GlobalResearch
Center for Research on Globalization

Internet Security: NSA Exploited Heartbleed Bug For YEARS, Leaving Consumers Vulnerable To Attack

By Washington's Blog

Theme: Intelligence

Global Research, April 12, 2014

Washington's Blog 11 April 2014

NSA: Making Us All Less Safe

Top computer and internet experts say that NSA spying breaks the functionality of our computers and of the Internet. It reduces functionality and reduces security by – for example – creating backdoors that malicious hackers can get through.

Remember, American and British spy agencies have *intentionally* weakened security for *many decades*. And it's getting worse and worse. For example, they plan to use automated programs to infect millions of computers.

NSA also encourages large internet companies to delay patching vulnerabilities, to allow the NSA time to exploit them. See this and this. In other words, the NSA encourages companies to allow vulnerabilities to remain unfixed.

You've heard of the scary new "Heartbleed" computer vulnerability?

The NSA has exploited it – and kept it hidden from consumers and security experts – for years. Bloomberg reports:

> The U.S. National Security Agency knew for at least two years about a flaw in the way that many websites send sensitive information, now dubbed the Heartbleed bug, and regularly used it to gather critical intelligence, two people familiar with the matter said.
>
> ***
>
> Heartbleed appears to be one of the biggest glitches in the Internet's history, a flaw in the basic security of as many as two-thirds of the world's websites.
>
> ***
>
> Putting the Heartbleed bug in its arsenal, the NSA was able to obtain passwords and other basic data that are the building blocks of the sophisticated hacking operations at the core of its mission, but at a cost. Millions of ordinary users were left vulnerable to attack from other nations' intelligence arms and criminal hackers.
>
> "It flies in the face of the agency's comments that defense comes first," said Jason Healey, director of the cyber statecraft initiative at the Atlantic Council and a former Air Force cyber officer. "They are going to be completely shredded by the computer security community for this."

Yes, they will.

The original source of this article is Washington's Blog

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Washington's Blog**

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca