Global Cyber Bi-Weekly Report by INSS January 1, 2020

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

Contributors: Simon Tsipis, Donal Byrne, Thomas Abma, Lea Abramski, David Murcia Briceño

ISRAEL

China might have stolen the secrets to Israel's Iron Dome missile defense

According to a report published by Cyber Engineering Services, a cybersecurity firm based in Maryland, hackers breached the corporate networks of three top Israeli defense technology companies, including Elisra Group, Israel Aerospace Industries, and Rafael Advanced Defense Systems. Brian Krebs, a cybersecurity analyst, states that attackers succeeded to steal a significant amount of critical data constituting intellectual property and technical documents— apparently part of the Iron Dome defense technologies. The cybersecurity company suspects the attackers to be part of the "Comment Crew," a hacking group allegedly linked to the Chinese military body. Another company based in Virginia, Mandiant, identifies this group as "the 2nd Bureau of the People's Liberation Army General Staff Department's 3rd Department," also known as Unit 61398. This unit has been particularly active in stealing US sensitive information and several of its alleged members have been already indicted by the US Department of Justice.
https://bit.ly/2sAn8NY

Open banking requires rethinking about API protection

The Bank of Israel's open banking pronouncement reveals the need for application programming interfaces (APIs) protection solutions. According to Doron Chema, CEO of L7 Defense, "an API is any 'logical point' on application servers or a website that can respond to requests from outside, such a 'point'

can send files in response to a request, stream songs, execute money transfers in an app and more. In fact, every user action on a site or in an app usually activates a large number of APIs behind the scenes." The shift to open banking promoted by the Bank of Israel will facilitate third party FinTech companies' access to customer bank data and will roll out in three stages. Chema further explains that "implementation of this regulation requires information disclosure via bank APIs to third parties, to protect information in today's open world; each API needs separate handling for specific needs. Existing solutions such as Legacy Web Application Firewalls (WAFs) aren't specific and only protect against average characteristics of APIs in the context of an app or website."
https://bit.ly/37oEbBl

Popular messaging app is UAE spy tool, developed by firm employing ex-NSA and Israeli intelligence officers

According to a New York Times report, the communication platform ToTok that was recently developed by an Emirati firm Breej Holding and has been available for a few months is actually a spying tool used by the Emirati government. Since its creation, the app has been downloaded by millions of users in the United Arab Emirates and abroad, becoming one of the 50 most popular free apps in many countries, such as the United Kingdom and Saudi Arabia. The American newspaper stated that Emirati intelligence services used the app to access personal information of its users, messages and conversations, localization data, contacts, camera, and microphone. The firm that designed the app is suspected to be owned by DarkMatter, an Abu-Dhabi-based cybersecurity firm allegedly linked to the UAE intelligence agency that has already been subject of controversy regarding its activities and practices. In fact, the company was recently criticized for trying to attract ex-Israeli intelligence officers by offering them high salaries and a comfortable life in Cyprus. While the FBI has reportedly started to conduct cybercrime investigations, Google and Apple shut down the platform. Furthermore, the app's founder, Giacomo Ziani, denied spying allegations and

assured that the app respected data privacy rules in accordance with local and international standards. He explained that the firm was currently working with online stores to reinstate it.

https://bit.ly/2tbHFZ8

https://bit.ly/2ZB62LN

https://bit.ly/2swmTDz

Cyber giant Check Point acquires Jerusalem start-up Protego

With the aim of advancing cloud security capabilities, prominent cybersecurity company Check Point Software announced the acquisition of the Jerusalem-based start-up Protego for an undisclosed amount; Check Point secures more than 100,000 organizations globally. Protego develops serverless security technology that "prevents malicious attacks on serverless functions in run-time, and prevents vulnerable code from being deployed into production." Vice President of Products at Check Point, Dr. Dorit Dor, states, "on their journey to cloud transformation, organizations require a new security paradigm to protect against 5th and 6th generation of cyberattacks."

https://bit.ly/2ubSGu9

UNITED STATES

Coast Guard says Ryuk ransomware hit systems that monitor cargo transfers at maritime facility

Despite the US DHS's Cybersecurity and Infrastructure Security Agency ransomware advisory, in addition to the Coast Guard bulletin, one of the Coast Guard's marine transportation facilities was breached. The US Coast Guard revealed their computer networks were breached by Ryuk ransomware, resulting in the disruption of the "entire corporate IT network, camera and physical access controls, among other tasks." Primary operations were shut down for about 30 hours.

https://bit.ly/2tebA2R

CyberCom mulls aggressive tactics if Russia interferes in next election: report

According to the Washington Post, the US Cyber Command has a new strategy in order to counter possible Russian interference in the US 2020 election. Nevertheless, the strategy is not directed against Russian president Vladimir Putin, as it could be a "provocative measure." According to a report compiled by the intelligence community from November 2019, Russia's "top goal for its 2020 operations would be to sow discord" in the United States; for this reason, the Defense Department spokesperson Elissa Smith argued that actions will be taken in order "to disrupt or degrade malicious nation-state cyber actors ability to interfere in U.S. elections." These measures are on the backdrop of previous efforts taken during the 2018 midterm election, as in blocking "internet access for a major Russian troll farm."
https://tiny.cc/1ew7hz

2019: The year ransomware targeted state and local governments

The recent year has been a challenge for cybersecurity experts in order to protect financial and information data in the United States. Since 2019 started, multiple cyberattacks have been registered in states like Louisiana, Texas, and Florida. Hospitals and local institutions have suffered cybercrimes. However, regular citizens are the favorite target for ransomware, especially as it relates to financial operations. According to experts, the reason for this growth in cyberattacks at the local level is the lack of preparation. Hackers see a better opportunity to commit cybercrimes on a small scale, since the risk of being discovered is much lower than it is with large banks or government departments such as the Department of Defense. Another reason is once a small entity is victim of a cyberattack and its numbers are affected, it has to respond to its costumers soon, even if it was not at fault; thus, the time of taking action is much less than it is for a larger company, since they can have better options to respond to these crimes. The number of cyberattacks has

increased with several consequences. Between January and October, 2019, 140 local governments, police stations and hospitals were affected by cyberattacks. For example, hospitals in Alabama had to stop accepting new patients because ransomware had damaged their databases. Unfortunately, the expectations for 2020 regarding cybercrimes is hopeless, since experts affirm there will be new targets, so enterprises have to be aware.
https://tiny.cc/h0w7hz

Licensing, cybersecurity power BlackBerry's beat, shares rise 10%

The Canadian company Blackberry Ltd. beat quarterly profit estimations. The key was its patent licensing and cybersecurity businesses; in nine months, the enterprise increased its shares by 10%. The famous company, a pioneer for the sales of smartphones, decided to offer data security for diverse organizations. Today, Blackberry has acquired diverse cybersecurity enterprises, and one of them is Cylance, the Californian company that created software that uses machine learning to evade security breaches. This acquisition meant 40 million dollars in revenue for Blackberry. Cybersecurity has become an international concern and a rentable business. Blackberry revenues for the third quarter are $280 million dollars. Nevertheless, there are fields where the company is not competitive, such as in the sales of software. According to Reuters, the company reported a decrease of 3% or US $145 million dollars in technology solutions and enterprise software and services.
https://tiny.cc/tdx7hz

EUROPE

Ransomware hits Maastricht University, all systems taken down

Maastricht University (UM) announced that almost all of its Windows systems were encrypted by ransomware following a cyberattack that took place on December 23. It is currently unknown if the hackers also accessed and

exfiltrated scientific data during the attack. UM says that all the university's systems were taken down as a precautionary measure during investigations.
https://bit.ly/35cYJLr

Sweden's defense minister on relations with America, Russian threats, and the European Union

Swedish Defense Minister Peter Hultqvist visited Washington DC recently and shared his thoughts on the security situation in the region. "The nation expects to complete a new defense funding agreement in the coming year, which should set the tone for military modernization through 2025." Since the signing of the trilateral agreement a year and a half ago between the United States, Finland, and Sweden, the countries have exercised together and shared information, nurturing interoperability. In terms of cyber capabilities, Sweden has 100,000 activities in the arena annually.
https://tiny.cc/7jx7hz

Researchers: Chinese advanced persistent threat espionage campaign that bypasses 2FA

An advanced persistent threat espionage campaign with suspected ties to the Chinese government quietly targeted business and governments in ten countries over two years, bypassing two-factor authentication. Wocao, as the campaign is dubbed, managed to stay under the radar, according to the Netherlands-based security firm that reported about the campaign. The report further notes that after bypassing the authentication, the attackers proceeded to collect and exfiltrate data and communicate with the command and control of the affected organizations. Several European countries, the United States, and companies within China itself were likely targeted.
https://bit.ly/2u4gOyN

RUSSIA

Unplugged internet: New challenge for Russian government

After several tests, the Russian government has announced its success at providing internet to the whole country; however, according to experts, this technological advance could be understood as a new control measure over citizens, although the debate is open. In recent years, the Russian government has implemented several measures of control, as it is necessary for the Kremlin to strengthen cybersecurity. Nonetheless, citizens have protested because it is considered a new policy of control, following the example of Iran and China, which have controlled the freedom on the internet. The Russian measure permits wide connectivity, but also restricts access to foreign web pages or external information. For example, the BBC news pointed out that Russia is planning to create its own Wikipedia, called the Great Russian Encyclopedia. "Regarding Wikipedia. .. it's better to replace it with the new Big Russian Encyclopedia in electronic form. It will be, in any case, reliable information in a good, modern form," Putin said. Also there is a bill that bans the sale of smartphones that do not have Russian software pre-installed. This measure is not a new one. In the last years, the Russian government has tried to increase online control, but regarding this new measure, there is a lack of information. The only information available is reported by the state-owned Tass News Agency about the ability of this measure to stand up to "external negative influences."

https://tiny.cc/vgx7hz

https://bit.ly/2swQ9Kq

Yandex, Youtube, Artificial Intelligence: Medvedev answered questions from journalists

The Russian government has developed its own national internet network and is integrating Russian-made software in electronic devices in order to secure itself from the World Wide Web. Russia's most acute concern is that nobody "would cut us off the internet, if someone suddenly desires to do so," said

Prime Minister Dmitry Medvedev at a large annual press conference in Moscow. Among other topics, Medvedev elaborated on regulation of activities among IT companies, stating they are necessary but should not be "excessively tough," highlighting Yandex, one of the heavyweights in the domestic IT markets. Such companies, including Youtube, fuel the Russian economy in which Medvedev reiterated its significance. The discussions centered on Russia's RuNet (Internet) Law—entered into force on November 1, 2019—enabling Russian authorities to control data traffic and access to the global internet, the latter perceived as allowing the government the power to disconnect the country from the global internet. Medvedev reiterated that the law "is not aimed at banning" anything but provides for "integrity, stability and security of the internet in the event of external threats." The conversation continued on the topic of artificial intelligence, which Russia has been developing in recent years; according to the Ministry of Communications, the market has the potential to grow to 160 billion RUB by 2024.
https://bit.ly/2QatKLK

Police expose "world's most harmful cyber crime group" Evil Corp

Russian hacking group Evil Corp is considered by the US authorities as the most dangerous and the biggest hacking gang in the world today, due to the sophistication of the hacking attacks and the global scale of their operation. Two members of the notorious Russian hacking group have been indicted in the United States following an international law enforcement operation, which included the FBI, the NCA, and the National Cyber Security Center. Maksim Yakubets from Moscow and Igor Turashev from Yoshkar-Ola have been charged with computer hacking and bank fraud schemes that netted the gang hundreds of millions over the last ten years.
https://bit.ly/2SBlYfK

Putin signed a law on the pre-installation of Russian software on gadgets

Russian authorities are to obligate manufacturers of local electronic devices and importers of foreign-made gadgets to pre-install them with Russian-made software. This includes operational systems, platforms, and apps. In particular, Russia's President Vladimir Putin signed a law on the mandatory pre-installation of Russian software on electronic equipment, including smartphones, computers, and televisions with the Smart TV function.
https://bit.ly/2Quo7Hj

APAC

This China-linked espionage group keeps trying to hack the Cambodian government

A Chinese espionage organization known as Rancor has been particularly active in attempting to break into the network of an unnamed Cambodian government organization and deploy their custom malware. First, the group laced a Microsoft Excel document with previously undocumented malware in an attempted breach of the Cambodian organization. While this failed, Rancor packed a computer script with a number of potentially infectious codes. This highlights the lengths to which well-resourced groups will go to develop their own hacking tools. It is believed none of the attacks on the Cambodian government organization were successful; the target blocked the malware in every attempt. The exact Cambodian government organization that is being targeted is not publicly known; however, it is believed to be an organization in which the attackers have a specific interest and will continue to attack. The Chinese government has looked to project its military and economic power throughout the Southeast Asia region. Furthermore, prior to the July 2018 general election in Cambodia, China-linked hackers breached the networks of the opposition political party.
https://bit.ly/2ZCjhfd

Chinese state "likely" linked to cyber spies targeting human rights workers

A new report has claimed that it is "likely" that a cyber spy group linked to the Chinese state has targeted human rights campaigners working on issues related to China for up to five years. Dubbed Bronze President, the espionage group deployed malware against its alleged victims in order monitor their activities and steal documents. One of the alleged targets is understood to be a human rights group that has raised concerns about the treatment of hundreds of thousands of Uighur and other Muslim minorities in China. It has also written about pro-democracy activists in Hong Kong. The non-governmental organization (NGO) asked not to be named in relation to the report. Secureworks said it was aware of a "handful" of NGOs that it believes had been targeted but that the number could be higher. As well as NGOs, the cyber spies also allegedly targeted law enforcement agencies and political entities operating in countries surrounding China, including India and Mongolia. Secureworks said its researchers had been observing the activities of the cyber espionage group since the middle of 2018, but the campaign could have begun as far back as 2014.
https://bit.ly/2QbdudN

Strengthening cybersecurity in ASEAN

At present, Southeast Asian countries are behind when it comes to their cybersecurity capabilities. Based on a report by global management consultants AT Kearney, ASEAN countries are also subject to numerous cyberattacks, with Indonesia, Malaysia, and Vietnam serving as global launchpads for malware attacks. In October 2017, the personal information of around 46 million mobile subscribers in Malaysia was compromised. The personal details leaked included home addresses, national identification card numbers, and SIM card information. Singapore has also been the victim of cyberattacks. In 2017, the country was the target of three major cyberattacks, namely the Ministry of Defence cyber breach in February, WannaCry

Ransomware attacks in May, and Petya Ransomware activity in June. These incidents highlight how far behind the region is in terms of cybersecurity. According to data from AT Kearney, Southeast Asia is not spending enough to protect its citizens from cybersecurity attacks. Despite high levels of growth, data shows that ASEAN member states spent an estimated US$1.9 billion in 2017 or only 0.06 percent of the region's gross domestic product (GDP) on cybersecurity. The financial impact from cyberattacks on the region can be crippling and devastating going forward.
https://bit.ly/2te9IXS

Cybersecurity market in India rise to US$3.05 billion by 2022: Study

India's cybersecurity market is expected to register an annual growth of 15.6 percent and rise to USD 3.05 billion by 2022 from USD 1.97 billion in 2019, a report has said. The transaction value of digital payments in India is estimated to grow annually at a rate of 20.2 percent from about USD 64.8 billion in 2019 to USD 135.2 billion in 2023, the report by PwC India and Data Security Council of India (DSCI) said. "Driven by the digitization of the country's business environment and the Digital India mission, among others, the cybersecurity market is expected to rise from USD 1.97 billion in 2019 to USD 3.05 billion by 2022—a CAGR of 15.6 percent— almost 1.5 time the global rate," it said. Digital growth, rising cyberattacks, and stringent regulatory mandates are the three main factors driving India's cybersecurity market. India's cybersecurity market will be defined by three key sectors—banking and financial services industry (BFSI), information technology (IT), and information technology-enabled services (ITeS), and government—and altogether, these sectors will account for 68 percent of the cyber market share.
https://bit.ly/36azUkV

MIDDLE EAST

Iran wants to create cryptocurrency to confront "economic hegemony of United States"

President of the Islamic Republic of Iran, Hassan Rouhani, proposed the creation of a Muslim cryptocurrency at an Islamic Conference in Malaysia. Indeed, as the Iranian president was invited to this conference in Malaysia, gathering leaders of major Muslim countries such as Turkey and Qatar, he suggested the idea of a Muslim cryptocurrency as a mean to fight against American economic hegemony. It was the first time Iran and Turkey publicly announced the opportunity of creating a cryptocurrency. It is not the first time that countries try to circumvent US economic sanctions with the creation of a cryptocurrency, enabling them to avoid the use of the US dollar. North Korea already announced in September 2019 that it will design its own cryptocurrency and Venezuela showed how this project could be achieved by launching its Petro —national oil-baked cryptocurrency—in 2018.
https://bit.ly/39yV0vo

Twitter removes nearly 6,000 accounts spreading Saudi-backed propaganda

The social media platform Twitter announced the removal of 5,929 accounts allegedly tied to a man suspected to be recruiting Twitter employees to obtain personal data of Saudi dissidents. Indeed, the company stated that the accounts were part of a "significant state-backed information operation" operating from Saudi Arabia. According to Twitter's blog article, the accounts were apparently part of a larger campaign counting more than 88,000 accounts intended to spread favorable information about the Saudi Kingdom on social media. Twitter attributes the campaign to a Saudi marketing firm, Smaat, co-led by Ahmed Almutairi. In fact, the Saudi national Almutari, also known as Ahmed Aljbreen, is already wanted by the FBI for similar charges since he allegedly succeeded to convince two Twitter employees to gather information on Saudi activists in the past.

https://bit.ly/36eM3Fc

DIFC's regulator rolls out platform to help reduce cybersecurity risks

The Dubai Financial Services Authority's (DFSA) chief operating officer, Waleed Al Awadhi, stated that the DFSA is taking cyber risks and threats very seriously and is willing to improve awareness and resilience. Indeed, the financial authority plans to design and launch a platform helping companies in the Dubai International Financial Center to implement measures aiming to prevent them from cyberattacks and vulnerabilities. The project will be the first of its kind regulator-led cyber intelligence platform in the region and will be operated and managed as part of a joint initiative coordinated with Help AG, a cybersecurity firm. According to Bryan Stirewalt, chief executive of DFSA, the platform aims to strengthen the cybersecurity area and to fight against non-traditional threats by fostering public-private partnerships.
https://bit.ly/2Q77qmu

LATIN AMERICA & CARIBBEAN

Online purchases spike in Latin America, Caribbean as millennials gain greater economic power

Millennials have become an international cultural reference. Born between 1981 and 1999, the generation has a tendency especially for living in the moment. According to the report "Examining the Latin American and Caribbean E-commerce Market," online sales in Latin America and the Caribbean are expected to grow 21.3 percent. It means at the end of 2019, the expectation is around US $71.34 billion. The report points that this growth is linked to the fact that millennials represent 30 percent of the population in Latin America and the Caribbean. For example, the selling of smart devices, such as mobile phones, has enabled the rise of online acquisitions. In countries like Colombia, Mexico, and Brazil, women and men between 18 to 50 years are considered regular online costumers. Brazil leads the frequency

of online purchases. In countries like Peru and Chile, online purchases are less frequent, averaging one purchase every month. The report points out that the common fears of people when they are doing online-shopping, including that the credit card data could be robbed or that the shipping costs are too high. Biometrics become a useful tool in protecting information.
https://tiny.cc/6ux7hz

The Organization of American States (OAS) recommends patience regarding implementation of National Cybersecurity Strategy

In the second semester of 2019, the Mexican Government published the National Cybersecurity Strategy. After this success, several cybersecurity events have occurred affecting bank operations, insurance companies, and telecommunication companies. These irregularities affected the National Oil Enterprise Pemex. However, a high officer of OAS revealed that Mexico is facing a regularization process, meaning several changes in institutions, such as the National Guard, and therefore patience is necessary for implementing the strategy. It is important to note that OAS was a crucial actor during the implementation of the National Cybersecurity Strategy in 2017. Nevertheless, as the officer argued, OAS has a monitoring process, but it is the responsibility of each state. Colombia is a good example in terms of cybersecurity, since the South American nation has implemented a tracking matrix in order to supervise diverse cybersecurity strategies. OAS has a cybersecurity program with several years of experience, and since 1999, the international program works in three different aspects: (i) Policy Creation; (ii) Capacity development; and (iii) Research and knowledge generation.
https://tiny.cc/0wx7hz

28 women highlighted in cybersecurity in Chile

The Chilean Cybersecurity Alliance awarded 28 women for their duty in the field of digital security. With this recognition, the Chilean Cybersecurity

Alliance seeks to make visible the labor of many women who work in multiple areas within the digital field. It also wants to challenge the stereotypes about women in a field dominated by men. Among those present at the ceremony were the presidential advisor in cybersecurity and the undersecretary of the Ministry of Women and Gender Equity, as well as scholars and representatives of centers of knowledge. The group of 28 women included engineers, lawyers, managers, teachers, and communicators, all experts in cybersecurity. According to statistics presented by the World Economic Forum in its Global Gender Gap report, the presence of women within the technological labor market is minimum. For example, just 12 percent work in cloud computing, 15 percent in big data and 26 percent in artificial technology. Finally, the undersecretary of the Ministry of Women and Gender Equity, Carolina Cuevas emphasized the relevance of social networks nowadays, since there are massive channels of information where users can find fake news or disinformation, for that reason it is fundamental to understand the participation of women in this field.
https://bit.ly/37n1nzK

Cybersecurity firm Adjust expands its footprint in Latin America

Latin America is increasingly becoming a remarkable region for companies to expand its business. Adjust Company is a great example. The German corporation, which provides fraud prevention and cybersecurity services, has announced its expansion of operations with a new office in Mexico City. This new strategy of Adjust is the response to new growth of the cybersecurity market in Latin America. For this enterprise, Mexico is a great opportunity "to invest in the market and help app marketers there unify and safeguard their advertising efforts." The German company has had remarkable feedback and outcomes in cities like São Pablo. Currently, Adjust is planning to inspire data-driven marketers in building apps in Mexico. According to its web page, Adjust has tested around of 30.000 apps worldwide for international organizations such as Procter & Gamble, Rocket Internet, and Tencent Games.

In addition, the Company has 16 international offices with 400 employees. Clients of the company include Dafiti and FinTech firm Itaú.

https://bit.ly/36bxdzo