Published on *Atlantic Council* (http://www.acus.org)

Stuxnet: All Signs Point to Russia

By *Chris Demchak*
Created *11/26/2010 - 15:15*

[1]

No smoking gun cleanly identifies the author of Stuxnet but three broad streams of evidence suggest it is unlikely to be the usual suspects of Israel, the US, or China. The code characteristics, the delivery mechanisms, and the geopolitical effects suggest one look for a state open to using proxies for relatively high value targets in cyberspace and a good reason to derail, but not destroy, the intended targets if they were the Iranian nuclear reactors [2].

First, the code [3] is highly modular, consistent with software outsourcing in a major production project. That there were a number of authors is suggested not only by the enormous number of patches it accommodated across Windows operating systems, but also the small inconsistencies across the wide variety of modules. A single professional group in a normally risk-averse westernized agencies or China would have made more effort to ensure consistency, lest a small error sink the whole complex and valuable application. That the final version was more or less 'good enough' is, however, consistent with the output of cybercrime communities.

Second, since largescale nuclear facilities are almost always individually tailored, one would have needed a physically similar testbed to have reasonable confidence the program would work. If the targets were Iranian nuclear reactors built with Russian expertise [4], reactors that are close enough equivalents are found in Russia or its clients, not the US, Israel, or China.

Third, the delivery is not consistent with the precision tendencies of highly professionalized intelligence agencies, but it is quite common in cybercrime to send applications out widely [5] in pieces and see what works. Stuxnet in various iterations floated around for at least a year [6] before it was discovered publicly in summer 2010. It is unlikely a small exceptionally talented group working professionally in a state organization would toss some sophisticated future crown jewels out into the world just to see if they hit a target valued apparently so

highly. A broad spectrum of infections could be an initial mistake by westernized national agencies culturally, legally, and financially loathe to impose uncontrolled collateral damage, but they certainly are unlikely to keep updating [7] an application so seemingly out of control and possibly exposed. Deep secrecy predilections would have kept the variants down to something closer to one or two with more highly precise targeting and delivery, lest the whole project be prematurely exposed or once exposed, no longer usable for all the expense.

Furthermore, Stuxnet showed up relatively widely in Chinese manufacturing facilities. For the level of expertise the Chinese government has sought in cyberspace for at least ten years, to deliberately allow such a blowback into Chinese production would at best be much too unsubtle or unprofessional, given the quality of other exploits widely viewed as Chinese [8] in origin. At worse, the unfettered infections in China could easily be viewed as "un-patriotic hacking". Although the Chinese government is seen to use a wide variety of Chinese hacker groups as proxies, it is exceptionally hard on hacking that blowbacks on China [9] itself.

Fourth, the physical and geostrategic effects did not destroy the Iranian reactors, but reputedly disabled [10] them in ways that seems to have simply frustratingly delayed them. If a nation were behind this infection, then it is worth asking who benefited from delay rather than destruction of the facilities. Had either the US or Israel orchestrated this outcome, destroying the reactors permanently would have been preferred. While the Stuxnet code could probably have allowed a more extensive destroy command, it did not. For its part, China has not shown eagerness for the rise of a nuclear Iran with no Chinese strings [11] for control if needed. In case of a technical problem with large nuclear facilities, China is unlikely to be seen in Iran as the first country to call. Despite being seen as Iran's closest ally on the UN Security Council, China revealed Iran's nuclear arms ambitions [11] to the UN in 2008.

For these likely suspects, logic and available evidence about Stuxnet does not seem consistent with their known normative, institutional, or operational predilections. However, if the originating state was Russia, the pieces fit reasonably enough. It is a state with a healthy cyber expert community on its territory especially found in its cybercrime networks, direct access to Russian-design nuclear facilities to use as a test bed, experience with success in achieving aims by wide distributions, and a strong national reason to slow, but not destroy, Iranian nuclear ambitions. Russian government is alleged widely to successfully employed proxies in Estonia 2007 and Georgia 2008, and it reputedly has deep connections with elements of the very highly skilled cybercriminal Russian business network (RBN [12]). Along with its extensive list of cybercriminal associates for exceptional dispersed production, delivery, and targeting networks, the RBN business model would certainly include spreading around the infected thumbdrives without a great deal of concern for collateral damage.

Logically, Russia had a reasonable expectation of being called to help with the Iranian reactors – as the nation whose firms designed and built them and who was eager to continue the relationship via reprocessing fuel. For Russia, nuclear expertise [13] has become a mainstay of export growth after oil and gas. But in 2007, nuclear support relations between Iran and Russia severely declined [14] over insufficient payments by Iran. Relations have been up and mostly down in the interim, with no reactors completed in Iran. In June 2010, the Russian government voted in the UN for a fourth round of sanctions on Iran for its lack of compliance in nuclear matters. Nonetheless, after Stuxnet was publicly known, the Iranian government eased up on the Russian offer seemingly rather rapidly. Now the Iranian Bushehr reactor is scheduled to go to full operations in January with Russian reprocessing [15] of the spent fuel rods.

If this analysis is correct, there is no downside to Stuxnet for the Kremlin. It has proved a rather impressive fingers-free (for a nation) example of a new wave of computer 'DNA swarming' [16] operations. With it, Russia reacquired a paying client strongly dependent on Russian strength in nuclear skills, facilities, and deliveries. Furthermore, admitting authorship indirectly in quiet conversations in the corridors could provide considerable international political leverage well beyond public view. Certainly the more that Russian reprocessing

processes control the inventory of weapons grade material acquired from Iranian reactors, the more kindly the US, Israel, and others feel towards whoever orchestrated that outcome. Indeed, this is the outcome preferred [17] by the US and at least five other westernized nations.

Whoever did it first, the demonstration effect [18] is already spreading. Despite its complexity, governments, computer industry experts, and cybercrime ateliers are now trying to see if they can re-engineer something like Stuxnet for whatever purpose they have in mind. The original programmers are still out there, able to do it or something like it again, probably for a healthy price that presumably has just gone up. And there will be buyers of such products across nations and non-state actors. As they buy and deploy, there will also be considerable national institutional changes in response – likely institutional trends across nations that are developing as part of the emerging cybered conflict age will be the subject of the next set of blogs.

Chris Demchak is an Associate Professor at the US Naval War College and at the University of Arizona. The views expressed are her own and do not reflect those of the Navy or the U.S. government. This article is the fourth in a series titled **Cybered Conflict** [19]. .

Trackback URL for this post:

http://www.acus.org/trackback/26125

Cyber Security Cyber Threats Cybered Conflict International Security Nuclear Weapons Russia

Source URL: http://www.acus.org/new_atlanticist/stuxnet-all-signs-point-russia

Links:
[1] http://www.acus.org/content/digital-mindjpg
[2] http://www.computerworld.com/s/article/9188018/Iran_confirms_massive_Stuxnet_infection_of_industrial_systems?source=richi
[3] http://www.symantec.com/connect/blogs/stuxnet-breakthrough
[4] http://www.computerworld.com/s/article/print/9186920/Was_Stuxnet_built_to_attack_Iran_s_nuclear_program_?taxonomyName=IT in Government&taxonomyId=13
[5] http://www.france24.com/en/20100927-stuxnet-worm-rampaging-through-iran-it-official
[6] http://www.computerworld.com/s/article/9186920/Was_Stuxnet_built_to_attack_Iran_s_nuclear_program_?source=richi
[7] http://warsclerotic.wordpress.com/2010/10/07/the-story-behind-the-stuxnet-virus-forbes-com/
[8] http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf
[9] http://www.cio.com/article/492317/As_Hacking_Hits_Home_China_Strengthens_Cyber_Laws
[10] http://www.zdnet.com/news/stuxnet-worm-strike-iranian-nuclear-plant/468939
[11] http://www.telegraph.co.uk/news/worldnews/1583682/China-reveals-Irans-nuclear-secrets-to-UN.html
[12] http://www.eweekeurope.co.uk/news/news-security/russian-police-and-internet-registry-accused-of-aiding-cybercrime-2164
[13] http://www.csmonitor.com/2007/0717/p01s04-woeu.html
[14] http://www.thebulletin.org/print/web-edition/columnists/pavel-podvig/behind-russia-and-irans-nuclear-reactor-dispute
[15] http://www.nytimes.com/2010/10/27/world/middleeast/27nuke.html?scp=1&sq=Iran UN Russia spent fuel&st=cse
[16] http://www.acus.org/new_atlanticist/stuxnet-first-physical-weapon-cybered-conflict-age
[17] http://www.france24.com/en/print/5087058?print=now
[18] http://www.cnn.com/2010/TECH/web/11/17/stuxnet.virus/index.html?iref=NS1
[19] http://www.acus.org/tags/cybered-conflict