Written by **C. Mitchell Shaw** on March 8, 2016

McAfee: Gov't Backdoors Are Destroying National Security

As the Apple/FBI case heats up, the surveillance hawks continue to insist that backdoors into the encryption that protects smartphones are necessary to address the threat of terrorists and other dangerous criminals "going dark." But one of the most respected voices in computer security says that "solution" is more dangerous than the problem it proposes to solve.

John McAfee (shown), who is famous for the anti-virus software his company makes, wrote an article for *Business Insider* in which he says, "Software, if properly weaponized, could be far more destructive than any nuclear arsenal." The "weaponized" software to which he refers is the type of software used to penetrate systems. Backdoors fit neatly into that category.

McAfee makes the case that such software is a danger in and of itself and that it must be guarded against. The prime example he uses to illustrate his point is the Juniper Networks hack reported late last year:

> I will give an example of what happens in the real world when back doors are put into software. On December 17th of last year, Juniper Networks — a major provider of secure network systems, [whose] customers include nearly every US government agency, announced that it had discovered two "unauthorized" back doors in its systems.

Along with the announcement, Juniper made patches available to its customers to close the backdoors. McAfee says the backdoors must have been inserted by "a rogue employee in the software development department," since the code for those backdoors would have had to have been written into the firmware before the product was shipped. He wrote:

> For those of my readers who do not understand how back doors are created — they can only be created by the manufacturers of the software. There is, absolutely, no other way.
>
> So, the company had to have a rogue employee in the software development department. This much is clear.

He cites a top secret document, dated February 2011, leaked by the hacktivist group Anonymous, which "reveals that the British spy agency GCHQ, with the knowledge and apparent cooperation of the NSA, acquired the capability to covertly exploit security vulnerabilities in 13 different models of firewalls made by Juniper Networks."

Remember that the only way for the backdoors to have been inserted into the firmware of the systems is for it to have been written into the code by what McAfee called a "rogue employee." So, who put that

employee up to helping the NSA and GCHQ hack Juniper's hardware? The natural — if not only — conclusion is that the employee was an agent of the NSA. McAfee wrote:

> I hope we all understand now what "acquired the capability" means. The NSA planted a programmer within Juniper Networks. There was no other way to "acquire" this capability.
>
> Nothing new in this. Black hat hackers have been planting themselves in target agencies for years. It was just such a plant that brought down Ashley Madison last year. So it's no surprise that the NSA uses this technique as well.

And, lest that seem like wild conjecture, he cites a *Wired* article dated December 2015 which says:

> But what makes the Juniper backdoor even more interesting and notable is the fact that it appears to be based on another backdoor the NSA allegedly created years ago in the Dual_EC algorithm for its own secret use.

The NSA's reasons for wanting the backdoor are obvious: About 30 percent of the security systems created by Juniper are sold into Europe, the Middle East, and Africa and about 20 percent are sold into Asia. Many of the nations and organizations that are considered enemies of the United States wind up using Juniper's products. As McAfee wrote:

> So, in 2011 the NSA surreptitiously got their back door into a powerful piece of security software used by many enemies of the US. They could now monitor these enemies easily.

What the surveillance hawks apparently overlooked in their anxious enthusiasm is that the other 50 percent of Juniper's customers are in the United States — and the majority of those customers are government agencies. So, by creating a backdoor to spy on our enemies, we opened a backdoor into many of our own systems. And our enemies noticed. As McAfee pointed out in his article:

> The Internet underground knew of these back doors within weeks of their release, and so did the Chinese, and so did the Russians. An so did every hacker on the planet. Monitoring changes within major software systems is the simplest of all things. Every hacker toolkit contains a compare program that will outline all changes made to a piece of software by the manufacturer. Disassembly tools tell the hacker what each change does.

As a direct result of the NSA and GCHQ installing backdoors into Juniper's products, U.S. government agencies became the victims of the very surveillance tools that were intended to be used to spy on our enemies. The largest hack in U.S. history — the penetration of secured systems within the Office of Personnel Management (OPM) — is the direct result of those NSA backdoors.

As McAfee explains:

> Last year alone, the Defense Department was hacked. Using the NSA's back door the Chinese walked off with 5.6 million fingerprints of critical personnel. The same back door was used to hack the Treasury Department on May 27th of last year in which millions of tax returns were stolen. And again, our most devastating hack as a nation was the Office of Personnel Management hack, in which 22 million sensitive files were stolen. The Chinese gained access through the Defense Department's Juniper Systems and then using inter-operability with the Personnel Office, took what they wanted. Again, courtesy of the NSA's back door.

So, by creating backdoors, the NSA (and its British cousin, GCHQ) have given our enemies the keys to our most sensitive systems in the name of "protecting America." And yet the surveillance hawks continue to demand even more backdoors as the best — if not only — way to keep us safe. They

continue to promise security if Americans will give up more privacy. The data shows that their policies will continue to cost us the latter without delivering the former.

The heads of the intelligence organizations and the politicians who serve on the congressional committees tasked with holding those agencies responsible are surely aware of the damage backdoors have already caused and will certainly continue to cause. It appears that rather than protecting America's interests, the surveillance hawks have their own agenda. And it has been succeeding.

Photo of John McAfee: AP Images