NSA, NOT CHINA, THE GLOBAL BIOS SUICIDE CYBER-BOMBER

Remember when, to fearmonger as part of 60 Minutes NSA propaganda, they warned of a Chinese attack on the US economy that, if launched, would have amounted to China acting as a suicide cyber-bomber?

The attack would have targeted computers' BIOS.

> Then there's the scary BIOS plot.
>
> I'll need to go back and review this, but the jist of the scary claim at the heart of the report is that the NSA caught China planning a BIOS plot to shut down the global economy.
>
> To.
>
> Shut.
>
> Down.
>
> The.
>
> Global.
>
> Economy.
>
> Of course, if that happened, it'd mean a goodly percentage of China's 1.3 billion people would go hungry, which would lead to unbelievable chaos in China, which would mean the collapse of the state in China, the one thing the Chinese elite want to prevent more than anything.
>
> But the NSA wants us to believe that this was actually going to happen.
>
> That China was effectively going to set off a global suicide bomb. Strap on the economy in a cyber-suicide vest and … KABOOOOOOOM!
>
> And the NSA heroically thwarted that

> attack.

The invocation of a BIOS attack was meant to provide authenticity and (for those who didn't realize how obvious this is, mystery), I think.

But I find it particularly ironic that inserting backdoors into BIOS is (or was, back in 2008) the preferred method of NSA's Access Network Technology group, which provides tools to access hardware and software.

> It also develops software for special tasks. The ANT developers have a clear preference for planting their malicious code in so-called BIOS, software located on a computer's motherboard that is the first thing to load when a computer is turned on.
>
> This has a number of valuable advantages: an infected PC or server appears to be functioning normally, so the infection remains invisible to virus protection and other security programs. And even if the hard drive of an infected computer has been completely erased and a new operating system is installed, the ANT malware can continue to function and ensures that new spyware can once again be loaded onto what is presumed to be a clean computer. The ANT developers call this "Persistence" and believe this approach has provided them with the possibility of permanent access.

Again, this is not surprising. It's just a means of doing what the NSA wants to acquire.

Still, it highlights the degree to which most fearmongering claims the NSA makes may well be projection about its own activities.

That said, given the list of companies whose products they've compromised, it may serve as a kind of suicide bomb against the tech industry:

- Juniper Networks
- Cisco
- Huawei
- Western Digital
- Seagate
- Maxtor
- Samsung

Again, that ANT tampers with Huawei products is not surprising, but it is ironic, given that we not only won't let Huawei do business in the US, but increasingly want to keep them out of our close allies' networks, all because of concerns China would require the company to insert back doors into Huawei equipment.

Maybe those back doors are really NSA's?