Iran: Cyber Attack on U.S. Banks Part of Covert War (9/24/12)

Summary

Recent cyber attacks against the websites of JP Morgan Chase (NYSE: JPM), Bank of America (NYSE: BAC), and Citigroup (NYSE: C) probably are a sign of increased capabilities of Iran's so- called 'cyber army' and indicate that Tehran is escalating its covert war against America and its Western allies.

The recent denial of service attacks against financial institutions, reportedly carried out by Iran, could be the latest instances of American adversaries – including China and North Korea – engaging in difficult-to-detect cyber attacks against the United States and its allies. If Iran was behind the attacks against the bank websites, it would reflect an increasing Iranian cyber warfare capability to target Western commerce as well as to steal industrial and government secrets.

Background

The new cyber attacks are part of a growing threat to government and corporate websites. U.S Secretary of Defense Leon Panetta said in Senate testimony last June these threats are growing so serious that the United States could be hit by a "cyber Pearl Harbor." General Keith Alexander, who heads the Pentagon's new Cyber Command, warned at an American Enterprise Institute conference in July that on a 1-to-10 scale, American readiness for a major cyberattack is "around a 3."

On September 18, Bank of America and JP Morgan's websites experienced technical difficulties that prevented customers from accessing the sites. The problems experienced at both banks continued for another day before being mostly resolved.

Both banks reportedly were targeted by denial-of-service attacks. Denial-of-service attacks overwhelm websites, rendering them inaccessible to legitimate users. A denial-of-service attack is similar to calling a landline telephone simultaneously from multiple phones until there is a busy signal. By overwhelming a website with user calls or requests, the servers hosting the target website become inundated with traffic to such an extent that it overloads and collapses – effectively achieving a busy signal.

A group of self-proclaimed Middle Eastern hackers claimed responsibility for the cyber attacks in an internet forum. The hackers justified their actions by claiming it was in response to an anti- Mohammed YouTube video that has sparked anti-American protests in Muslim countries over the last two weeks.

A U.S. official stated that the attacks were "significant and ongoing" and that the purpose of the attacks was squarely targeted at achieving "functional and significant damage" at Citigroup and Bank of America, according to NBC.

However, there are strong indications that the recent cyber attacks were not a stunt by a group of amateurish hackers but a state-sponsored attack by Iran. On September 21, Chairman of the Senate Homeland Security and Governmental Affairs Committee Senator Joseph Lieberman stated, "I don't believe these were just hackers who were skilled enough to cause disruption of the websites . . . I think this was done by Iran and the Quds Force, which has its own developing cyber attack capability."

Lieberman, who receives regular classified briefings from the U.S. Intelligence Community, stipulated that he believes the cyber attacks were carried out by Iran although intelligence analysts have not formally concluded this. Lieberman said, "I don't want to put it forward as a conclusion of the intelligence community yet . . . there's more than just theory; there's some basis for believing this was an Iranian sponsored attack."

Lieberman's claims are consistent with what former CIA Director Michael Hayden told LIGNET in an April 2012 interview that Iran is recruiting a hacker army to target the U.S. power grid, water systems and other vital infrastructure. Hayden said it is not the cyber talent that Iranian officials are amassing that worries him. He is more concerned about the enormous vulnerability of U.S. computer systems that makes such attacks possible.

Senator Lieberman also said he believed the recent cyber attacks were in response to increased pressure from international sanctions against Iran, noting that "it's a warning to us that if we take action against their nuclear weapons development program that they have the capacity to strike back at us."

NBC cited unnamed U.S. national security officials last week who also said Iran was behind denial of service attacks on the bank websites.

Iran denied responsibility for the cyber attacks.

Analysis

If Iran was behind the denial-of service attacks on Western banks, it was probably a sign of a continuing escalation of Iran's covert war against the West largely in response to increased sanctions. This covert war has included increased support for terrorism, a plot to assassinate the Saudi ambassador to the United States last fall, and almost a dozen failed plots over the last year to kill American, British, and Israeli diplomats in several countries.

U.S. defense officials reportedly have concluded that Iran has added cyber warfare to the arsenal of covert weapons and tactics it is using against the West. National security journalist Bill Gertz said in a September 18 Washington Free Beacon article that a recent classified Pentagon briefing concluded that "Iran's cyber aggression should be viewed as a component, alongside efforts like support for terrorism, to the larger covert war Tehran is waging against the West."

Recent cyber attacks on Western banks may reflect advances in the capabilities of Iran's cyber command which has been described as a cyber army to both defend the country from cyber attacks and to engage in cyber warfare against the country's adversaries. Iran's offensive cyber capabilities reportedly include disrupting commerce, sabotaging critical infrastructures such as power grids, and stealing government and industrial secrets.

To read more about Iran's 'cyber army,' see LIGNET's May 18, 2012 analysis, Iran is Leading Threat to U.S. Power Grid.

Conclusion

While no serious damage reportedly was done by the recent denial-of-service attack on Western bank websites, they probably indicate the increasing capabilities of Iran's 'cyber army' to conduct cyber warfare against the West and could be retaliation for increased Western sanctions. Cyber warfare by Iran and other rogue states are likely to continue and could inflict damage on Western commerce because of the vulnerability of corporate websites to hackers.