Global Cyber Bi-Weekly Report by INSS August 15 2018

Editor-in-chief: Gabi Siboni, **Editor:** Hadas Klein, Gal Perl Finkel

Contributors: Simon Tsipis, Ido Sivan, Anna Danilova, Bryan McCarthy, David Libin

ISRAEL

Israeli educational program trains teen girls for elite cyber jobs

Each year, CyberGirlz—a program that is part of the Rashi Foundation's broader effort to promotes equal opportunities across business sectors—hosts a special summer camp for dozens of teens, the goal being to train and ultimately recruit the next generation of women for the hi- tech sector as well as the Israeli army's elite cyber units. The program was formed five years ago by Tali Ben-Aroya, after she walked into a room at a technology company in the United States and realized that among the thirty-odd entrepreneurs, she was the only woman. CyberGirlz is a prestigious initiative that encourages and prepares Israelis girls of high school age to enter the cutting-edge field of cybersecurity. "Girls in middle school don't tend to choose STEM [science, technology, engineering and mathematics], computer science or cyber security [careers]. I realized that if we wanted to make a change and if we want [equal representation], then we need to start at [a young] age," Ben-Aroya explained.

https://bit.ly/2Mk9kPB

Hamas tries to hack Israelis with fake rocket warning app

An Israeli cyber security firm warned that Hamas was trying to hack Israelis through a fake version of the Code Red rocket warning app. The warning came amid the worst round of violence between Israel and Hamas since 2014, with Hamas firing some 180 projectiles into Israel. Hamas was trying to take advantage of this and had put out a counterfeit app that mimicked the real software that warns Israelis of incoming rockets and mortars, said ClearSky Cyber Security. ClearSky warned that this could be the first stage of a concentrated effort by Hamas to launch cyberattacks against Israel as part of

the ongoing round of violence. However, the firm said that it appeared the malicious app had been discovered at an early stage and had not infected very many phones.

https://bit.ly/2Bb9wMC

UNITED STATES

The Cybersecurity 202: Def Con hackers could not crack a mock voter database, a rare bright spot for election security

At this year's Def Con in Las Vegas, this news might alleviate a small number of the American public who have fears concerning election system interference. Although every major electronic voting system put before the hackers at the convention was successfully hacked, one key item was not. The database of registered voters, modeled on an actual database from Ohio, was not successfully breached or manipulated.

https://wapo.st/2L00ly6

How long is too long for a cyber operation? NSA has an idea

The NSA has been keeping an eye on its cyber operatives to see how the stress of operations affects outcomes. It turns out that five hours is when the effectiveness of the operator drops off due to stress and target/mission fixation.

https://bit.ly/2MuDK1s

Cyber Flag: Exclusive peek inside Cyber Command's premiere annual exercise

US Cyber Command recently conducted its "Cyber Flag" joint and combined forces training exercise. Cyber Commands J7 stated the goals of the exercise were to identify how the military can include cyber effects in an operation; determine if teams can identify characteristics of the terrain either in an offensive or defensive environment, depending on the team's mission set; as well as to find out how teams react when critical infrastructure is

compromised, and identify how the military can share information with partners and allies.

https://bit.ly/2wgzzwn

EUROPE

Three hackers arrested in Europe in connection with tens of millions of dollars in losses

Three people associated with the hacking group FIN7, also known as Carbanak, have been arrested in Europe and are in custody, the United States said in a court filing. The three, Fedir Hladyr, Dmytro Fedorov, and Andrii Kolpakov, were arrested in Europe between January and June of this year, the court filing said. Hladyr is in US custody, and US authorities are seeking the extradition of the other two. The three were arrested in connection with computer hacks of more than 120 US companies in order to steal customer payment card data and other information, the filing said. According to the court filing, the group has caused tens of millions of dollars in losses.

https://reut.rs/2n3rp63

UK online fraud blasts past £2 billion

Cyber-enabled fraud losses have rocketed over the past twelve months with more than £2 billion collectively stolen from the bank accounts of UK cardholders, according to Compare the Market. A poll of 2000 adults in the United Kingdom revealed that 9 percent had been defrauded over the past year, which roughly equates to 4.7 million people nationwide. The figure is significantly less than the 5.5 million estimated to have lost money between May 2016 and May 2017. However, the amount stolen has risen 38 percent over the period, from £600 per person to £833.

https://bit.ly/2KObO3C

RUSSIA

The "leftovers" from the Russian US elections fraud are still there

More than thirty pages and accounts on the social networks Facebook and Instagram were removed on July 31 as part of the attempt to stop the spread of inaccurate information, according to a statement by Facebook. This action is part of a continuous efforts against fake social network pages, which were accused by US authorities as being related to Russia's support of Donald Trump in the US elections. In particular, the charges related to a Russian organization, the Internet Research Agency from St. Petersburg. In April, Mark Zuckerberg, the founder of Facebook, announced that more than 270 pages and accounts that were managed by this organization had been blocked.

http://bit.ly/2vCBqM7

Russia's US electricity and nuclear hacking becomes real

Following previous US announcement that Russian hacker might have penetrated US nuclear and electricity facilities, the Wall Street Journal referring to sources in the White House, reported that "Dragonfly" and "Energetic Bear" groups, which allegedly receive instructions directly from the Russian authorities, intend to arrange a blackout for Americans. According to the US Department of Homeland Security, hackers connected with Moscow infiltrated US energy companies as early as the spring of 2016 and have since been trying to disable them. In recent months, attacks have increased. Washington fears that criminals will have access to control systems of thermal power plants.

http://bit.ly/2B3PDHe

Telegram continues its fight with the Russian government's "machine"

The Supreme Court of Russia recognized the order of the Russian Federal Security Service (FSB) that the Telegram messenger service provide the FSB with the keys to decrypt the messages of Telegram users and dismissed the complaint of the representatives of the messenger service. On April 13, the Tagansky District Court of Moscow recognized the request of Russia's state

censor, Roskomnadzor, to block access to Telegram with the failure of FSB keys to decrypt users' messages.

http://bit.ly/2nxSzlU

New discovery in US cyber fraud investigation of Russia

US investigation of Russian involvement in the recent presidential election might have received information about further Russian involvement in the Gulf crisis between Qatar and Saudi Arabi and the United Arab Emirates more than a year ago. The Mueller investigation suggests not only Russian cyber efforts to influence the US election but also involvement of Russian nationals in the cyber war in the Gulf and potential links between the two operations.

http://bit.ly/2B2q35k

ASIA PACIFIC

State-linked group likely carried out massive cyberattack on Singapore's health records

In Singapore, Minister for Communications and Information S. Iswaran said in the Parliament that the government's detailed analysis of last month's cyberattack on SingHealth records found that the attack was the work of an "advanced persistent threat." According to the minister, the use of customized malware indicates that the group had access to sophisticated tools, and is therefore likely state sponsored. However, the minister would not reveal which state was behind the attack. One interesting aspect of this attack is that it specifically targeted the health records of Singapore's Prime Minister Lee Hsien Loong.

https://bit.ly/2Bcbs7y

German cyber chief visits Singapore to discuss cooperation

Germany's chief of Cyber & Information Domain Service Ludwig Leinhos has made his first visit to Singapore. Singapore's capabilities in this area have become attractive to foreign partners. During his visit, Leinhos met with a range of Singapore officials, including Defense Minister Ng Eng Hen, Permanent Secretary for Defense Chan Yeng Kit, and Chief of Defense Force

Melvyn Ong. The reliance of Germany on Singapore's cyber capabilities shows the advanced preparedness which Singapore has achieved.

https://bit.ly/2KT8XXu

China's information law requiring the disclosure of data from foreign firms takes effect

The law requires anything critical to information infrastructure to be disclosed to the Chinese government and effectively puts more Chinese and foreign companies under state control. The law is open to interpretation, however, and can be used as a tool by the Chinese government to leverage foreign and domestic companies. China's only concession has been to push back the date of the law's implementation.

https://tcrn.ch/2rXY0OI

MIDDLE EAST

The UAE and Kuwait are most vulnerable among Gulf states to cyberattacks

According to cybersecurity firm Trend Micro, the UAE and Kuwait are among the most vulnerable to cyberattacks, with both being rated first and second in ransomware and malware attacks. The UAE accounted for 2.4 million of the 1.7 billion ransomware attacks detected globally. Kuwait accounted for 1.9 million. The Trend Micro report added that the reason for these countries being considered so vulnerable was due to their rapid digitization of the economy, which increases the risk of premeditated cyberattacks.

https://bit.ly/2IpshKD

Iran identified as number one cyber threat in Accenture report

According to a cyber report by Accenture, the Pipefish cyber espionage group continues to expand its capabilities. State-sponsored groups have been primarily targeting critical energy infrastructure for espionage purposes. According to the report, Iran now domestically produces its own malware, which highlights its self-reliant security concept. The report also highlights the

increased risk of attacks in critical infrastructure. Uncovered malware from Pipefish has the ability to execute remote commands and to upload and download files from the victim's system.

https://accntu.re/2vszcyW

Cyber reform in the Gulf region taking shape

Recently, the Gulf states have undergone major organizational changes in preparation for the new waves of cyberattacks that will affect the region. In Saudi Arabia, plans have been announced to establish the Presidency of State Security, the new state security agency responsible for counter-terrorism, domestic intelligence, and cybersecurity. In Bahrain, the newly established Central Agency for Information will form plans for an integrated electronic security system. The UAE has established the National Electronic Security Authority to develop, monitor, and supervise the implementation of cybersecurity standards across for information infrastructure.

https://bit.ly/2w5TWMy

LATIN AMERICA

Mexican Space Agency to develop cyber products for Mexican government and industry

The Mexican Space Agency is planning on establishing a center with a focus on technological development. Hugo Montoya, director of innovation at Agencia Espacial Mexicana, said that the agency will work to increase Mexican sovereignty over technology and add competition to the country. The products developed at the agency will be exported to Mexico's government. The center will develop products related to information security but will also invest in computational research and artificial intelligence.

https://bit.ly/2MhKSyY

Cybercriminals in Brazil capitalize on older vulnerabilities in D-Link routers for financially motivated phishing attacks

Five hundred attacks on older D-Link DSL models modems have occurred since June 8. These attacks change the DNS settings victim's routers and allow

the infiltrator to replace legitimate websites with phishing sites. The Banco De Brasil was targeted in this kind of attack, which could be alleviated by adopting new routers and technology.

https://bit.ly/2vGWEIL