Symantec. Confidence in a connected world.

Symantec.com > Business > The Stuxnet Worm

The Stuxnet Worm

Stuxnet is a computer worm that targets industrial control systems that are used to monitor and run large scale industrial facilities like power plants, dams, assembly lines and similar operations.

Free Assessment for Qualifying Enterprises

How Stuxnet Worm Works

Stuxnet looks for industrial control systems and then changes the code in them to allow the attackers to take control of these systems without the operators knowing. In other words, this threat is designed to allow hackers to manipulate real-world equipment, which makes it very dangerous.

It's like nothing we've seen before – both in what it does, and how it came to exist. It is the first computer virus to be able to wreak havoc in the physical world. It is sophisticated, well-funded, and there are not many groups that could pull this kind of threat off. It is also the first cyberattack we've seen specifically targeting industrial control systems.

The worm is made up of complex computer code that requires lots of different skills to put it together. Symantec security experts estimate it took five to ten people to work on this project for six months. In addition, knowledge of industrial control systems was needed along with access to such systems to do quality assurance testing; again indicating that this was a highly organized and well-funded project.

"We've definitely never seen anything like this before," said Liam O'Murchu, Researcher, Symantec Security Response. "The fact that it can control the way physical machines work is quite disturbing."

W32.Stuxnet Dossier
Download the White Paper
Read the Symantec Security Response Blog

Get More Details and watch the video report! Double Click Here

Stuxnet in the News

DEBKAfile
We Start Where the Media Stop | Est. 2000

Russian experts flee Iran, escape dragnet for cyber worm smugglers

DEBKA*file* *Exclusive Report* *October 3, 2010, 1:13 PM (GMT+02:00)*

Tags: Stuxnet ›› cyber war ›› Iran nuclear ›› Russians ››

Iranian nuclear czar with Russian experts in happier days

DEBKA*file*'s intelligence sources report from Iran that dozens of Russian nuclear engineers, technicians and contractors are hurriedly departing Iran for home since local intelligence authorities began rounding up their compatriots as suspects of planting the Stuxnet malworm into their nuclear program.

Among them are the Russian personnel who built Iran's first nuclear reactor at Bushehr which Tehran admits has been damaged by the virus.

One of the Russian nuclear staffers, questioned in Moscow Sunday, Oct. 3 by Western sources, confirmed that many of his Russian colleagues had decided to leave with their families after team members were detained for questioning at the beginning of last week. He refused to give his name because he and his colleagues intend to return to Iran if the trouble blows over and the detainees are quickly released after questioning.

According to our sources, these detentions were the source of the announcement Saturday, Oct. 2, by Iranian Intelligence Minister Heidar Moslehi that several "nuclear spies" had been captured. "The enemy had sent electronic worms through the internet to undermine Iran's nuclear activities," he said. This was the first high-level Iranian admission that the Stuxnet virus had been planted by foreign elements to sabotage their entire nuclear program - and not just the Bushehr reactor. The comprehensive scale of the damage is attested to by the detention of Russian nuclear experts also at Natanz, Isfahan and Tehran.

Moslehi added: "We are always facing destructive activities by these espionage services and of course we have arrested a number of nuclear spies to block the enemy's destructive moves.

This statement is expected to prompt a second wave of Russian nuclear specialists to flee Iran.

The prime aim of their interrogation is to find out if Russian intelligence knowingly planted the destructive worm in Iran's nuclear facilities, possibly for under-the-counter pay, or were the unwitting carriers of equipment on order by Iran that had been previously infected.

DEBKA*file*'s Western sources report that the hundreds of Russian scientists, engineers and technicians employed in Iran were responsible for installing the Siemens control systems in Iran's nuclear complex and other facilities which proved most vulnerable to the cyber attack.

They were the only foreigners with access to these heavily guarded plants. At Bushehr, for instance, the Russian personnel enjoyed full access to all its systems.

'Stuxnet created by Siemens insider'

Graham Cluley is one of the world's leading experts in viruses and spam, and works as Senior Technology Consultant at Sophos.

Fri Oct 1, 2010 1:4PM

The Stuxnet worm, dubbed the world's first cyber superweapon, may have been originated from German giant Siemens, says a senior technology consultant at system security developer Sophos.

The worm may have been written by someone with detailed knowledge of Siemens' computer systems, Graham Cluley said on Friday.

Speaking to Computer and technology news website, *V3*, Cluley said the person may possibly be a current or former employee of the German industrial giant whose control systems are widely used to manage industrial facilities such as oil rigs and power plants.

"The message I got was that it appears to have been written by someone with inside knowledge of how Siemens' systems work," he said after attending the Virus Bulletin 2010 conference in Vancouver in Canada.

He added that none of the presenters at the conference, where the malware took center stage, "gave any evidence about who wrote it and against who it was targeted."

Cluley also pointed out that the evidence for this being a targeted attack on Iran is patchy since anti-virus maker Symantec reported that more attacks had been reported in India and Indonesia than in Iran.

Another expert on the issue, Mikko Hypponen, chief research officer at F-Secure, told *V3* that based on evidence he'd seen, the worm looks like a government attack.

"If you look at the level of difficulty and complexity behind Stuxnet, it has to be a government effort," he further explained.

Media reports emerged in July, claiming that Stuxnet had targeted industrial computers around the globe with Iran being the main target of the attack.

Iran's Telecommunications Minister Reza Taqipour, however, announced that the computer worm had caused no serious damage to the country's industrial sites.

Iranian experts say the worm may have been created by a state-sponsored organization in the US or Israel to target specific control software being used in the Iranian industrial sector, including the Bushehr plant -- Iran's first nuclear

Cyber war is on: Apocalypse.com

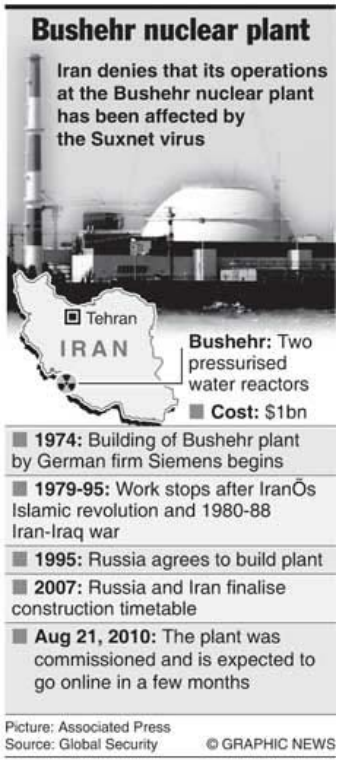
FRIDAY, 01 OCTOBER 2010 00:29

Future wars will be fought from a desk in a closed-up room. No missiles will be fired, no drone attacks will be launched on civilians and no soldiers will die. Nuclear weapons will be of no use. Yet nations will be brought to their knees by the press of a button. Yes, it is all but official that the era of cyber warfare has begun.

A virus called Stuxnet has hit 60,000 computers in Iran, including those at the Bushehr nuclear plant. Experts say the attack bore all the hallmarks of a "nation-state".

Kevin Hogan, senior director at computer security giant Symantec, said 60 percent of computers worldwide infected by the Stuxnet worm were in Iran, suggesting its industry was the target.

According to the European digital security company, Kaspersky Labs, Stuxnet is a working and fearsome prototype of a cyber-weapon that will lead to the creation of a new arms race in the world.

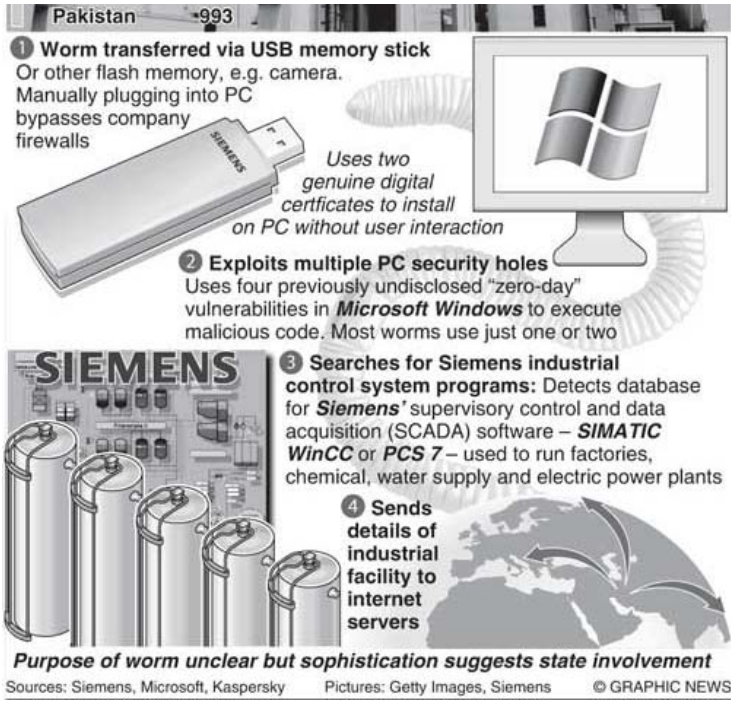


Hackers damaging computers is no big news. Even computers at the Pentagon have come under attack from worms or malicious computer software (malware) introduced by hackers via email, internet, USB drives and other means. Such attacks have prompted states, companies and institutions to install sophisticated anti-virus guards to protect their computerized systems. But, the hackers are often one step ahead of the anti-virus software suppliers. The sophistication of the Stuxnet virus is such that experts believe it could not have been created by one hacker. It is the work of a group with vast resources or a nation state. The worm they created tells an industrial equipment to behave in a manner contrary to its programming.

For instance, if a nuclear missile of country A is programmed to hit country B, Stuxnet could either neutralize the command or reverse the path of the projectile to hit the country A itself. The day is not far away when thousands of computer experts will have the knowledge to hack computers that control nuclear weapons. The nuclear holocaust is at the fingertip of a hacker. The world is on the brink of an apocalypse. When a cyber-attack happens, it is difficult to know from where the attack originated. It could be from an enemy country, or from a ship in international waters, or from atop the Himalayas, or from within one's country itself.

What if a terrorist hacker masters the knowledge to cause havoc in a target country? The LTTE had resorted to cyber terrorism and had limited success. A paper presented by Sri Lanka's European Union Ambassador Ravinatha Aryasinha at the EU-US international seminar on the LTTE in 2008 said: "The Patterns of Global Terrorism Report 1997 identified the LTTE as being responsible for the first known attack by a 'terrorist group' on a target country's computer system, when in August 1997 a group calling itself 'Internet Black Tigers' claimed responsibility for 'suicide e-mail bombings' aimed at disrupting the electronic information network/communications systems used by Sri Lanka's missions abroad. This brazen act of 'information warfare' paralysed the communication systems of most of Sri Lanka's overseas missions. At the time the US said the incident 'did cause us to sit up and take notice' because it was the first of its kind involving a group branded as a terrorist organization by Washington, and was a possible 'portent of worse things to come'."

Cyber terrorism that could cause catastrophic consequences is a reality. But sadly, it is the states that show the way for terrorists to move into the theatre of cyber war. Who could it be? The suspicion naturally falls on Israel, which has said that sabotage is one way of slowing Iran's nuclear programme.



Major-general Amos Yadlin, Israel's chief of military intelligence, last year said his country's armed forces had the means to provide network security and launch cyber attacks of its own.

The United States is another country capable of carrying out such sabotage or cyber wars. In fact, the United States has an ongoing cyber war programme.

An article published in the New York Times on April 28, 2009 exposed the existence of such a programme and specifically mentioned Iran as a target.

The article by David E. Sanger, John Markoff and Thom Shanker said that just as the invention of the atomic bomb changed warfare and deterrence 64 years ago, a new international race has begun to develop cyber-weapons and systems to protect against them.

The authors also revealed that President George W. Bush had ordered new ways to slow Iran's progress toward a nuclear bomb and approved a plan for an experimental covert programme to bore into Iran's computers and undermine the project.

The programme, which has also won the approval of the Barack Obama administration, is not only aimed at sabotage but also defending the United State's vital installations from possible attacks, especially from China and Russia.

The authors of the New York Times article said: "The most exotic innovations under consideration would enable a Pentagon programmer to surreptitiously enter a computer server in Russia or China, for example, and destroy a 'botnet' — a potentially destructive program that commandeers infected machines into a vast network that can be clandestinely controlled — before it could be unleashed in the United States.

"Or American intelligence agencies could activate malicious code that is secretly embedded on computer chips when they are manufactured, enabling the United States to take command of an enemy's computers by remote control over the Internet. That, of course, is exactly the kind of attack officials fear could be launched on American targets, often through Chinese-made chips or computer servers."

It is not so much Iran's nuclear ambitions but rather worries about China's growing power that prompted Washington to put its cyber-war programme on a fast track. The United States maintains friendly relations with China — also with Russia. But mutual suspicion and cold-war-type rivalry remain a powerful undercurrent.

In November 2008, the US congressional panel — the US-China Economic and Security Review Commission — warned that China had developed such a sophisticated and active cyber warfare programme that the US "may be unable to counteract or even detect" an attack. The panel charged that networks owned by the US government, defence contractors and US businesses were the focus of Chinese cyber attacks.

It said China was aggressively pursuing cyber warfare capabilities that could provide it with an asymmetric advantage against the United States. "In a conflict situation, this advantage would reduce current US conventional military dominance," the panel warned.

It is naïve not to assume that China and Russia are taking counter-measures to protect their vital installations from US cyber-attacks. It is also naïve not to think that Iran is also adopting counter-measures. Iran has said the virus has not affected the operation at the Bushehr nuclear plant. Probably, it is not revealing the full extent of the damage.

To protect itself from cyber attacks, however, Iran will not only take counter measures but also develop its own cyber-weapons to target Israel and the United States.

Cyber-attacks and counter-cyber attacks have the potential to cripple countries. True they won't kill people directly. But they can cause severe hardships by shutting down power grids, banking networks, traffic lights system. The more

But they can cause severe hardships by shutting down power grids, banking networks, traffic lights system. The more hi-tech a country is the more vulnerable it is to cyber attacks. When the possibility of nuclear weapons being manipulated by a hacker or terrorist with a remote control looms large, isn't it time to go for the total nuclear disarmament? The less hi-tech one is, the safer it is.

Printed from
THE TIMES OF INDIA

Israeli unit behind Iran Nuclear plant attack

IANS, Oct 1, 2010, 02.19pm IST

LONDON: An Israeli military unit that undertakes cyberwarfare is responsible for creating a virus that attacked Iran's computer systems and stopped work at a nuclear power station, an expert has said.

A Biblical reference has been detected in the code of the computer virus that points to Israel as the origin of the cyber attack.

Daily Telegraph reported that the code contains the word "myrtus", which is a reference to the myrtle tree. Myrtle's Hebrew word is Hadassah and it was the birth name of Esther, the Jewish queen of Persia.

In the Bible, "The Book of Esther" tells how the queen persuaded her husband to launch an attack before being attacked themselves.

Israel has threatened a pre-emptive attack on Iran's facilities so that the Islamic state can't threaten its existence.

German researcher Ralf Langner claimed that the signals intelligence arm of the Israeli defence forces carried out the computer virus attack by infiltrating the software into Iran's Bushehr nuclear power station.

"If you read the Bible you can make a guess," Langner was quoted as saying.

Experts have spent a long period of time to trace the origin of the Stuxnet worm, a malware that infected operating systems made by the German firm Siemens.

Those who are tracking Stuxnet worm believe that it was most likely introduced to Iran on a memory stick, possibly by one of the Russian firms that are helping to build Bushehr. The same firm has projects in Asia, including India and Indonesia which were also attacked.

Langner said: "It would be an absolute no-brainer to leave an infected USB stick near one of these guys and there would be more than a 50 percent chance of him pick it up and infect his computer."

Cyber security experts said that Israel was the most likely perpetrator of the attack and had been targeting Iran but that it had not acknowledged a role to its allies.

"Nobody is willing to accept responsibility for this particular piece of malicious software which is a curious, complex and powerful weapon," an expert was quoted as saying.