

## Re: DNS poisoning block list?

**Source:** <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2005-04/0147.html>

---

**From:** Newsbox (*nospam\_for\_me\_please\_at\_thanks.invalid*)

**Date:** 04/11/05

Date: Mon, 11 Apr 2005 02:47:03 -0400

On Wed, 06 Apr 2005 03:31:07 -0500, Bit Twister wrote:

> *On Wed, 06 Apr 2005 01:51:29 -0400, Newsbox wrote:*

>>

>> *So we have multiple Zero days, but my thought is to make their Zero days*

>> *shorter.*

>

> *But you were hinting it came from someone's list. They will not show up*

> *on the list until it is tooo late. Even the sans report indicated*

> *several of the posioned .coms would not allow their name to be mentioned.*

> *And it was a week before the site ip showed up because they did not*

> *want the blackhat to know they were on to them.*

I have checked lists, and as an individual user they are really so far beyond my reach for now. Give me a few days. I appreciate the suggestions that I have received and plan to follow them all, God willing. RSYNC is a whole new ball game to me.

SANS has listed info including several nameservers, and has today listed another. I know that the blackhats can put up sites and servers faster than any list can list them. But that doesn't mean that those known (mal) sites and servers are taken down in any big hurry. There's lots going on that doesn't look legit, even after info is published. Take a look at the whois for take4look.com. (YIKES!! WHY is that site still alive??!!) That site is still answering my pings 11 days after the packet captured (see reference at the bottom). And as it would seem to be a known nameserver site for DNS poisoning, I don't know why I shouldn't try to explicitly block access to it from my systems.

The "layers" that I will use for defense will include the ckip.pl script. And I see no compelling reason why those layers could not or should not explicitly ban communications to that host. Admittedly, the list might be feeble compared to the actual threat. And banning my systems' access to that host would not prevent my ISP's DNS server from being poisoned by it. But I would be really REALLY upset to be fleeced by a fake login site that I was served from a poisoning DNS server like this that I had taken the time to read about. The ckip.pl script should take care of it all, unless the DNS was poisoned with the same fake IP address when I added the

comp.os.linux.security: Re: DNS poisoning block list?

site as when I went to use it. I already talked with my ISP about this, given them details, and expressed concern. They seem to be good and competent people. How many layers do I need?

"Just because you're not paranoid doesn't mean that THEY are not out to get you."

>  
>> *I don't want them to snatch my snatch at all, but if it is 3  
>> minutes (might be more than enough for them), and if I can wait 4 minutes  
>> for some magic to work, then I can beat them. That's all that I need.*  
>  
> *Guess you type your login/id kinda slow if you need a 4 minute window  
> at some web site. :-)*

Yes, I do type slowly compared to some (faster than many!) My point was that I would gladly wait for some "magic" to work to avoid the potential cost of the security liabilities involved. :-)

>  
>> *Please tell more about your script (MUCH more!) And thanks.*  
>  
> *You can snatch a copy of ckip.pl at  
> [http://double\\_null\\_bucket.home.comcast.net/](http://double_null_bucket.home.comcast.net/) I munged it up to run on  
> windows for friends, so you will have to change the first line to  
> suit your system.*

This is the way I changed it to run on my fc2 box. (Cool!)

```
#!/usr/bin/perl
```

>  
>> *I noticed the yahoo.com anomaly myself, but didn't know how to react. It  
>> all came back into line after a while. Was this due to DNS poisoning, do  
>> you think? Was there harm done? What is your view, please?*  
>  
> *I was guessing they were in the mist of server shuffle because it has  
> been solid since, with the new/current values. I had seen other bank  
> login server ip move in and out depending on time of day.  
> I guessed a server ip toggled when the login load was high.*  
>  
> *When my browser would not launch I would keep running the script to  
> see what was going on and was doing reverse lookups to see if they  
> were matching. I still waited until the value settled down before  
> logging into the site.*  
>  
>> *What, please, are the underlying poison-unpoison mechanisms that need to  
>> be corrected to get out of all this? Asking from a single user's  
>> background.*  
>  
> *Not much us end users can do about it. Hopefully ipv6 will keep this  
> from happening in the future.*

Re: DNS poisoning block list?

comp.os.linux.security: Re: DNS poisoning block list?

>  
>> *And is there any expectation in your view that a blocklist, already  
>> established or new, could be useful in preventing requests to mal-sites?*  
>  
> *You have seen my zero day view on lists. You load a bunch of ip  
> addresses into your iptables and it is going to get dead dog slow.*  
>  
> *I hate ad and ad tracking sites. My solution to that is to add them  
> to my /etc/hosts file to block them. Very small snippet follows:*  
>  
> *127.0.0.2 aboutwebservices.com  
> 127.0.0.2 abroadsoftware.com  
> 127.0.0.2 absoluagency.com  
> 127.0.0.2 acc.adintelligence.net*  
>  
> *Host file additions will not require a iptables or network reboot to  
> take effect.*

>  
Think I can understand and respect, and share your dislike for ad and ad tracking sites. The outstanding suggestion for me here is to put the blockage into the /etc/hosts file. Not sure I'm fully alert to the implications of CPU and memory usage, but it looks like a possible plus compared to iptables rules. I run older, "memory-challenged" systems, and urgently strive to avoid "dead dog slow" responses. Maybe this is where a blocklist could and should best be employed, if ever. Thank you, I think.

> *You need to think about you automagich system change very carefully.  
> The yahoo.com is a good example.*

Sorry for the delay in response, but I am still interested in tracking this and protecting...

Today's posting has more details, here:

<http://isc.sans.org/diary.php>

The DNS poisoning issue is apparently resolved now in terms of understanding it. Deployment of protections still depends on my ISP and their upstream DNS providers. And I'm not saying they aren't doing a good job, just that I still need to be continuously vigilant to this or following issues of this type. (You know, if some creep steals my bank login, it will still be MY problem.)

I think all the responses in this thread were wonderful and great, and I appreciate all of them, even if I don't respond to each individually. Some will take longer for me to understand and implement.

I'm just an individual end user. And the support and knowledge offered by this community is outstanding. Thank you.

Thank you very much.

Re: DNS poisoning block list?

comp.os.linux.security: Re: DNS poisoning block list?

Ask me again and I'll tell you, at

newsbox/At/customers-of-adelphiaDOTorg

Thanks again! Thanks for the bandwidth.