ESISC EUROPEAN STRATEGIC INTELLIGENCE AND SECURITY CENTER

BRIEFING 26/10/2015

CYBER-JIHAD IS BECOMING A PRIORITY FOR ISLAMIC STATE

By Mohammed Fahmi,
research intern

The series of hacking attacks against US and British interests on September 11 and 12, as well as a series of hacking campaigns in October against Israeli interests, carried out by the new IS cyber unit, the Islamic Cyber Army, indicates that Islamic State pays increasing attention to cyber-jihad and in integrating hacking divisions in its organizational structure.

To recall, Islamic State announced the creation of its new cyber division on September 7, ahead of the anniversary of the 9/11 terrorist attack. In its first statement, the Islamic Cyber Army claimed that "jihadists did not forget the September 11 attack and your war against Islam" and urged to launch a wave of large-scale hacking attacks against the US on the same date in 2015, using a hacking model, developed by the group. A series of hackings, which were organized by members of the group, demonstrated that IS is increasing its competence in cyber warfare and its ability to launch future hacking campaigns should not be underestimated.

Such type of attacks, while failing to cause any important damage, still produces a significant media effect and is often timed to commemorate the anniversary of some major terrorist attacks. For example, similar cyber campaigns could be launched by IS against France on January 7-8, in commemoration of the Charlie Hebdo and Kosher supermarket shootings.

Such new trend in IS strategy triggered important security concerns by IT and terrorism experts and caused numerous speculations in media. The British newspaper The Mirror reported on September 12 that "An investigation by the intelligence agencies has discovered that extremists linked to ISIS have been targeting information held by some of David Cameron's most senior ministers, including Theresa May, the Home Secretary." This information proves that IS may be trying to intercept top secret intelligence and use it for its own agenda. Meanwhile, till the present moment numerous hacking attacks, claimed by IS supporters, failed to cause any real damage or data leakage.

The increasing propaganda on cyber-jihad and the developments of tools and guidelines that would facilitate such attacks clearly demonstrate that the scale and impact of such IS-inspired cyber attacks risk to rise in the nearest future.

Today, the Islamic Cyber Army is allegedly composed of 9 members, identified as Abu Hudheifa al-Sinawi, aka "Abo-7ozyfa", Abu al-Qasam al-Misri, aka "Abu al-Qasam", while the others are identified only by their nicknames: Dr. ISIS, Eng ISIS, SKWO 808, Hacker Aldmar, Cyber, Hcer Arkan and the alleged leader of the hacker terrorist group, Syria Virus. The unit is still too small to have a real impact on worldwide cyber security. In addition, their accounts on Twitter are most of time suspended despite their claim of having over 47,000 backup accounts. Meanwhile, as in the past months, Islamic State regularly issues propaganda documents, calling IT specialists to join the terrorist group.

Despite its lack of power, the IS cyber units began to gain experience long before the creation of the Islamic Cyber Army. It was the case of the Cyber Caliphate that is now a division of the Islamic Cyber Army. The Cyber Caliphate was established by Junaid Hussain, a young British hacker called Abu Hussain al-Britani. On December 24, 2014, the group hacked its first target, a Mexican newspaper called Albuquerque journal. A few months later, the group launched 7 hacking operations in order to promote IS propaganda. Cyber Caliphate hacked the Malaysia Airlines website on January 26, 2015; the WBOV-TV16 American website on February 10, 2015; and the French TV channel "TV5 monde" on April 2015. With hackers of Cyber Caliphate joining the Islamic Cyber Army, the members of this new cyber unit are thus not novices.

Moreover, the adhesion of the Cyber Caliphate to the Islamic Cyber Army proves that IS succeeded in gathering pro-IS hackers under one umbrella cyber organization and constantly increases its membership. At the same time, we should remain skeptical regarding the potential threats to business and governmental websites that can be caused by hacking attacks of IS cyber units. As de-facto the Islamic Cyber Army so far is represented only by a group of pro-IS activists, their competency and number are not high enough to be able to intercept intelligence reports or to cause operational damage to industrial sites.

Since its establishment, Islamic State has become a sort of "trendsetter" for international terrorist networks, bringing online propaganda on a new level. It is thus not surprising that today the group became a pioneer of the idea of "cyber jihad" as a new way of attacking Western interests. Similarly to IS-inspired lone wolf attacks, such cyber attacks can be perpetrated by individuals or groups that have no physical, direct links with the international terrorist network. As in the case with real lone wolf terrorists, the prevention of "lone wolf cyber hacking" is very complicated, while the significant media effect of these hackings risks to trigger a chain reaction among radical Islamist IT specialists, provoking further copycats against Western interests across the world.

FIN