The Tower

Iranian Hackers Targeting U.S. Electrical Grid

by TheTower.org Staff | 12.21.15 12:19 pm

Iranian cyber-attackers have been targeting the U.S. electrical grid's networks and stealing highly sensitive data, an Associated Press investigation revealed on Monday.

Brian Wallace, a researcher at the cyber-security firm Cylance, discovered that critical files from Calpine Coroporation, which operates 82 power plants in 18 states and Canada, were stolen in a breach that began around August 2013 and may be ongoing. The information in those files included passwords, diagrams, and sensitive engineering designs of power plants, at least one of which was marked "Mission Critical." After analyzing circumstantial evidence, investigators concluded that the data was compromised by Iranian hackers.

Robert M. Lee, a former U.S. Air Force cyber-warfare operations officer, told AP that having this level of control could allow Iran to launch an attack on America's electrical infrastructure at any time. "If the geopolitical situation changes and Iran wants to target these facilities, if they have this kind of information it will make it a lot easier," he warned.

Cylance researchers determined that the stolen files were stored on unencrypted servers and embedded with code to spread malware, as well as software to mask the hackers' Iranian IP addresses.

Last December, Cylance found "bone-chilling evidence" that Iranian hackers had taken control over airports in three countries, including Pakistan. At the time, reports noted that the Taliban had previously launched an attack at a gate in Karachi's Jinnah International Airport that had been hacked by Iranians, though it is unclear whether the hacked information was used to facilitate the attack. Monday's AP report mentioned that Wallace determined that the hackers who targeted Calpine also carried out attacks against Pakistan International Airlines.

Col. (res.) Dr. **Gabi Siboni**, director of the Cyber Security Program at Israel's **Institute for National Security Studies**, warned earlier this year that the next 9/11-style terror attack would be perpetrated by hackers taking control of critical computer systems.

A recent increase of cyber-attacks against American government personnel is believed to be linked to the recent arrest of Iranian-American businessman Siamak Namazi in Tehran. Namazi's computer was confiscated by Iran's Revolutionary Guard Corps after he was detained. A scheme by Iranian hackers to get sensitive information from professionals in the defense and telecommunications industries using fake LinkedIn profiles was discovered and shut down in October.

Earlier this year, the U.S. recruited Israel and Great Britain to help fight growing cyber threats from Iran. An Israeli cyber-security firm identified a wave of Iranian-backed hacking attacks on Israeli, Saudi Arabian, and Yemeni targets in June. In August, it was reported that Iranian hacking attempts also targeted political dissidents.

In Iran Has Built an Army of Cyber-Proxies, which was published in the August 2015 issue of The Tower Magazine, Jordan Brunner warned that the risk posed by Iran's cyber-proxies should not be underestimated:

For the most part, the United States and its allies do not see these private cyber-actors as a real threat, certainly not on the level of nation-states like Iran, China, Russia, and North Korea. One reason appears to be that attacks from states like China are part of a global strategy, while proxies like those employed by Iran concentrate on local areas. A perfect example would be the case of the SEA, whose primary role is to stifle internal dissent. Even if cyber-actors like the SEA are able to reach beyond their borders and attack regional allies or the U.S. itself—as was the case with the SEA's attacks on American news organizations like the Associated Press, The New York Times, CNN, and even The Onion—the Obama administration tends to see these attacks as unsophisticated and "clearly a nuisance" rather than a serious threat.

But this ignores a problem that could turn deadly in certain circumstances. The idea that private cyber-actors are not a threat because they tend to be "local" in nature not only ignores the danger as "not our problem," but also ignores the fact that it could very quickly become our problem. Illicit cyber-activity in the Middle East causes instability, which harms U.S. interests. If the U.S. is drawn into a fight directly or through groups like the Syrian rebels, it could see itself devastated by attacks against its cyber-infrastructure, either at home or abroad. In addition, nations like China also use their cyber-capabilities to quell internal dissent. Yet China uses the same capabilities to strike the U.S. The two are not mutually exclusive.

http://www.thetower.org/2720-iranian-cyber-attackers-targeting-u-s-electrical-grid/