GlobalResearch
Center for Research on Globalization

NSA able to Target Offline Computers using Radio-waves for Surveillance, Cyber-attacks

By RT
Global Research, January 15, 2014
RT

Region: USA
Theme: Intelligence, Police State & Civil Rights

AFP Photo

The National Security Agency has implanted software in about 100,000 computers around the world, allowing the United States to surveil those machines while creating a trail that can be used to launch cyber-attacks.

Though most of the software is installed by gaining access to computer networks, the NSA can also employ technology that enters computers and alters data without needing internet access.

The secret technology uses covert radio waves transmitted from small circuit boards and USB cards clandestinely inserted into targeted computers, The New York Times reported. The waves can then be sent to a briefcase-sized relay station intelligence agencies can set up just miles away, according to NSA documents, computer experts and US officials.

The radio frequency technology – which often needs to be physically inserted by a spy, manufacturer or unwitting user – has helped US spies access computers that global adversaries have gone to great lengths to protect from surveillance or cyber-attack.

The NSA calls use of the infiltration software and radio technology – all part of a program known as Quantum – *"active defense"* against cyber-attacks, though it has condemned use of similar software by Chinese attackers against American companies or government agencies.

"What's new here is the scale and the sophistication of the intelligence agency's ability to get into computers and networks to which no one has ever had access before," James Andrew Lewis, cyber security expert at the Center for Strategic and International Studies in Washington, told The Times. *"Some of these capabilities have been around for a while, but the combination of learning how to penetrate systems to insert software and learning how to do that using radio frequencies has given the U.S. a window it's never had before."*

Quantum targets

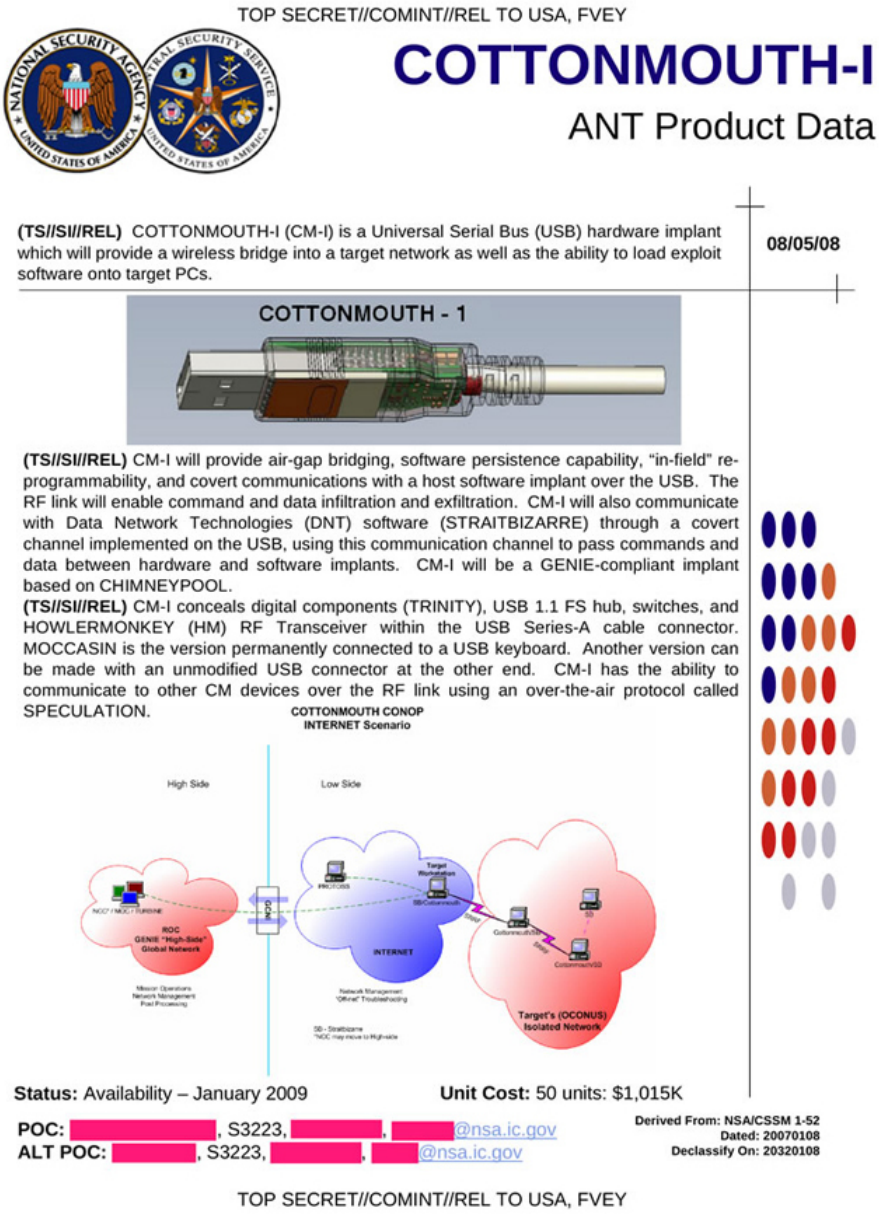
The Chinese Army has been the most frequent target of Quantum. The US has accused the Chinese Army of infiltrating American industrial and military targets to often pilfer secrets or intellectual property.

Other Quantum targets include Russian military networks, systems used by Mexican police and drug cartels, trade institutions within the European Union and even allies like Saudi Arabia, according to American officials and NSA materials that show sites that the agency calls *"computer network exploitation."*

There is no evidence that Quantum's capabilities were used in the US. While not commenting on the scope of the program, the NSA said Quantum is not comparable to actions by the Chinese.

"NSA's activities are focused and specifically deployed against — and only against — valid foreign intelligence targets in response to intelligence requirements," Vanee Vines, an agency spokeswoman, said in a statement. *"We do not use foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of — or give intelligence we collect to — U.S. companies to enhance their international competitiveness or increase their bottom line."*

Parts of Quantum were revealed by documents leaked by former NSA contractor Edward Snowden. A Dutch newspaper published a map indicating where the US had inserted spy software, usually in secret. Der Spiegel recently published the NSA's collection of hardware products used for transmitting and receiving digital signals from computers, known as ANT.



The NSA's Spy Catalog (Image from spiegel.de)

An NSA advisory panel, ordered and staffed by President Barack Obama to review NSA practices following the Snowden leaks, recommended the spy agency cease exploiting flaws in common software in the name of US surveillance. The panel also suggested the NSA stop undermining vital encryption protections.

"Holes in encryption software would be more of a risk to us than a benefit," said Richard A. Clarke, a former intel official and member of the review group. *"If we can find the vulnerability, so can others. It's more important that we protect our power grid than that we get into China's."*

President Obama is scheduled to announce Friday what portions of the panel's recommendations he is accepting. Reuters reported Tuesday that one policy suggestion from the panel received criticism from an unlikely place recently.

In a letter sent to Obama on behalf of the federal judicial system as a whole, former federal judge John Bates, the director of the Administrative Office of the US courts, warned against a

possible *"Public Interest Advocate,"* which would represent privacy and civil liberty concerns before the Foreign Intelligence Surveillance Act court. The secretive FISA court approves US government spying requests.

100,000 implants worldwide

A 2008 map, revealed in the Snowden leaks, offers 20 programs to gain access to major fiber optic cables in the US and places like Hong Kong and the Middle East. The map indicates that the US has already conducted *"more than 50,000 worldwide implants."* Though a more recent budget document said that by the end of 2013, the figure would be at around 85,000. A senior officials told The Times the figure was more like 100,000.

Officials told The Times most of the implants, by far, were for surveillance and to serve as early warning for a cyber-attack aimed at the US. One official likened them to buoys used to track submarines.

The US has targeted a Chinese Army unit thought to be responsible for most of the bigger cyber-attacks wielded against the US. Documents from Snowden's trove show the US has two data centers in China from which it can insert malware into computers.

The US maintains Quantum is not used for economic purposes, as it has complained that Chinese attacks have done.

"The argument is not working," said Peter W. Singer, co-author of a new book called *"Cybersecurity and Cyberwar." "To the Chinese, gaining economic advantage is part of national security. And the Snowden revelations have taken a lot of the pressure off"* the Chinese.

The radio-transmission technology employs many gadgets revealed by Der Spiegel in December. Among them is Cottonmouth I, a normal-looking USB plug with a small transceiver that transmits information from a computer "through a covert channel" that allows *"data infiltration and exfiltration."* Most of the revealed products are at least five years old, The Times reports, but have been updated to make the US less dependent on hardware installation in its surveillance operations.

The NSA would not discuss the devices despite publication of the documents describing them by the European news outlets.

"Continuous and selective publication of specific techniques and tools used by NSA. to pursue legitimate foreign intelligence targets is detrimental to the security of the United States and our allies," said Vines.

Meanwhile, a bipartisan group of US House lawmakers introduced legislation on Tuesday that would require President Obama to unveil budget figures for all 16 spy agencies. The secretive "black budget" for US intelligence agencies was reported to be $53 billion for fiscal year 2013, based on documents from Snowden reported by The Washington Post.

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: RT