Sunday, 19 May 2013

Middle East in spotlight amid escalating cyber attacks

The Middle East has become a hotspot for cyber attacks, experts warn, amid an escalation of computer-led warfare across the globe.

Dmitri Alperovitch, co-founder of Crowdstrike, a security technology specialist firm, told last week's Reuters Cybersecurity Summit in Washington that he is most concerned about cyber attacks linked to Iran, particularly if there is a spike in tensions in the Middle East.

He said that there is a worry that hackers from unspecified countries could destroy or modify crucial financial data in the United States, following attacks on more than a dozen U.S. banks in the past nine months.

"Attacks that focus on modifying data in the stealth way, sabotage, integrity attacks - those are the ones that are most insidious and those are the ones we really should worry about," Alperovitch said, according to Reuters.

So-called 'cyber wars' in the Middle East have been escalating in recent years.

In 2009, a computer worm dubbed Stuxnet attacked Iran’s nuclear facilities, aimed at harming Iran’s uranium–enrichment program.

The source of that attack was never officially identified, but the U.S. or Israel, or both, are believed to be behind it, according to the New York Times.

Stuxnet may have had the potential to seriously damage Iranian targets, but the worm was “neither effective nor well-timed and, in hindsight, may have been of net benefit to Tehran,” said a report by the Royal United Services Institute (RUSI), an independent organization engaged in defense and security research.

The report claimed that the attack notified Iran of flaws in its security facilities, which may otherwise have gone unnoticed.

More recently, the Saudi Press Agency (SPA) reported last Friday that a series of Saudi governmental websites, including that of the Interior Ministry, were “exposed to several coordinated and simultaneous cyber-attacks over the past few days.”

The Interior Ministry’s website crashed on Wednesday after receiving a huge amount of service requests, an unnamed official source at the National Centre of the Electronic Security at the Ministry of Interior told SPA.

The cyber-attacks targeted four ministries: the Ministry of Interior, Ministry of Foreign Affairs, Ministry of Finance, and the Ministry of Labor, Mansour al-Turki, spokesman of the Ministry of Interior in Saudi Arabia told al-Watan newspaper.

The attack was traced back to hundreds of international addresses, added al-Turki. However, he refused to name any countries “due to lack of evidence” on whether the attacks were related to the respective states.

In August 2012, another cyber-attack targeted Aramco, Saudi’s national oil and natural gas company, and a main source of income to the kingdom. The virus infected 30,000 of its workstations. The company's website had to be taken off for a few days as a result of the attacks, reported Reuters.

In February, $45 million was stolen from Muscat Bank and RAK Bank. Investigations later revealed that this was a global cyber-heist involving a number of offenders in over 27 countries.

The frequent cyber-attacks in the Middle East come at a time of escalating activity globally, experts say.

National Security Agency director Keith Alexander, the top U.S. general in charge of cybersecurity, warned that attacks on his country are set to worsen.

"Disruptive and destructive attacks on our country will get worse," he told the Cybersecurity Summit, Reuters reported. "Mark my words, it will get worse."

Janet Napolitano, the U.S. Secretary of Homeland Security, told the Reuters Cyber Security Summit that the "known unknown" threats are of most concern to the United States.

“We don't have the identity of all the adversaries who are trying to either commit crimes or acts over the cyber networks. The things we know about, we can deal with. It's the known unknown,” Napolitano said, according to Reuters.

Other recent cyber attacks have targeted key social media accounts belonging to the likes of the Financial Times and Associated Press.