Global Cyber Bi-Weekly Report by INSS 15 December, 2019

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

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

ISRAEL

Inside the hate factory: how Facebook fuels far-right profit

A covert group using a network of Facebook pages to spread information, including fake news to over a million users for almost a two-years period, was revealed by the Guardian after investigations. According to the newspaper, the group was based in Israel and operated through a coordinated campaign aiming to disseminate fake and distorted news—over a thousand per week—mainly directed against Muslims communities and left-wing entities. The report stated that the campaign was linked to 21 far-right Facebook accounts from many countries, including the United States, the United Kingdom, and Australia. At least 165,000 published articles and more than 14 millions of likes, comments, and shares have been counted. The efforts also implied the use of ad, which allowed the group to generate revenues from users' views. Some of the pages and the contents shared have already been removed. This revelation has occurred as the social media giant has already been the target of critics, who have accused it to be the preferred platform for foreign actors (states as well as individuals), and is willing to interfere in countries' politics and disinform users.

https://bit.ly/2YxM9Vm

https://bit.ly/2Rz2dot

Satellite built by Israeli students successfully put into orbit by ISRO

Three young Israelis will go to Southern India to take part of the launch of the satellite "Duchifat 3," which they designed and built. The satellite will be

launched from the Srikarikota site directed by the Indian Space Research Organization (ISRO). This event is the achievement of three years of work led by a group of almost 60 students supported by HSC and the Israeli Space Agency. The satellite was named after Israel's national bird Hoopoe (duchifat in Hebrew). Sir Stephen Waley-Cohen, the president of ICA, the organization that founded the project and is mainly active in the fields of education and agriculture, explained that ISRO was chosen for the project because of its reliability and prices. In addition to the great experience that the initiative will provide for the students, the satellite aims to help farmers collect information about rural parts of Israel by providing them pictures and data from the satellite.

https://bit.ly/35iPs5A

'Ultimate' MiTM attack steals $1 million from Israeli startup

Checkpoint's cybersecurity analysts uncovered an attack targeting an Israeli start-up and a Chinese venture capital firm by using a "man-in-the-middle" (MiTM) technique. The hackers used several techniques to fool the two companies, including spoofing tactics. Indeed, they were able to break into the communication between the two companies and send emails to both sides using domains that look alike to spoof email addresses. The hackers disrupted transactions and were able to modify financial information in order to receive the funds sent by the Chinese vendor dedicated to the Israeli start-up. The Checkpoint experts were able to track the stolen money and they discovered that the bank account accessed by the hackers belonged to a Hong Kong-based business. The analysts said that this incident was a warning to anyone willing to make wire transfers and they gave recommendations to secure transactions.

https://bit.ly/36yo5ol

UNITED STATES

New bill gives Department of Homeland Security authority to get ISP info

A bipartisan bill recently introduced would enable the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to subpoena customers' information from internet service providers (ISP). This would further allow CISA to retrieve information on critical infrastructure that is vulnerable and convey to the owners that they are prone to attacks. "Under the legislation, CISA would receive the power to detect, identify and receive information about critical infrastructure systems only for cybersecurity purposes through administration subpoenas. If enacted, CISA would have to notify the owner of the critical infrastructure within one week of receiving the information. After six months, CISA must destroy it."
https://tiny.cc/xflohz

How hackers breached an Air Force system

At the 2019 DEFCON held in Las Vegas, the Air Force held a contest for ethical hackers to try to intrude into actual operational equipment—a data transfer system for the F-15 tactical fighter aircraft. Will Roper, assistant secretary of the Air Force for acquisition, technology, and logistics, said, "What they told me was the ways we got in were not the things you've told industry to design. They were the things industry doesn't know is in their supply chain—it's the ports that weren't cut off, the dry functions that weren't cut off. These are the thing you need to tell industry don't do . . . Our defense companies are assemblers from the supply chains that they don't require the suppliers to tell them what code, what software functionality is running on components because we don't tell industry to do that."
https://tiny.cc/5mlohz

Healthcare provider agrees to cough up $6 million to settle data breach lawsuit

In June 2016, Arizona healthcare provider Banner Health suffered a data breach that exposed the private health and financial information of 2.9 million patients for nearly two weeks, including names, addresses, dates of birth, prescription information, medical histories, social security numbers, and credit card particulars. Hackers were able to infiltrate the company's network through the payment processing systems "used in the food and beverage outlets of the healthcare provider's hospitals." Banner Health operates 28 hospitals and specialized facilities across six states and is the largest employer in Arizona. The class action law suit alleged the failure of the company to implement appropriate security measures, such as firewalls, data encryption, and multi-factor authentication resulted in the cyberattack and consequently in several attempts of identity fraud. The suit was settled with Banner for $6 million and also offered victims two years of credit monitoring and identity theft protection.

https://tiny.cc/39rkhz

Microsoft: 44 million users' passwords have been breached

According to Microsoft's threat research conducted in the first two months of the year, millions of customers are using previously breached login credentials, out of 3 billion credentials checked. "It found a match for over 44 million Microsoft Services Accounts, used primarily by consumers, and AzureAD accounts, which is more worrying for businesses. For the leaked credentials for which we found a match, we force a password reset. No additional action is required on the consumer side. On the enterprise side, Microsoft will elevate the user risk and alert the administrator so that a credential reset can be enforced." According to a 2018 study of around 30 million users, "it was found that password reuse was common among over half (52%), while nearly a third (30%) of modified passwords were easy to crack within just 10 guesses. A Google poll of 3,000 computer users released

earlier this year found that just a third (35%) use a different password for all accounts, and only a quarter (24%) use a password manager."
https://tiny.cc/ottkhz

EUROPE

ISP 1&1 hit with €9.6 million GDPR fine

1&1, owned by United Internet, an internet service provider (ISP) and hosting company has been fined nearly €10 million (US $11 million) by Germany's Federal Data Protection Authority (BfDi) for data protection (GDPR) infractions. The incident involved "[exposed] contractual information," and according to United Internet, occurred in 2018 and has been resolved. According to compliance specialists, "under GDPR, organizations are obliged to put in place adequate technical and organizational measures (TOMs) to prevent unauthorized access to personal data. In this case, the BfDi felt that 1&1 had not put adequate TOMs in place after callers were able to obtain information on customers simply by giving the name and date of birth of a customer." The United Internet subsidiary, which operates across Europe and the Americas, will be appealing the penalty. United Internet has "agreed to introduce a new authentication process to make it harder for callers to access the personal data of others." The following case is among the accumulating incidences of GDPR infraction penalties, including earlier examples of the United Kingdom's Information Commissioner's Office (ICO) fines on British Airways for €183 million and Marriott International for €99 million.
https://tiny.cc/wztkhz

Thousands of UK political ads went missing from Facebook archive searches

Two days before Britain's general elections, thousands of political ads went missing from the searchable advertising database of tech giant Facebook. The library service, which was launched in the United Kingdom in 2018, is a public tool for users to view political advertising on the platform. Facebook said in a

statement that all of the ads affected are now back in the library. The library has been a cornerstone in efforts to increase transparency about its role in elections, but researchers say it is poorly maintained. A spokesman also confirmed that some ads in the United States were affected but declined to answer questions about the issue there.
https://reut.rs/2PtNOao

General election 2019: Reddit says UK-US trade talks document leak "linked to Russia"

American website Reddit announced it had suspended 61 accounts that were part of a coordinated effort of a Russian campaign. Leaked documents detailing trade talks between the United Kingdom and the United States were posted on the website by an account linked to a campaign "originating from Russia," according to Reddit. The leak was used by the campaign of UK Labour Party leader Jeremy Corbyn. Reddit's post did not provide any further details about the evidence behind its conclusion, but it said a group of suspect accounts "provides us with important attribution for the recent posting of leaked UK documents, as well as insights into how adversaries are adapting their tactics."
https://bbc.in/2E7kXDE

Australian and European police shut down access to popular criminal hacking tool

European and Australian law enforcement officials claim to have taken down a remote-access hacking tool that has been sold to 14,500 buyers in 124 countries. The so-called Imminent Monitor Remote Access Trojan's (IM-RAT), according to officials, had been used to steal personal data from tens of thousands of victims. The hacking tool gave anyone access to a victim's computer to steal photographs, passwords, and video footage for just $25. Thirteen of its most prolific users have been arrested. The identity of IM-RAT's

creator is not publicly known, but evidence points to a contact address in Australia.

https://bit.ly/2YMtN3d

RUSSIA

The Russian submarine tragedy that killed 14 was on a mission to cut undersea internet cables

On July 1, a Russian navy submarine caught fire, killing 14 sailors on board. The vessel caught fire near the naval base of Severomorsk. Russia's Defense Ministry said in a statement that the sailors died of smoke inhalation. Two independent Russian news outlets reported that the vessel was the AS-12 "Losharik," a nuclear-powered vessel that US officials have said is designed to cut undersea cables that keep the world's internet running. Moscow officials have remained secretive about the type of vessel and whether it was nuclear-powered, prompting accusations of a cover-up. However, BBC Monitoring described US officials as saying the AS-12 is designed to cut undersea internet cables and other communication infrastructure lines. US and other Western officials have long warned that Russian ships have been active near major undersea fiber-optic cables that carry calls, emails, texts, and trillions of dollars' worth of daily financial transactions.

https://bit.ly/2yTOBJS

FSB now can shut down any site without court

One of the branches of the Federal Security Service (FSB) dealing with cybersecurity—the National Coordination Center for Computer Incidents (NCCTC)—can now start the process of depriving sites of their domains should they violate Russian law. Unlike blocking through the courts and Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor), this new obligation includes that everyone who registers a domain agrees with the possibility of domain blocking in the case of violations. The speed of the procedure is compensated by the limited

scope as it will not work against sites registered outside the Russian national domain zones .ru and .rf.

https://bit.ly/2N4zJRx

UK military deploys special social media division to fight Russia

Lieutenant General Ivan Jones, the commander of Britain's field army, announced the formation of a cyber warfare unit. The new special cyber operations unit, 6 Division (6 Div), will move beyond the typical cyber capabilities within the military sphere into full-blown social media "information warfare." And here the primary adversary is Russia, which has turned the dark art of peddling fake news and political propaganda across major social media platforms into a national security strategy. Much of the work of the new unit will be relatively traditional signals activities—jamming and intercepting enemy communications—supporting the field world of allied intelligence agencies. But as a sign of the times, the new unit also has an offensive and defensive propaganda mission of taking the social media fight to Russia.

http://bit.ly/2H0Nj4a

APAC

North Korean hackers tap power of new TrickBot module

The North Korean Lazarus Group has been associated with a new set of tools, enhancing concealed data embezzlement, referred to as the "Anchor module." According to SentinelOne, the collection of tools is designed "for targeted data extraction from secure environments and long-term persistency." The firm further states that the "anchor presents . . . an all-in-one attack framework designed to compromise enterprise environments using both custom and existing toolage." According to Cybereason, the tool framework utilizes the "PowerRatankba PowerShell backdoor," used in many attacks targeting financial, manufacturing, and retail enterprises, designed to steal

financial credentials. The malicious capabilities have been implemented in TrickBot, a successful botnet that has been used in numerous campaigns, from "banking Trojans to ransomware and data theft." According to threat intelligence firm Blueliv, the bot's utility was found to have increased by 283% in quarters two and three.

https://tiny.cc/ibtkhz

Facebook accuses two Chinese nationals of using hacked accounts to spread ads

Facebook is taking legal action against two Chinese nationals and one Hong Kong advertising company. This comes after they have been accused of using the platform to distribute malware to push misleading advertisements in order to generate money. The lawsuit, which was filed in the Northern District of California, accuses ILikeAd Media International Company Ltd. and two individuals, Chen Xiao Cong and Huang Tao, of a scheme to persuade users into downloading malware. They then used hacked accounts to advertise counterfeit goods and diet pills. Since April, Facebook has been notifying hundreds of thousands of users that their accounts may have been compromised by the scheme and have instructed them to change their passwords, according to the complaint. Facebook has paid more than $4 million to reimburse victims for the fraudulent ads. The defendants also allegedly relied on a technique called "cloaking" to hide the true destination of ad links to subvert Facebook's review protocols. It is the latest move by Facebook to use the federal courts to curb alleged malicious use of its products. The social media giant has also taken the surveillance vendor, the NSO Group ,to court for allegedly orchestrating a cyberattack on some 1,400 mobile devices using WhatsApp, which is also currently owned by Facebook. The NSO Group denies the allegations. In March, Facebook sued two Ukrainian men for allegedly using the platform's quiz apps to distribute malware.

https://bit.ly/2qNgZgq

Chinese residents worry about rise of facial recognition

A survey conducted by a Beijing research institute has indicated a growing pushback against facial recognition among the public across China. Some 74% of respondents said they wanted the option to be able to use traditional ID methods over the technological methods in order to verify their identity. The survey also found that worries about the biometric data being hacked or otherwise leaked was the main concern cited by the 6,152 respondents. Facial recognition systems are being rolled out in stations, schools, and shopping centers across the country. The survey, first reported in the West by the Financial Times, was released by the Nandu Personal Information Protection Research Center. Some 80% of respondents said they were concerned that facial recognition system operators had lax security measures. Separate research suggests that they have good reason to be concerned. China was ranked the worst of 50 surveyed countries in a study examining how extensively and invasively biometric ID and surveillance systems are being deployed. It found that China had no "specific law to protect citizens' biometrics" and highlighted a "lack of safeguards for employees in the workplace." In addition, 84% of people said they wanted to be able to review the data that facial recognition systems had collected on them and to be able to request that it should be deleted. The majority of respondents said they wanted an option to be able to use ID cards, driving licenses, and/or passports as an alternative. China has more facial recognition cameras than any other country, and they are often hard to avoid.

https://bbc.in/2qMPuDF

Japan joins NATO cybersecurity drills to counter Chinese hackers

Japan has become a fully-fledged participant in NATO's cybersecurity war games, as Tokyo and other Western nations become increasingly weary of potential hacking threats from China. The Cyber Coalition exercise, which lasted for one week, poses scenarios including cyberattacks during cross-border conflict as well as compromised state computer systems. One scenario

in the exercise involved participants striking back against a virtual enemy. Furthermore, Japan has upgraded its role from observer status, a position the country held between 2015 and 2018, as neighbor China reportedly builds its cyberwarfare capabilities. "Japan has little experience in international exercises in the cyber field," a Defense Ministry official said. "There are multiple issues we need to overcome, like the language barrier. Participation in multilateral exercises is very meaningful, since it lets us prepare for actual operations." Japan's cyber defenses have faced criticism as trailing those of Western nations, raising the possibility that the United States and the European nations could suffer damage as a result of an attack on Japanese computers. Japan shares not only geographic proximity with China but also deep economic ties. China is home to hacker groups whose numbers are said to grow each year. They have been linked to attacks on government and corporate servers worldwide. Beijing is thought to have created a government-controlled cyberwarfare unit in as early as 2015, as part of a sweeping reorganization of its military. The NATO alliance's Cyber Coalition, with its command center in Estonia, is one of the world's largest exercises of its kind. The more than 30 participants this year included the United States, the European Union, and Ukraine.
https://s.nikkei.com/2LU57AK

Preaching blockchain in North Korea gets an American in trouble at home

An American man has been arrested for allegedly trying to help the North Korean government evade US economic sanctions by using blockchain technology. Virgil Griffith, who is 36, is accused of traveling to North Korea despite US officials warning him not to, in order to deliver a presentation on blockchain and cryptocurrency at a Cryptocurrency Conference in April. While attending the conference, it is alleged that Griffith interacted with attendees who worked for the North Korean government. The North Koreans allegedly quizzed Griffith about the technical aspects of blockchain, the distributed ledger technology that creates a secure record of transactions and is the

backbone of cryptocurrencies, such as bitcoin. Griffith also allegedly discussed how cryptocurrencies could be used to launder money. This is a keen interest of the North Korean government. Griffith is accused of violating the International Emergency Economic Powers Act (IEEPA), which bars US citizens from exporting goods, services, or technology to North Korea without a license from the Department of Treasury. That law is part of a number of economic sanctions the US government has imposed on Kim Jong Un's regime for its pursuit of atomic and ballistic missiles programs. North Korean hackers successfully breached at least five cryptocurrency exchanges in Asia between January 2017 and September 2018, causing $571 million in losses, according to a UN panel. Griffith was arrested at a Los Angeles airport, and he appeared in a federal court, according to a statement by the Department of Justice.

https://bit.ly/35mnu8U

MIDDLE EAST

Iran says it foiled "massive" cyberattack on infrastructure

Minister of Telecommunications Mohammad Javad Azari Jahromi stated that Iran was the target of a wide and massive cyberattack, which was identified by authorities and defused. The government did not provide any further information on the nature of the attack, the instigators, or the potential damages. This statement comes after the dismissal of documents showing that Iranian banks were the victim of a recent hack leaking personal information of thousands of customers (15 million credit cards). However, the minister of telecommunications denied the attack on Iranian banks and said that the data theft was operated by a contractor as part of a blackmailing case. According to experts cited by the New York Times who were interrogated on this incident, this kind of breach is likely to be operated by state actors considering the advanced technical tools that were used and the size of the leak.

https://bit.ly/2EcmisO

https://bit.ly/2rHK9y3

IBM sounds alarm about more data-wiping malware from Iran

IBM's experts uncovered a malware allegedly developed by Iranian hackers and used in data-wiping operations directed against industrial targets around the Middle East. Indeed, the firm, which nicknamed the malware "ZeroCleare," stated that it was spread to devices in order to disrupt the network infected, potentially leading to considerable damages and requiring months to recover. Security analysts assessed that the virus may be linked to the Iranian government and to the Iranian hacker group APT34. According to IBM's analysts, the "ZeroCleare" virus is close to the "Shamoon" virus and considered one of the most dangerous malwares of the past decade. The report also suspects these attacks to be part of a coordinated effort operated by several groups and not only one actor, targeting sensitive organizations in the region. The company remained silent regarding the name of the attack's victims.

https://bit.ly/2Psa3xB

Cyber Shield 2019 to simulate malware, phishing attacks

Cyber Shield 2019, an international cybersecurity simulation organized by Turkey's Ministries of Transport and Infrastructure and Information and Communications Technologies (ICT), will take place in Ankara from December 19 to 20, 2019. The exercise aims to simulate cyberattacks and will offer the opportunity to explore many technical solutions to risks and threat in cyberspace. For example, phishing attacks and malware infections will be operated. The Deputy Minister of Transport and Infrastructure Omer Fatih Sayan said that the simulation was designed to improve preparedness and boost Turkish capabilities in terms of cyber response to attacks. Many countries might participate to the exercise following the invitation of Turkey, such as Iran, Brazil, and Azerbaijan.

https://bit.ly/348DytI

UAE Central Bank says it "does not approve any private cryptocurrencies"

Following an article stating that the governor of the Central Bank of United Arab Emirates was approving the creation of a "cryptocurrency trading platform," the Central Bank denied the allegation. The organization said the information published on a "fraudulent website" was false and reaffirmed the disapproval of the UAE Central Bank regarding any private cryptocurrency or trading platform. The institution also added that crypto activities were not considered by the UAE because of the risks implied by a high volatility of prices and dangers linked to money laundering and terror financing.
https://bit.ly/2rnxRLd

LATIN AMERICA AND THE CARIBEANS

Mexican neobank ALBO increased its value in market to around US $26.4 million

The Giant North-American country is betting for a new era of alternative banks that are more reliable for customers. This is the example of ALBO. The unconventional company started its participation in Serie A with US$7.4 million in January 2018, and now the capital of the company is worth US$26.4 million. The causes for this considerable increase is due to recent financial upgrade to the US venture capital fund, Valar Ventures. ALBO's main duty is to provide security but also comfort to its 200,000 customers. According to Contxto portal news, 45% of Mexico's population is underbanked, meaning that people have bank accounts but prefer to use other mechanisms to save money. For that reason, ALBO wants to provide its customers with multiple opportunities to use banking services without long lines or conventional processes. However, there are multiple challenges for alternative banks when it comes to attracting customers. In countries like Brazil, alternative banks ask for prior spending history. Mexico has a similar situation, but the heterogeneous market permits companies, such as ALBO, to work without these requirements.

https://bit.ly/2EibI3x

Microsoft: Mexico must strengthen its cybersecurity politics

According to José Antonio Vázquez, Microsoft's director of cybersecurity in Mexico, the country has not focused enough attention on cybersecurity. Despite several national plans and governmental initiatives, the Latin American nation lacks public policy to improve and protect different cyber systems. However, Vázquez emphasizes this duty is a responsibility not only of the state but also of companies and other organizations in the private sector, and they must be involved in order to achieve cybersecurity awareness. In May 2019, Microsoft held its annual event in Mexico. In the conference, Gina Marie Hatheway, senior director of Cybersecurity Solutions Group Microsoft made a presence. In the conference, multiple points were established, such as the relevance of cybersecurity, and workshops with bank entities either for employees or clients. For example, Forbes Magazine points out that around 3,500 Microsoft workers are constantly monitoring and protecting customers from possible cyberattacks. The company uses artificial intelligence to analyze 6.5 billion global threats. Microsoft has undertaken several efforts to approach the Mexican government in order to establish a dialogue regarding cybersecurity protection. Last month, two chiefs of Microsoft met with Mexico's President Andrés Manuel López Obrador in order to work together in multiple areas of cyber protection.

http://tiny.cc/utnkhz

Jamaica to create a national cybersecurity policy in 2020

The cybersecurity policy is a priority for Jamaica's government. According to Dr. Horace Chang, Jamaica's minister of National Security, the main objective for the National Plan is to protect the citizens from cybercrime through a reliable and robust cyber platform. As a result the Caribbean island will deliver a quality and safe online service. Moreover, the Jamaican minister emphasized the duty of governmental agencies such as e-Gov Jamaica for achieving cyber

protection. It is important to mention that from January 2019, each citizen of Jamaica has been given a randomized nine National Identification Number (NIN). This number will be used for a person's entire life as a form of identification. In addition, the Jamaican government is working to create a data protection bill, which aims to provide a framework and guidelines for securing and protecting people's data. The bill stipulates that data gathered may not be used for aspects other than the initial purpose. Finally, Minister Chang pointed out the relevance of working with local and international agencies, such as the Organization of American States or Inter-American Committee against Terrorism, to protect the islanders' personal data.
https://bit.ly/2tlHlXV