Global Cyber Bi-Weekly Report by INSS February 1 2018

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

Contributors: Simon Tsipis, Ido Sivan, Matan Tomer, Sanjana Rathi, Anna Danilova

ISRAEL

Artificial Intelligence cyber-hacking arms race at full throttle

A group of Ben-Gurion University (BGU) experts warn that cyber defense can waste no time in playing catch-up. BGU expert Bracha Shapira said that cyberattackers using artificial intelligence (AI) "are winning . . . their role is easier . . . things are not great at this moment." In order "to defend, you must find all of the holes," and plug them, whereas AI cyberattackers "just need to find one hole." Shapira also said that AI is also important for defense, because even if cyberattackers have an advantage, simply using AI to slow them down could get them to move onto a different target. Another BGU expert, Yuval Elovici told the Davos Forum that "AI aims to create intelligent machines . . . When the attacker conducts malicious activity . . . he must make sure that he will remain undetected . . . the attacker employs various obfuscation techniques. The attacker conducts an AI-based detection analysis in a lab environment in order to understand whether the malicious code will be detected by an anti-malware tool. AI tests the code vis-à-vis every possible detection engine, and automatically re-crafts it, so it will remain undetected by existing tools and methods."

https://goo.gl/1Bd4FT

Israeli railway cyber protection company Cylus raises $4.7m

In May 2017, a cyberattack penetrated the German railway company's communications network. In the United Kingdom, four cyberattacks penetrated the railway's operating network in 2016 alone. Israeli startup Cylus, which develops cyber protection solutions for railways, has announced that it closed a $4.7 million round of seed funding. Cylus CEO Amir Levintal said that "The cyber products currently in the market do not speak the railways' language. The standard

technologies are adapted to IT, and we're dealing with signal communications—the mobile communications of a passenger train. Wireless communications that facilitates remote control of the train is subject to exploitation by an attacker trying to control the train and do harm to the passengers." Cylus CEO also said that a system, such as a firewall, which is capable of monitoring communications in the trains' systems, is liable to damage a train's operations. "A firewall is liable to make an error and block communications needed to control the train, thereby affecting the train and its safety. We don't intervene at all in the traffic on the network; we only detect the attacks and make it possible to deal with them."

https://goo.gl/NNYCGv

IDF sees move south as way to rebrand as tech giant

As the Israel Defense Forces prepares for the massive move of many of its units to the southern city of Beersheba —as part of a multi-year plan to streamline and digitalize the giant institution—it is using the logistical campaign to spruce up its game as well. The IDF aims to make sure, among other things, that the best and the brightest minds stay within the army ranks, rather than get lured away by the salaries that the tech giants are offering in the civilian market. The soldiers to be transferred to Israel's south "are the startup nation people. Our tech people—our tech front," said Lt. Col. Itai Sagi, who is responsible for setting up what the army calls its "tech campus in Beersheba," which will be the new home of the computer services directorate, also known as C4i, and the Cyber Defense Directorate in the south. The tech units are the most significant part of the IDF's relocation to Beersheba.

https://goo.gl/YtSS6p

UNITED STATES

Heat map released by fitness tracker reveals location of secret military bases

The popular fitness tracking app Strava proudly published a "2017 heat map" showing activities from its users around the world, but unfortunately, the map revealed what it should not have—locations of US military bases worldwide. Strava, which markets itself as a "social-networking app for athletes," publicly made available the global heat map, showing the location of all the rides, runs, swims, and downhills taken by its users, as collected by their smartphones and wearable devices like Fitbit.

http://bit.ly/2rOto3A

ATM makers warn of "jackpotting" hacks on US machines

Diebold Nixdorf Inc and NCR Corp, two of the world's largest ATM makers, have warned that cyber criminals are targeting US cash machines with tools that force them to spit out cash in hacking schemes known as "jackpotting." The two ATM makers did not identify any victims or say how much money had been lost. Jackpotting has been rising worldwide in recent years, although it is unclear how much cash has been stolen because victims and police often do not disclose details. The attacks were reported by the security news website Krebs on Security, which said they had begun last year in Mexico.

http://reut.rs/2FmLPy3

EUROPE

Government warns critical industries to prepare for cyberattack

The British government is urging critical industries to do more to protect themselves from the growing threat of cyberattacks. It is appointing sector-specific regulators to ensure that essential services are protected and has warned organizations that they risk fines of up to £17 million if they do not have effective cyber security measures in place.

http://bit.ly/2DK5He8

Government tackles digital skills with £40m Institute of Coding

Prime Minister Theresa May has announced a digital initiative aimed at solving the digital skills shortage in the United Kingdom. The £40 million Institute of Coding is a partnership deal with leading tech firms, universities, and industry bodies, in an effort to bolster future digital skills in this country. Last year, the National Audit Office (NAO) warned that the government's planning to provide itself with specialized digital skills did not keep pace with the scale of the challenges that lay ahead.

http://bit.ly/2no492F

Cyber venture capital firm, backed by ex-intelligence chiefs, plans European deals

A venture capital fund advised by former British and US intelligence officials is planning a string of acquisitions to create a pan-European cyber security specialist. C5 Capital aims to create a regionally-managed security service leader, combining the latest cloud-based cyber defenses, high levels of automation, and local regulatory knowledge, two of the fund's partners said in joint phone interview. "We have a pipeline of six to eight acquisitions we plan to do across Europe," C5 Chairman and partner Andre Pienaar, a former head of the risk management firm Kroll's African and Natural Resources business, told Reuters. C5 is advised by a strategic board, including the recent heads of the Government Communications Headquarters (GCHQ) and British Special Forces, the former chairman of the US Joint Chiefs of Staff, and a former top National Security Agency official.

http://reut.rs/2EaAhib

Major cyberattack on United Kingdom a matter of "when, not if," says security chief

The head of the National Cyber Security Center has warned that a major cyberattack on the United Kingdom is a matter of "when, not if," raising the prospect of devastating disruption to British elections and critical infrastructure. In remarks underlining newly released figures showing the number of cyberattacks on the United Kingdom in the last fifteen months, Ciaran Martin said the United Kingdom had been fortunate to avoid a so-called category one (C1) attack, broadly defined as an attack that might cripple infrastructure, such as energy supplies and the financial services sector. The United States, France, and other parts of Europe have already faced such attacks. Interference in elections would also constitute a C1 attack, as would a deliberately provocative move by a hostile state.

http://bit.ly/2n46rDN

RUSSIA

The British Ministry of Defense: Russia prepares attacks on critical infrastructure

According to the statement of British Defense Minister Gavin Williamson to the *Telegraph*, Russia is currently studying the British critical infrastructure and, in particular, the mainland power stations. This is necessary to carry out cyberattacks aimed at sowing panic and chaos in the country. In the event of a strike on the critical infrastructure and power plants in the United Kingdom, "thousands, thousands and thousands" may die," the minister warned.

http://bit.ly/2DHtz25

The Dutch secret services have been spying on Russian hackers since 2014

According to the Netherland's de-Volkskrant, the General Intelligence and Security Service of the Netherlands (AIVD) have been spying on the members of the Russian

hacker group Cozy Bear (also known as APT29), who are suspected of attacking the servers of the Democratic Party during the US election campaign in 2016.
http://bit.ly/2DG6tNn

Messenger platforms in Russia "fell prey" under the Anti-Terrorism Directive

The struggle of the Russian authorities with terrorism was reflected in the adoption of new laws, in particular, the law regulating messengers. It prescribes that from January 1, 2018, the instant messengers' platforms will be required to identify users by phone number on the basis of the relevant contract with the telecommunications operator. In case of non-compliance with this condition, messenger platforms will be punished with fines, and users may lose the opportunity to communicate.
http://bit.ly/2rIxhXF

MIDDLE EAST

Iran's main mobile operator establishes a CERT team

The Mobile Telecommunication Company of Iran (MCI) has established a computer emergency response team (CERT) to help educate consumers about cybersecurity and assist them in case of emergencies. The company has 47 million active users and they were quoted as saying they are open for collaborations with other operators and ICT-related firms. The main threats addressed by the company include fake mobile apps of popular apps like Avast, WhatsApp, and Waze, and list-dedicated malwares for smartphones that spread over mobile networks. The goal of the established team is to create a trusted database and emergency center that people can turn to when facing a cyberattack.
http://bit.ly/2DMNWif

Iran's "Halal" internet provides control and improved economic commerce at the same time

Iran faces a double standard when it comes to the internet. On the one hand, it seeks to strictly control cyberspace and social media and the flow of information to the public. On the other, the authorities encourage Iranians to widely use the internet, hoping to generate the benefits of a more modern economy. But the vast increase in smartphone usage in the past four years (from 2 to 48 million devices) also helped to spread the recent unrest and protests across the country. The regime's solution has been to create the so-called "Halal net," Iran's own locally controlled version of the internet aimed at restricting what the public can see online. In these settings, the encrypted messaging platform Telegram spread significantly, estimated to be used by over 40 million Iranians. The government had to temporarily block Telegram to control the recent unrest, but this also quickly brought complaints from business people who use Telegram to promote and sell their goods. The "Halal net" has some 500 government-approved national websites that stream content far faster than from websites based abroad, which are intentionally slowed down. According to an opposition group based in San Francisco, the Iranian regime have had success in getting business to work within its controlled internet and the more they do so, "the easier it will be for them to shut down the real internet when they want to."

http://bit.ly/2BAjC4s

Turkish defense contractors face spear-phishing attacks

An unknown actor purporting to be from the tax collection arm of the Turkish government has been carrying out spear-phishing campaigns against Turkish defense contractors. The targeting has been of a specific organization since November 2017, using documents that download a remote access Trojan named Remcos, which logs keystrokes, takes screenshots, records audio and video, and manages files. The targeting email supposedly comes from the Turkish government entity responsible for taxes. The email states that there is a possible tax exemption in place for the

receiver if they fill out the attached documents. Although the sender domain, gerlirler.gov.tr, is valid, the actual email Sender Policy Framework (SPF) verification failed in analysis.

http://bit.ly/2DzC1nR

A vulnerability in critical infrastructure systems was exposed in the Middle East

The France-based Schneider Triconex Safety Systems, which are heavily used across critical infrastructures worldwide, were exposed as vulnerable in Saudi Arabia. The company said that hackers had exploited a flaw in its technology in a watershed incident discovered last month, which halted operations at an undisclosed industrial facility. The system is used in nuclear facilities, oil and gas plants, mining, water treatment, and other plants to safely shutdown industrial processes when hazardous conditions are detected. It is the first reported cyberattack on this type of system and the US Department of Homeland Security is involved in the investigations.

http://reut.rs/2BCXW80

CHINA and APAC

India's Foreign Secretary Vijay Gokhale: Cyber security, big data are new areas of India-Israel cooperation

On the occasion of Prime Minister Netanyahu's visit to India, India's Foreign Secretary Vijay Gokhale announced in a press briefing that the two countries will be cooperating in new areas such as in the oil and gas sector and cybersecurity. A total of nine pacts were signed to boost cooperation after extensive talks were held between the prime minister of India and Israel to bolster ties in strategic areas. The critical issues discussed also included defense, trade, and terrorism. Furthermore, a large business meeting took place, in which cybersecurity and technology innovation were some of the discussed topics.

http://bit.ly/2GvWPdJ

Maersk Line invests heavily to secure its operators from cyberattacks

Maersk Line, the biggest container line operator serving India, has termed the 2017 cyberattack as an "extremely difficult" episode and has assured investment in its network to prevent any other global breach in the future. It has also assured that the system architecture has been revised to prevent risk and future attacks and was reported to have revised its business continuity plan again.

http://bit.ly/2rUGps6

Singapore and Malaysia ahead in cybersecurity, but concerns remain

According to a report by the global consulting firm A.T. Kearney, Singapore and Malaysia are leading the Association of Southeast Asian Nations(ASEAN) with an advanced cybersecurity policy and plan in place. The report also highlighted that a few countries have set up national agencies to consolidate and coordinate cybersecurity agendas. However, cybersecurity spending levels are still relatively low in Malaysia, when benchmarked against other countries, albeit higher than the regional average. Perhaps the most disturbing consequence of underinvestment in tackling cybersecurity threats is that companies in the ASEAN face a growing risk of cyberattacks, which could expose the region's top listed firms to a US$750 billion erosion in current market capitalization, the report found.

http://bit.ly/2BEo2as

Australia's cyber defenses "relatively weak, uncoordinated," former Australian Security Intelligence Organization boss David Irvine warns

David Irvine, a former spy boss who also heads the overseas intelligence agency the Australian Secret Intelligence Service (ASIS), has warned Australia that its ability to counter cyber threats and criminal activity is "relatively weak and uncoordinated." He has also called for a single Commonwealth-led cooperative agency, along the lines of the Cyber Security Research Center (CSRC). He has also asserted that Australia's national capacity to counter threats and criminal activity using cyber

investigative tools is relatively weak, uncoordinated, and dispersed across a range of agencies in both Commonwealth and state jurisdictions.

http://ab.co/2E2W3XD