THE INSTITUTE FOR NATIONAL SECURITY STUDIES

Cyber Security Program

Global Cyber Bi-Weekly Report by INSS November 15, 2016

Editor-in-chief: Gabi Siboni, Editor: Hadas Klein; Contributors: Jeremy Makowski, Simon Tsipis, Gal Perl Finkel, Ido Sivan, Paola Aurucci

ISRAEL

Israeli missile boats reinforced against cyberattacks

Russian aircraft carrier Admiral Kuznetsov recently arrived at the shores of Syria, accompanied by its companion vessels. The ships are in the area as a deterrent measure, and are also collecting intelligence via electronic means. In response, the Israeli Navy has upgraded its cyber warfare capabilities, placing special crews onto its missile boats. "The (fight) isn't just with the possibility of infiltration into your systems – you need to ensure that if there is an infiltration, the infiltrator won't be able to cause damage or collect critical intelligence and will be identified quickly," said an IDF cyber warfare official.

http://www.ynetnews.com/articles/0,7340,L-4879413,00.html

Israel Aerospace wins $15m Asian cyber deal

Israel Aerospace Industries Ltd. (IAI) (TASE: ARSP.B1) has announced that it has signed a contract worth $15 million for a cyber intelligence system with a customer in Asia. The contract is for an advanced, national-level, strategic cyber solution, which combines cellular systems and cyber. It also includes establishing an intelligence center and infrastructure and providing unique sensors. The contract will be executed by one of ELTA/IA's cyber subsidiaries and development centers.

http://www.globes.co.il/en/article-israel-aerospace-wins-15m-asian-cyber-deal-1001158794

UNITED STATES

US vote hacking

The possibility that hackers would disrupt the voting process was real. Federal and state officials already were concerned before the elections, and focused on five

possible ways hackers could interfere with the elections. Those methods included hackers penetrating voter registration rolls and making their own alterations; taking down websites with an attack of so much data that voters cannot get information about their polling places, as well as directly making mischief with voting machines. Last month, the Obama administration alleged that the Russian government was trying to influence the election by stealing and disclosing emails from the Democratic National Committee. Among the email accounts hacked was that of John D. Podesta, the campaign chairman for Democratic presidential candidate, Hillary Clinton.
http://nyti.ms/2eXeCM5

EUROPE

Romania: 24 cyber criminals arrested in a Europol operation

The Romanian police, in close cooperation with the Europol cybercrime center, EC3, arrested 24 cyber criminals who were part of a gang responsible for massive payment card fraud. After investigating eighteen houses located in six Romanian counties, the police found electronic devices, computers, mobile phones, and specific equipment used to make card skimming devices, as well as €50,000 in cash. The EC3 center said that the gang installed skimming devices on automatic cash machines in different EU states. The goal of a skimming device is to copy the payment card information stored on the magnetic strip to duplicate the card and then use it to withdraw cash money. Furthermore, the investigation also led to the identification of 47 individuals involved in various activities within the cybercriminal group. Skimming fraud has been one of the most popular ways of stealing payment card information with Point of Sale malware over the past few years. A lack of regulation, as well as counter measures regarding automatic cash machine, allows cyber criminals to easily install fraudulent electronic devices and steal millions.
http://www.computerweekly.com/news/450402767/24-cyber-criminals-arrested-in-

Europol-operation operation

France voted for the creation of 600 new positions in cyber defense

The French parliament recently voted for the creation of 600 new positions to strengthen its cyber defense. Indeed, as part of its plan to place cyber defense at the top level of priority, France has been constantly developing its national cyber defense by opening new cyber expert positions as well as a cyber defense center. These 600 new cyber defense positions will be added to the first wave of 600 already created positions, in addition to another 2,000 positions planned for 2018-2019. Member of Parliament Gwendal Rouillard said that, "Most of these 3,200 specialists will join the cyber excellence cluster in the Brittany region." France seeks to make this region the center of its cyber defense. Indeed, it has several cybersecurity laboratories as well as an engineering school with cybersecurity specialties for training the future experts of the nation. Furthermore, France aims to increase its cyber defense to become one of the top nations in cyber defense, such as the United Kingdom, which is currently more advanced in this domain. As one of the most targeted countries of cyberattacks and cyberterrorists in Europe, France needs to drastically increase its level of security to protect its critical infrastructures.

http://www.letelegramme.fr/france/cyberdefense-priorite-nationale-et-enjeu-breton-06-11-2016-11281773.php

RUSSIA

US intelligence officials: we penetrated Russian cyberspace to secure our elections

Following the report by NBC, based on US intelligence officials, the US military's hacking division penetrated some of the more essential Russian infrastructure and government offices, including the Kremlin headquarters, and were ready to cyberattack Russia in case it tried to disrupt the US elections. Russian presidential spokesman, Dmitry Peskov reacted by declaring that Russian cybersecurity measures were in place to prevent any cyberattacks, in case these were real threats and that Russian cyberspace and government infrastructure were safe.

https://ria.ru/world/20161105/1480706124.html

http://www.nbcnews.com/news/us-news/u-s-hackers-ready-hit-back-if-russia-disrupts-election-n677936

https://ria.ru/politics/20161105/1480713091.html

Russian Security Council discusses cybersecurity tightening shortly after US threat

The press service of the Russian Security Council apparatus stated on November 7, 2016, that members of the scientific section of the Russian Security Council made suggestions aimed at increasing the protection of critical facilities of the Russian Federation from cyberterrorism. It was not stated, however, that these suggestions came shortly after the report about possible US threats to Russian critical infrastructure.

https://ria.ru/society/20161107/1480785398.html

Russia rated first in financial and banking systems' cyber vulnerability

Specialists at Kaspersky Lab have claimed that at the end of the third quarter of 2016, Russia ranked first in the world in terms of financial risks for users of personal computers, as well as for owners of mobile devices. Today, extortionate software remains one of the most urgent threats for Russian banking and financial systems, Kaspersky Lab specialists said.

http://www.securitylab.ru/news/484392.php

LinkedIn blocked in Russia

Following the law passed August 4, 2016, the Russian Federal Service for Supervision in the Sphere of Telecom, Information Technologies, and Mass Communications sued LinkedIn, regarding non-fulfillment of the Russian law of personal data localization in the country. On November 10, the court found that LinkedIn had violated the law of the inviolability of personal data. Thus, the Russian court has recognized the legitimacy of blocking the US social network for business networking and Job Search – LinkedIn.

https://ria.ru/incidents/20161110/1481103032.html

Russia to sue Microsoft on Russian antitrust law violations

The Russian Federal Antimonopoly Service (RFAS) has initiated proceedings against Microsoft on grounds of abusing a dominant market position. These proceedings are a result of the antivirus software "Windows Defender," developed by Microsoft itself for its systems. Microsoft allows only six days for other third party developers to try to adapt their antivirus software to Microsoft system, instead of a two-month period. As the Deputy Head of RFAS Anatoly Golomozin explained, this goes in contrary to Russian antitrust law.

https://ria.ru/incidents/20161110/1481102991.html

Putin: Russia to lead world's exports in IT and software

President Putin announced on November 10, at the "cyberbank" anniversary conference, that Russia's goal is to be the leading exporter of IT and software in the coming years. The Russian president claims that Russian IT industry exports are currently $6 billion, whereas Russia's military technology industries exports are $11 billion. IT industry needs to catch up with and overtake Russian arms sells, the president said.

https://www.youtube.com/watch?v=LCWUjWO9V38&feature=youtu.be

MIDDLE EAST

Iran's nuclear chief: Thanks to cyberattacks by the United States and Israel, our nuclear ambitions are more secure

The chief admitted that these attacks raised the awareness and security levels of Iran's nuclear cyber infrastructures.

http://opensources.info/iranrsquos-nuclear-chief-thanks-to-u-s-israeli-cyber-attacks-islamic-nationrsquos-nuclear-ambitions-are-more-secure/

Cybersecurity should be top priority of firms in the Gulf

Experts in a conference in Dubai expressed the importance of cybersecurity of the constantly threatened firms in the Gulf.

http://english.alarabiya.net/en/business/technology/2016/11/12/Cyber-security-attacks-must-be-top-priority-for-firms-in-UAE.html

ISIS' cyber recruiting hits new levels

Internet-based manpower was crucial to ISIS' expansion, says a new IDC report.

http://www.jpost.com/Middle-East/ISIS-cyber-recruiting-financing-hits-new-levels-471873

CHINA and ASIA PACIFIC

Asian financial body says Chinese cybersecurity law could make risk management difficult

Mark Austen, chief executive of the Asia Securities Industry and Financial Markets Association (ASIFMA), said the law marked a "worrying" development because regulators globally must work together to address cyber risks rather than attempt to isolate their jurisdictions. Austen, from one of Asia's most prominent financial trade bodies, also said that the new cybersecurity laws in China could make it harder for foreign companies operating in the country to manage risk as cyberthreats become increasingly cross-border. Austen spoke at the Thomson Reuters Pan-Asian Regulatory Summit in Hong Kong,

China adopted a cybersecurity law to counter what the government said were growing threats, such as hacking and terrorism. Foreign business and rights groups expressed concern that the law could, for instance, bar foreign companies from certain sectors. The legislation, set to take effect in June 2017, includes requirements for security reviews and for data to be stored on servers in China.

http://reut.rs/2fdxl9S

China adopts a tough cybersecurity law

China adopted a new cybersecurity law on November 7, 2016, to take effect in June 2017. The law is designed to strengthen local networks against malicious hackers. In fact, the law looks very much like a techno-nationalist Trojan horse. The law affects both domestic and foreign firms operating on the Chinese mainland and covers a wide range of activity relating to use of the internet and information and communications technologies (ICT). Many foreign businesspeople agree with James Zimmerman, chairman of the American Chamber of Commerce in China, who assessed that "this is a step backwards for innovation in China that won't do much to improve security." This is a headache for multinational firms, which typically rely on cross border flows of business data. Firms worry that the law will not only require expensive new investments, but also increase the risk of data theft. Another thorny provision requires companies to get security certifications for important network equipment and software. Foreign firms fear this might be used to force them to turn over security keys and proprietary technologies, which could be passed on to state-owned rivals.

http://econ.st/2fH9L64

Dr. Tobias Feakin appointed as Australia's ambassador for cyber affairs

Julie Bishop, Australia's minister for foreign affairs and Minister Assisting the Prime Minister for Cyber Security Dan Tehan have announced the appointment of Dr. Tobias Feakin as Australia's first ambassador for cyber affairs. Feakin was a member of the Independent Panel of Experts that supported the Australian Cyber Security Review to produce Australia's AU$230 million cybersecurity strategy. He has been the director of national security programs at the Australian Strategic Policy Institute (ASPI) since 2012 and established the institute's International Cyber Policy Centre; he has also held many research and advisory positions, including with the Royal United Services Institute for Defence and Security Studies, the Oxford University Global Cyber Security Capacity Centre, the Global Commission on Internet Governance, and the Global Commission on the Stability of Cyberspace. His role will be to support cyber capacity building in the region, advocate against state censorship of the

internet, and promote Australia's view that opportunities provided by the internet should be available to all people.

http://zd.net/2eS6yvZ

Indian Army officers get fake messages; advisory issued by PCDA

Defence sources said that for over a month until fifteen days ago, several army officers, including seniors, received messages through phone messaging services like WhatsApp and through social networking sites and mails stating that the Principal Controller of Defence Accounts (Officers), PCDA (O), had developed an app through which they could access information about their pay and allowance. The PCDA (O) has now issued an advisory to the officers not to open these links and clarified that no such app has been developed by the office. The office of PCDA (O), located in Pune, caters to over 46,000 serving officers, from the Chief of Army Staff to lieutenants. "When these links were checked, it came to light that the browser was redirecting the user to a suspicious link. This was a potential cybersecurity threat, which could have led to stealing of personal data of the officers, including their usernames and passwords for the PCDA (O) website," said an officer on the condition of anonymity.

http://bit.ly/26wVjjz

The Indian government strengthens cybersecurity measures

Information Technology Minister Ravi Shankar Prasad said that the Indian government is preparing for a bloodless war by strengthening cybersecurity measures. In addition, the Indian Computer Emergency Response Team (CERT-In) is being strengthened. "We are preparing for bloodless war, by strengthening cybersecurity measures. A national cyber coordination center is being set up to provide near real time situational awareness and rapid response. The Rs 985 crore project is to be completed in five years," said Minister Prasad.

http://bit.ly/2fQZsuu

Malaysia, Korea form cybersecurity alliance

National digital security agencies, CyberSecurity Malaysia and Korea's Internet & Security Agency (KISA), signed a memorandum of agreement. Both agencies have agreed to exchange, develop, and consolidate their knowledge and experiences of cybersecurity incidents. The purpose of the agreement is to better collaborate on critical infrastructure and cybersecurity issues. This will enhance response, threat and risk management, as well as include training, research, and development and protection of critical information infrastructure. In addition, the agencies also said they will exchange human resources to speed up the development of national cybersecurity legal and regulatory frameworks.

http://bit.ly/2fm34mP

AFRICA

ISSAN to raise cybersecurity awareness in Nigeria

Microsoft, a US-based technology company, and Information Security of Africa Nigeria (ISSAN), have joined forces to raise cybersecurity awareness in wake of current global cyberthreats. David Isiavwe, the president of ISSAN, said at a public function recently in Lagos State that cyberattackers are getting more refined so that the number of days it takes to detect a cyberattack has increased from 58 days three years ago to 200 days today. He said the cyberattackers have devised new ways to successfully attack individuals and organizations, saying that Nigeria loses N128 billion yearly.

http://bit.ly/2eS6I6C

Joint police cybersecurity lab for East Africa

Tumwebaze Frank, Uganda's minister of ICT and National Guidance, has said that East African countries are seeking funds for the construction of a cyber and forensic intelligence center, aimed at combating the rising challenge of countering cross-border cybercrimes, which threaten the peace and stability in the region. The establishment of the center is primarily intended to assist law-enforcement agencies in combating information communication technology (ICT)-related crimes in the

region. According to Emmanuel Gasana, Rwanda's inspector general of police, the East African region is experiencing an increase in online criminal activities which include financial fraud, drug and human trafficking, and terrorism, which require immediate intervention.

http://bit.ly/2eWnQvb

Nigeria to collaborate with Israel on cybersecurity

Nigeria is planning to collaborate with Israel in tackling cybercrimes and providing security in the country. The Israeli Ambassador to Nigeria, Guy Feldman, has said that "Israel, as a country, has suffered from cyberattacks; it is not a problem for us but a challenge. This is because we have the technology and human resources to deal with the challenge." Nigeria's Minister of Interior, Abdulrahman Dambazau said that cybersecurity will continue to be a major issue in all the nations for which collaboration is required. Chief of Staff, Brigadier-General Bala Saleh, said Nigeria would benefit from Israel's technical advancement in security. "It is hoped that the huge intellectual human capital which our country is well known for, will benefit from this collaboration to generate similar technological capacity which our Israeli friends bring to the table." He added.

http://bit.ly/2eWmiRO