North Korea's Asymmetric Attack on South Korea's Nuclear Power Plants

Jesse Min
February 11, 2017

Submitted as coursework for PH241, Stanford University, Winter 2017

Introduction

Physical or conventional terrorism against nuclear facilities (See Fig 1) around the world had long been an issue. Stringent regulations and security measures have been imposed on nuclear power plants including the Energy Policy Act of 2005, which articulated security measures for nuclear facilities and materials in detail. [1] However, as nuclear facilities become more digitalized and automated, the number of cyber threats against nuclear plants has been growing. [2] In particular, the Republic of Korea, which is bordering North Korea, has focused on the defense and surveillance of North Korea's physical nuclear weapons since the Korean War. Nonetheless, recently, rather than using the physical nuclear weapons to threaten South Korea, North Korea has frequently used its asymmetric power to attack South Korea's nuclear facilities. One of such asymmetric attacks is North Korea's cyber attack against South Korea's civil nuclear power plants.

Fig. 1: Nuclear Power Plant (Source: Wikimedia Commons)

Hacking of Korea Hydro & Nuclear Power Co.

On December 23, 2014, Korea Hydro & Nuclear Power (or KHNP) formally announced that its computer systems had been hacked. The group that hacked KHNP's server gained access to some plant computers and released stolen blueprints of nuclear reactor, details on various support systems, and personal data on over 10,000 employees. The hackers also posted on their Twitter stating that "Unless you stop operating the nuclear power plants until Christmas and give us $10 billion, we will continue to release the secret data related to the facility." According to the investigation report from the South Korean government, the North Korean hackers sent the emails with "Kimsuky" malware (a type of malware known to be frequently used by North Korean hackers) planted to 3,571 KHNP employers using IP address located in China and Russia. [3]

Loophole in Cyber Security

Most of the files such as the blueprints of facilities were not leaked directly from KHNP internal intranet network, but through phishing emails sent to employees of third-party partners of KHNP. [3,4] In detail, the hackers sent the phishing emails, such as "Your password was leaked. Please read this email." to retired workers of KHNP and employees of subsidiaries of KHNP. When such mail was clicked, a password change window appeared and the user was prompted to input the password. In other words, instead of directly targeting a loophole in the server of nuclear power plant, the hackers targeted the related groups such as affiliates and retired employees of KHNP to collect passwords and then publicized the data collected for several months from the e-mail accounts and social networks. It is noteworthy that the hackers executed an indirect cyber attack bypassing the robust firewalls by targeting weakness in third parties' network and in a format of modern hacking paradigm, "social hacking."

Future Countermeasures

First, there must be a well-synchronized, structured collaboration system for relevant agencies. As South Korea is in a temporary armistice with North Korea, South Korea should be aware that this cyber threat will not only be continued but in fact increase. Many different government branches in charge should not be bound by bureaucratic system and all relevant organizations such as National Intelligence Service, the National Police Agency, the Korea Communications Commission, KISA, and the Department of Defense should cooperate with each other to the highest standard to protect their citizens from North Korea's minacious cyber attack targeted toward civil nuclear plants. [5]

Also, a comparable or higher security measure should be imposed upon network and data used by subsidiaries, affiliates, and retired members of nuclear facilities as well. As shown in the KHNP incident, while it is usually almost impossible for hackers to directly attack intranet server of nuclear power plant covered with multiple firewalls and security programs, the hackers easily bypassed such security barriers by attacking the third-parties related to the facility management and were eventually able to retrieve some secret information from targets' social network accounts. This is an epitome of social hacking - exploiting people's extensive use of social network services - and a sly application of social hacking to attack secret facilities such as nuclear power plants protected by the utmost security.

References

[1] "Energy Policy Act of 2005," United States Pub. L. No. 109-58, 119 Stat. 594 (2005).

[2] B. Kesler, "The Vulnerability of Nuclear Facilities to Cyber Attack," Strategic Insights **10**, 15 (2011).

[3] "Intermediate Investigation Result of KHNP Cyber Terror Incident." National Joint Investigation Group on North Korea's Hacking Attack on KHNP, March 2015.

[4] J. S. Kwaak, "North Korea Blamed for Nuclear-Power Plant Hack," The Wall Street Journal, 17 Mar 15.

[5] N. Lee, *Counterterrorism and Cybersecurity: Total Information Awareness* (Springer, 2013), pp. 119-136.