UNCLASSIFIED



Executive Cyber Intelligence Bi-Weekly Report by INSS-CSFI

June 1st, 2015

This document was prepared by The Institute for National Security Studies (INSS) – Israel and The Cyber Security Forum Initiative (CSFI) – USA to create better cyber situational awareness (Cyber SA) of the nature and scope of threats and hazards to national security worldwide in the domains of cyberspace and open source intelligence. It is provided to Federal, State, Local, Tribal, Territorial and private sector officials to aid in the identification and development of appropriate actions, priorities, and follow-on measures. This product may contain US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Some content may be copyrighted. These materials, including copyrighted materials, are intended for "fair use" as permitted under Title 17, Section 107 of the United States Code ("The Copyright Law"). Use of copyrighted material for unauthorized purposes requires permission from the copyright owner. Any feedback regarding this report or requests for changes to the distribution list should be directed to the Open Source Enterprise via unclassified e-mail at: dcoi@inss.org.il.

CSFI and the INSS would like to thank the Cyber Intelligence Analysts who worked on collecting and summarizing this report.

ISRAEL

Cyber-attack threat against Israel from Lebanon

Lebanon's hackers threatened to lunch a cyber-attack on Israel on 25/05/15 in order to mark the 15th anniversary of the IDF's withdrawal from Lebanon. The hackers published a picture of Imad Mughniyah, a Hezbollah commander who was allegedly eliminated by Israel, and wrote under the picture in Hebrew and Arabic: "The day of judgment… coming." According to the announcement, the attack was supposed to be in in memory of "The Shahid's (those who died in the name of Allah) that sacrificed their lives in honor and pride." Despite the threats, no actual attacks were reported.

Israel vulnerable to cyber-attack

A recent survey shows that approximately 60% of the companies in Israel are not prepared for cyber-attacks. The survey reveals that almost half of the managers who participated reported that their organization was under a cyber-attack at least once in the last 3 years. About 200 managers have answered the survey, and its findings point to the chaos that exists in Israel regarding the cyber security area. This chaos is due to the lack of state guidance for the civil market, unlike the situation in the security companies.

USA

Penn College of Engineering is a target for cyber-attacks

Officials from Pen State College of Engineering announced the University was under two cyber-attacks, at least one originating from China. The FireEye cybersecurity forensic unit Mandiant who was hired by the university shortly after the breach was discovered confirmed the hackers are a Chinese group, associated with the Chinese government. The attack, as investigated and announced by the Mandiant group, used a sophisticated malware to breach the university's firewall and other security means. University officials claim no personal data, such as social security numbers, has been taken in the attack; however, usernames and passwords have been stolen in the breach. About 18,000 people had their information stored with the university and were affected by attack.

RUSSIA

New Internet state segment for Russian Federation

Russian President Vladimir Putin signed a decree "On some issues of information security of the Russian Federation," the main idea of which involves the formation of the state segment of the Internet. According to the document published on the official website of legal information of the State, the segment of the Internet under the jurisdiction of the Federal Security Service (FSS), is to be transformed into the Russian state network segment. A number of government agencies will be required to post information on the Internet only through the government segment. In particular, this requirement applies to the Russian Presidential Administration, Government of Russia, executive authorities, executive bodies, and subjects of the Russian Federation. According to the decision, all of these structures must connect

their information systems and networks to the state Internet segment until 31 December 2017.

ARAB COUNTRIES

Islamic State threatened to launch large cyber-attack against US critical infrastructure

A week and a half ago, an incognito, hooded male, who affiliated himself with ISIS, threatened to wage an all-out cyber-war against US and European critical infrastructure. While it is most certainly safe to say that so far ISIS has not shown a significant cyber ability, a concern from the threat of an all-out cyber war is being treated with the appropriate seriousness. Experts, both civilian and military/federal, have not taken the threat lightlys. James Comey, the director of the FBI, has said in a conference at the Cybersecurity Law Institute at Georgetown University that ISIS is looking into the cyber field to see if it has the ability to do so. Civilian cyber experts say ISIS had already gained cyber capabilities by recruiting computer science academic degree holders from European universities, among them is the famous "Jihadi John" who is responsible for numerous beheadings. The fear is that by the end of 2015, ISIS or its affiliated hackers, will conduct an "electronic war" as the hooded man said, and according to John Cohen, a former counterterrorism coordinator at the Department of Homeland Security, it could take place in two forms: by the organization's own activists or by outsourcing to an already trained cyber fighters.

Baku 2015 European Games - Information Security

Ensuring information security in Azerbaijan is one of the most relevant issues against the backdrop of the upcoming First European Games in Baku, an Azerbaijani minister told reporters. Ali Abbasov, Azerbaijan’s minister of communications and high technologies, said that the number of cyber-attacks is expected to grow, but has assured its guests it will be able to guarantee absolute safety and security.

Abbasov said that the country's security agencies, structures operating in the sphere of IT, as well as the foreign partners, have mobilized their efforts. The work on preparing Azerbaijan's telecommunication infrastructure for the First European Games has been completed, and currently working tests have been successfully conducted, according to the minister.

Baku 2015 is the first ever European Games, an exciting and innovative multi-sport event for the continent which will take place on June 12-28, 2015. There will be a total of 20 sports at Baku 2015: 16 Olympic sports and 4 non-Olympic sports. More than 6,000 athletes from across Europe will be representing their nations over 17 days of competition.

Recently Azerbaijan has received $2 billion for five years in the sphere of information technologies of Azerbaijan during the Azerbaijan investment summit.

CHINA and APAC

China to issue 5-year security plan to safeguard state secrets

Beijing: Chinese official media reported that China's state secrets and data are set to be more effectively secured with a far-reaching five-year state-run cybersecurity program, announced against the ever-growing cyber confrontation with the US.

The paper quoted Chen Wei, the director of the ministry's software bureau, as saying that the plan is expected to refocus software purchase of the national government agencies and institutions to domestically-developed products.

In February, Reuters reported that China had dropped some of the world's leading technology brands from its approved state purchase list, while approving thousands more locally made products, in what some said was a response to revelations of widespread Western cyber surveillance. A draft national security law posted online in China earlier in May stipulated the utmost necessity for national cyberspace "sovereignty," mentioning "harmful moral standards" practiced by unnamed powers.

EUROPE

The UK government to ban encryption in move to counter terrorism

Recently the Islamic State recruited a British teenager, through an encrypted application that was used to send instructions on how to cross the Syrian borders. After this event, the UK government is now considering banning message encryption systems in order to prevent extremist and terrorist organizations from recruiting people. Professor Mike Jackson, a cyber-security expert from Birmingham City University, launched this initiative. He explained that he would like the UK government to ban encryption systems because he believes they could ultimately be used to spread terrorism across the country. Indeed, over the past decade, encryption systems tools have seen an increase in use by terrorist organizations to communicate and escape security authorities. Since 2007, Al-Qaeda has been using their own developed encryption software named Mujahideen Secrets for web and cellular communications in order to avoid the authorities' surveillance programs. In addition, it has been noted that since 2014, the organization has been using new encryption tools and services, such as mobile instant messaging. However, Jackson explained that despite the UK governments' communication interception capabilities, there is always a possibility thatt certain communications will not be intercepted by the government surveillance systems. Furthermore, according to him, "The only way out to prevent such happenings is by banning all but the simplest encryption techniques." This initiative could therefore potentially help in reducing the terrorism recruitment phenomenon; however, terrorist organizations will more than likely find yet another way to communicate and/or recruit people by using the Darknet.