

Did Hackers Take Russian Nuclear Sites Offline?

by Don Jackson
May 27, 2008

On May 20 and 21, 2008, some Russian blogs posted false reports of planned evacuations from the city of Sosnovy Bor due to a radiation leak at the Leningrad nuclear power plant¹ near St. Petersburg in northwestern Russia. That plant is the only one in Russia not officially operated by Rosenergoatom, the power generation division of the state-owned nuclear company, Rosatom. Technically, the Leningrad plant is a separate facility; however, Rosatom is closely involved in the plant's operation and controls its public relations functions.

In Russia today, the public has access to real-time readouts from large networks of radiation monitoring devices installed around each of Russia's nuclear facilities. This data is provided via public websites via ASKRO. ASKRO, or Automatic Radiation Environment Control System, is part of an "environment and sanitary control system" which is responsible for informing the public on radiation security (leaks, etc.).

When people concerned by the false reports attempted to access the ASKRO data, the service was unavailable. This prompted rumors of a cover-up.

In replies posted to the hoax reports, some people said they were going to start taking iodine and urged others in the area to do so as well. After similar unsubstantiated reports of a problem at the Volgodonsk nuclear power plant last year, several dozen individuals fell ill from iodine poisoning after ingesting large doses in attempts to counteract possible radiation damage. Greenpeace posted a related news article saying that any incident at the Leningrad plant was unconfirmed, and reminded readers to avoid iodine poisoning.² However, some people took the dosing schedule and the link to a Greenpeace memo regarding what to do in the event of a nuclear emergency³ as signs that Greenpeace endorsed starting an preventative iodine regimen.

On May 21, Sergey Komarov, Deputy Director of the Institute for Regional Energy Development for Rosatom, denied any cover-up, saying that "Russia is not the USSR".⁴ This is an allusion to the partial reactor core meltdown of Unit Number 1 in December 1975, which leaked radiation into the Gulf of Finland for more than a month. With help from the KGB, that accident was suppressed by the Soviet government until after the collapse of the Soviet Union.⁵ Komarov also said that the false reports were "one more stupid provocation" and that "if somebody likes poisoning himself with iodine, it's his own problem."

On May 22, Mikhail Grishankov, First Vice Chairman of the Duma Security Committee, said the rumors were "one of the methods of information war."⁶ He stated that the rumors are an attempt to discredit the Russian nuclear energy program.

By May 23, RIA Novosti, the respected Russian News and Information Agency, quoted an unnamed Rosatom spokesperson as saying that the websites hosting the ASKRO monitoring data — including the official site of the plant⁷ and the main Rosatom web site⁸ — were unavailable because of a coordinated denial-of-service (DoS) attack orchestrated by hackers and timed to coincide with the false reports.⁹ The official said that because of the cyber attack, users were unable to obtain reliable information from ASKRO regarding the true situation at the plant for several hours, adding that access to the ASKRO data had now been fully restored.

On May 24, less than four days after the Leningrad plant rumors, Rosatom Press Secretary Sergei Novikov addressed a new wave of reports regarding the Ignalina nuclear power plant in Lithuania, denying their validity. Novikov said the reports were similar to the Leningrad NPP reports in that they originated in the "blogosphere" and were part of a disinformation campaign which also employed SMS

(text messaging), ICQ (a popular on-line chat service), and even social engineering phone calls.¹⁰ Russian officials said such deliberate campaigns may be criminal and will be investigated.

While these campaigns made use of technology, there is still no evidence of the reported cyber attack on the ASKRO system and no signs of the hackers behind it. The news of a coordinated DoS cyber attack by hackers was quickly picked up and reported by several intelligence agencies, including one highly regarded private (non-government) intelligence firm. Some may have misinterpreted Grishankov's comments about "information war" in the context of what appeared to be a denial-of-service condition at some related websites. No one has come forward with any information on the attack — no traffic patterns, no IP addresses, etc. — and unlike many hacktivism attacks, no evidence of any plan for a cyber attack on the affected websites — aspirational or operational — was found on any hacker or activist websites monitored by intelligence services.

One Russian cyber defender who works for a respected security tools provider proposes an alternative explanation. The Leningrad plant has a history of incidents. In addition to the partial meltdown covered up by the Soviet government, the plant experienced a major nuclear leak in March 1992¹¹ and a non-nuclear explosion in December 2005.¹² Just days before the rumors surfaced, Unit Number 3 at the Leningrad plant suffered an emergency shutdown;¹³ however, radiation levels reported by the 23 ASKRO dosimetry monitors in the 30 km zone around the plant remained normal.¹⁴ Possibly, because of the plant's history and a perceived correlation between the emergency shutdown and the later reports of increased radiation levels, many more people than normal rushed to the sites which relied in the ASKRO data, resulting in a common denial-of-service condition under benign but higher-than-normal load. That is, it was entirely unintentional, and the highly coordinated hackers are, in reality, just a lot of concerned Russian citizens.

However, the coordinated disinformation campaign does appear to be real. Russian officials blame those that want to disrupt the success of the Russian nuclear power initiatives. Some suggest that it could be anti-nuclear activist groups or industrial rivals for a bid to build a new nuclear power plant in the Kaliningrad region by 2015, saying that others are carrying out a "secret war on fair competition." The Russian officials say it will be difficult to track down those responsible, but they say they are committed to doing just that.

¹also referred to as Leningrad NPP, Russian: Ленинградская атомная электростанция (literally, Leningrad Atomic Energy Plant), Ленинградская АЭС, acronym: ЛАЭС, also transliterated as SELA or LAES

² <http://www.greenpeace.org/russia/ru/news/2030102>

³ <http://www.greenpeace.org/russia/ru/news/2030102/2030120>

⁴ http://www.rosatom.com/en/comments/10127_21.05.2008

⁵ <http://www.decomatom.org.ru/?q=node/19>

⁶ http://www.rosatom.com/en/comments/10126_22.05.2008

⁷ <http://lennpp.rosenergoatom.ru/>

⁸ <http://rosatom.ru/>

⁹ <http://en.rian.ru/russia/20080523/108202288.html>

¹⁰ http://www.rosatom.ru/news/10156_24.05.2008

¹¹ http://www.insc.anl.gov/neisb/neisb5/3d_sb.pdf (p. 50)

¹² <http://www.foxnews.com/story/0,2933,178896,00.html>

¹³ <http://www.rosenergoatom.ru/eng/press/news/article/?article-id=8A11C9E6-1AEB-48F4-AB44-173136C7A58B>

¹⁴ <http://www.laes.ru/danora.shtml>

Copyright © 2008 Don Jackson. This document can be freely copied and distributed as long as it includes this copyright statement.