Vodastalk; Vodafone and Bluecoat Stalking Subscribers

June 22, 2011 by Dephormation
Filed under: News

We recently covered the StalkStalk scam, whereby TalkTalk were exposed to be covertly monitoring their customers internet use. (See earlier articles here and here).

In the course of investigating TalkTalk/Huawei, we developed some tools that allow us to analyse the behaviour of an ISP, and detect this kind of illegal online stalking behaviour.

Out of curiosity, I tested various other ISPs, to see how common this illegal practice might be.

When I tested my Vodafone dongle, I got a bit of an unwelcome surprise. I found Vodafone are disclosing the URLs their subscribers are visiting to a 3rd party (Bluecoat) in the USA, who are immediately and covertly replaying their requests.

For example, here's a log from a web server running the test tool;

> ***Date/Time:*** *2011-02-21 11:49:46 (GMT)*
> ***Remote Address:*** *212.183.xxx.xxx*
> ***Remote Host:*** *212.183.xxx.xxx* ***Vodafone UK – My Dongle***
> ***User Agent:*** *Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.1.16) Gecko/20101130* ***Firefox****/3.5.16*
> ***Request URI:*** */testurl/ <GLOBALLY UNIQUE USER ID>/index.php?personal_guid= <GLOBALLY UNIQUE USER ID>*
> ***Query String:*** *personal_guid= <GLOBALLY UNIQUE USER ID>*
> ***Referer Site:*** *http://www.myhost.com/testurl/registration.html*
>
> ---
>
> ***Date/Time:*** *2011-02-21 11:49:46 (GMT)*
> ***Remote Address:*** *199.19.249.196*
> ***Remote Host:*** *199.19.249.196* ***Bluecoat California.***
> ***User Agent:*** *Mozilla/4.0 (compatible;* ***MSIE 7.0****; Windows NT 5.1; InfoPath.1; .NET CLR 2.0.50727; .NET CLR 1.1.4322; MS-RTC LM 8; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)*
> ***Request URI:*** */testurl/ _<GLOBALLY UNIQUE USER ID>/index.php*
> ***Query String:***
> ***Referer Site:***

The dead giveaway…? I was the only person on the face of the planet who would know the URL, which incorporated a globally unique id. The page did not exist until seconds beforehand.

Another dead giveaway…? I wasn't using Internet Explorer, and would avoid it like the plague. Yet here in my logs are uninvited entries from someone using Internet Explorer.

Another giveaway…? Look at the time of the requests – identical.

In some instances, I found Bluecoat had already received copies of the pages I was requesting seconds before they had even appeared on my screen;

> ***Date/Time:*** *2011-02-21 22:06:41 (GMT)*
> ***Remote Address:*** *199.19.249.196*
> ***Remote Host:*** *199.19.249.196* ***Bluecoat California.***
> ***User Agent:*** *Mozilla/4.0 (compatible;* ***MSIE 7.0****; Windows NT 5.1; InfoPath.1; .NET CLR 2.0.50727; .NET CLR 1.1.4322; MS-RTC LM 8; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)*
> ***Request URI:*** */stalker/personal_id_4d625156a8d434.99373420/index.php*
> ***Query String:***
> ***Referer Site:***
>
> ---
>
> ***Date/Time:*** *2011-02-21 22:06:42 (GMT)*
> ***Remote Address:*** *212.183.xxx.xxx*
> ***Remote Host:*** *212.183.xxx.xxx* ***Vodafone UK.***
> ***User Agent:*** *Mozilla/5.0 (Windows; U; Windows NT 5.1; en-GB; rv:1.9.1.16) Gecko/20101130* ***Firefox****/3.5.16*
> ***Request URI:*** */stalker/personal_id_4d625156a8d434.99373420/index.php?personal_guid=personal_id_4d625156a8d434.99373420*
> ***Query String:*** *personal_guid=personal_id_4d625156a8d434.99373420*
> ***Referer Site:***

I went into a Vodafone store and asked for an explanation… the staff were as surprised as I was. I showed them the evidence.

RECENT POSTS
- One Last Protest: Avon and Somerset PCC Police Public Forum
- Why I'm Leaving the UK
- Time
- WPAD: The Internet Explorer Security Flaw that Threatens all UK Microsoft Users
- Digital Universe; Blasting the British Library into the 403 (Forbidden) Void

LINKS
- NoDPI Forum
- Leaked BT Report
- Mr Bohm – Legal Analysis
- Dr Clayton – Technical Analysis
- FIPR vs Home Office
- Mr Hanff – Covert Trials
- BadPhorm
- Cableforum – Monster Thread
- Video Petition
- Inphormation Desk

ARCHIVES
- November 2013
- October 2013
- May 2013
- April 2013
- March 2013
- February 2013
- September 2012
- August 2012
- June 2012
- May 2012
- March 2012
- February 2012
- December 2011
- November 2011
- October 2011
- August 2011
- July 2011
- June 2011
- May 2011
- March 2011
- February 2011
- November 2010
- October 2010
- September 2010
- August 2010
- June 2010
- February 2010
- January 2010
- December 2009
- November 2009
- October 2009
- September 2009
- August 2009
- July 2009
- June 2009
- May 2009
- April 2009
- March 2009
- January 2009
- December 2008
- November 2008
- October 2008
- September 2008
- August 2008
- July 2008
- June 2008
- May 2008

Looking for an explanation, I made contact with Vodafone customer services, and was told;

> *Good Afternoon Felix*
>
> *Thank you for your email.*
>
> *The Bluecoat filter you refer to classifies every internet site into one or more of over 70 categories. In order to apply the adult bar to protect our younger customers, Vodafone take these 70+ categories and rates them as either Adult of Universal. As the internet is growing at an ever increasing rate, so there are a percentage of sites not yet classified by Bluecoat as they are too new. To be on the safe side, when a user requests a site that is not classified, the Bluecoat system pulls the page requested and checks to see if there is any obvious content that would make it necessary to classify it. If it does appear adult, then the warning page is displayed. If not, it is served to the customer in the normal way. In order that we preserve customer service in terms of performance, but do not compromise safety, this is all done simultaneously.*
>
> *Vodafone do not retain any of this information. The site will be dynamically rated on each visit. If the site is a more popular one, it is added to the database and the checking process would stop occurring*
>
> *If a customer is over 18 then they can access any internet site they wish with the exception of sites dealing with child abuse images as classified by the IWF. If a customer is under 18 then where content is regarded as unsuitable we serve a warning page.*
>
> *Bluecoat does not constitute 'spyware'. It is a network operation applied to every internet request and we are required to to this in order to meet our regulatory and industry obligations.*
>
> *This is not a question of intercepting customer communications but the safety of our younger customers in a dynamic environment. Other network operators use the same or similar systems.*
>
> *I hope this information reassures you*
>
> *Kind Regards*
>
> *Lynn*
>
> *Lynn McGrath*
>
> *Customer Relations Advisor Shared Services*
>
> *Tel 08080 081 181*

I'm not reassured. Here's why.

First and foremost, I told Vodafone months beforehand I did not want my communications filtered in this way. As a web site owner, and an ordinary internet user, I don't want my communications covertly monitored or censored by my ISP (or anyone else). Particularly not someone in the USA.

Secondly, Vodafone are not entitled to monitor the content of my communications, far less disclose them to a third party oveseas, still less permit that third party to engage in a 'replay attack' against my web sites to determine the content of the web pages I've been viewing. That's simply international communications espionage.

Thirdly, while "Vodafone do not retain any of this information", Bluecoat certainly do (they process and classify the content of a private/confidential communication). Vodafone did not reveal what other data they are sharing with Bluecoat. I don't care how long it is retained; covertly disclosing it without consent from both parties is a criminal offence.

At the risk of repeating earlier blog articles, Vodafone's claims that they are are "required to to this in order to meet our regulatory and industry obligations" simply don't bear any technical, commercial or legal scrutiny. TalkTalk said almost exactly the same thing (and that was rubbish too).

To recap; the Anti-Terrorism, Crime & Security Act 2001 does not require Vodafone to gather and analyze the content of private/confidential communications. The ATCA draft code of practice states;

> *The data types here will be restricted solely to Communications Data and* ***exclude content of communication****.*
> *This will mean that storage under this code can only take place to the level of www.homeoffice.gov.uk/…….*

The ATCA draft code of practice also refers to the Data Protection Act, and states;

> *The retention of communications data is a form of personal data processing. As such,* ***it is subject to the Data Protection Act 1998.***

So what are ISPs required to retain? The EC directive 2006/24/EC requires ISPs to record data necessary to trace and identify the source of a communication (name, address, IP address), data necessary to trace and identify the destination of a communication (name, address, IP address), the internet service used, the date/time/duration of communication, and data necessary to identify users' communication equipment.

It is an urban myth that ISPs are required to record every web page URL that you visit.

The EC Data Retention Directives explicitly prohibit ISPs from recording the URLs you visit;

> ***2. No data revealing the content of the communication may be retained pursuant to this Directive.***

Yet the data gathered by Vodafone – the host name and web page address in a browser request to a web server – is the *content* of a communication, and those requests also *reveal the content of the reply* from the web server. (If they didn't reveal the content of the reply, Bluecoat's attempt to replay those requests would be completely pointless).

The data recorded under the Data Retention Directive is supposed to be held securely, protected against unlawful & unauthorised processing, and access must be restricted to authorised personnel. Not covertly disclosed to a third party overseas.

The Regulation of Investigatory Powers Act 2000 makes it an offence to intercept communications without consent from the sender and recipient (or authorisation from the Secretary of State). Vodafone are intercepting their customers communications without consent from them or the web sites that serve them.

The Fraud Act 2006 makes it an offence to obtain intellectual property using false representation. Web requests – particularly host names, paths and parameters – can be used to convey personal or group membership identifiers. By replaying these requests,

Vodafone are committing fraud… attempting to obtain intellectual property using a false representation that they are you (or a member of your group).

And for the avoidance of doubt "a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention)".

The Computer Misuse Act 1990 makes it a criminal offence to cause a computer to perform any function with intent to secure access to any program or data held in any computer without authorisation. Without authorisation, Vodafone are attempting to reuse the content of a private/confidential communication to obtain access to web servers and the data on them.

The Copyright Designs and Patents Act 1988 makes it an offence to copy intellectual property without a licence. Civil damages and criminal penalties apply for unauthorised commercial abuse of copyright protected works. Vodafone are obtaining intellectual property using illegal interception, fraudulent representations, and then processing that content to provide a commercial service. That is also a criminal offence. ISPs are allowed to copy communications for onward transmission, but they are not allowed to copy communications to enrich themselves.

There's the Privacy in Electronic Communications Regulations 2003, which require informed consent before *traffic data* is processed (traffic data is simply the IP addresses of the parties to the communication). The host names, the web page addresses, the URL parameters, are the *content* of a request message. Vodafone have been processing both traffic data *and* content data without consent.

And then there's the Data Protection Act. Making it an offence to process sensitive personal information without explicit consent of the data subject. Many of those web pages will contain sensitive personal information, such as information concerning a persons health, sexuality, political affiliations.

Sadly DPA and PECR are enforced by the UK's Information Commissioners… A hopeless bunch of incompetents (by their own admission) who claim to be under-resourced, and powerless whenever a UK telecom company abuses personal information or violates the terms of PECR.

By covertly stalking their customers, obtaining intellectual property using fraud, obtaining unauthorised access to computers and data, failing to protect retained data securely, failing to seek consent for processing… Vodafone have committed a series of criminal offences.

So. I reported Vodafone to my local Police force, Avon and Somerset, alleging illegal interception, fraud, computer misuse, and copyright theft . (I reported the BT/Phorm offences to them back in 2008, and was treated with contempt, so my expectations weren't high).

As expected my first complaint was dismissed. DC Gill told me;

> *On the evidence and information provided to me by you there appears to be potential offences committed under the Computer Misuse Act, the Fraud Act and possibly under RIPA regulations. I have not considered in detail the evidence provided but I have read all of the documents provided including copies of e mails from Vodaphone and your letter detailing the offences you feel have been committed.*
>
> *In consideration of whether it is in the Public Interest to Prosecute I am satisfied that it is not in the Public interest to prosecute this matter. In my opinion I am satisfied that even if found guilty of any offence the court would impose a nominal penalty on those found guilty. Some of the offences that could be considered for prosecution would be Summary only and as a consequence subject to a maximum fine of £5000 or a 6 months prison sentence, which in the circumstances would be unlikely.*
>
> *The circumstances of this case indicate that there has been no substantial financial loss or gain to any individual, accepting that potential the data obtained could be used for a commercial purpose.*
>
> *The offences which could have potentially been committed primarily concern the retention and disposal of Data, which in my opinion should be investigated by the Information Commissioners.*

Apparently Avon and Somerset Police believe it is not in the public interest, or even the national interest, to stop unauthorised nationwide covert communications espionage in the UK.

I hope you'll understand why I didn't bother wasting my time on the Information Commissioners. They are a lazy, incompetent, corrupt, parasitic waste of time, money, and space.

So. What next?

I've written to the CPS asking permission for a private prosecution, and received a request for evidence. If you have evidence that Vodafone/Bluecoat are monitoring your communications – as a subscriber, a web site owner, or both – please do get in touch. Send me a personal message, leave a comment below, or use my email form.

If you value the privacy, security, and integrity of your communications… use a trustworthy ISP. Do not use Vodafone, BT, Virgin, or TalkTalk.

If you're a Vodafone subscriber or web master with evidence of illegal interception by Vodafone/Bluecoat, please get in touch.

If you operate a web site serving internet users in the UK, you should be using SSL encryption for all of your communications.

Tags:

Comments

5 Comments on Vodastalk; Vodafone and Bluecoat Stalking Subscribers

1. Alan Cameron on Sat, 25th Jun 2011 10:23

   I agree with you. The evidence you present shows a prima facie case for prosecution.
   You are to be commended for your perseverence.
   Is there any avenue that you can take with the EEC?
   They have already, as I am sure you will know, condemned the UK Government for it's inaction in protecting citizens under data protection laws..

2. Ninho P. on Thu, 30th Jun 2011 20:22

   I agree too – on the principle. I live in France, and wondering whether similar (or worse) things are covertly

done by our dear ISPs. How would I go along repeating tests like you did ?
As for the Establishments – Justice, Police, Commissions… I fear prosecutions here would meet the same kind of obstacles you are facing. (I don't gather what/who exactly the CPS is in the UK. This side of the Channel, a complaint would be examined by the Procureur de la République, who has the power of "classer sans suite" – give no followings, even without providing reasons. At least you got a written explanation of why Police did not feel like prosecuting the case you submitted!)

Good luck anyway… I feel you'll need a dose of perseverance ;=) Keep us informed please

3. Mark - ISPreview UK on Thu, 7th Jul 2011 13:21

Not sure if you guys remember but we also covered this back in March and reached some similar conclusions.

http://www.ispreview.co.uk/story/2011/03/07/vodafone-uk-accused-of-stalking-their-users-mobile-broadband-internet-surfing.html

4. Tom on Fri, 22nd Jul 2011 12:37

Perhaps you can refer this to the EU – they will force the UK government to comply with privacy – they appear to take it more seriously than UK authorities. The fact that EU nationals are being spied upon is a matter they should address

5. David Earl on Tue, 31st Jul 2012 13:13

Much more seriously, the default behaviour in Internet Explorer is to transmit most URLs visited to Microsoft, who probe them some time later (for much the same reasons, though protecting their users against Phishing is their main concern I think). You can turn it off, but of course, most people don't.

I've followed up some of these in the past as I get notified when someone tries (and, because of the site security, fails) to access certain download URLs out of the context in the page in which they are offered. The Microsoft probes are via anonymous servers, and it is quite hard to discover that Microsoft is the owner of the IP address.

The moral is, if a URL is accessible, it is effectively public. If you want to protect things, use a password not just obfuscation. Even if this wasn't your ISP or browser provider, packet sniffers can obtain your URLs and you have no idea who is watching.

The UK is currently proposing a bill (see http://www.liberty-human-rights.org.uk/campaigns/no-snoopers-charter/no-snoopers-charter.php) which will require all ISPs to capture and store every URL you visit (and every email address you communicate with.