systems, and other infrastructure–supporting network services that have previously functioned as expected.

The IP that is currently being used in response to all invalid queries listens on port 25 (a SMTP server called 'Snubby Mail Rejector Daemon v1.3') and appears to respond with a very similar pattern for each SMTP session. This complicates mail delivery troubleshooting and confuses some spam filtering MTAs.

New resource–exhaustion attacks on caching name servers are possible and likely. Diagnosing DNS problems has become an order of magnitude more difficult.

Non–lowest–precedence mail exchangers will not receive mail if the primary mail exchanger's address record is in an unregistered, second–level zone.

These are simply a few of the primary effects that will happen as a matter of course. There are untold new methods of abuse and misuse available to employees, contractors, and owners of Verisign's network devices (who issues SSL certificates.) Not to mention the additional 'useless traffic' generated by unintended TCP connections.

Mitigating Factors

This redirection will most likely cause a denial–of–service on the Verisign network preventing a large portion of the traffic from reaching them. [and it has, but not as significantly as I had expected]

If we act quickly and collectively we can minimize the amount of traffic misdirected from our systems.

What Can You Do?

If you reside in the US, call, email, and fax your representatives. Tell them that Verisign is no longer capable of administrating the infrastructure with which they have been entrusted. Urge them to draft a resolution to remove their authority to operate .com/.net and immediately delegate that authority to an alternate entity. This is not the first time that the public trust has been violated by Verisign and it will not be the last unless their custodial role is minimized.

[The paragraph above was a little harsh, but given their response of 'tell us what's broke and if we feel like it we'll tell you how to fix it,' they demonstrate that they have little concern for the millions of dollars that this will cost companies to modify their systems to adapt to the 'new normal.' It appears that ICANN <http://www.icann.org/> the US department of Commerce <http://www.doc.gov/> and the US Congress have jurisdiction over this matter.]

Redirect traffic for Verisign's 'Site Finder system' IP range to a server under your control and put up a web site there describing the situation. Note that there is a 15–minute timeout on the A record for the wildcard entry. This means that they can change the IP in less than 15 minutes. It is currently 64.94.110.11 which is part of a /24 (256 addresses) from an InterNAP /16 (65536 addresses.)

Encourage your upstream ISP(s) to null route traffic for these Verisign IP addresses or change the behavior of their name servers to revert to the previous non–wildcard status. Patches are available for both the Internet Software Consortium's BIND and D. J. Bernstein's djbdns software. Unfortunately, changes to the DNS system can be catastrophic for network connectivity and should be undertaken only as a last resort by experienced DNS admins. Modifying DNS server operation will most likely lead to unforeseen fallout in the future.

NT-Bugtraq: Re: DNS Hijacking: The largest single breach of privacy and security thus far online...

Resources

Concise overview of the Domain Name System:

<http://www.secondarydns.com/support/dnsprimer.html>

The Definitive Guide to DNS:

<http://www.oreilly.com/catalog/dns4/>

Verisign's Description of their 'Search System':

<http://www.verisign.com/resources/gd/sitefinder/implementation.pdf>

Slashdot discussion of this issue:

<http://slashdot.org/articles/03/09/16/0034210.shtml>

An Internet Draft from 2/03 Suggesting Clarifications to Wildcards in DNS

<http://www.ietf.org/internet-drafts/draft-lewis-dns-wildcard-clarify-00.txt>

Are You "Certifiable"? Summer's Hottest Certification Just Got HOTTER!
With a growth rate exceeding 110%, the TICSA security practitioner
certification is one of the hottest IT credentials available. And now, for
a limited time, you can save 33% off of the TICSA certification exam! To
learn more about the TICSA certification, and to register as a TICSA
candidate online, just go to
<http://www.trusecure.com/offer/s0100/>
