Cyber experts warn Iranian hackers becoming more aggressive

Tue, May 13 2014

By Jim Finkle

WASHINGTON (Reuters) - Iranian hackers have become increasingly aggressive and sophisticated, moving from disrupting and defacing U.S. websites to engaging in cyber espionage, security experts say.

According to Silicon Valley-based cybersecurity company FireEye Inc (FEYE.O: Quote, Profile, Research, Stock Buzz), a group called the Ajax Security Team has become the first Iranian hacking group known to use custom-built malicious software to launch espionage campaigns.

Ajax is behind an ongoing series of attacks on U.S. defense companies and has also targeted Iranians who are trying to circumvent Tehran's Internet censorship efforts, FireEye said in a report to be published on Tuesday.

Many security experts have said that Iran is behind a series of denial-of-service attacks that have disrupted the online banking operations of major U.S. banks over the past few years.

"I've grown to fear a nation state that would never go toe-to-toe with us in conventional combat that now suddenly finds they can arrest our attention with cyber attacks," Michael Hayden, former director of the CIA and the National Security Agency, told the Reuters Cybersecurity Summit on Monday.

Security experts say Iranian hackers stepped up their campaigns against foreign targets in the wake of the Stuxnet attack on Tehran's nuclear program in 2010. The Stuxnet computer virus is widely believed to have been launched by the United States and prompted Iran to ramp up its own cyber programs.

According to FireEye, the Ajax Security Team was formed by hackers known as "HUrr!c4nE!" and "Cair3x," and began by defacing websites. The group became increasingly political after Stuxnet, FireEye researcher Nart Villeneuve said.

"This is a good example of a phenomenon that we are going to increasingly see with hacker groups in Iran. If their objective is to attack enemies of the revolution and further the government's objectives, then engaging in cyber espionage is going to have more impact than website defacements," he said.

In one recent campaign, the Ajax hackers infected computers of U.S. defense companies by sending emails and social media messages to attendees of the IEEE Aerospace Conference and directed them to a fake website called aeroconf2014.org, which was tainted with malicious software, FireEye said.

FireEye declined to name the companies that were targeted and said that it had not been able to determine what data might have been stolen.

The Ajax hackers used a malicious software dubbed "Stealer" that sought to collect data about compromised computers and record keystrokes, according to FireEye. It could also grab screen shots and steal information from web browsers and email accounts.

"Stealer" encrypted that data, temporarily stored it on compromised machines, then sent it to servers controlled by the hackers.

Using "Stealer," Ajax ran a separate operation that targeted people who were using software to try to circumvent Iran's system for censoring content, such as pornography and political opposition sites, FireEye said.

Villeneuve said FireEye had also uncovered evidence that Ajax engaged in credit card fraud, which suggests the hackers were not under the direct control of the Iranian government.

Leonard Moodispaw, chief executive of cybersecurity firm KEYW Corp (KEYW.O: Quote, Profile, Research, Stock Buzz), said that for now, Iranian hackers appeared to be increasingly spying and stealing money but not launching Stuxnet-like destructive attacks.

"They are more interested in IP and taking money than in shutting anybody down," Moodispaw told the Reuters summit. KEYW's biggest customers are U.S. intelligence agencies.

(Reporting by Jim Finkle; Additional reporting by Andrea Shalal, Mark Hosenball, Joseph Menn, Alina Selyukh and Warren Strobel; Editing by Tiffany Wu and Jim Loney)

(For other news from the Reuters Cybersecurity Summit, click on www.reuters.com/summit/Cyber14)