PHYS.ORG

Iran hackers penetrate key world networks: researchers

December 3 2014, by Rob Lever

Iranian hackers have managed to penetrate and steal information from governments and companies around the world since 2012, according to a new report by security firm Cylance

Iranian hackers have managed to penetrate and steal information from governments and companies around the world since 2012, posing a grave security threat, researchers say in a new report, The report by the security firm Cylance released Tuesday said the hackers have "extracted highly sensitive materials" from government agencies and major critical infrastructure companies in the united States, Britain, Canada, China, France, Germany, India, Israel, Kuwait, Mexico, Pakistan, Qatar, Saudi Arabia, South Korea, Turkey and the United Arab Emirates.

Cylance researchers called the effort "Operation Cleaver" and said it has "conducted a significant global surveillance and infiltration campaign."

The group is believed to work from Tehran, with help from others located in the Netherlands, Canada, and Britain, the report said

Targets include government networks as well as companies involved in military, oil and gas, energy and utilities, transportation, airlines, airports, hospitals, telecommunications, technology, education, aerospace and other sectors.

"During intense intelligence gathering over the last 24 months, we observed the technical capabilities of the Operation Cleaver team rapidly evolve faster than any previously observed Iranian effort," the report said.

"As Iran's cyber warfare capabilities continue to morph, the probability of an attack that could impact the physical world at a national or global level is rapidly increasing. Their capabilities have advanced beyond simple website defacements."

Retaliation for Stuxnet worm

The report said Iran appeared to ramped up its cyberwarfare capabilities after being hit by attacks including the Stuxnet worm, a program widely believed to be led by the United States or Israel, and which targeted its nuclear energy program.

"Stuxnet was an eye-opening event for Iranian authorities, exposing them to the world of physical destruction via electronic means," Cylance researchers said.

"Retaliation for Stuxnet began almost immediately in 2011."

Cylance said it has likely uncovered just "a fraction of Operation Cleaver's full scope" and added that "if the operation is left to continue unabated, it is only a matter of time before the world's physical safety is impacted by it."

Cylance said the effort is a "state-sponsored campaign" with the potential to affect airline safety, industrial systems and other critical networks.

"This campaign could be a way to demonstrate Iran's cyber capabilities for additional geopolitical leverage, due to the breadth and depth of their global targets," the report said.

It also said the hackers may be looking at collaborating with counterparts in North Korea to attack companies in South Korea. The group is also recruiting from universities in the United States and elsewhere and potentially using "hackers for hire."

"Perhaps the most bone-chilling evidence we collected in this campaign was the targeting and compromise of transportation networks and systems such as airlines and airports in South Korea, Saudi Arabia and Pakistan," the report said.

The infiltration mean "their entire remote access infrastructure and supply chain was under the control of the Cleaver team, allowing permanent persistence under compromised credentials."

This led to "complete access to airport gates and their security control systems," and a takeover of payment systems to allow fraudulent purchases.

The 86-page report says evidence of Iranian involvement is clear, with Persian hacker names used throughout the campaign and many domains used registered in Iran.

Citation: Iran hackers penetrate key world networks: researchers (2014, December 3) retrieved 24 April 2024 from https://phys.org/news/2014-12-iran-hackers-penetrate-key-world.html