

As PC World [pointed out](#) last November,

The sophisticated Stuxnet is a "game changer" for companies and governments looking to protect their assets, said Sean McGurk, acting director of the National Cybersecurity and Communications Integration Center, U.S. Department of Homeland Security.

As of last week, there were still about 44,000 computers infected with Stuxnet worldwide, with about 1,600 of them in Iran, said Dean Turner, director of Symantec's Global Intelligence Network. About 1,600 of 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 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 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, the bad things can happen. Your plant can blow up and neither your operators nor your safety system 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 not specific. 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. 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 several countries (Israel not included) in green. "So unfortunately, the biggest number of targets for such attacks are in the Middle East. They are in the United States, in Europe and in Japan. So all the green areas, these are target-rich environments. We have to face the consequences 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 c 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 "hack underground" as the possible threat:

"You fail to understand that the hacker underground has been studying control systems for years w any success. You fail to understand that this community will eagerly dismantle Stuxnet as a bluepri 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 s 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 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 othe tsunami. I have pointed to this possibility early on, that the quake and control disruptions could have 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 *massive* earthquake and the *enormous* tsunami which knocked out the power (although I suppose a viru exacerbated the damage).

There have been a lot of strange stories about unexplained nuclear power plant shutdowns. For example, [reported](#) last week:

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

I have no idea whether or not the shutdowns were caused by Stuxnet accidentally spreading to other reac 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 or rogue hackers.

o COMMENTS:

POST A COMMENT

→ Thank you for contributing to the conversation by commenting. We try to read all of the comments (but don't always have the time).

→ If you write a long comment, please use paragraph breaks. Otherwise, no one will read it. Many people still won't read it, so shorter is usually better (but it's your choice).

→ The following types of comments will be deleted if we happen to see them:

-- Comments that criticize any class of people as a whole, especially when based on an attribute they don't have control over

-- Comments that explicitly call for violence

→ Because we do not read all of the comments, I am not responsible for any unlawful or distasteful comments.

Comment as: 

Subscribe to: [Post Comments \(Atom\)](#)