GlobalResearch
Center for Research on Globalization

NSA Spy Agency Behind "Malware" Infection of Computer Hardware Used by "Enemies" of the U.S.?

IT Independence is National Security

By Ulson Gunnar
Global Research, March 29, 2015
New Eastern Outlook

Theme: Intelligence

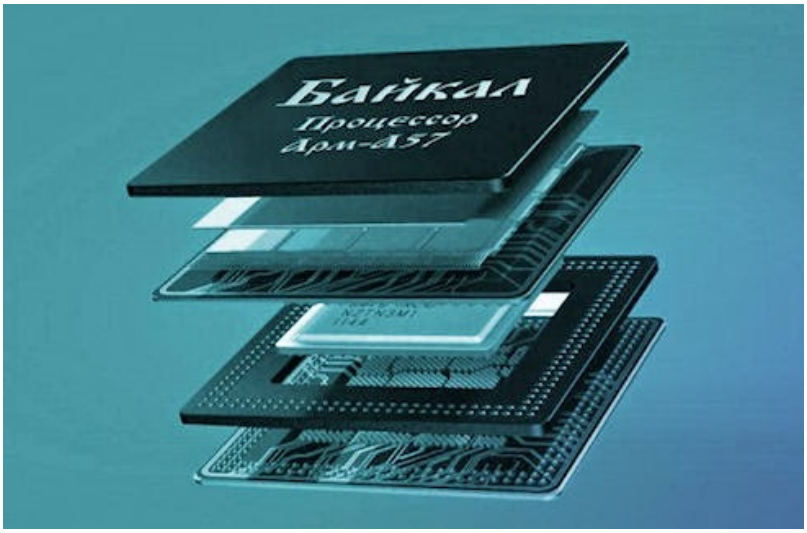
The NSA's "Equation Group" is apparently behind the infection with malware of hard drive firmware on computers used by nations considered "enemies" by the United States. The installation of the malware is believed to have required access to trade secrets of IT manufacturers as well as physical access to the soon-to-be infected computers. Popular Science in their article "The World's Most Sophisticated Malware Ever Infects Hard Drive Firmware"suggests that the NSA intercepted computers in transit through global logistical chains.

However, a simpler and more logical explanation remains, though it is one manufacturers vehemently deny; that the NSA had/has direct access to the factory floors of several IT giants. These include Western Digital Corpororation, Seagate Technology, Toshiba Corporation, IBM, Micron Technology and Samsung Electronics.

The infection of hardware starting on the factory floor is nothing new. Australia's Financial Review revealed in 2013 in an article titled, "Intel chips could let US spies inside: expert," that, *"one of Silicon Valley's most respected technology experts, Steve Blank, says he would be "surprised" if the US National Security Agency was not embedding "back doors" inside chips produced by Intel and AMD, two of the world's largest semiconductor firms, giving them the possibility to access and control machines."*

Blank made his comments after it was revealed that many processors posses potential backdoors that could allow intelligence agencies to rig a computer's encryption process, rendering it virtually useless.

Such concerns have already prompted Russia to begin requiring computers used for the government sector to include Russian-made processors. With hard drives now potentially compromised, the NSA has once again given the world a reason to boycott US tech giants and those within America's sphere of influence, and replace them with locally produced alternatives manufactured under tighter security controls.



Besides access to factory floors, several high profile "cyber attacks" attributed to China targeting US tech giants, may have been in fact the NSA itself attempting to steal source code required to rewrite hard drive firmware.

Reuters in its report "Russian researchers expose breakthrough U.S. spying program" would claim, *"concerns about access to source code flared after a series of high-profile cyberattacks on Google Inc and other U.S. companies in 2009 that were blamed on China. Investigators have said they found evidence that the hackers gained access to source code from several big U.S. tech and defense companies."*

When big US tech and defense companies aren't directly cooperating with the NSA, it appears they are pillaged regularly by them. This was also likely the case regarding Dutch SIM card manufacturer Gemalto, which was also recently compromised by the NSA and its British equivalent, GCHQ. The hijacking of the company's SIM cards required direct access to company trade secrets and likely involved the NSA and GCHQ stealing encryption keys from company servers.

The dangerous dance the NSA and industry leaders perform often makes it difficult to tell who is leading and who is following. It was during the 2011 Arab Spring uprisings that it became clear US Internet giants Google, Facebook and Twitter were directly involved with the US State Department in helping organize unrest across much of North Africa and the Middle East. Source code being raided in 2009, then turning up as the key ingredient necessary to cook up what is believed to be NSA malware in 2015, suggests every once in a while the NSA steps on its partners' toes.

IT Independence is National Security

Regardless of whether or not US tech giants are directly involved, or the hapless victims of NSA info-piracy, nations finding themselves at the receiving end of American cyber espionage have found the necessity of working toward developing their own independent IT infrastructure. Nations like Russia, China and Iran, for instance, have created their own indigenous versions of Google, Facebook and Twitter. Russia, as already mentioned, is already working on replacing hardware with locally produced equipment to mitigate the threats of tampered hardware, firmware and software imported from US tech giants and other manufacturers susceptible to NSA infiltration.

Like a ship at sea built out of a multitude of watertight compartments to stave off sinking in

the event its hull is compromised, IT infrastructure should likewise include compartmentalization. The idea of a handful of manufacturers producing the world's hard drives makes the unsavory work of organizations like the NSA easy. Decentralizing hardware manufacturing nationally, then decentralizing it even further domestically, means the NSA must compromise an increasing number of physical locations and networks online to infect the same number of machines as it has easily done by compromising a handful of locations and networks worldwide before.

Instead of water passing through a single hole in the ship's hull and sinking it, it would be required to pass through and flood dozens or more compartments. On a national scale and in terms of IT, particularly in a country like Russia, China or Iran with the considerable geographical and demographic dimensions of each, the NSA would be faced with hundreds if not thousands of targets it would have to compromise before it could achieve the same scale in spying it has previously achieved.

Each agency, department or ministry in each country could even develop its own software and hardware houses where complex and close relations make it even harder for outsiders to compromise. Nationally, security breaches could be quickly mapped, traced back to their sources and isolated in infrastructure distributed in this manner.

Ultimately, independence in technology is national security. Allowing one's nation to be dependent on outside corporate or government interests is to resign freedom and a degree of control over one's own destiny and security. The age of monopolies allows malevolent organizations to easily compromise large segments of the global population. In order to stop this, these monopolies must be replaced by a more localized and more tightly controlled infrastructure.

If a nation lacks the human resources to build this infrastructure, then national security requires such human resources to be developed, implying greater investment in technical education as well as in research and development. It appears that nations like Russia, China and Iran understand these lessons and have already begun down this road. Other nations might benefit by following suit. As the doors close on the NSA in one region of interest around the world, it will turn its attention toward others.

***Ulson Gunnar**, a New York-based geopolitical analyst and writer especially for the online magazine "New Eastern Outlook".*

Articles by: **Ulson Gunnar**