Global Cyber Bi-Weekly Report by INSS January 1 2019

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

Contributors: Simon Tsipis, Anna Danilova, Gal Sapir, Michal Beit Halachmi, Stefan Weenk

ISRAEL

Boost and transform: Israeli developers are building the next big thing in blockchain in 2019

Industry experts have high hopes for Israeli developers and academics in 2019 to continue to transform uses for blockchain technologies. Yale Rozencwajg, founder of blockchain Israel says: "Blockchain will be the next big thing in Israel because it mixes all the technologies that we have here including AI, IoT, cloud, cybersecurity, etc., we have them all. Most of the products blockchain needs are here." The global community seems to acknowledge that Israel is a good country for blockchain innovations, as shown by the many investments from foreign organizations in Israel. "Israel is on the forefront of solving the real issues plaguing the blockchain world," Josh Liggett, a fintech and blockchain investment analyst, tells NoCamel.

https://bit.ly/2EYcAvQ

Intel prepares to expand manufacturing in Israel as part of global plan

Tech giant, Intel corporations, is expected to begin multi-year construction activities in 2019 to expand its manufacturing sites in the United States, Ireland, and Israel. "With the biggest market opportunity in Intel's history ahead of us, we will take the necessary steps to prepare our global manufacturing network for flexibility and responsiveness to changes in demand," Ann Kelleher, senior vice president and general manager of Manufacturing and Operations at Intel, wrote. The opportunities came about through the company's transitioning from being a maker of silicon computer chips to a data center company. The new activities range from manufacturing chips to developing safety features in vehicles, wireless phone connections, drones, and cloud-based technologies.

https://bit.ly/2LFJjar

Microsoft mulls acquisition of Israeli chipmaker Mellanox—report

Microsoft is currently negotiating with Mellanox, a Yokne'am-based firm, with the help of investment bankers Goldmann Sachs. Israel's Mellanox Technologies Ltd., a maker of servers and storage switching solutions, was already a key-client of Microsoft. The company is valued at $798 billion. The US technology giant sees the acquisition as a way to strengthen its services in cloud computing as it competes with Amazon and Google, the Marker said. Mellanox's revenue records increased 24 percent to $279.2 million from the growth in demand for its high-speed Ethernet adapters, switches and cables, for use in the cloud and enterprise data centers.

https://bit.ly/2EVy5gR

UNITED STATE

BevMo payment breach affects thousands, with researchers pointing to Magecart

The California based alcoholic beverage retailer fell victim to a data breach affecting its online store, exposing its customers from August 2 until September 26. Through malicious code installed on the checkout page, hackers retrieved customer's names, addresses, phone numbers, payment card credentials including numbers, expirations dates, and security codes. NCR Corporation, BevMo's supplier of point-of-sale systems and provides IT services, notified the retailer of the breach. BevMo branches are in four states but ships online orders to an additional eight states. The estimated impact is of 14,580 customers. Although not confirmed, aspects of the breach resemble JavaScript code associated with Magecart, a group of hackers known for targeting online payment information platforms and is linked to cyberattacks on British Airways, Ticketmaster UK, and Newegg. BevMo is conducting an independent investigation, cooperating with law enforcement and payment card companies.

https://bit.ly/2Ajn85p

US claim of broad spying campaign prompts Chinese rebuke

Chinese nationals Zhu Hua and Zhang Shilong, associated with Advanced Persistent Threat 10, were recently indicted and accused of coordinating an "extensive" hacking campaign estimated to have breached at least forty-five US companies and government agencies, spanning the banking, financial, telecommunications, biotechnology, automotive, health care, and mining industries. The hackers gained access to the computer system of the US Navy stealing personal data of more than 100,000 people, as well as successfully infiltrating NASA's Jet Propulsion Laboratory. China's Foreign Ministry spokeswoman Hua Chunying stated the accusations are "baseless" and the charges should be withdrawn "so as to avoid serious damage to bilateral relations." Echoed by both US Secretary of State Pompeo and Homeland Security Secretary Nielsen, the operation concerns a violation against the 2015 agreement between the United States and China regarding intellectual property theft and "forced technology transfers." These issues have intensified the current trade negotiations that the two countries are working on; since mid-summer, "the two countries have imposed tariffs on a combined $360 billion on each other's imports." The UK Foreign Office joined in agreement against the charges by releasing a statement claiming the hacking group is responsible for a cyber campaign "targeting intellectual property and sensitive data in Europe, Asia, and the U.S."

https://bloom.bg/2AkgVq4

Caribou Coffee reports data breach including payment information at 265 stores

Between August 28 and December 3, hackers had access to customer financial information from 265 branches across twelve US states out of 450 stores in the United States and 297 stores abroad. According to the American coffee retailer, point-of-sale systems were breached at affected locations, facilitating unauthorized access to customers names, payment card credentials as in numbers, expiration dates, and security codes. Caribou suspected abnormal activity in late November and hired Mandiant, a cybersecurity company owned by FireEye. The coffee seller is working with the FBI and has stated its ongoing efforts in strengthening its network security and improving its payment systems. Customers have been notified through email and a notice posted to the company's website. Particulars about the aggressors and the

scope of how many customers were affected is unknown. https://bit.ly/2s0hq4b

EUROPE

European Union to fund bug bounty programs for open source projects in January 2019

The European Union will foot the bill for bug bounty programs for fourteen open source projects, EU Member of Parliament Julia Reda announced this week. The bug bounty programs (recognition and compensation for reporting bugs) are being sponsored as part of the third edition of the Free and Open Source Software Audit (FOSSA) project.

https://zd.net/2AjTe0T

Stolen UK identities selling for as little as £10 on the dark web

Stolen personal data of UK citizens is selling for as little as £10 on the dark web, offering hackers all the information needed to carry out online fraud and identity theft, The Independent has discovered. So-called "fullz"—hacker slang meaning a "full ID" package—of UK citizens have been listed on several popular online black markets. A full ID package typically contains an individual's name, address, online passwords, banking data, and other key identifying information. Security researchers say the illicit trade of such data is being fueled by a seemingly ceaseless succession of high profile hacks.

https://ind.pn/2Ria8a9

Cyber security breaches rising across UK defense sector

UK defense secrets are increasingly being exposed to hostile nation states after the number of security breaches in the sector rose this year. Heavily-redacted records obtained by Sky News show an increase in incidents reported to the Ministry of Defence (MoD) between January and October compared to the same period in 2017. Sky News previously revealed the MoD and its partners failed to protect military and defense data in thirty-seven incidents throughout the whole of last year, with military data exposed to nation-state level cyber risks on dozens of occasions.

https://bit.ly/2R4AI6s

UK launches long-awaited cyber skills strategy

The UK government has launched a new cybersecurity skills strategy designed to reduce industry shortages and a new independent body to help shape the future of the profession. The Initial National Cyber Security Skills Strategy sets out not only to recruit more skilled professionals into the industry but also raise the awareness levels of the general workforce, improve education and training, and ensure the United Kingdom has a "well structured and easy-to-navigate" profession. To that end, a new UK Cyber Security Council will receive £2.5m of public funding to help in its mission to "lay the structural foundations" of the profession.

https://bit.ly/2Qi4UGO

RUSSIA

Britain military sees ISIS threat replaced by Russia, especially in cyber

Mark Carleton-Smith, the UK chief of the General Staff, claimed that Russia is a much bigger threat than was posed by al-Qaeda or ISIS, whereas its main battlefield is in non-traditional areas of cyber. "After the defeat of ISIS, we see Russia as a potential threat to British security," military official said.

http://bit.ly/2TgR49q

Putin's order to fight leaks of sensitive personal data implemented

Russia's Communications Ministry released draft legislation bill aimed at stopping leaks of personal information from state agencies. Sensitive data, including recent personal data of more than hundred GRU agents, was leaked due to an active black market of databases in Russia. All state agencies that handle personal data of government employees, including military, are now to consult with the Federal Security Service (FSB) regarding the means of collection, operation, storage, and security of sensitive data bases. The bill was published in response to direct instruction by President Vladimir Putin.

http://bit.ly/2AmFqml

Mueller's investigation uncovered twelve GRU agents who hacked Democrats

Special Counsel Robert Mueller, investigating Russian interference in US elections, reveals twelve names of Russian hackers as operative GRU agents, who hacked the Democratic Congressional Campaign Committee, the Democratic National Committee, and the Hillary Clinton campaign. All twelve GRU agents worked for GRU's Unit 26165 and Unit 74455.

https://thebea.st/2Vh0MdL

Russian authorities to suit Google for illegal operation of its search engine

A lawsuit was initiated by the Russian Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor) against Google, claiming that according to Russian legislation, search engine operators must exclude links to resources with illegal information from the search results. In order to comply with the Russian law, Google must be connected to the Federal State Information System, which contains a list of prohibited resources.

http://bit.ly/2GWUaOu

Mueller's final countdown: All that is left is to find Trump's connection to Assange

A document, leaked to the US press about Mueller's investigation, revealed a potential hint at President Trump's linkage to Russian intelligence, the GRU, during US presidential elections. As was revealed earlier, the US Special Counsel has alleged that Russian intelligence officers have hacked leading Democrats' emails and provided some of that material to WikiLeaks. It was also stated that the CIA confident that Julian Assange cooperates with Russia. Now Mueller is occupied with finding Trump associates' contacts with WikiLeaks. Thus, Mueller views all this as Russian interference operation, in which the GRU "provided" documents to WikiLeaks, with the remaining open question being whether Trump campaign associates were involved.

http://bit.ly/2rZdqRh

MIDDLE EAST

NYU Abu Dhabi-led cybersecurity research receives funding from Intel

NYU Abu Dhabi has been rewarded a research grant of three years of funding by Intel, equivalent to US $300,000 to support NYU Abu Dhabi Associate Dean of Engineering Ozgur Sinanoglu's research into new ways of securely testing and configuring computer chips by third-party companies. The NYU Abu Dhabi Associate Dean said, "The development of this obfuscation process represents a central breakthrough in the production of the computer chip. The NYUAD Design for Excellence team are immensely proud of the recognition that this project has received thus far." The NYUAD Design for Excellence lab is leading global developments on cybersecurity, providing both industry bodies and academic circles with insights around securer and safer computer systems.

https://bit.ly/2R09IG8

MBRF, DarkMatter team up to develop UAE cybersecurity talent

A new collaboration between the Mohammed bin Rashid Al Maktoum Knowledge Foundation (MBRF) and DarkMatter Group will develop digital talent for the UAE's cybersecurity sector. The partnership seeks to develop a steady stream of local professionals capable of taking on the challenges of cybersecurity. DarkMatter Group has created the Associate Talent Program (ATP), an initiative that will have the cybersecurity company partner with universities and government organizations in the UAE to jointly develop and employ local cybersecurity talent. The ATP program will undertake a series of collaborations between the public and private sectors on research and the publication of data. It will be focused on the acquisition of talent, promoting research and internet protocol while supporting wider moves toward digitization for the whole country.

https://bit.ly/2GM0pVx

APAC

Australia Anti-Encryption Law could risk privacy and security of smartphone users

The new law, which was passed by Australian Parliament on December 6, grants police and security agencies the right to ask app developers, agencies, and anyone dealing with communication services to produce encryption bypasses. Apple, Twitter, Google, Facebook, among others, sent out a strongly worded letter against the new law, claiming it is "deeply flawed, and lacking in independent oversight over the new authorities." Tech providers are concerned about the new law's ability to issue technical capability notices (TCN), which require the recipients to build decryption capabilities. Refusing to act can cost up 10 million AUD in fines. Apple claimed the law is not needed, as it cooperates with the Australian law enforcement, and over the last five years alone processed over 26,000 requests for information, to help in criminal and counterterrorism cases. Lawmakers said they will discuss amendments and concerns regarding the new law, when the Parliament reconvenes in the beginning of February 2019.

https://goo.gl/nnjgp1

North Korea's defectors' personal details leaked

In the first of its kind large-scale leak, personal details of nearly 1,000 North Koreans defectors were leaked via a personal computer in a center helping defectors in South Korea. There are twenty-five such centers, which contain information about nearly 30,000 defectors. North Korea is known for silencing dissidents who engage in anti-regime activities. The classified information was leaked from one of the computers, as a staff member opened an email with a malicious code. The Hana center, located in North Gyeogsang Province, South Korea, conducted a thorough inspection after the hack was discovered and claimed that it did not find any other leaks, while it promised to increase the centers' efforts and alertness to prevent further hacking attempts in the future.

https://goo.gl/TKmSV7

Two Chinese nationals indicted on charges of hacking US government and military targets

The two hackers, named Zhu Hua and Zhang Shilong, worked for the Chinese company Huaying Haitai and with the Chinese Ministry of State Security's Tianjin State Security Bureau, sought to steal data from roughly forty-five US tech companies. The operation's time span started as early as 2006 and involved aviation, satellite tech, pharmaceutical, oil and exploration companies, and more. One of the hackers was part of a Chinese crew dubbed APT10. NASA was one of the only named companies in the indictment, which had discovered hacking attempts of their Goddard Space Center and Jet Propulsion Lavatory. APT10 is also accused of stealing personal data of over a 100,000 navy personal. US Deputy Attorney General Rod J. Rosenstein said that more than 90 percent of the Department of Justice cases involve China, violating a commitment that China made in 2015 to stop attempts to steal economic trade secrets and confidential information.

https://goo.gl/DtuKFW