Stuxnet malware is 'weapon' out to destroy … Iran's Bushehr nuclear plant?

http://news.yahoo.com/s/csm/327178

- *By Mark Clayton Mark Clayton* – Tue Sep 21, 3:08 pm ET

Cyber security experts say they have identified the world's first known cyber super weapon designed specifically to destroy a real-world target – a factory, a refinery, or just maybe a nuclear power plant.

The cyber worm, called Stuxnet, has been the object of intense study since its detection in June. As more has become known about it, alarm about its capabilities and purpose have grown. Some top cyber security experts now say Stuxnet's arrival heralds something blindingly new: a cyber weapon created to cross from the digital realm to the physical world – to destroy something.

At least one expert who has extensively studied the malicious software, or malware, suggests Stuxnet may have already attacked its target – and that it may have been Iran's Bushehr nuclear power plant, which much of the world condemns as a nuclear weapons threat.

The appearance of Stuxnet created a ripple of amazement among computer security experts. Too large, too encrypted, too complex to be immediately understood, it employed amazing new tricks, like taking control of a computer system without the user taking any action or clicking any button other than inserting an infected memory stick. Experts say it took a massive expenditure of time, money, and software engineering talent to identify and exploit such vulnerabilities in industrial control software systems.

Unlike most malware, Stuxnet is not intended to help someone make money or steal proprietary data. Industrial control systems experts now have concluded, after nearly four months spent reverse engineering Stuxnet, that the world faces a new breed of malware that could become a template for attackers wishing to launch digital strikes at physical targets worldwide. Internet link not required.

"Until a few days ago, people did not believe a directed attack like this was possible," Ralph Langner, a German cyber-security researcher, told the Monitor in an interview. He was slated to present his findings at a conference of industrial control system security experts Tuesday in Rockville, Md. "What Stuxnet represents is a future in which people with the funds will be able to buy an attack like this on the black market. This is now a valid concern."

A gradual dawning of Stuxnet's purpose

It is a realization that has emerged only gradually.

Stuxnet surfaced in June and, by July, was identified as a hypersophisticated piece of malware probably created by a team working for a nation state, say cyber security experts. Its name is derived from some of the filenames in the malware. It is the first malware known to target and infiltrate industrial supervisory

control and data acquisition (SCADA) software used to run chemical plants and factories as well as electric power plants and transmission systems worldwide. That much the experts discovered right away.

But what was the motive of the people who created it? Was Stuxnet intended to steal industrial secrets – pressure, temperature, valve, or other settings –and communicate that proprietary data over the Internet to cyber thieves?

By August, researchers had found something more disturbing: Stuxnet appeared to be able to take control of the automated factory control systems it had infected – and do whatever it was programmed to do with them. That was mischievous and dangerous.

But it gets worse. Since reverse engineering chunks of Stuxnet's massive code, senior US cyber security experts confirm what Mr. Langner, the German researcher, told the Monitor: Stuxnet is essentially a precision, military-grade cyber missile deployed early last year to seek out and destroy one real-world target of high importance – a target still unknown.

"Stuxnet is a 100-percent-directed cyber attack aimed at destroying an industrial process in the physical world," says Langner, who last week became the first to publicly detail Stuxnet's destructive purpose and its authors' malicious intent. "This is not about espionage, as some have said. This is a 100 percent sabotage attack."

A guided cyber missile

On his website, Langner lays out the Stuxnet code he has dissected. He shows step by step how Stuxnet operates as a guided cyber missile. Three top US industrial control system security experts, each of whom has also independently reverse-engineered portions of Stuxnet, confirmed his findings to the Monitor.

"His technical analysis is good," says a senior US researcher who has analyzed Stuxnet, who asked for anonymity because he is not allowed to speak to the press. "We're also tearing [Stuxnet] apart and are seeing some of the same things."

Other experts who have not themselves reverse-engineered Stuxnet but are familiar with the findings of those who have concur with Langner's analysis.

"What we're seeing with Stuxnet is the first view of something new that doesn't need outside guidance by a human – but can still take control of your infrastructure," says Michael Assante, former chief of industrial control systems cyber security research at the US Department of Energy's Idaho National Laboratory. "This is the first direct example of weaponized software, highly customized and designed to find a particular target."

"I'd agree with the classification of this as a weapon," Jonathan Pollet, CEO of Red Tiger Security and an industrial control system security expert, says in an e-mail.

One researcher's findingsLangner's research, outlined on his website Monday, reveals a key step in the Stuxnet attack that other researchers agree illustrates its destructive purpose. That step, which Langner calls "fingerprinting," qualifies Stuxnet as a targeted weapon, he says.

Langner zeroes in on Stuxnet's ability to "fingerprint" the computer system it infiltrates to determine whether it is the precise machine the attack-ware is looking to destroy. If not, it leaves the industrial computer alone. It is this digital fingerprinting of the control systems that shows Stuxnet to be not spyware, but rather attackware meant to destroy, Langner says.

Stuxnet's ability to autonomously and without human assistance discriminate among industrial computer systems is telling. It means, says Langner, that it is looking for one specific place and time to attack one specific factory or power plant in the entire world.

"Stuxnet is the key for a very specific lock – in fact, there is only one lock in the world that it will open," Langner says in an interview. "The whole attack is not at all about stealing data but about manipulation of a specific industrial process at a specific moment in time. This is not generic. It is about destroying that process."

So far, Stuxnet has infected at least 45,000 industrial control systems around the world, without blowing them up – although some victims in North America have experienced some serious computer problems, Eric Byres, a Canadian expert, told the Monitor. Most of the victim computers, however, are in Iran, Pakistan, India, and Indonesia. Some systems have been hit in Germany, Canada, and the US, too. Once a system is infected, Stuxnet simply sits and waits – checking every five seconds to see if its exact parameters are met on the system. When they are, Stuxnet is programmed to activate a sequence that will cause the industrial process to self-destruct, Langner says.

Langner's analysis also shows, step by step, what happens after Stuxnet finds its target. Once Stuxnet identifies the critical function running on a programmable logic controller, or PLC, made by Siemens, the giant industrial controls company, the malware takes control. One of the last codes Stuxnet sends is an enigmatic “DEADF007.” Then the fireworks begin, although the precise function being overridden is not known, Langner says. It may be that the maximum safety setting for RPMs on a turbine is overridden, or that lubrication is shut off, or some other vital function shut down. Whatever it is, Stuxnet overrides it, Langner’s analysis shows.

"After the original code [on the PLC] is no longer executed, we can expect that something will blow up soon," Langner writes in his analysis. "Something big."

For those worried about a future cyber attack that takes control of critical computerized infrastructure – in a nuclear power plant, for instance – Stuxnet is a big, loud warning shot across the bow, especially for the utility industry and government overseers of the US power grid.

"The implications of Stuxnet are very large, a lot larger than some thought at first," says Mr. Assante, who until recently was security chief for the North American Electric Reliability Corp. "Stuxnet is a directed attack. It's the type of threat we've been worried about for a long time. It means we have to move more quickly with our defenses – much more quickly."

Has Stuxnet already hit its target?It might be too late for Stuxnet's target, Langner says. He suggests it has already been hit – and destroyed or heavily damaged. But Stuxnet reveals no overt clues within its code to what it is after.

A geographical distribution of computers hit by Stuxnet, which Microsoft produced in July, found Iran to be the apparent epicenter of the Stuxnet infections. That suggests that any enemy of Iran with advanced

cyber war capability might be involved, Langner says. The US is acknowledged to have that ability, and Israel is also reported to have a formidable offensive cyber-war-fighting capability.

Could Stuxnet's target be Iran's Bushehr nuclear power plant, a facility much of the world condemns as a nuclear weapons threat?

Langner is quick to note that his views on Stuxnet's target is speculation based on suggestive threads he has seen in the media. Still, he suspects that the Bushehr plant may already have been wrecked by Stuxnet. Bushehr's expected startup in late August has been delayed, he notes, for unknown reasons. (One Iranian official blamed the delay on hot weather.)

But if Stuxnet is so targeted, why did it spread to all those countries? Stuxnet might have been spread by the USB memory sticks used by a Russian contractor while building the Bushehr nuclear plant, Langner offers. The same contractor has jobs in several countries where the attackware has been uncovered.

"This will all eventually come out and Stuxnet's target will be known," Langner says. "If Bushehr wasn't the target and it starts up in a few months, well, I was wrong. But somewhere out there, Stuxnet has found its target. We can be fairly certain of that."