# All your router are belong to us...

**Gary Newe, 2014-05-03**

With the recent headlines about vulnerabilities in home broadband routers, http://www.scmagazineuk.com/concerns-over-asus-and-linksys-router-vulnerabilities/article/334710/ and http://www.bbc.co.uk/news/technology-26417441 ,

I was reminded of something that happened to me.

A True Story

I was spending time with my extended family over Christmas and, as usual, we all had our heads in our phones or “i” devices. Working in IT I generally spend my holidays fixing “computer issues” for my friends and family. I won’t ever tell them my secret, turn it off trick or else I may lose my payment in beer privileges…

We were all engrossed in our online devices when my wife asked me to look at her laptop. She was reading a well-regarded news site when, all of a sudden, there were a lot of ads popping up on her screen.

As I was a few beers in at this stage I decided I would look at in the morning, assuming it was some sort of malware and nothing that a quick scan wouldn’t fix.

Imagine my surprise when the same adds started appearing on my iPad.

"Gentlemen, you had my curiosity. But now you have my attention.” (Calvin Candie: [to Django and Schultz] - Django Unchained (2012)).

What could have been causing this?  I was really intrigued. As far as I knew it was very unlikely that my iPad had been compromised like this and, because it was now happening on all devices on the home WiFi, it could only be one thing:

The Router

The router in question, which was not a Linksys or Asus, but another major vendor, was in its usual place and all the correct lights were shining. I decided to take a look and logged on.

Everything looked ok, nothing major jumped out, then I spotted an unfamiliar DNS server. I can’t actually remember what it was now but I changed it back to the “trustworthy” Google DNS of 8.8.8.8 and do you know what happened?

All the ads disappeared - they stopped popping up on all the devices. So what happened and how can you prevent it?

The most likely cause - and I say most likely because I did not spend too much time looking at it, I needed to get back to Christmas TV and my beer – is that someone, quite possibly form a generic port scan, spotted a vulnerable router and executed some remote code to update the DNS settings.

I have to admit this particular device was using the default password, so it was not much of a challenge. Changing the DNS server was a very clever ploy.  By doing this they could effectively respond with any address they wished, for any website that was being accessed from that router.

All we managed to see were ads, so they were cashing in on selling ads for some of those dodgy link sites, but they could also have acted as a proxy for all internet traffic from this router.

Imagine this: I access my bank account, unknown to me all my details are being intercepted and possibly stolen or used later to log on to my bank account.

Now what can be done? Well, there are a couple of things. Don't leave routers with default passwords and keep the software up to date.

But what about my bank or the other sites I access? Could they do anything? Well actually there is a very simple solution that can protect any brand on the internet.

A very simple tool called DNSSEC. It is the process of digitally signing a DNS request and getting a verified response back from the site you want to go to.

It relies on a chain of trust within the DNS infrastructure form the ROOT to the individual organisations, so when a user tries to find your site they can be assured that they are looking at your actual site and not being routed through a proxy.

In this case, when I accessed my bank's website, I would have requested a DNSSEC response form my bank and unless the response actually came from my bank I would have seen an error, so I would have been able to take action at that point, regardless of where the actual issue was.

The top level .uk domain has been signed since 2011 and it is relatively simple to enable on a domain. using something like F5 GTM you can transparently add DNSSEC to any DNS server without changing anything.  It is really that simple.

DNS is the forgotten security tool and can be used in your defence policy to help protect your brand online and provide an additional layer or protection to your customers and users.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

| F5 Networks, Inc. | F5 Networks | F5 Networks Ltd. | F5 Networks |
|---|---|---|---|
| Corporate Headquarters | Asia-Pacific | Europe/Middle-East/Africa | Japan K.K. |
| info@f5.com | apacinfo@f5.com | emeainfo@f5.com | f5j-info@f5.com |

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113