ESISC EUROPEAN STRATEGIC INTELLIGENCE AND SECURITY CENTER

BRIEFING 06/08/2013

WHAT IS THE REAL THREAT POSED BY “JIHADIST HACKERS”?

By Ludovic Terren, Research Intern

Latest reports on cyber incidents highlight the increasing prevalence of what we can call “Jihadist hacking”, meaning that states will need to “rearm” themselves and make determinant choices in the face of this slowly but surely growing cyber threat.

Indeed, as the contemporary world is increasingly reliant on Information Technology (IT) based systems, the threat posed by ‘Jihadist hackers’ is of an ever-increasing relevance. The ability of Islamist terrorists to turn the vulnerabilities of information systems to their advantage in order to strike their opponents has given rise to this relatively new concept of ‘cyber-Jihadism’, which can be summarized as the struggle for Islamic fundamentalism by Jihadist hackers.

Over the last years the term ‘cyber Jihadism’ has become extremely popular in the media. It means the use of internet by Islamist activists for organization purposes such as fundraising, planning meetings or coordinating attacks. Here we operate with the term ‘Jihadist hackers’ (Jihadist hacking) that should be understood as an act undertaken by Islamist hackers or groups of hackers who attack (mostly western interests) exclusively by operating through the internet. These attacks can take multiple forms such as denial of services, defacing of government or financial institutions’ websites, disrupting government systems, among many others.

It is also important to differentiate between hacking for money purposes in order to raise funds before undertaking a ‘real-life’ terrorist attack and hacking as the terrorist act in itself, in which Jihadist hackers aim at destabilizing various political or financial infrastructures in the name of Jihad, as opposed to what is usually understood by a ‘terrorist act’, namely the killing of (innocent) people or the material destruction of various strategic sites.

To place this phenomenon in current affairs, we can name a few cyber attacks that were undertaken and threats that were sent in the last few months by some of whom we can call ‘Jihadist hackers’.

- During the first week of July 2013, ESISC reported that several media outlets had turned their attention to a Jihadist hacker based in Mauritania who calls himself "Mauritania Attacker", and who is the coordinator of a considerably active group of hackers ("AnonGhost") from across the Maghreb, Southeast Asia and even the West. They claim to be fighting for the dignity of Muslims worldwide and promoting "correct Islam" by targeting servers hosted by countries they consider as hostile to Shariah Law.

For example, in April 2013, the group launched a cyber attack (named 'OpIsrael') that blocked access to several Israeli websites. The online archive of hacked websites 'Hack DB' shows more than 10,400 domains that "AnonGhost" has allegedly disfigured in the past seven months, making them one of the most active hacker collectives in 2013, according to the Cyber Defense Magazine.

- In March 2013, a group called "The Cyber-army of al-Qaeda" or "al-Qaeda Electronic Army" stated on several Jihadist websites that it was planning a massive 'cyber campaign' against U.S. financial and governmental websites for the summer of 2013. As the group appealed to all Muslim hackers to join their campaign through social media, a Tunisian hacker collective called "The Tunisian cyber-army" said it would participate. During the same month, both groups of hackers claimed responsibility for cyber attacks on U.S. customs and border protection website.
Yet, as late as August 2013, despite the fact that these threats do not seem to have been fully translated into action, the latest attacks on U.S. customs and border protection websites should remind us to stay cautious.

Other influential and currently active groups that have carried out "Jihadist-oriented" cyber attacks include:

"TeaMp0isoN", which was created by Junaid Hussain alias "TriCk" fights for the liberation of Muslims in Palestine, Kashmir and other conflict-prone Muslim-majority regions. Between 2010 and 2012, they targeted NATO, as well as various UK and US government agencies, such as the UK's Anti-terrorism hotline. During this attack - which lasted for two days – Hussain ("TriCk") was able to eavesdrop on confidential phone conversations between UK counterterrorism and law enforcement officials. The recordings ended up on Youtube, fully available to other activists and terrorist organizations that could use the information for counterintelligence purposes.

Similar Jihadist hacker collectives emerged around this last group: "ZCompany Hacking Crew" (ZHC) was created in 2010 and claim to be fighting against injustice, Zionism and illegal occupation. They have been involved in credit card thefts by accessing data from servers based in the U.S., UK and Australia.

"TeaMp0isoN" and "ZCompany Hacking Crew" have been affiliated with other Jihadist hacking groups such as the "Mujahideen Hacking Unit" (MHU) or the "Muslim Liberation Army" (MLA) who carried out low-level websites' defacements in the name of Jihad.

Another influent cyber-Jihadist is "0xOmar", a Saudi hacker who conducted high-profile attacks on the Israeli national airline, the Tel Aviv Stock Exchange and the websites of three Israeli banks. One day after these widely broadcast cyber attacks, a prominent Kuwaiti Imam (Dr. Tariq al-Suwaidan) posted on his Twitter account (followed by 240,000) to "unite behind Muslim hackers in their endeavor of electronic Jihad against the Zionist enemy".

Al-Qaeda also showed its support for Jihadism in the web in several statements and videos in which they called for more cyber attacks in the name of Jihad against the United States. In one of these statements, they compared the flaws present in vital American computer networks to the vulnerabilities of American aviation security prior to the 9/11 terrorist attacks.

According to the 2013 U.S. Worldwide Threat Assessment, whereas the likelihood of a large-scale cyber attack on a U.S. critical infrastructure will be low in the next two years, one should not underestimate the potential destructiveness of cyber-Jihadism and the possibility of major cyber attacks in the future.

Although hacking in the name of Islam has lately been on the rise and has a considerable potential for proliferation through the creation of increasing numbers of obscure and hardly controllable or localizable groups, the real threat that it represents remains relatively low when it comes to the hypothesis of major attacks which could successfully target critical western infrastructures, leaving them on a long-term standstill. This is partly due to a lack of organization and technical capabilities on the side of these rather loose groups of hackers as well as ones operating individually.

However, a look at the jihadist hacking attacks in the last one or two years suggests a progressive refinement of their modus operandi coupled with an increasing ambition from young Jihadists who see cyber warfare as a new, efficient and relatively easy way to fight for propaganda of radical Islam worldwide.

END.