Global Cyber Bi-Weekly Report by INSS April 01 2019

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

Contributors: Simon Tsipis, Anna Danilova, Gal Sapir, Michal Beit Halachmi, Robin Veldwijk

ISRAEL

Cybersecurity researchers find security flaws in Likud, Labor party Android apps

Researchers at the cybersecurity firm Check Point Software Technologies Ltd. said that they had found security breaches granting access to highly sensitive personal information in the Android phone apps of the Likud and Labor parties. They found several vulnerabilities that made it possible for hackers to access the entire list of Likud members, including personal details like home address, emails, cellphones, and credit card numbers. Furthermore, the operators of the app set up an algorithm that enables them to map out the relationship of the person to the people within the contact list, by studying how their details are saved within the phone. All they needed to do was gain access to the phone of a person with the Likud app downloaded on their phone and input that person's ID or cellphone number.

https://bit.ly/2CHymlH

Iran denies hack as Netanyahu blasts Gantz: Tell world what Tehran has on you

Iran's Foreign Ministry spokesman, Bahram Qasem, denied that Tehran had hacked the phones of several senior Israeli politicians. Israeli reports state that Iranians had tapped the phones of ex-general Benny Gantz, former Prime Minister Ehud Barak and Prime Minister Netanyahu's wife and son. Last week, it claimed that Gantz, chairman of the Blue and White Party, was the victim of Iranian hackers during the election campaign and that they possess the contents of his phone. Later, according to Channel 12, Iran purchased former Prime Minister Ehud Barak's computer and cellphone after hackers accessed the devices. The next day, according to a Saudi publication in a report in the

Independent, Iran had hacked the phones of Sara and Yair Netanyahu. The Prime Minister's Office responded to the report it was clear that the report was false.

https://bit.ly/2JPwDk7

UNITED STATES

Saudis gained access to cellphone of Amazon CEO Bezo according to security chief

Earlier this year, the National Enquirer (TNE) exposed intimate text messages and photos sent from Amazon CEO Jeff Bezos to former TV anchor Lauren Sanchez, suggestive of a premarital affair. Bezos launched a private investigation lead by security consultant Gavin De Becker to determine how his personal data was obtained, recently issuing limited findings; results have been turned over to federal officials. Bezos blamed David Pecker, chief executive of American Media Inc. (AMI) parent company of TNE, of black mail and extortion, threatening to publish more unfavorable text messages and photos unless Bezos publicly rescinded his claim that the tabloid newspaper's coverage of Bezos was politically motivated and deny any "electronic eavesdropping or hacking in their newsgathering process." Evidence points to Saudi involvement in gaining access to Bezos' phone; it is not certain to what degree AMI was involved, and Saudi Arabia has rejected its involvement. In this context, the Washington Post—also owned by Bezos—has been accused several times of aggressive coverage of the current administration as in Pecker's recent federal immunity deal related to concealing damaging stories about the president during the election campaign. Bezos has suggested that the motive for his targeting include Pecker's association with the Saudi government and the murder of Jamal Khashoggi at the Saudi Consulate in Istanbul.

https://reut.rs/2HQsACb

Ex-NSA contractor pleads guilty to vast classified data leak, faces nine years in prison

One of several classified data breaches in the last couple of years, described as one of the biggest breaches in the United States, has come to a near end. Former intelligence contractor Harold T. Martin III, 54, has been in custody

since August 2016, when Kaspersky Lab discovered that his accounts possibly had sensitive information. The exposure came to fruition around the same time the "Shadow Brokers" leaked classified NSA hacking tools, although a direct connection to Martin has not been publicized. The former lieutenant stole nearly 50 terabytes of data, entailing "details of sensitive NSA policies and cyber operations." He pleaded guilty on a felony count facing nine years in prison and three years of supervised release; his sentencing will follow in July.

https://bit.ly/2TJjKb8

EUROPE

Mind the Brexit gap in cybersecurity

One area in doubt is the level to which EU cyber-related standards will continue to apply in the United Kingdom. For example, while the Network and Information Systems Regulations (NIS), which is based on an EU directive, has now been put into law in the United Kingdom, some aspects of it require cross-EU cooperation, such as the participation in a Computer Security Incident Response (CSIR) team network. The nature of this cooperation will depend on the final deal between the United Kingdom and the European Union.

https://bit.ly/2CHV3WT

Huawei opens a cybersecurity transparency center in the heart of Europe

Huawei had announced its plan to open a European transparency center last year but at the speech at the opening ceremony for the center held recently, the company's rotating CEO, Ken Hu, said, "Looking at the events from the past few months, it's clear that this facility is now more critical than ever." Huawei said the center, which will demonstrate the company's security solutions in areas including 5G, IoT, and cloud, aims to provide a platform to enhance communication and "joint innovation" with all stakeholders, as well as providing a "technical verification and evaluation platform for our customers."

https://tcrn.ch/2C73tXn

RUSSIA

Cyber warfare stays primary in possible Russian 2016 US elections meddling

Although Special Counsel Robert Mueller and congressional investigators did not uncover any direct evidence of a conspiracy between the Trump campaign and Russia, more facts still may yet be revealed. US intelligence agencies assess that the operation began as an effort to sow chaos and morphed into a plan to help Trump win. It included the hacking and leaking of embarrassing Democratic party emails and the use of bots, trolls, and fake accounts on social media to boost Trump, criticize Democratic candidate Hillary Clinton, and exacerbate political differences. "There's never been a campaign in American history . . . That people affiliated with the campaign had as many ties with Russia as the Trump campaign did," one investigator from Mueller's team said to NBC. By many counts, Trump and his associates had more than 100 contacts with Russians before the January 2017 presidential inauguration. However, Senate investigators say it may take them six or seven months more to write their final report. The report, the Democrats say, will not be good for Trump.

https://nbcnews.to/2YBfrlY

Similar to US 2016 cyber fraud now revealed in Venezuela crisis

On February 1, Facebook and Twitter reported the removal of hundreds of user accounts allegedly implicated in aggressive campaigns to promote the interests of Moscow, Caracas, and Tehran. In particular, Twitter eliminated 1,960 accounts related to Venezuela, recording attempts at "foreign influence" on events in this country. 764 allegedly Venezuelan accounts are suspected of working in a foreign country, since the behavior of their owners is similar to the work of employees of the "troll factory" of now well-known manipulator and Russian oligarch Yevgeny Prigogine, also known as "Putin's chef." The company promises to provide all found accounts and related information to journalists for further analysis.

http://bit.ly/2uxIusv

Russia claims, US hackers committed major cyberattack

Russia's ambassador to the United States, Anatoly Antonov, said that in March this year, three million cyberattacks were recorded on Russian IP addresses originating from the United States. Russian officials have appealed to their US counterparts for explanations.

http://bit.ly/2I1WToT

Russian "sovereign" internet: Apparently one of most major projects in modern times

The Russian Ministry of Defense has started creating a multi-service transport communications network (abbreviated as MTCC), which will become the basis for the "sovereign" internet, as reported by Izvestia. According to the Defense Ministry, the MTCC will be fully ready in two years, and the first stage will be completed by the end of 2019. By this time, the military intends to lay a fiber-optic cable through the Arctic. It is noted that a search engine will be created for the network, an electronic log of actions, as well as its own user identification system. The network will be completely closed to the world internet and will not have any traffic exchange points with it. All information will be stored on the servers of the Ministry of Defense, which has already begun to create geographically distributed data processing centers.

http://bit.ly/2HN3aFJ

Will Russia's offense of global positioning system stay unpunished?

According to both Finland and Norway, Russia may have intentionally disrupted global positioning system (GPS) signals before and during Western military exercises, affecting the navigation of civilian air traffic in the Arctic in November 2018. Now, Oslo has solid proof that Russian forces also disrupted GPS signals during recent NATO war games, the Nordic country's defense minister said.

https://reut.rs/2OzV8R5

APAC

Personal data of over 800,000 blood donors in Singapore accessed illegally and possibly stolen

The personal data of over 800,000 blood donors in Singapore has been accessed illegally and possibly stolen. The information included the names, identity card numbers, gender, and number of donations of people who had donated or registered to donate blood in Singapore since 1986. The data breach was discovered by a US cyber security expert, who said he did not intend to disclose the data and had spotted the vulnerability in the server that stored it. He informed the authorities and has been working with them to secure it. However, a preliminary check by an independent security group working with the Health Sciences Authority revealed that the server was also accessed by several other IP addresses between October and March this year. This is the third time a breach of data has been discovered in recent months in the Health Sector. In January, the Ministry of Health (MOH) revealed that confidential information of 14,200 HIV-positive individuals had been leaked online, and in February, the MOH said that a computer error caused 7,700 people to receive inaccurate healthcare subsidies when they applied for or renewed their Community Health Assist Scheme cards in September and October last year.

https://bit.ly/2I5vVgj

Cyber Security Malaysia is the first Asian corporate company to join the Intelligence Network

The Intelligence Network is an industry initiative launched by BAE Systems and involves a global community of experts and researchers, working together to tackle cyber security threats and practices. The cooperation will bring an ASEAN context to the initiative and will enable better understanding of the unique threats in Malaysia's corporate world. The signing ceremony was attended by Kevin Jenkins, the first secretary, Defense and Security, from the British High Commission in Malaysia and Barry Johnson, the country manager for BAE Systems in Malaysia.

https://bit.ly/2WDR44Z

The rising risks to Asia Pacific's cyber threats

The latest yearly report of Microsoft's Security Intelligence outlines the four biggest threats to the Asia Pacific region: Malware, cryptocurrency mining, ransomware, and drive-by download attacks. India, Sri Lanka, and Indonesia have the highest record of APAC countries in crypto currency mining malware, which is nearly 17 percent higher that the global average, while China, Australia, and Japan have the lowest record. Indonesia, India, and Vietnam recorded highest in ransomware attacks, while Japan, Australia, and New Zealand were the lowest.

While drive-by download attacks have decreased globally by 22 percent, they are still high in APAC, with 22 percent more attacks than the rest of the world, with Taiwan, Malaysia, and Indonesia leading in the number of attacks, and New Zealand, Japan, and South Korea with the lowest record. Globally, malware has decreased by 34 percent, but the APAC encounter rate was 37 percent more than the global average. In this type of attack, Indonesia, Vietnam, and Philippines take the lead, due to their human development rate and poor cybersecurity readiness, as well as low user awareness. Japan, Australia, and New Zealand's record is significantly lower due to better cybersecurity infrastructure and communication with citizens on cyber risks. Microsoft warns of growing phishing attacks and the rise of software supply chain attacks, such as the one where attackers compromise a legitimate component in software packages updates or application.

https://bit.ly/2FPqa4D