UNCLASSIFIED



Executive Cyber Intelligence Bi-Weekly Report by INSS-CSFI

September 1st, 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 U.S. 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

Behind ~~the~~ Israeli cyber battle of Operation Protective Edge

According to an article written by Daniel Cohen and Danielle Levin, researchers from the Institute for National Security Studies, cyber-attacks targeting Israel during Operation Protective Edge demonstrate~~d~~s Israel's implementation of government policy in the cyber sphere~~,~~ and application of~~applying~~ the systematization learned since 2012's Operation Pillar of Defense. There was a significant improvement in coordination of Israel's cyber defense organizations, including the functioning of Israel's security systems and the increase~~d~~~~ing~~ cooperation between the civilian and ~~the~~ defense sector~~s~~. The objective of the main attack during the Operation was to cause Israeli networks to collapse ~~through~~ by overloading the system. Cohen and Levin explain that these attacks focused on distributed denial of service (DDoS) and Domain Name Service (DNS) attacks on communication and Internet companies in an attempt to swamp the Israeli Internet networks. The Shin Bet stated that international hacking groups conducted the attacks during the operation. The Israel Defense Force (IDF) maintained Iran had a large role in the increase of ~~cyber attacks~~cyber-attacks on civilian infrastructure. An Israeli security firm later confirmed that most of the attacks were from the Middle East origin, and later the IDF confirmed Iran partook in ~~cyber-attacks~~cyber-attacks targeted to Israel. Both the IDF and the Shin Bet were able to foil any damaging attempts ~~on~~to Israeli government networks and critical infrastructure. The Shin Bet confirmed they were able to secure all ~~cyber-attacks~~cyber-attacks targeted towards Israelis government networks and systems. Shin Bet, through its cyber division, acted in coordination with private contractors, the Israeli Ministry of Communications, and the media in taking preemptive measures against these straightforward ~~cyber-attacks~~cyber-attacks. The IDF worked with an integrated communications network of the Military Intelligence and cyber companies related to the Ministry of Defense, which assisted in recognizing and removing all cyber threats from attackers related to these attacks. The Head of the IDF cyber defense unit revealed that infiltration had also been attempted on IDF networks~~,~~; but he verified Israel's high technological capabilities were elevated in order to ensure breaches did not occur.

U~~.~~S~~.~~A

Major cyber-attack against United States banks

A weak ago, the US financial sector experienced a massive cyber-attack. Several banks, including JP Morgan Chase and others, were targeted by a series of cyber-attacks ~~including JP Morgan, Chase and others~~. According to a vast investigation, the hackers infiltrated the banks networks and stole gigabytes of data, including customer~~'~~s' details and employee~~'~~s' information. According to the FBI (who are conducting the investigation in cooperation with the United States Secret Service), the identities and motivation of the hackers have not been yet determined. However, without any certitude, it appears the hackers originated from Russian or Eastern European countries. ~~–~~This is not the first time US banks are experiencing cyber-attacks. US banks have often ~~become~~ been victim~~s~~ of hackers targeting credit card~~s~~ number~~s~~ and cvv to sell ~~it~~ on the Internet. ~~–~~Moreover, iSight Partners, a security company, warned banks about online threats and insisted banks should

prepare to face several cyber-attacks from Russia in retaliation for Western economic sanctions. When it comes to financial fraud and banks, Russian hackers are the most organized and powerful cyber-criminals. They are well skilled and very motivated.

RUSSIA

Most of the cyber-attacks targeting Western Europe come from Russia

According to a study conducted by Alert Logic, a Houston Web Security Company, hackers directly from Russia conducted the vast majority of cyber-attacks targeted at Western Europe. In turn, China has become the leader in the number of hacking attacks against the United States. Analysis showed that 40% of hackers targeting users in Northern European countries were carried out from Russia. Western European countries subjected to hacking attacks were conducted from China (32%), United States (21%), India (17%), and Russia (9%). 63% of attacks on the countries of the Asia-Pacific region have been carried out from the USA, experts reported. The most frequent were infections caused by the Conficker-A malware Conficker A.

ARAB COUNTRIESAND MUSLIM WORLD

The Iranian cyber offensive during Operation Protective Edge

An analysis of Iran's cyber activity during Operation Protective Edge indicates growing maturity in the Islamic Republic's operational capabilities and shows that it is capable of conducting an extensive military cyber operation against a range of targets using a wide spectrum of methods, according to an article by Dr. Gabi Siboni and Sami Kronenfeld, researchers from the Institute for National Security Studies,. Moreover, Iran's focus on cyberspace during Operation Protective Edge may indicate the start of a process in which cyberwar replaces classical terrorism as the main tool in Iran's doctrine of asymmetrical warfare. Cyberwar, which offers the attacker distance and deniability, two features the Iranians consider extremely valuable, enables serious damage to the civilian front of an enemy enjoying military and geostrategic superiority. Thus far, Iran's cyberspace capabilities remain inferior to Israel's and to those of the leading technological powerhouses, but it is rapidly and efficiently closing the gap.

Hackers related to ISIS took down Sony -PlayStation's network

"Lizard Squad," a pro ISIS cyber group, claimed responsibility for hacking the Sony-PlayStation's network. Using a distributed denial of service attack (DDoS) attack, the group managed to overload the SPN server and cause the crash. Other services affected -included Xbox LIVE, Battle.net log--ins for Blizzard titles, League of Legends, and Path of Exile. As posted on Twitter, the group is connected with the Islamic State (IS), claiming to be loyal to the Calipha and acting as part of the IS against the greediness of corporations, such as Sony. Nevertheless, many of the hackers from Lizard Squad were traced back to IPs in Europe.

Qatari technology helps Hamas build sophisticated cyber systems to attack Israel

Before and during Operation Protective Edge, Hamas was funded by Qatar. Qatar invested hundreds of millions of currency in both defensive and offensive cyber-capabilities for the terrorist organization. According to Aviad Dadon of the Israeli

cyber-security firm AdoreGroup~~, he informed~~: “We have sourced 70% of the cyber-attacks on Israeli government sites in recent weeks to IP addresses associated with Qatar." According to Dadon, not only is Qatar investing time and money into cyber-attacks, but it is also training Hamas terrorists in how to use sophisticated equipment and systems to manage its extensive terror tunnel system~~.~~ in addition~~,~~ to systems ~~to~~ for fir~~e~~ing rockets at Israel using automatic, timed launching systems. Qatar has hired hackers to hit Israeli government and infrastructure sites trying to disrupt the operations of electricity, water, and other critical systems during the 50 day operation.

CHINA and APAC

Budget cuts increase~~s~~ Australian cyber-security risks

Australia's cyber-security-focused Co-Operative Research Centre (CRC) had not been funded for the second time. CRC dates back to 1990 and had provided funds and guidance to encourage research collaboration between universities and the private sector. Once the cuts hit the research institutes, a significant drop in R&D is imminent. However, a plan for the Australian Cyber-Security Research Institute is supposed to be announced later this year. Experts think this may be a little too late.

Hacker targets info on MH370 probe

The computers of high-ranking officials in agencies involved in the MH370 investigation were hacked, and classified information was stolen. The stolen information was allegedly being sent to a computer in China before Cybersecurity Malaysia (a Ministry of Science, Technology and Innovation agency in Malaysia) had the transmissions blocked and the infected machines shut down. The national cyber-security specialist agency revealed that sophisticated malware or malicious software, disguised as a news article reporting that the missing Boeing 777 had been found, was e-mailed to the officials on March 9, a day after the Malaysia Airlines plane vanished during its flight from Kuala Lumpur to Beijing.

LATIN AMERICA

Ecuador is ~~the~~ latest country ~~who faced a~~to face cyber-espionage campaign

Kaspersky Lab~~'~~s revealed that Ecuador is the latest country faced with a cyber-espionage campaign known as "Machete." The campaign started in 2010 with hundreds of gigabytes of classified information breached. The campaign began with infected PowerPoints. Once accessed, the attackers intercepted messages from the keyboard, recorded audio from the computer microphone, took screenshots, and stole files from remote serves. Stolen information was also used through a special USB. ~~—~~"The attackers were not interested in money, but in highly classified information of military… basically everything that involves national security of a government," Dmitry Bestuzhev explained, Director of the Security Team for Latin America at Kaspersky Lab. Latin American countries of Colombia and Venezuela were also affected, in addition to the embassies of Russia, France, China and more.

EUROPE

~~The~~ UK Ministry of Defense ~~is~~ launching ~~a~~ £2 million cyber defense project

The Uk Ministry of Defense decided to launch a £2 million cyber defense project. This project is a ~~completion~~ competition aim~~ed~~ed~~ing~~ ~~to~~at find~~ing~~ a solution to automate cyber response, collect data, and identify cyber-attacks to ensure ~~a~~ better protection to the UK MoD computer systems. The competition has been organised by the MoD's Centre for Defence Enterprise, which explained "once a system is compromised a cyber-attack can quickly escalate, so automated responses are an essential part of cyber defence processes, while recognising that the user may wish to revert to human decision making." The MoD declared it does not necessarily expect one winner for this ~~completion~~ competition, and all good ideas will be reviewed. The budget has been split into two parts, £1 million each. The first part will be launch~~ed~~ed in September at an Innovation Network even in London. ~~In addition,~~Then the second ~~one~~part will be awarded ~~to the most successful project. In addition, the second one will be awarded~~ on a per-project basis to the most successful bidders. The UK MoD spokesperson explained that "the whole aim is to support people with ideas or small businesses that have ideas that don't necessarily have the funds to develop them further. If they do prove successful, then there's the potential to take them forward." ~~-~~The UK, ~~who~~ which is one of the most advanced ~~country~~ countries for cyber defense, seems to adopt a participatory strategy involving British civilian companies to ~~has~~ get involved in the UK defense. This type of project is a plus for countries~~, which~~ that are looking ~~for developing~~to develop their response capabilities to multiple cyber-attacks.

Germany ~~is~~ working on ~~a~~ cyber ~~-~~security law to protect ~~its~~ critical infrastructure

The German interior ministry is thinking of launching a cyber ~~-~~security law to protect its national critical infrastructure. The Interior Minister, Thomas de Maiziere, submitted a draft law imposing stronger cyber security requirements on companies and national agencies in charge of critical infrastructure, such as information technology, telecommunications, energy, transportation, health, water, food supply, finance, and insurance. Part of this new cyber security law is to oblige these companies to report any hacking incidents of which they were victims. According to the Minister, Germany's critical infrastructure needs to be "the safest in the world." Moreover, other German federal government departments have been asked to look at the proposals and then the debate will take place. The Ministry also declared that the cyber security draft proposals are part of Germany's ~~the~~ 2014-2017 ~~German's~~ 'digital agenda,' which has been approved by the German federal government. Despite a great cyber ~~-~~security strategy, Germany still suffers from several cyber-attacks against its critical infrastructure. This new proposal~~s~~ should help to strengthen their critical infrastructure and national security.

AFRICA

South Africa's IT Governance ~~has~~ launched four ISO 27001 package~~d~~ solutions to help South African organisations tackle cyber crime~~.~~

IT Governance's ISO 27001 package~~d~~ solutions offer world-class cyber security resources, training, and consultancy online to help businesses protect their information assets. In a recent statement from the University of Johannesburg's Centre for Cyber Security, Professor Basie von Solms said, ~~that~~ "Business is also guilty of not doing enough to tackle cyber crime." According to the 2013 Norton Report,

South Africa has the third highest number of cyber crime victims after Russia and China.

Kenya urges concerted efforts to fight crime

Kenya called for concerted efforts in the fight against organized crime in Africa in order to help spur development in the continent.

Deputy President William Ruto told a regional conference for spy chiefs that working together will eliminate competition and create synergy in the fight against crime, which he said was threatening economic efforts. He also mentioned that there was need for closer collaboration among the police, military officers, national intelligence service, and immigration officers in the fight against crime.

The spy chiefs will review security challenges in the continent and exchange intelligence to develop a shared understanding of common security problems.