PHYS ORG

Iran poses growing cyber threat to US

April 16 2015, by Dan De Luce

Iran poses a growing threat to America's computer networks and has launched increasingly sophisticated digital attacks and spying on US targets, according to a new report released on April 16, 2015

Iran poses a growing threat to America's computer networks and has launched increasingly sophisticated digital attacks and spying on US targets, according to a new report released Thursday.

Iran's far-reaching hacking efforts indicate the regime is searching for vulnerable infrastructure that could be hit in future cyber assaults, said the study by private cyber security company Norse and the American Enterprise Institute think tank.

"Iran is emerging as a significant cyber threat to the US and its allies," the study said.

Iran's skill in the cyber realm has markedly improved in recent years and "Iran has already penetrated well-defended networks in the US and Saudi Arabia and seized and destroyed sensitive data," it said.

The hacking, including espionage and attacks, has expanded despite economic sanctions and high-stakes negotiations between Iran and world powers on Tehran's nuclear program, it said.

The study cited data from a network of millions of sensors set up by Norse. The sensors are designed to look like real websites or other computer systems—for banks or power plants—that might attract the interest of a hacker.

The data showed Iran was staging cyber assaults and probes from inside Iran as well as outside the country.

Iranian state companies, including some with links to Iran's elite Revolutionary Guards, are allegedly hosting servers and other computer systems located in the West to carry out digital attacks, according to the report.

"Simply by registering and paying a fee, Iranian security services and ordinary citizens can gain access to advanced computer systems and software that the West has been trying to prevent them from getting at all," the study said.

The report argued that the hacking conducted outside Iran could be countered by Western companies that own the systems and software, denying access to Iranian organizations already blacklisted for rights violations or links to militants.

The study reflects warnings from US intelligence officials that Iran has made strides in its cyber capabilities, though China and Russia are considered the most skilled when it comes to digital warfare.

Hacking casinos, banks

National Intelligence Director James Clapper in February blamed Iran for a cyber attack on Sands Casino in Las Vegas that stole confidential data and shut down many of the casino's operations.

The assault came after the billionaire owner of Sands, Sheldon Adelson, said in 2013 that "Iran should be nuked."

US intelligence officials also believe Iran was behind denial of service attacks on major US commercial banks in 2011 and a damaging malware assault on Saudi Arabia's oil and gas company, Saudi Aramco, in 2012.

Iran's cyber prowess has grown since it suffered a devastating digital attack on its uranium enrichment plants in 2010.

The United States and Israel orchestrated that operation, which employed a computer worm dubbed "Stuxnet" introduced through an infected USB flash drive, according to reports from the New York Times.

Similar to the Stuxnet attack, Iran also has focused on SCADA systems, or supervisory control and data acquisition systems, that are used to manage industrial operations at factories or electrical grids, according to the study.

Sensors that emulate such SCADA systems "were probed several times in the course of our study's timeframe," over the past 13 months, it said.

"It seems clear that elements within Iran are working to build a database of vulnerable systems in the US, damage to which could cause severe harm to the US economy and citizens."

Under a framework nuclear agreement, international economic sanctions would be lifted on Iran. And the report's authors argue that removal of sanctions would allow Tehran to devote more resources to cyber warfare.

"Whatever the final outcome of the nuclear negotiations, we must expect that the threat of a cyber attack from Iran will continue to grow," the authors wrote.

Cyber security firms such as Norse often portray digital threats as numerous and increasing. But it was unclear if Norse would have an incentive to link hacking to any specific state.

Citation: Iran poses growing cyber threat to US (2015, April 16) retrieved 19 April 2024 from https://phys.org/news/2015-04-iran-poses-cyber-threat.html