Global Cyber Bi-Weekly Report by INSS 1 July 2019

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

Contributors: Simon Tsipis, Thomas Abma

ISRAEL

Ministry of Defense and Ben Gurion University inaugurate first building of IDF's new technology campus

The Israeli Ministry of Defense (IMOD) and Ben-Gurion University have introduced "the first building of the IDF Technology Campus." The building serves management overseeing the building plans of the "smart campus." According to Brig. Gen. (res.) Itzik Cohen, "to create the smart campus, we are bringing innovative technologies that will serve the needs of thousands of soldiers from the most elite IDF units. This infrastructure has the ability to reinforce the military's operational capabilities. At the same time, the collaboration between academia, the private sector, local government, and the military will turn the Negev into Israel's cyber capital."
http://bit.ly/2XwUUBl

Unique technological incubator at Israel's innovation ecosystem

Incubit, a subsidiary of Elbit Systems, is at the forefront of Israel Innovation Authority's technological cultivation efforts. The Israeli startup incubator aims at promoting highly technological and scientific startups, while striving to reinforce "open innovation," by engaging and endorsing collaboration across actors in the public and private sectors. It is a unique profile resulting from a variety of elements, notably adhering to a business strategy distinguished by a technological forward orientation as opposed to a financial one. In the first half of 2019, Incubit already invested in four startups, with a goal to invest in

two more by the end of the year with its current portfolio composed of fifteen companies.

http://bit.ly/2Xk5TP1

UNITED STATES

Another Florida city is making a ransomware payment, worth nearly $500,000

Lake City, Florida was hit with a malware attack in mid-June, branded as a "Triple Threat" attack, preventing the access or use of their communications systems, excluding the emergency system. The city made the ransomware payment of roughly $490,000 in bitcoin to hackers in order to re-claim phone and email systems. The city will cover $10,000 while their insurer, Florida League of Cities will pay the balance. The incident emerged only a week after Riviera Beach, Florida was hit with a ransomware attack and agreed to pay $600,000. In addition, the city of Baltimore was attacked only a month earlier, resulting in a significant payout of $18 million "after lawmakers declined to pay." Recorded Future published a report illustrating the growing trend of ransomware attacks on state and local governments, with total number of 169 attacks between 2013 and May 2019.

http://bit.ly/2XIfNJy

http://bit.ly/2LrILqM

Facebook fails to kill class action lawsuit over data breach

Facebook did not succeed to convince US District Jude William Alsup that the company should not be "liable for failing to protect users' information." The proceeding class action lawsuit is associated with the 2018 data breach that affected 30 million users. The judge "previously warned Facebook's legal team he would authorize a 'bone-crushing' discovery process on behalf of affected users, according to Law360." The company additionally is in the process of settling an estimated $5 billion dollars with the Federal Trade Commission regarding the Cambridge Analytica incident.

http://bit.ly/2KOmuEa

Congress: New devices=new threats=new security?

A bipartisan and bicameral bill related to the cybersecurity of internet-connected devices purchased by the government is awaiting a floor vote. The Internet of Things (IoT) Cybersecurity Improvement Act of 2019 bill was first introduced in 2017 in the Senate and in 2018 in the House of Representatives. The bipartisan bill determines the National Institute of Standards and Technology (NIST) to cultivate security standards for federal IoT devices and to address "secure development, patching, identity management, and configuration of internet-connected devices." In the event the legislation becomes law, the Office of Management and Budget is responsible to enforce the measures on relevant entities, contractors, and vendors, among other responsibilities. In the upcoming years, it is estimated that "tens of billions of devices" will enter the IoT environment, resulting in an increase of "countless new entry points into our networks, we need to make sure they are secure, particularly when they are integrated into the federal government's networks," stated Sen. Cory Gardner, R-Colo.

http://bit.ly/2Y83XFT

http://bit.ly/2YdJdMU

http://bit.ly/2YjIEkO

EUROPE

Electric cars: New vehicles to emit noise to aid safety

According to an EU rule coming into force, new electric vehicles will have to feature a noise-emitting device. The decision comes underway as rising concerns about whether pedestrians will be able to hear the low-emission cars and vans. The upcoming legislation will encompass all new types of four-wheel electric vehicle while the device sounds like a traditional engine. The device—Avas—referred to as "the acoustic vehicle alert system," will also make a sound when a vehicle is "reversing or traveling below 12 mph."

http://tiny.cc/lma18y

Automated border control kiosks at busy border crossing

The Schengen area consists of twenty-six European countries that have eliminated all passport and all other types of border control. As an alternative, some states, including Iceland, Italy, France, and Germany, are adopting an automated kiosk-based border control solution. The implementation of the BorderXpress promotes the Entry/Exit System (EES) created by the members, and on the horizon, it will satisfy the EU General Data Protection Regulation.
http://bit.ly/303tvEH

RUSSIA

Trump: I sanctioned a cyberattack on Russia in 2018

According to Russian news agency RIA, the US military launched a cyberattack on few Russian enterprises, including the Internet Research Agency (IRA) in St. Petersburg in November 2018, which is under US sanctions due to being connected to Russian cyber meddling in the 2016 US presidential elections. The leak about the attack was mentioned by Donald Trump himself in one of his recent interviews, where he said he promised the US intelligence "not to talk about it openly." US NATO allies also were not aware of any apparent attacks conducted by the United States against enterprises in Russia; however, IRA's executives confirmed that a Trojan was planted in the company's network from outside.
http://bit.ly/2Njya3C
http://bit.ly/2Njyu2k
http://bit.ly/2FxPzzi

United States changes its stance on cyber warfare against Russia

As was announced in an extraordinary report by the New York Times, the United States is stepping up its digital incursions into Russia's essential infrastructure sites. The US Cyber Command, a secretive arm of the Pentagon, is responsible for the cyberattacks and has recently shifted toward a more offensive strategy. The actions include the classified deployment of American computer code inside Russia's power grid and other targets. As part of these attacks, the United States has placed potentially crippling malware inside the Russian system at a depth and with an aggressiveness that had never been tried before. The unprecedented move means that United States is now poised to conduct cyber strikes in the event of a major conflict with Russia. Senior government officials have described how US efforts to infiltrate key Russian targets has become "far, far more aggressive over the past year."
http://bit.ly/2ZQyPeg

Russia on its way to complete abandonment of foreign-made IT software

The Russian technical Committee for Standardization Cryptographic Information Security (TC 26), controlled by the Russian Federal Security Service (FSB), has prepared draft recommendations on the use of the Russian-made cryptographic algorithms "Magma" (Magma) and "Grasshopper" (Kusznechik) in key protocols used to protect information on the internet. These standards were elaborated following the Russian "Sovereign internet" project and will first be distributed on the websites of government agencies and later to the entire segment of the Russian internet.
http://bit.ly/2KFKXex

MIDDLE EAST

Iran says US cyberattacks failed, hints talks are possible

Iran claims that US cyberattacks carried out on its military have failed. US media reported earlier that cyberattacks had been launched despite US President Trump calling off an airstrike on Friday morning. The Washington

Post said that the cyber campaign had been planned previously and that it successfully disabled Iranian launch systems. US officials have declined to comment.

https://reut.rs/2RtUu98

Number cyberattacks in of United Arab Emirates fall 43 percent so far in 2019

The Telecommunications Regulations Authority (TRA) of the United Arab Emirates (UAE) has reported a sharp decline in the number of cyberattacks on government, semi-government, and private sector entities in the UAE during the first five months of 2019. Defacing and blocking of government websites, including denial of service, hacking, deception, fraud, and identity and document theft are among the most common motives of hackers. The TRA says it has been launching awareness campaigns and shares best practices in the field to counter the cyber threat.

http://bit.ly/2RwIbcd

Sudan court orders company to end military-ordered internet blackout

A Sudanese court reportedly ordered local telecoms operator Zain Sudan to restore internet services, according to a lawyer. The blackout was order three weeks ago by Sudan's military rulers as a security measure, but it is harming the economy and humanitarian operations. The protesters are demanding that the military hand over power to a civilian authority.

http://bit.ly/31QeMyt

Microsoft launches cloud services in UAE

Tech-giant Microsoft will launch two regional cloud services from its new data center in Dubai and Abu Dhabi, according to the general manager for Microsoft Gulf. It joins a growing number of tech companies moving data centers into the region. Having the services run from local data centers allows

companies to meet regulatory requirements that data be stored in the country as well as allowing Microsoft to offer its services at higher connection speeds.
http://bit.ly/31QAmD5

APAC

Hackers hit global telecommunications in possible Chinese espionage campaign

Cybereason, a US-Israeli cybersecurity firm, first uncovered a significant espionage campaign targeting at least twenty individuals about a year ago. The hackers associated with Operation Soft Cell are thought to be linked to China. They hacked into ten global telecommunication companies, gaining unauthorized access to their networks, retrieving a large amount of personal and corporate data, as in call records, and as opposed to deploying malware. According to the Wall Street Journal, "Operation Soft Cell gave hackers access to the carriers' entire active directory, an exposure of hundreds of millions of users . . . creating high-privileged accounts that allowed them to roam through the telecoms' systems, appearing as if they were legitimate employees."
http://tiny.cc/1i808y

How apps power Hong Kong's "leaderless" protests

In response to the controversial extradition law in Hong Kong, it is estimated that "more than two million people have taken to the streets... to express opposition." The protests are assisted by Telegram and other online platforms powering the "protest turned civil disobedience campaign." The encrypted messaging apps enable anonymity and have a double-fold mechanism of security. "Some groups have up to 70,000 active subscribers, representing about 1 percent of Hong Kong's entire population. Many provide updates and first-hand reports relating to the protests, while others act as a crowdsourced lookout for police, warning protesters of nearby activity. There are also smaller groups made up of lawyers, first aiders, and medics. They provide legal advice

and get supplies to protesters on the front lines. Demonstrators say the online co-ordination of protests offers a convenient and instant way to disseminate information. The chat groups also let participants vote—in real time—to decide the next moves."

http://tiny.cc/64908y