Apple Inc denies 'backdoor' access for NSA

by staff report via lexi - AFP *Tuesday, Dec 31 2013, 10:24pm*
international / prose / post

Well, they would, wouldn't they ...

> There are billions of dollars at stake; all the major IT corporations are in damage control as a result of revelations before and after Snowden -- major telcos, essential software packages and IT integrated gadget manufacturers have provided access to US spy agencies!

But this is old news which has been sensationalised today -- the most infamous backdoor to the spy agencies was exposed in Windows OS by firewall software developers in the 90's; so what makes people think it stopped there, mass media distraction perhaps? Of course illegal and clandestine spying only accelerated since Microsoft was exposed, today various methods and inducements are used with evermore agency intimidation, 'legal' and financial inducements, zillions in 'funding' etc and other methods, 'accidents and sudden suicides' of non-compliers.

The case of AT&T physically hardware routing, at a location in California, ALL its communications directly to the NSA was widely publicised years ago, as was leaks/lists of iPhone's unique IDs and intentional 'flaws' which allowed remote access -- the list of corporate servility to spy networks is long and very compromising for the so-called independent commercial operators, particularly overt CIA partner Google, the chief offender and most pervasive data collector in the world.

However, we must first ask why the privately owned CORPORATE mass media is pushing this type of old 'news' hysteria at this time -- including Snowden, who continues to withhold compromising (according to him and Greenwald) information on the NOW PROVEN criminal US government!?

It would appear at this stage that minority ruling elites (plutocrats) are softening the public to pan-surveillance by first exaggerating claims then appearing to reduce spying -- a trick played on kids and morons.

The current reality is stark and simple, almost all MAJOR telcos and digital communications companies comply with NSA and CIA demands -- two of the most nefarious, lawless organisations on the planet. Remember, the old adage, "you are known by the company you keep," Mr Eric 'Bilderberg, Google' Schmidt!

It is perfectly safe to assume that all major IT companies are in obfuscation and deception mode as a result of recent news. BUT it's all an intentionally created storm in teacup in order to deploy another major illegality and loss of privilege on the public, have you guessed why, MORONS?

Simply because the PUBLIC is able to contain the NSA, CIA and government anytime it is of a UNIFIED MIND to do so! Well, duh, morons! You have just been REMINDED of an enduring social REALITY. But I'm sorry to pull you away from Miley Cyrus scratching her cunt, you nose-ringed, brain dead, COWARDLY SLAVES -- you deserve everything you get.

As for the elite digital underground, the more the world becomes dependent on digital technology the more powerful and freer we become -- a very pleasing reality I can assure you.

BUT YOU, THE UNSKILLED MASSES ARE ABLE, VIA SOCIAL MEANS, TO CHANGE THE STATUS QUO ANYTIME YOU WISH! But that would take a modicum of courage and social unity, so forget it! Look, Miley has stuck her moronic tongue out again, you missed it, morons!

Report from The Indian Express follows:

> **Apple Inc denies 'backdoor' NSA access to iPhones**
>
> Apple Inc said it had no "backdoor" in its products after a security researcher and a leaked document suggested the US National Security Agency had unfettered access to the iPhone.
>
> Apple said that it "has never worked with the NSA to create a backdoor in any of our products, including iPhone."
>
> The statement added that " we have been unaware of this alleged NSA program targeting our products."
>
> Security researcher Jacob Applebaum described the NSA program based on a purportedly leaked document about NSA access to the iPhone, in comments made in Germany.
>
> Apple said it "is continuously working to make our products even more secure, and we make it easy for customers to keep their software up to date with the latest advancements... and will continue to use our resources to stay ahead of malicious hackers and defend our customers from security attacks, regardless of who's behind them."
>
> Applebaum told a security conference in Germany that the program called DROPOUTJEEP allowed the NSA to intercept SMS messages, access contact lists, locate a phone using cell tower data, access voice mail or activate an iPhone's microphone and camera.
>
> He described it as "an iPhone backdoor" that allowed the NSA to access any iPhone.
>
> The documents were also described in the German newspaper Der Spiegel.
>
> Security researcher Graham Cluley said in a blog post that Applebaum's presentation and the documents show a "broader range of tools that the NSA apparently deploys against other technology companies and products, including HP (Hewlett-Packard) servers, Cisco firewalls, Huawei routers, and so on."

But Cluley said the document "does not mean that the NSA has complete control of your iPhone" because physical access to the device would be needed.

"It may be that they have since found unpatched vulnerabilities in iOS to install the spyware onto targeted devices remotely... but that's not what the leaked documents say," Cluley said.

Cluley also noted that the document dates from 2008

"Let's hope that Apple has improved its software's security since 2008. And if it's not true, we've all got a huge problem," he said.

Google chairperson, Eric 'Bilderberg' Schmidt

http://www.indianexpress.com/news/apple-inc-denies-backdoor-nsa-access-to-iphones/1214085/0
