Cyber war on Iran has only just begun

July 13 2012, by Dan De Luce

An Iranian security man stands next to journalists outside the Russian-built Bushehr nuclear power plant in southern Iran in 2010, which was the suspected target of the Stuxnet worm computer. A US cyber war against Iran's nuclear program may have only just begun and could escalate with explosions triggered by digital sabotage, experts say.

A US cyber war against Iran's nuclear program may have only just begun and could escalate with explosions triggered by digital sabotage, experts say.

Although the Iranian regime remains vulnerable to more cyber attacks in the aftermath of the "Stuxnet" worm that disrupted its uranium enrichment work, Tehran may be receiving help from Russian proxies for its digital security, some analysts say.

The nuclear program is "really not that well protected" from more digital assaults and Iran will be hard-pressed to safeguard its uranium enrichment efforts from tainted software, said David Albright, president of the Institute for Science and International Security.

"With Stuxnet, they lost about a year. And it caused a lot of confusion. They really didn't know what hit them," he said. "It looks like a viable way to disrupt their program."

The United States, which reportedly masterminded the Stuxnet operation along with Israel, has every incentive to press ahead with a cyber campaign to undermine Iran's atomic ambitions, according to analysts.

The next cyber attack, possibly in combination with more traditional spycraft, could shut off valves or issue incorrect orders that might cause an explosion at a sensitive site.

"I think that it could get more violent," Albright told AFP. "I would expect more facilities to blow up."

A major explosion at a missile plant in Iran in November sparked speculation that the incident was the result of sabotage.

"There is of course the possibility of sending in a team to modify a system in a way that would make it vulnerable, and then use a cyber weapon at a later date as a trigger event," said David Lindahl, research engineer at the Swedish Defense Research Agency.

A new wave of cyber attacks could involve inserting hardware with infected chips into the industrial process, possibly through an agent or a duped employee, or penetrating diagnostic software used to gauge uranium enrichment or other work, Lindahl said.

But some cyber security experts suspect Russian proxies could be assisting Iran with its digital defenses, and possibly helped Tehran trace the origins of Stuxnet.

"The part that we probably miscalculated on in Stuxnet was the (possible) assistance of the Russians in attribution," said James Lewis, senior fellow at the Center for Strategic and International Studies.

"The Iranians never would have figured this out on their own," said Lewis, a former senior government official with the Departments of State and Commerce.

The elaborate Stuxnet malware, which was reportedly introduced using a thumb drive, contained malicious code that caused centrifuges used to enrich uranium to spin out of control. The worm, meanwhile, sent back signals to operators indicating the centrifuges were operating normally.

After the malware was discovered in 2010, at least a thousand centrifuges had to be removed and analysts estimate Tehran's program was set back by at least a year.

By pushing the boundaries of cyber warfare, the United States has left itself open to retaliation. But US officials clearly view the risks associated with digital strikes as dwarfed by the dangers of an all-out war with Iran.

Bombing raids are "more likely to explode the region and certainly could lead to a conflict with Iran, and that would be very messy," said Lewis. "Cyber is much cleaner."

Although unnamed officials told The New York Times that the United States and Israel were behind the digital operations, cyber attacks -- unlike air strikes -- allow for "plausible deniability," he said.

The Stuxnet worm broke new ground by successfully hijacking a program designed to supervise power plants or other large industrial systems, said Sean McGurk, a consultant who previously led cyber security efforts at the Department of Homeland Security.

"Stuxnet demonstrated going from a disruptive capability to a destructive capability and that's what made it unique," he said.

The super virus also was unusual for the way it sought out a specific target while sidestepping systems that did not fit certain criteria.

"Almost all cyberattacks are 'to whom it may concern' but Stuxnet was a bullet with someone's name on it," Lindahl said.

"Repeating something like Stuxnet or (computer virus) Flame will be much more difficult, because they (the Iranians) will spend a lot more energy trying to stop those activities," he added.

"But the defender needs to plug all holes, while the attacker need only find one."

Citation: Cyber war on Iran has only just begun (2012, July 13) retrieved 19 April 2024 from https://phys.org/news/2012-07-cyber-war-iran-begun.html