Wednesday, October 12, 2016 5:49 PM ET Exclusive

Nuclear plant cyberattack: Stuxnet decoder warns that ransomware is coming next

By Andrew Coffman Smith

The revelation that a nuclear power plant was the target of a "disruptive" cyberattack has the cybersecurity expert who decoded the Stuxnet computer virus, which sabotaged Iran's nuclear program, warning that plants are at risk of being held hostage by ransomware.

Yukiya Amano, director of the United Nations' International Atomic Energy Agency, or IAEA, publicly revealed during a visit to Germany on Oct. 10 that the cyberattack two to three years ago caused "some disruption" at an unidentified nuclear plant. The head of the United Nations' nuclear watchdog said the nuclear plant had "to take some precautionary measures" as a result but did not shut down.

"This is not an imaginary risk," Amano told Reuters. "This issue of cyberattacks on nuclear-related facilities or activities should be taken very seriously. We never know if we know everything or if it's the tip of the iceberg."

Ralph Langner, a German control system security consultant based in Munich and Northern Virginia, said in an interview that he is not surprised that a nuclear power plant's computer systems were infected despite industrywide "air gap" security measures blocking direct access to nuclear plants' computers over the internet. He is also disappointed with the IAEA for failing to provide any details on the attack to help "people in the trenches" like himself "who actually cyber-protect nuclear power plants for a living every day."

"The media and the general public have been fed the idea that nuclear power plants or other critical infrastructure facilities are super-secure because they are 'air-gapped,'" Langner said. "And, as anybody can know after Stuxnet, that's just dumb nonsense."

Langner came to international prominence for cracking the code of the Stuxnet malware computer virus. The computer worm, which is believed to have been made by U.S. and Israeli foreign intelligence to prevent Iran from acquiring nuclear weapons, ruined the country's nuclear program in 2010 by spinning centrifuges out-of-control until they were rendered useless while providing false feedback to Iranian controllers. Stuxnet infiltrated Iran's Natanz nuclear facility via an infected USB flash drive while brandishing a trust-worthy digital certificate to bypass network security.

On top of many nuclear power plants falling short of actually being "air gapped" once thoroughly inspected, Langner said Stuxnet and the ability to infiltrate and infect the computers of contractors that work at nuclear power plants show that air gap is not a "silver bullet" for protecting the control systems of digitized facilities.

In order to prevent such attacks, Langner recommends that nuclear plant operators not rush towards digitizing their hack-proof — but aging — analog control systems. However, he also acknowledged that keeping control systems forever analog is a "not a solution" as digital computer systems are more efficient and flexible. He also said the industry should gauge their threats and narrow the "credible" threats.

"What some people tend to forget is when we discuss the cybersecurity of nuclear facilities, we are not considering hackers… They have probably zero percent chance of ever hitting a nuclear facility," Langner said. "When you start serious discussion on nuclear cyber security, you're discussing more potent and sophisticated and organized threat[s] … that could involve organized crime, … rogue nation states [like North Korea], and terrorists."

The German cybersecurity expert and consultant is particularly fearful that organized crime's ever-popular "business model" of infecting and encrypting computers with so-called ransomware until the locked-out user pays is the future of cyberattacks on nuclear power plants and other critical infrastructure.

"If you shut down a nuke plant for one day, they're losing $1 million per unit," he said. "We have seen … over the last 12 months… this spike in ransomware and I predict that it's only going to be a matter of couple of months until the usual suspects discover the much more-juicier targets."

Langner believes nuclear power plants can be made reasonably cyber secure but said the industry is not there yet. "We can do this if we are smart and if we are creative like our adversaries," Langer said. "It still requires a lot of effort but we know how to do it and I encourage everyone in the nuclear space … to push the ongoing efforts [to enhance cybersecurity] and, if we make that happen, we have little to fear."