

Global Cyber Bi-Weekly Report by INSS

February 1, 2020

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

Contributors: Simon Tsipis, Yael Elharar, Rachele Buffa, David Murcia Briceño

ISRAEL

Fear of information leakage: Discount Paybox application malfunction

Israel Discount Bank reported on the Israel Stock Exchange that as a result of a malfunction in the Paybox payment app, partial information of customers was leaked. Users were notified that they were disconnected from the account and had to reconnect. The bank became aware of the incident on January 19, but it was disclosed only ten days later. The incident reported that some of the users' details were leaked, but no information that could cause them direct financial damage. The information leaked included phone numbers, the last four digits of credit cards, usernames, and dates of birth. To date, users have not experienced any harm as a result of this incident. Discount Bank purchased the Paybox app three years ago with a pool of 180,000 users and currently has 1.7 million downloads. The Bank of Israel issued a statement, that it is closely monitoring the incident, and after having consulted with the National Cyber Directorate, it instructed Discount Bank on the necessary actions to be taken to handle the case. The privacy authority announced that this is a serious information security breach and is still examining the extent of the violation to Paybox customers and compliance.

<https://bit.ly/2v1wltS>

Harel Insurance has become a stakeholder in the cyber company Tufin

Harel insurance company has become a stakeholder in the Tufin cyber company. Tufin is listed on the New York Stock Exchange for \$515 USD

million. According to a report issued by Harel Insurance to the US Securities and Exchange Commission, it holds 5.4 percent of the company's shares, at the current value of \$28 USD million. Harel is the first institutional body in Israel to become a stakeholder in Tufin. Harel may have made the deal after identifying an opportunity due to the fall of the stock three weeks ago in light of Tufin's earnings warning. Tufin provides cyber solutions aimed at helping organizations enforce information security policies in various environments. Tufin was founded by CEO Ruby Kittuv and VP Reuven Harrison. It was issued on Wall Street for the first time last year at a value of \$480 USD million. As mentioned, Tufin's earnings warning issued in early January dropped the stock to a low of \$13 USD a share, but since then it has recovered slightly and the stock is now worth \$14.8 USD a share, having decreased from \$17 USD a share at the end of 2019.

<https://bit.ly/2tnYdO5>

Check Point has discovered severe security weakness in the TikTok application

Israeli company Check Point has discovered serious security weaknesses in the popular TikTok app, the popular video-sharing social networking service used to create short lip-sync, comedy and talent videos. The application is widely used among young people from around the world and Israel and currently has over one billion users. According to Check Point investigators, the security breach allowed attackers to send a malicious link via a message from within the app's messaging system. Once users clicked on the attacker's link, the attackers could manipulate the videos in a variety of ways: upload, delete, and take further action without permission. In addition, through a sub-site of the app, attackers could access users' personal information. Check Point informed TikTok of its findings, and TikTok corrected the weaknesses and announced that it encourages information security investigators to pass on weaknesses so that it can immediately rectify them and maintain a high level of information protection. The TikTok app was developed by Chinese giant ByteDance and is gaining popularity among Westerners as well, raising US concerns that the

Chinese government could take advantage of the service to compromise US national security. Oded Vanunu, head of Product Weaknesses at Check Point, who heads the current study, warned that users of the most popular applications assume that they are very secure, but, in fact, "hackers invest a great deal of resources and efforts to penetrate them, due to the vast amount of personal information available to each user. Our research proves that even the most popular apps in the world are at risk."

<https://bit.ly/2u5mAAy>

UNITED STATES

Pentagon finalizes first set of cyber standards for contractors

The Pentagon has finalized the long anticipated cybersecurity standards, contractors will have to follow before winning contracts from the Department of Defense, a new process called the Cybersecurity Maturity Model Certification (CMMC) 1.0. The model is a tiered cybersecurity framework that grades companies on a scale of one to five based on the level of classification and security necessary for the work they are performing. Previously, the Pentagon did not have a unified standard for cybersecurity that businesses needed to follow when bidding for contracts. Officials explained at the end of January that the CMMC will follow a crawl, walk, run approach to ensure companies are not unprepared for the change. The accreditation board is in the process of training the auditors that will oversee the certification. Once the requirements are met, a company's certification is good for three years.

<http://tiny.cc/tebijz>

Exclusive: FBI probes use of Israeli firm's spyware in personal and government hacks – sources

The FBI is investigating the role of Israeli spyware vendor NSO Group Technologies in possible hacks on US residents and companies as well as suspected intelligence gathering on governments, according to four people familiar with the inquiry. The probe began in 2017, when FBI officials began

investigating whether NSO obtained from American hackers any of the code it needed to infect smartphones, said one person interviewed by the FBI then and again last year. NSO said it sells its spy software and technical support exclusively to governments and that those tools are to be used in pursuing suspected terrorists and other criminals. NSO has long maintained that its products cannot target US phone numbers, although some cybersecurity experts have disputed that. The FBI conducted more interviews with technology industry experts after Facebook filed a lawsuit in October accusing NSO itself of exploiting a flaw in Facebook's WhatsApp messaging service to hack 1,400 users, according to two people who spoke with FBI agents or Justice Department officials.

<http://tiny.cc/ctaijz>

WhatsApp to stop working on millions of phones

Android and iPhone devices that only support outdated operating systems will no longer be able to run the Facebook-owned app. WhatsApp said the move was necessary in order to protect the security of its users. Smartphones using Android 2.3.7 and older and iPhone iOS 8 or older will be affected by the update. The operating systems that WhatsApp is ceasing to support are legacy operating systems, which are no longer updated or installed on new devices. Most users will simply be able to update their operating systems in order to continue using the messaging service. However, certain devices, such as the iPhone 4—which only supports iOS 7—will no longer be compatible with the app. "WhatsApp clearly had no option but to ensure its service remains secure, however it faces the difficult side-effect that the app is no longer compatible with older smartphones," said CCS Insight analyst Ben Wood. "This is likely to disproportionately impact the long-tail of its users, particularly in growth markets where there is a high proportion of older devices." WhatsApp, which was one of the most-downloaded apps of the decade, first warned users that these changes would happen back in 2017.

<http://tiny.cc/bwaijz>

Treasury wants more info on financial sector cybersecurity risks

The Department of the Treasury wants to better understand cybersecurity risks facing the US financial sector's critical infrastructure. According to a recent notice in the Federal Register, the department is soliciting comments from the public and federal agencies about an information collection effort Treasury wants to start "to enhance the security and resilience of financial services sector critical infrastructure and reduce operational risk." The new information collection is being proposed by Treasury's Office of Cybersecurity and Critical Infrastructure Protection.

<http://tiny.cc/2mbijz>

EUROPE

Why Britain's Huawei decision frustrated lawmakers

The decision by UK officials to allow Chinese telecom company Huawei to build parts of the country's 5G network was met with ire from members of the US Congress on January 28, as several members argued the decision will hurt the relationship between the two allies. Senior US officials have lobbied allies to ban Huawei technology outright from networks. However, according to a statement from the British government, Huawei could build parts of the country's 5G infrastructure but will be restricted from working on pieces of the network that are "critical to security."

<http://tiny.cc/dkbijz>

Italy watchdog threatens Facebook with another fine over improper use of data

The Italian Competition Authority has sued Facebook for lacking transparency in storing and exchanging the personal information of the users. The legal action has terminated with the infliction of a fine valued at 5 million euros to the company, which has accepted to rectify and adopt a more correct policy with regards to the "terms of service" and to the source of its income.

<https://reut.rs/2OgquNU>

Cyber security: Signed accord between CIOC and the University of Naples Federico II

Brig. Gen. Francesco Vestito, the commander of the Joint Cyber Command (Comando Interforze per le Operazioni Cibernetiche) and Prof. Gaetano Manfredi, the dean of the University of Naples Federico II have sealed an operative agreement for the execution of the joint cybersecurity activities to study the IT system of the academic institution and understand its vulnerabilities. This deal is a milestone for the implementation of the so-called "cyber ecosystem," i.e., a virtuous and self-sustaining circle to fulfill the public administration and nation cybersecurity needs through a multidisciplinary approach. The aim of this initiative is twofold: guaranteeing trained and skilled personnel of the defense and the widespread availability of sectorial expertise. Indeed, Brig. Gen. Vestito has highlighted the central role of the university to prepare adequately the future ruling class both in the civil and military sphere who will be called upon to confront the growing cyber threat. Indeed, this university is also party to another important agreement, with Leonardo Company to execute "the Aerotech Academy." This is an aerospace training course for young professionals focused on a multilayer approach providing the necessary skills and operational competencies applicable to the high technology industry.

<http://bit.ly/2RW1MmP>

<http://bit.ly/2Gtsi1z>

The Italian cybersecurity is law, so Parliament has strengthened the perimeter

The urgent necessity to guarantee and consolidate cybersecurity has prompted Italy to tackle three challenging actions. The first is the adoption of the ad-hoc law on "the national perimeter of cyber security;" the second is the fulfillment of the Directive NIS obligations (EU Directive on security of

network and information systems); and the last concerns the identification of the competent actors and their relationship with the Ministry of Economic Development. On September 21, 2019, the Decree Law 105/2019 went into force; its goal is to formulate a framework of the national cybersecurity and to guarantee a high level of protection to the IT systems, the public administration's computer services, and to the governmental and private entities operating essential functions for Italy's national security. This law introduces the following aspects: first, the novel risk management approach is according to the graduality parameter; second, the Centro di Valutazione e Certificazione Nazionale (Center of National Evaluation and Certification) has a crucial role in identifying and managing those actors intending to supply the ICT goods, systems, and services, and therefore, it is crucial to introduce an effective monitoring system for the standardization and harmonization of the ICT procurement; third, the scope of the provisions concerning the government's "special domains" in the sector of high-technological intensity is extended; fourth, the accuracy in defining the modalities and the timeframe associated with the obligation to notify within the exercise of the special domains; lastly, the concept of the external actor of the EU is redefined. Concerning the repercussions of such a trend, the adoption of the Decree-Law, coupled with the growing market needs in the cybersecurity field, are reflected in the necessity to define new professional profiles.

<http://bit.ly/3aQDqUg>

<http://bit.ly/2O43SQz>

<http://bit.ly/2vtEXPU>

<http://bit.ly/3aNVVbH>

RUSSIA

Apple to leave Russia due to "domestic-software-only" law

On July 1, 2020, a new law will enter into force, obliging the pre-installation of domestic, made-in-Russia software on foreign-made digital equipment sold in Russia. Pre-installation of domestic software will be required for all smartphones, tablets, personal computers, and smart TVs. The main list will

include antiviruses, navigation and search engines, social networks and instant messengers, government services, and payment systems. Many companies, according to their internal policies, do not support the pre-installation of third-party software on their products. Apple, Microsoft, and Intel did not support the law from the very beginning. Experts predict that Apple may leave the Russian market after the law enters into force.

<http://bit.ly/2U3Yhh0>

In the wake of the GRU officers: New details in the “case of Russian hackers”

The investigation of the Russian interference in the US presidential elections considers twelve Russian citizens guilty of organizing cyberattacks on computers of the Democratic Party during the 2016 election campaign. Nine of the defendants are, according to the investigation, officers of the Russian GRU military intelligence. The indictment from Miller’s commission additionally states that the US intelligence agencies have not only independently collected the data for the investigation but also have received information from insiders; that is, someone working for either the Russian FSB, the GRU, or both.

<http://bit.ly/2uCx4qY>

Russian security and organized crime are tightly intertwined by cyber hacking

Russian hacker Maxim Yakubets, who is wanted by the FBI and British authorities on charges of embezzlement of more than \$100 million from companies and private accounts, with a reward of \$5 million for the information about his whereabouts, is connected with both Russia’s security agencies and its organized crime. In particular, a connection was found between the Russian hacker and the “legendary” Russian kingpin Vyacheslav Ivankov, nicknamed “Yaponchik,” who was killed in 2009. Indictment in the case of theft using Dridex virus against Yakubets were declassified and

published in December 2019 by the US authorities. Yakubets is the founder of the Evil Corp cyber group, which was taken “under the wing” by Russian FSB special services.

<http://bit.ly/30XTdvM>

APAC

Artificial intelligence created medicine to be used on humans for first time

Created by the British start-up Exscientia and Japanese pharmaceutical firm Sumitomo Dainippon Pharma, the drug will be used to treat patients who have obsessive-compulsive disorder (OCD). Typically, drug development takes about five years to get to trial, but the AI drug took just twelve months. Exscientia chief executive Prof. Andrew Hopkins described it as a “key milestone in drug discovery.” He told the BBC that “We have seen AI for diagnosing patients and for analyzing patient data and scans, but this is a direct use of AI in the creation of a new medicine.” The molecule—known as DSP-1181—was created by using algorithms that sifted through potential compounds, checking them against a huge database of parameters. The first drug will enter phase one trials in Japan, which, if successful, will be followed by more global tests. The firm is already working on potential drugs for the treatment of cancer and cardiovascular disease and hopes to have another molecule ready for clinical trials by the end of the year.

<http://tiny.cc/u2aijz>

Apple supplier Wistron to assemble key iPhone component in new India plant

Taiwan’s Wistron Corp plans to assemble printed circuit boards (PCBs) for iPhones at its new plant in southern India, two sources said, highlighting Apple push to expand manufacturing in the world’s second-largest smartphone market. The local assembly of PCBs by Wistron’s India unit will be a first for the contract manufacturer, which began making Apple’s low-priced

SE model in the southern tech hub of Bengaluru in 2017. It currently assembles the 6S and 7 iPhone models there as well. Wistron's second iPhone plant, some 65 km (40 miles) from Bengaluru, is expected to become operational by April, the sources said, adding that it will make iPhone 7 and 8 models, some of which will be exported. The facility will be capable of producing up to 8 million smartphones annually, they said. The plan is part of Wistron's 30 billion rupee (\$422.12 million) investment proposal submitted to the Karnataka state government in 2018.

<http://tiny.cc/nm9hjz>

Apple to close all China mainland stores due to virus outbreak

Apple said it would shut all of its official stores and corporate offices in mainland China until the second week of February, out of fear over the mounting coronavirus outbreak and the death toll that has more than doubled to over 250. It is joining a handful of overseas retailers, including Starbucks and McDonald's, that are temporarily shutting storefronts as a precautionary measure. Many other companies meanwhile have called for employees in China to work from home and cease non-essential business travel in the first week of February. Normally, businesses in China would be preparing to return to normal operations following the end of the week-long lunar New Year holiday.

<http://tiny.cc/up9hjz>

As coronavirus misinformation spreads on social media, Facebook removes posts

Facebook said it will take down misinformation about China's fast-spreading coronavirus, in a rare departure from its usual approach to dubious health content that is presenting a fresh challenge for social media companies. The coronavirus outbreak has stoked a wave of anti-China sentiment around the globe. Hoaxes have spread widely online, promoted by conspiracy theorists and exacerbated by a dearth of information from the cordoned-off zone around China's central city of Wuhan, where the outbreak began. Nearly

12,000 people have been infected in China, according to local health authorities, and more than 130 cases have been reported in at least 25 other countries and regions. Facebook said in a blog post that it would remove content about the virus "with false claims or conspiracy theories that have been flagged by leading global health organizations and local health authorities," saying such content would violate its ban on misinformation leading to "physical harm."

<http://tiny.cc/dlajjz>

LATIN AMERICA & CARIBBEAN

Orange economy, investment engine in technology

According to Antonio Amador, country manager of Check Point—the Israeli cybersecurity company—enterprises must promote good practices of security in order to protect customers. Recently, Check Point presented its program Infinity Next, a platform designed to protect companies from next-generation cyberattacks. As Amador explains, the Latin America market represents 37 percent of revenues, an emerging region significant for sales. In countries like Colombia, Check Point has been working for the last 22 years. The company has a strong presence in nations such as Panama, Guatemala, and Costa Rica. Amador affirms that every day, big and small enterprises are becoming conscious of cybersecurity. According to data, companies invest between 12 to 15 percent in technology.

<https://bit.ly/2UmflOo>

Brazil takes its industry to India in search of defense agreements

Following the announcement of the agreement between the Brazilian manufacturer of ammunition CBS, its subsidiary Taurus Armas, and the Indian company SSS Defense, the South American giant has become a strong operator in the arms and defense business. According to Infodenfensa news portal, Brazil wants to increase its industrial defense base by \$1,000 USD

million in the next five years. According to Marcos Degaut, secretary of defense products of the Defense Ministry, both countries are in the last stage of the trade agreement regarding cooperation, development, and defense product marketing. Brazil is in the final negotiation stage of two defense agreements with India. Additionally, Brazil's President Jair Bolsonaro has established talks with the Indian government for signing binational agreements in the area of defense, space, and cybersecurity.

<https://bit.ly/392Tlrc>

Cybersecurity is not a priority in Mexico

Despite the relevance in the last years regarding cybersecurity and the massive attacks that Mexico suffers every day, Director of Cybersecurity of Microsoft José Antonio Vázquez claims that "the national strategy to combat this type of crime is not optimal." He continues by describing an inadequate culture of awareness and prevention. Vázquez points out that cybersecurity in Mexico seems not to be a priority and enterprises do not realize the risks behind cyberattacks. In addition, experts have affirmed that it is not a duty only for governments or companies like Microsoft, but also for every citizen in particular to be aware that he or she might be a potential victim of a cyberattack. The report entitled "Habits of cybersecurity users in Mexico 2019" published by the federal government, indicates that 27 percent of cybersecurity users have been victims of identity theft in digital networks, while 21 percent of users have suffered financial fraud. Gina Marie Hatheway, the director of the Corporate Cybersecurity Group at Microsoft for Latin America, explains that people have to think as a hacker in order to prepared.

<https://bit.ly/2vCs06f>