UNCLASSIFIED



Executive Cyber Intelligence Bi-Weekly Report by INSS-CSFI

October 15th, 2014

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: inssdcoi@gmail.com.

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

ISRAEL

IDF building new cloud-base infrastructure

The Israeli Defense Force will begin developing a cloud-based infrastructure slated to take effect in 2015. Colonel Asher Dvash, head of the body overseeing the C4i Core Facilities in the South, introduced the concept. The benefits of the cloud are not only economical, but it will allow the IDF to minimize the large number of data centers it holds. This, in turn, will free up a substantial number of personnel maintaining the centers and instead utilize them for developing operations. The project will also improve IDF continuity and inner development capabilities and enable every branch to manage their own applications and renewals. The army will begin with VMware Technology; however, the IDF may turn to another supplier in the future based on performance.

USA

Apple updates iOS after major hack on iCloud

100s of celebrities' iCloud services were recently hacked, specifically their photo streams, which were illegally uploaded onto various social media websites. In the wake of this, Apple has added an extra step when accessing iCloud on a computer device – effectively saying that using the two factor authentication will make it more difficult to access or hack another person's iCloud. Though Apple previously stated the celebrity hack was not a complication with the iCloud, it nonetheless provided this security upgrade to its iOS. The hack of Apple devices represented one of the first times Apple and the Cloud have been majorly breached via iCloud forensic software. This only brings into question the security of other cloud devices such as Dropbox, Google Drive, etc.

NetScout to acquire communications business of Danaher Corp and expand cyber intelligence expertise

A US provider of integrated computer networks, NetScout, plans on acquiring the communications company Danaher in a $2.6 billion deal in order to expand NetScout's cyber intelligence expertise. As stated by the NetScout CEO, Anil Singhal: "This business combination will expand NetScout's global reach and help broaden our presence with customers in both the service provider and enterprise markets. In addition, it will jump-start our planned entry into the cyber intelligence market, particularly within the advanced persistent threat area." The NetScout Company originally specialized in network products including packet Sniffer and nGenius packet flow recorder. This new cyber intelligence perspective will provide the company with a global vision of cyber security. Such as all multinational high tech corporations, NetScout developed its technology over time and is today one of the leaders in the market. Today, cyber intelligence is a key point of the cyber security field and must to be considered as relevant as every other security system or service proposed in the different variations of cyber security.

RUSSIA

Russia will not give government full power over Internet

Russia will not transfer the Internet to full state control. Russian President Vladimir Putin announced this decision at a meeting of the Security Council, Reuters reports. Nevertheless, he demanded a solution to protect Russian networks from hacker activity, which President Putin claims has increased due to the aggravation of international relations. “We do not intend to restrict access to the network and put it under total control. Freedom of the media, the right of citizens to receive and impart information is the basic principle of any democratic government, and we will do just that,” President Putin expressed. Previously, Deputy of the LDPR party Hudyakov, addressed the Head of the Federal Service for Supervision of Communications, Information, and Technology and requested to eliminate and “blacklist” Wikipedia pages with articles addressing the “incorporation of the Crimea and Sevastopol,” which can be interpreted as “annexation.”

ARAB COUNTRIES

Jordan to open cybercrime center in Amman

The Jordanian Ministry of Information and Communications Technology has begun developments for a cybercrime center located in Amman, dedicated solely to fighting cybercrime and cyber security threats targeting Jordan's financial sectors and its national security. The new center would reinforce the existing cybercrime law and help introduce new laws. According to Lt. Col. Sahm al-Jamal, Director of the Cybercrime Unit of the Public Security Directorate's Criminal Investigations Department, the center's existence is necessary due to “the authorities’ need to prevent this type of crime… Our department dealt with around 1,300 cybercrimes during 2013.”

Qatar isthird most targeted country in cyber threats and attacks

According to FireEye’s report, Qatar is the third most targeted country in cyber-attacks in the Middle East; Saudi Arabia and Turkey are 1 and 2, respectively. Qatar faced close to 2,000 cyber-attacks in the first half of 2014, dealing with 1,824 advanced cyber-attacks that bypassed traditional security layers. Saudi Arabia faced the highest number (8,564) of cyber-attacks in the first half of the current year. Turkey and Kuwait were the other countries targeted by cyber-attacks. The attacks were mostly related to political or financial motives.

Anonymous hacker group launches cyber war against Islamic State militants

The Anonymous hacktivist group launched a cyber-war against the Islamic State (IS). A member of the group stated: “We plan to attack several countries that were knowingly supporting ISIS financially, including Turkey and Saudi Arabia. We warned that if they continued to support ISIS we would be forced to destroy their virtual infrastructure. In addition, yes we have those who can do this. What we decided to do is instead of attacking them directly we decided to attack their ideologies with truth and logic. We took this initiative in order to establish two things: one - we needed the public to understand how urgent the situation is in Iraq… the second reason was that we needed to make sure the public knew that ISIS did not represent the Islamic religion.”

CHINA and APAC

Chinese Army calling to strengthen domestic cyber security software media

The Chinese Army is planning to strengthen its national cyber security and speed up their software media. According to the official People's Liberation Army Daily, "Information security must be considered an underlying project in military battle preparedness." Besides being the Chief of the Chinese Army, the Chinese President Xi Jinping helms a government agency in charge of Internet security and to concentrate in making China an international cyber power. This structure shift comes as recent tense relations between China and the West have accelerated, contributing to the Chinese wishing to strengthen their cyber security software. Currently, both Microsoft and Qualcomm are being investigated by Chinese authorities to look for potential cyber espionage activities. According to the Chinese government, Chinese corporations and financial institutions have been replacing their foreign computers' software with local software. The US have recently accused several Chinese soldiers for cyber espionage activities against the US, causing diplomatic tensions between the two superpowers.

AFRICA

Cyber criminals target Africa's food and beverage sector

A recently released report from Cisco found that global geopolitical events like West Africa's Ebola outbreak have significantly expanded the risk landscape in the African region. Cyber criminals are increasingly taking advantage of such events to trick people into clicking on links to compromised websites. Mobile and web malware attacks are on the rise. The African region's food and beverage industry has been one of the hardest hit; the report indicates that the industry where most of the attacks emerge has been the food and beverage industry. It has remained unclear as to why this industry has been such a strong target, but Cisco's assumption is that it may be tied to this sector's interest in general news and how it affects the food and beverage space.

Zambia hosted first Cyber security drill

Zambia hosted the first cyber drill for Africa. The cyber drill provided a platform for incident handlers from various African countries to come together, collaborate, communicate, and enhance their incident handling skills. Government officials said they hope the initiative grows to greater heights as nations join together in the fight against cybercrime.

Ethiopia to Host Second Annual Cyber Security Africa's Banking & ICT Summit 2014

Cyber Security Africa has announced the second annual Ethiopia Banking & ICT Summit 2014 edition. The Summit will take place on November 21st, 2014, at the Sheraton Hotel, Addis Ababa, Ethiopia.

EUROPE

London Metropolitan Police launched anti-fraud cybercrime unit

The London Metropolitan Police launched a new cyber unit. The FALCON (Fraud and Linked Crime Online) is charged with countering financial fraud and cybercrime. This new cyber unit can count on more than 500 police officers working to counter malware, DDoS, phishing attacks, and other cybercrimes that result in financial losses. This new unit is also aiming to educate organizations about the threat of cybercrime in order to improve security and prevention. The British Minister for Modern Slavery and Organized Crime declared the following: "National Security Strategy has ranked cybercrime as a major threat. The Government is putting in £860m over five years to cope with it. We are also increasing knowledge throughout local police forces with specialist training." Besides the new FALCON unit, the London Metropolitan Police Service owns a Police Central e-Crime Unit (PCeU), which aims to improve the police response to online crime and developing cyber capabilities for police service across England, Wales, and Northern Ireland. Like the PCeU, the FALCON unit will cooperate with the National Cyber Crime Unit of the UK National Crime Agency to counter cyber threats and fight cybercrimes.

Estonian to launch first e-residency card

The Estonian government recently decided to offer an e-residency status to people around the world. This new digital identity will give access to services like online banking, education, or healthcare. According to Siim Sikkut, who is the ICT policy adviser at the Government Office of Estonia, once one has this digital Estonian card, he/she can easily do all online operations such as banking, government, private company, and medical visits. He added that the "e-residency gives secure access to online services and the ability to digitally sign in a legally binding manner, just like Estonians do." According to the Estonian government, this service is first aiming to help those who deal with Estonia, either through business, studying, or as a tourist. The government is also expecting that this new project will attract new customers and investors. The new identity card would be in use at the end of the year. Moreover, the e-residency card will only be available at first from a Police and Border Guard office in Estonia, but the government is planning to extend the e-residency applications at Estonian embassies all over the world by the end of 2015. Estonia is probably one of the most advanced countries in terms of digital operations and high tech. This new project seems to be an innovative idea; however, many questions can be asked about how secure this new e-residency card will be and what will happen in the case of hacking and/or identity theft.