GlobalResearch
Center for Research on Globalization

America and Israel Created a Monster Computer Virus Threatening Nuclear Reactors Worldwide

By Washington's Blog
Global Research, November 12, 2013
Washington's Blog

Even Threatens the International Space Station

In their obsession to stop Iran from developing nuclear weapons, the U.S. and Israel created a computer virus (called "Stuxnet") to take out Iran's nuclear reactors.

The virus appears to have spread to other countries.

One of the world's top computer security experts – Eugene Kaspersky – said this week that the virus has attacked a Russian nuclear reactor. As The Register notes:

> The infamous Stuxnet malware thought to have been developed by the US and Israel to disrupt Iran's nuclear facilities, also managed to cause chaos at a Russian nuclear plant, according to Eugene Kaspersky.
>
> The revelation came during a Q&A session after a speech at Australia's National Press Club last week, in which he argued that those spooks responsible for "offensive technologies" don't realise the unintended consequences of releasing malware into the wild.
>
> "Everything you do is a boomerang," he added. "It will get back to you."
>
> ***
>
> "Unfortunately, it's very possible that other nations which are not in a conflict will be victims of cyber attacks on critical infrastructure," said Kaspersky.
>
> "It's cyber space. [There are] no borders, [and many facilities share the] same systems."
>
> Not finished there, Kaspersky also claimed to have heard from "Russian space guys" in the know that even machines on the International Space Station had been infected "from time to time" after scientists arrived aboard with infected USBs.

Watch for yourself:

Other security experts agree.

As British security website V3 – in an article entitled "Stuxnet: UK and US nuclear plants at risk as malware spreads outside Russia" – reports:

> Experts from FireEye [background] and F-Secure [background] told V3 the nature of Stuxnet means it is likely **many power plants** have fallen victim to the malware ….
>
> F-Secure security analyst Sean Sullivan told V3 Stuxnet's unpredictable nature means it has likely spread to other facilities outside of the plant mentioned by Kaspersky.
>
> "It didn't spread via the internet. It spread outside of its target due to a bug and so it started traveling via USB. Given the community targeted, I would not be surprised if other countries had nuclear plants with infected PCs," he said.
>
> Director of security strategy at FireEye, Jason Steer, mirrored Sullivan's sentiment, adding the insecure nature of most critical infrastructure systems would make them an ideal breeding ground for Stuxnet.
>
> ***
>
> Steer added the atypical way Stuxnet spreads and behaves, means traditional defences are ill equipped to stop, or even accurately track the malware's movements.
>
> "It's highly likely that **other plants globally are infected and will continue to be infected as it's in the wild and we will see on a weekly basis** businesses trying to figure out how to secure the risk of infected USB flash drives," he said.
>
> ***
>
> The use of XP in power plants is set to become even more dangerous as Microsoft has confirmed it will officially cut support for the 12-year-old OS in less than a year. The lack of support means XP systems will no longer receive critical security updates from Microsoft.

That's almost as brilliant as waging a global war on terror in such an idiotic way that it is *increasing* terrorism …
