Could a Rogue Computer Virus be Used to Shut Down Nuclear Plants Worldwide?

By Washington's Blog

Global Research, April 26, 2011
Washington's Blog 26 April 2011

Theme: Oil and Energy

It is now common knowledge that the U.S. and Israel developed the Stuxnet computer virus in order to slow down Iran's nuclear program.

As the New York Times noted in January:

> Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine Iran's efforts to make a bomb of its own.
>
> Behind Dimona's barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran's at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the Stuxnet computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran's nuclear centrifuges and helped delay, though not destroy, Tehran's ability to make its first nuclear arms.
>
> "To check out the worm, you have to know the machines," said an American expert on nuclear intelligence. "The reason the worm has been effective is that the Israelis tried it out."
>
> Though American and Israeli officials refuse to talk publicly about what goes on at Dimona, the operations there, as well as related efforts in the United States, are among the newest and strongest clues suggesting that the virus was designed as an American-Israeli project to sabotage the Iranian program.
>
> ***
>
> Officially, neither American nor Israeli officials will even utter the name of the malicious computer program, much less describe any role in designing it.
>
> But Israeli officials grin widely when asked about its effects. Mr. Obama's chief strategist for combating weapons of mass destruction, Gary Samore, sidestepped a Stuxnet question at a recent conference about Iran, but added with a smile: "I'm glad to hear they are having troubles with their centrifuge machines, and the U.S. and its allies are doing everything we can to make it more complicated."
>
> ***
>
> By the accounts of a number of computer scientists, nuclear enrichment experts and former officials, the covert race to create Stuxnet was a joint project between the Americans and the Israelis, with some help, knowing or unknowing, from the Germans and the British.

And the Telegraph noted last month:

> A showreel played at a retirement party for the head of the Israeli Defence Forces has strengthened claims the country's security forces were responsible for a cyber attack on the Iranian nuclear programme.
>
> The video of Lieutenant General Gabi Ashkenazi's operational successes included references to Stuxnet, a computer virus that disrupted the Natanz nuclear enrichment site last year, Ha'aretz reported.
>
> Although Israel has not officially accepted responsibility for the Stuxnet attack, evidence of its role has been mounting since it was first discovered last July.
>
> ***
>
> Attributing the source of cyber attacks in notoriously difficult, but security researchers say factors including complexity of the operation, which would have required human sources inside the Iranian nuclear programme, point strongly to the Israeli security forces.

As PC World pointed out last November,

> The sophisticated Stuxnet is a "game changer" for companies and governments looking to protect their networks, said Sean McGurk, acting director of the National Cybersecurity and Communications Integration Center in the U.S. Department of Homeland Security.
>
> ***
>
> As of last week, there were still about 44,000 computers infected with Stuxnet worldwide, with about 60 percent of them in Iran, said Dean Turner, director of Symantec's Global Intelligence Network. About 1,600 of the current infections are in the U.S., he said.
>
> ***
>
> "Stuxnet demonstrates that industrial control systems are more vulnerable to cyberattacks than in the past for several reasons, including their increased connectivity to other systems and the Internet," he said. "Further, as demonstrated by past attacks and incidents involving industrial control systems, the impact on a critical infrastructure could be substantial."

Indeed, one of the computer experts quoted by the New York Times, German cyber-security expert Ralph Langner, noted in a Ted talk last month that Stuxnet could be used to attack Western nuclear power plants and other types of automated plants:

As Israel National News writes today:

> [Langner] went on to describe the risk that Stuxnet could be used to blow up power plants:
>
> > "The idea here is not only to fool the operators in the control room. It actually is much more dangerous and aggressive. The idea here is to circumvent a digital safety system…. when they

> > are compromised, then real bad things can happen. Your plant can blow up and and neither your operators nor your safety system will notice it. That's scary. But it gets worse – and this is very important, what I am going to say. Think about this: this attack is generic. It doesn't have anything to do with specifics with centrifuges, with uranium enrichment. So it would work as well, for example in a power plant or in an automobile factory. It is generic. And as an attacker you don't have to deliver this payload by a USB stick, as we saw it in the case of Stuxnet. You could also use conventional worm technology for spreading. Just spread it as wide as possible. And if you do that, what you end up with is a cyberweapon of mass destruction."
>
> "That's the consequence that we have to face," he said, deliberately, while showing a map that marked Western countries (Israel not included) in green. "So unfortunately, the biggest number of targets for such attacks are not in the Middle East. They are in the United States, in Europe and in Japan. So all the green areas, these are your target-rich environments. We have to face the consquences and we better start to prepare right now."
>
> ***
>
> It seems possible that he thinks Israel could use the worm against Western targets. Why the German consultant thinks Israel would want to do this, one can only speculate.
>
> ***
>
> In a correspondence with cyber-security firm Symantec some six months ago, Langner named a "hacker underground" as the possible threat:
>
> > "You fail to understand that the hacker underground has been studying control systems for years without any success. You fail to understand that this community will eagerly dismantle Stuxnet as a blueprint for how to cyber-attack installations from the cookie plant next door to power plants."
>
> ***
>
> The New York Times recently reported that the Stuxnet virus could possibly still be infecting Iranian systems and that it may unleash additional havoc on new targets.

Has Stuxnet Already Caused Damage Outside Of Iran?

Since the Japanese earthquake, Michael Rivero has posted hundreds of articles arguing that the Stuxnet virus has "gotten loose" and attacked other nuclear power plants outside of Iran.

The former editor of the Japan Times – Yoichi Shimatsu – writes:

> Tepco engineers suggested that the electric power inside the plant was

> knocked out by something other than the tsunami. I have pointed to this possibility early on, that the quake and control disruptions could have made the control computers vulnerable to the Stuxnet virus.

According to Yomiuri, Stuxnet was in Japan as of October of 2010. However, I find it hard to believe that it was not the earthquake and the tsunami which knocked out the power, although I suppose a virus could have exacerbated the damage.

There have been a lot of strange stories about unexplained nuclear power plant shutdowns. For example, as Fox News reported last week:

> A nuclear reactor at Plant Vogtle in eastern Georgia has been taken out of service until authorities determine why it unexpectedly shut down.

I have no idea whether or not the shutdowns were caused by Stuxnet accidentally spreading to other reactors, instead of just hitting its intended target: Iran.

But at the very least, the virus created by the U.S. and Israel to slow down Iran's nuclear program has opened a "Pandora's box" which leaves our nuclear plants and other sensitive facilities open to attacks by hostile governments or rogue hackers.

The original source of this article is Washington's Blog

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: Washington's Blog

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

For media inquiries: publications@globalresearch.ca