INSS Insight No. 561, June 16, 2014

Iranian Cyber Espionage: A Troubling New Escalation

Gabi Siboni and Sami Kronenfeld

Anyone following the development of Iran's cyber capabilities is not surprised that Iran has slowly become a significant power in the cyber arena. Recently, a long term Iranian cyber espionage campaign in the United States was uncovered that made use of "social engineering" and phishing in order to gather information from important officials in the United States, Israel, Great Britain, and other countries. Even if the details revealed do not indicate Iranian use of advanced technology tools, they do show an evolving operational capability to carry out complex operations in cyberspace involving intelligence gathering and the use of an extensive and complex operational infrastructure.

The attack, dubbed "Newscaster," apparently began in 2011, around the time when the Stuxnet attack, intended to damage Iranian centrifuges, was exposed. The attackers collected intelligence and built personal profiles on social networking sites in order to create a complex and coordinated web of virtual identities with fictitious ties to media personalities, officials from the US administration and the military, diplomats, members of Congress, defense contractors, and others. They created detailed false social networking profiles on sites such as Facebook, LinkedIn, Twitter, and Google+ with credible and convincing covers and backgrounds. The attackers even set up a virtual system to support the background stories of the false personas, including a fictitious news website, NewsOnAir.org, where six of them ostensibly worked. The use of false personas is not new in the world of cyber espionage. However, the ability to create a set of false identities supported by a system of maintenance and management, in a way that can persuade the victims over time that the identity is real, shows that Iran has upgraded its operational capabilities in cyberspace.

Once these personas were created, the Iranians began to manage them and to make contact with officials whom they considered close to the administration and viewed as potential sources of valuable information. Among their targets were past and present government officials, journalists, think tank fellows, and defense industry figures. The attackers were patient and used sophisticated means of making contact and establishing trust with their targets, using the victims' social circles and effectively exploiting the various platforms provided by the social networks. The goal was to create sufficient trust

to allow them to send e-mails with malicious code. And in fact, once they succeeded in establishing this trust, they sent e-mails with code that installed itself on a victim's computer or directed the user to a fake page requiring private information so that this information would reach the attackers.

According to the information revealed, the attackers were able to create a network of more than 2,000 people, including hundreds of high quality targets. No mention was made of the type of information stolen or of which people and institutions fell into the trap. However, the general identity of the targets indicates that the attackers were seeking sensitive information concerning the defense technologies and military and diplomatic operations of the United States, Great Britain, Israel, and Saudi Arabia. The fact that they were seeking this type of information indicates that it was a political-diplomatic attack, not an attack by cyber criminals or classic industrial espionage.

The attack has been attributed to Iran on the basis of several pieces of evidence: the fake news website NewsOnAir.com is registered in Tehran, the servers the attackers used to activate the malicious code are hosted in Iran, Persian words were found in the code, and the times when the attackers were working match business hours in Iran. However, it is not clear whether the attack was carried out directly by the Iranian government, by a group connected to the government, or by private hackers who support the government or are working for it.

The attack is another step in the cyber warfare campaign being waged by Iran against its adversaries in the West and the Middle East. It is one of a number of high quality attacks attributed to Iran in recent years, including a large DDoS (distributed denial-of-service) attack on websites of major banks and financial institutions in the United States and a wave of attacks against control systems in American infrastructure and energy companies. However, the Newscaster attack shows the breadth and range of Iranian cyber operations. While previously, the attacks were high profile and focused on causing damage, the recently revealed attack is classic cyber espionage, conducted covertly over time.

The use of cyberspace for purposes of information gathering and monitoring is not foreign to Iran, which makes great use of phishing and social engineering to monitor the activities and opinions of Iranian citizens and to identify opponents of the regime and opposition activists. In June 2013, the time of the Iranian presidential elections, Google announced that it had identified and blocked a phishing attack carried out by elements within Iran that was directed against tens of thousands of e-mail accounts belonging to Iranian citizens. The attack involved e-mails, made to look like Gmail maintenance messages, which prompted users to enter their username and password. The information was passed directly to the attackers and gave them free access to the e-mail accounts.

However, the current attack is the first revelation that involves Iranian espionage in international cyberspace, where the main players today are Russian and China.

The recently revealed campaign is one of a long list of actions in cyberspace attributed to Iran designed to hurt the United States, Israel, and other Western countries. Although this latest campaign does not indicate a unique technological leap in Iranian cyber warfare capabilities, it does show a high level of operational and intelligence capabilities. It also indicates that Iran has cultivated long term cyber-related strategic objectives in recent years and that it is becoming one of the most active players in the international cyber warfare arena.