



A New Way To Track You

This is a most interesting and highly technical way to track people while they surf. I hope you all get a chance to read it and go to the test site and see if you are vulnerable. This is based on a White Paper out of Princeton U. that is [linked in the document](#). It uses your sound card as a tool to fingerprint you.

The White paper is good so check it out. Though technical in nature, most of it is readable to lay people. The paper also talks about less known methods like Canvas, WebRTC and several other lesser known methods of tracking now transpiring across millions of sites on the web. You may have never heard of these methods. You should take time out and find out more. And find some extensions or addons that block these methods. Now I have run these tests on different browsers and extensions and I find that only in Pale Moon has this new Audio tracking tool not worked. More and more I have come to respect that little browser as it is very fast (faster than FF) and has some built in security features that disallow a lot of tracking that FF refuses (that is the right word) to implement into its browser - like built in XSS support.

So what should you do? Well, first of all don't think all of this tracking is innocuous. Someone spent a lot of time, research and money to discover this new way of tracking. Why?

Because they want to track you, that's why!

This is one of those tools they were probably hoping no one would find out about. Now I can tell you that based upon some 'fingerprints' in that paper that someone in government wanted people to know about this new method. That is the good news. The bad news is that from what I gather, Google is the worst offender and the US government is all over Google.

This is one thing about Android you should all be most careful of. Google owns it and whenever you have that thing on, wherever you go, your data is going into the databases that no one can legally tell you about. No one will tell you how its being used, if its being sold to the Saudi's, Iranians, Chinese or Al Qaeda and don't laugh, unless somewhere the

law **in clear black and white forbids it**, they **will** do it. If there is a gray area in the law, they will drive a truck right through it.

This is one reason I was so disappointed when the folks at SailfishOS (Jolla) made a tablet and could only produce a few prototypes and had to stop making them. They ran into a sudden 'cash crunch' and then their suppliers started 'having problems' on them. You can read about [their ordeal here](#).

What I know is this. The US intelligence community has in the past gone after both domestic and foreign companies who threaten the NSA's and the CIA's dominance in the mobile technology market. Read that last sentence and internalize it.

When they see another player come along that threatens their dominance and their ability to track, monitor, data mine, do remote access (getting into your system reading your personal files and passwords with no warrant or probable cause), harass, set up and blackmail ordinary people, they will go after them or hire/encourage others to do it for them. Now, I fully confess, I don't know for a fact that this is what happened to the Jolla tablet. But given the Sailfish OS's difficulty in gaining a foothold in the US mobile phone market and the deep and often secret cooperation all of your mobile device makers, network providers and makers of Operating Systems have had here in the US with the NSA and the CIA, I don't think its too hard to do the math. This I know, People who use [SailfishOS](#) really, really like it. What is more the battery in some of their products is user replaceable, something that the US intelligence community **really** frowns upon. Why? I will tell you based on my experiences.

When they hacked my laptop, they had some kind of malware that scanned my Samsung Chronos HD. I could not stop it and I could not turn it off (the powerbutton was disabled by the malware). If I had a notebook with a battery that I could take out, I would have. I didn't so I couldn't. My Chronos' battery can be taken out, but it requires some serious effort tools and probably about 30 min of work the first time you try it.

Now you know why your tablets and phones don't have replaceable batteries and a hellfire missile is likely to 'accidentally' hit a factory that tries to make one.

I have long known about this vulnerability and did not want to really talk about it as I really do like to give our security the benefit of any substantial doubts I have about their tools. But since it is being abused to go after bloggers and not terrorists; the brothers and not violent neo-Nazi's, and hit out at activists and others who are trying to bring positive change to the nation - they need to be aware. Moreover the Intel community seems intent on attacking Americans rather than protecting them. So, until I see **some fundamental change**, I will from time to time, with great care talk about some of the things I discovered when the Feds turned operation 'nigger catcher' on me. I do this **ONLY** to help others who could very well come into their crosshairs to protect themselves from the skulduggery, often **illegal** skulduggery they engage in.

Someone in the US wants to kill any alternative to the two US dominant players and will do whatever it takes to make sure they keep it, including destroying someones legal, and legitimate business both here at home and overseas. Make it look like a comedy of errors so

that they would be shut down or unable to produce the offending piece of software or hardware.

The bad news is that the tablet is dead, but they do have a lot of phones about and their OS is being actively worked on. The threat to them? Some US intelligence front will go in and try and buy it up, fund it, and load it up with NSA spyware to make sure that they can do their dirt to people they want to target.

Now I am going to tell this. The Intelligence community when they were harassing me, hacked my site. They harvested my password and hacked my site. How did they do it? Filezilla the Mozilla owned FTP client was the vector. The intelligence community... I got enemies over there. A lot of them. They hate me. Some with a perfect hatred. Why? First off, I am a Christian. Second, I am Black. They don't like people in either group they cannot control. If they can find a Tom or a Judas, they'll love you. If you are a brother who really cares about fixing what's wrong in Black America and are not afraid to step on toes, *Black or White*, these guys will come after you. These guys are determined to keep what's broken in Black America as broken as possible and make sure that whatever works... gets broken. They use many of their sock puppet Black leaders to do it with

If you are Christian preaching the whole unvarnished word of God, they will come after you. They will find a legal way to do it. If you are Black they will call you a 'Violent Militant' even if you are dedicated to peace and do not or ever have owned a weapon. If you are a Christian they will call you a 'raving fundamentalist', even though you preach and live the law of love and seek peace with **ALL** men. But other activists and bloggers as well are under a very similar threat. They will come after you, sooner or later, one way or another they will 'seek and destroy' Americans who wish to bring in genuine positive change into American society. I will say this - those corporate ties between the NSA and the CIA? That is a big part of your problem. There are billions of dollars at stake in the 'people repression' business. When big business wants to take someone down or out, they [call in the hounds of hell over in the Intelligence Community](#).

Be warned.

Remember I passed on how this was [done last January](#). (excerpt follows)

I am sincerely hoping that the Intelligence Oversight Committee's will reel in the cowboy's over there at NSA and also in the CIA and put a leash on them made of tungsten steel and a whip that every time they hear it crack, they cringe in fear. Yes, I want them to be able do their jobs **when those jobs protect, rather than victimize Americans**, but to make sure that they know the boundaries, respect them and if they don't respect them, that clear and most unpleasant punishment is certain.

One thing I will pass on now is how the Intel boys got into the backend of my site and would (a few years ago) change my updates. This was **not** legal, but they did it. Let me start by saying this (I have to be careful). Mozilla has

'connections' into the intel community. I cannot say more about that but let me make that fact crystal clear.

The job of Intel people are to gather intelligence. They do that by exploiting 'grey areas' in US law (when it comes to US citizens) that allows them to or rather, they *think* allows them to do what most people assume they are prevented from doing. This is how they did it.

Yesterday morning, August 5, a Firefox user informed us that an advertisement on a news site in Russia was serving a Firefox exploit that searched for sensitive files and uploaded them to a server that appears to be in Ukraine. This morning Mozilla released [security updates](#) that fix the [vulnerability](#). All Firefox users are urged to update to Firefox 39.0.3. The fix has also been shipped in Firefox ESR 38.1.1.

The vulnerability comes from the interaction of the mechanism that enforces JavaScript context separation (the “same origin policy”) and Firefox’s PDF Viewer. Mozilla products that don’t contain the PDF Viewer, such as Firefox for Android, are not vulnerable. The vulnerability does not enable the execution of arbitrary code but the exploit was able to inject a JavaScript payload into the local file context. This allowed it to search for and upload potentially sensitive local files.

*The files it was looking for were surprisingly developer focused for an exploit launched on a general audience news site, though of course we don’t know where else the malicious ad might have been deployed. On Windows the exploit looked for subversion, s3browser, and **Filezilla** configurations files, .purple and Psi+ account information, and site configuration files from eight different popular FTP clients. On Linux the exploit goes after the usual global configuration files like **/etc/passwd**, and then in all the user directories it can access it looks for .bash_history, .mysql_history, .pgsql_history, .ssh configuration files and keys, configuration files for remina, **Filezilla**, and Psi+, text files with “pass” and “access” in the names, and any shell scripts. Mac users are not targeted by this particular exploit but would not be immune should someone create a different payload. [Update: we’ve now seen variants that do have a Mac section, looking for much the same kinds of files as on Linux.]*

The exploit leaves no trace it has been run on the local machine. If you use Firefox on Windows or Linux it would be prudent to change any passwords and keys found in the above-mentioned files if you use the associated programs. People who use ad-blocking software

may have been protected from this exploit depending on the software and specific filters being used. - Mozilla.org

Now I highlighted Filezilla for a reason. That was the FTP program I used to use. **I use it no longer.** Why not? **The same folks run both Firefox and Filezilla.** Moreover, I never liked the idea that my Filezilla password was stored in the clear - **no encryption** and no possible way to encrypt it. You can find it in the directory in the sitesettings.xml file **in plaintext.**

So when you went to certain sites (thousands of them) run by certain people who put the vulnerability in BOTH PIECES of the software to begin with (this was not an accident or oversight, despite claims to the contrary), they harvested the password to the back-end of your site. They probably did this will hundreds of thousands of bloggers and sites without their knowledge.

I know of at least one occasion for sure and I am fairly certain about a dozen times that my site was hacked in such a manner and I know who did it and why.

I just did not know *how*.

FYI, if you have one of those new 4th generation intel processors... brothers, they can [do similar things to you when your computer when it's not even connected to the internet.](#) More [here](#).

Why do I bring his up here? Because it is nearly impossible to find a good FTP client that is not somehow vulnerable to a similar hack. Some of the good older ones, well in Ubuntu, they stopped working in the latest version (Gftp). In windows... there is no such thing as anything that the Intel boys cannot hack with only a few exceptions. So what is the answer? How did this happen? Well, in the past quiet pressure is brought to bear on software makers to stop making software that they have difficulty in exploiting and using to set up and or kill bloggers and activists. This is particularly true in firewalls, antivirus makers and anything related to either security or tracking.

Why would someone want to make sure that FTP clients that bloggers use can be easily hacked?

So they can change, remove and otherwise alter stuff on their site or as I strongly suspect they tried to do with me, upload stuff on their server to entrap them. I had a lot of problems with my servers during their operation and it went down many times. But other things that pointed me to what they were trying to do made it plain **who** was behind it, but for the sake of others, I will not say more.

Yes, this is clearly and totally illegal.

With me, some were trying to upload classified material on my servers to set me up as some kind of a leaker. I have **no** classified data that has not already been leaked via

Wikileaks, released in mainstream news organizations or has been officially declassified. The only kinds of classified data I will ever post here are files officially declassified.

But upload data to my site I had never seen or had access to in order to set me up and accuse me?

Yet from what I understand, they were going to do it anyway. Those are the kinds of devils we have working in the Intelligence Community.

Simply put - activists need to get into reality and **get secure**. Real secure. If not, they will come after you and take you down. You won't even know what hit you or why when Uncle Sam hits you like a ton of bricks. Let me tell you this - A President Trump or a President Hillary are not going to protect you. Just the opposite, both are very likely to roll back any of the very tepid reforms already put in place. So keep that fact in mind.

Now.... I say the following without the slightest touch of arrogance, so take what I say here in the spirit it is given.

I know I am considerably smarter and more observant than most. Additionally I used to work in the IC and had a very, very high clearance and know how these guys operate. I had a distinct advantage that 99% of bloggers and activists don't have **and never will have**. It's not possible for them to get it. That is why I am still walking around and not observing the growth of grassroots from six feet under. I also have something most others who once worked in the IC don't have. That is courage. I will talk about these things... **carefully** but I will talk about them if the cowboys, traitors and half-wits over there **keep forgetting who they are supposed to be working for**.

But my courage comes from the fact that I know my God and he wants people **particularly Christians** to be wise as serpents in these times and that Christian's often are very naive about a lot of the harsher realities our world and nation face. They think patriotism is a shield from this kind of treatment. It isn't. It is a blindfold that keeps you from seeing the enemy approaching you with an axe, a bucket and a mop.

All three will be needed when he cuts off your head. Yes, I am using some colorful language here, but keep in mind just how the saints in the last days are appointed to die and who reigns with Christ during the millennium reign

*And I saw thrones, and they sat upon them, and judgment was given unto them:
and I saw **the souls of them that were beheaded for the witness of Jesus,**
and for the word of God, and which had not worshipped the beast, neither his image,
neither had received his mark upon their foreheads, or in their hands; and they lived and
reigned with Christ a thousand years. But the rest of the dead lived not again until the
thousand years were finished.*

This is the first resurrection.

(Rev 20:4-5, KJV)

Colorful? Yes. A bit shocking? Yes. But also biblically accurate.

Did you know how loyal Hitler's Brown-shirts were? They were the most loyal group of men Hitler had in his service.

[It did not save them](#) when their usefulness was over. Many gave the Hitler Salute and said 'Heil Hitler', just before they were executed.... by Hitler.

Let us all pause and consider these things and let Christian bloggers and others who seek love, faith righteousness and truth in Christ Jesus. Let us do our work while we can. Let us have the same mind of Christ in these matters who said...

*I must work the works of him that sent me, while it is day:
the night cometh, when no man can work.
(John 9:4, KJV)*

Beware brothers, the word National Security more and more these days is being used not to protect the nation, but to betray it. Spies and traitors **are** operating at very high levels and they know how to work the laws and system to destroy the nations security using the shield of 'National Security' to help them do it. They know the gray areas in the law so that they can betray the nation and not be prosecuted for it.

By,

Mark S. Watson

www.markswatson.com