Global Cyber Bi-Weekly Report by INSS January 15, 2020

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

Contributors: Yael Elharar, Simon Tsipis, Donal Byrne, Lea Abramski, David Murcia Briceño

ISRAEL

State comptroller to expand focus on cyber

Newly appointed State Comptroller Matanyahu Englman will continue examining Israel's promptness in the cyber domain, efforts that were initiated by former state comptroller Yosef Shapira. Englman desires to create a new subdivision to handle the oversight, which will focus on government ministries and other state bodies that deal with critical infrastructure and utilize digital services and products. "The Comptroller's oversight of cyber activities will likely have a significant effect on the Israel National Cyber Directorate, as well as current state regulators involved in cyber affairs. That is, if Englman also examines the effectiveness of the directorate's issued recommendations, their cost-effectiveness, and how well these recommendations are actually implemented."

https://bit.ly/369vIko

IMOD: A breakthrough in the development of laser-based weapon systems

Israel Ministry of Defense (IMOD) discovered a means that will enable the advancement of "high-power laser-based interception systems." The emerging technology will enhance the air-defense capabilities for the country. In accordance with the development, the IMOD Directorate of Defense Research and Development launched "three programs for the development of high-power laser demonstrator prototypes in cooperation with Rafael Advanced Defense Systems and Elbit Systems: development of a prototype

ground-based laser system that is to complement the Iron Dome system and provide an additional defensive layer; a maneuvering ground forces; and development of a prototype laser capable of intercepting threats above the clouds and defending more expansive areas that may be mounted on an airborne platform."
https://bit.ly/2tCOOSG

For the first time: The government will buy its own communications satellite from the aerospace industry

The State of Israel and Israel's aerospace industry has signed a contract for the development and construction of a new satellite called "Dror 1," which is designed to meet the state's satellite communications needs for the next 15 years. This is the first time Israel is purchasing its own non-spy satellite to replace the services they currently have from the communications space company. The satellite to be purchased is largely based on Israeli technologies and is valued at an estimated US $190–200 million. The satellite will be developed in the aerospace missile and space systems division.
https://bit.ly/2v0Wkao

Security breach: Personal information of patients leaked from MDA systems

Two serious information security incidences occurred at the Magen David Adom (MDA) organization in Israel—an organization that provides emergency medical services. The Privacy Protection Authority (PPA) revealed that personal patient information was leaked, including medical records, Israeli ID numbers, and credit card numbers. An additional breach targeted the volunteer management app, resulting in the exposure of the personal information of the organization's volunteers. According to the PPA statement, these were serious security breaches in systems developed for MDA by third-party vendors, where no security requirements have been defined in accordance with the State of Israel's Privacy Protection Regulations. MDA

knew about these events but did not report them as required by law. PPA's declaration that these events violated the law increases the likelihood that potential victims will file civil claims against MDA. MDA said in a response that "all of the organization's systems are highly secure. However, loopholes are sometimes discovered as hacker levels rise. Under no circumstance was confidential or significant information leaked."

http://tiny.cc/wn1xiz

UNITED STATES

Top DHS cyber official discusses when Iran may retaliate in cyberspace

According to a recent interview with the National Security Law podcast, Chris Krebs, the director of the Cybersecurity and Infrastructure Security Agency, stated that people should not be concerned about an "immediate cyber retaliation" from Iran. "The top cybersecurity official at the Department of Homeland Security (DHS) said that if Iranian cyber actors were to attack the United States in retaliation for a drone strike that killed an Iranian general on January 2, it would have already happened."

http://tiny.cc/pynziz

Estonia, United States launch effort to ease sharing of cyberthreat intel

Since the massive attack in 2007, Estonia has been on the frontline of cyber defense, resulting in mutual beneficial developments. The United States and Estonia are working to launch a new five-year project, "aimed at easing the transfer of cyberthreat information between the two nations." The venture should enable intelligence sharing between allies without creating security risks. Estonian company Cybernetica is the main contractor for the project. "This is the first-ever joint capability developed in the cyber domain between the two countries," CEO Oliver Väärtnõu stated.

http://tiny.cc/e1pziz

WeLeakInfo, a search engine for breached personal data, shut down

Following the FBI 2017 shutdown of LeakedSource, a website enabling users to search through databases of information breached. The US Department of Justice recently apprehended weleakinfo.com, operational since 2017, and arrested two men suspected in administrating the site, one from the Netherlands and the other from Northern Ireland. The database included different subscription levels, compiled of over 12 billion records from an estimated 10,000 data breaches intended to facilitate malicious activity. "Such sites offer a convenience not typically available on dark web forums, where much of the same information also is for sale. On those sites, which require anonymity software to access, sellers make much of that information available in bunches, sometimes combines with outdated financial information, though the databases typically are difficult to navigate, and may be unreliable."
http://tiny.cc/h5qziz

EUROPE

UK regulator dings tech retailer for breach that affected 14 million people

Britain's data protection authority stated it has fined Dixons Carphone for a data breach that apparently exposed financial information from around 5.6 million customers. The financial institution decided on the maximum fine allowed under law to sanction the electronics retailer. Indeed, the gravity of the breach is considerable since the malicious software responsible for targeting the electronics firm took advantage of vulnerability, lurking inside point-of-sale systems at stores for almost a year, from July 2017 to April 2018. Besides the collection of financial data, hackers also succeeded in accessing personal information, such as names and email addresses of around 24 million people.
https://bit.ly/378KjOt

Former Barclays executive to launch United Kingdom's first regulated crypto bank in 2020

The former head of technology for Barclays and co-founder and former CTO at Starling, Mark Hipperson, is about to launch his latest digital banking venture, Ziglu. The new venture will create all-digital accounts allowed to hold both digital and fiat currencies. The account will enable customers to hold and exchange multiple currencies, both foreign currencies and cryptocurrencies through exchanges platforms. According to the Ziglu's official website, the new crypto bank will allow people to spend their money, including cryptocurrencies, anywhere using a Mastercard debit card. Currently, applications to open an account are restricted to UK residents but plan to be expanded in the future. Ziglu has applied to the United Kingdom's Financial Conduct Authority (FCA) in order to issue electronic money.

https://bit.ly/38dwcaK

European Securities and Markets Authority prioritizes crypto-related regulation

The European Securities and Markets Authority (ESMA) published its strategic priorities in a document called "Strategic Orientation for 2020-22." The plan highlights the new risks created by digitalization and focuses on the need for more awareness and preparedness. The document states that "the dangers of cyberthreats to the financial system as a whole and a sound legal framework for crypto-assets are increasingly becoming areas of focus for ESMA together with the other ESAs, the ESRB, the ECB, and the European Commission." The ESMA's chair, Steven Maijoor, explained that among the authority's priorities is ensuring a consistent and coherent implementation of the Single Rulebook—the European set of rules that institutions throughout the European Union must respect. The document reveals full awareness of cyber threats and their danger to the European financial system.

https://bit.ly/364lMsp

RUSSIA

Most wanted Russian hackers turned to be relatives of Russian officials

Two Russian hackers, considered by US authorities to be the leading minds behind the hacker group Evil Corp—which according to the FBI is "one of the most prolific cyber-criminal organizations in the world"—are relatives of prominent Russian officials. Maksim Yakubets is the son-in-law of ex-head of the FSB special force "Vimpel" Eduard Bendersky, whereas Andrei Kovalsky is the son of the ex-governor of the Moscow district "Khimki," Vladimir Strelchenko. According to the FBI, in the past ten years of its existence, the group stole hundreds of millions of dollars from bank cards and citizens' accounts. Investigators say the hackers work from Moscow cafes. Both hackers are also indicted in the United States for working on behalf of Russian intelligence services.

http://bit.ly/2tcpPFD

http://bit.ly/30dED2V

National Security Secretary of Ukraine: In the next 5–10 years, cyber threats will bypass nuclear arms

Secretary of the National Security and Defense Council of Ukraine Alexey Danilov announced the increased danger of cybercrime during a meeting with a delegation of the US Senators. Danilov announced that in the framework of the developed Cybersecurity Strategy, Ukraine created a National Cyber Coordination Center. "In the next 5–10 years, cyber weapons will become the number one threat in the world, even nuclear weapons will recede into the background," Danilov said.

http://bit.ly/2tUSjDK

Twitter blocks Russian accounts

Twitter restricted access to a number of accounts from Russia, including the account of the Russian diplomatic mission in Syria after its publication on the

organization the "White Helmets." "Roskomnadzor"—The Federal Service for Supervision of Communications, Information Technology and Mass Media—addressed Twitter with a request to explain the restriction of access of the Russian accounts.
http://bit.ly/36PZgoo

Putin uses outdated and vulnerable Windows XP

After analyzing photographs of President Putin, published by the Kremlin press office, Russian sources claimed that President Putin uses a vulnerable operating system, Windows XP, on his computers both at work and at home. The observers concluded that he "really uses an outdated version" of the Microsoft operating system. It was reported that Putin's computer was running Windows XP, an operating system that Microsoft no longer supports and stopped releasing regular security updates already in April 2014.
http://bit.ly/2FIcJ5M

APAC

Skype audio graded by workers in China with "no security measures"

Microsoft contractors working in China were able to listen to people's Skype conversations and Cortana recordings through a system woefully lacking in cybersecurity. An anonymous Microsoft contractor who worked in Beijing for years said that he was able to listen to recordings of users with practically "no security measures." The contractor's work involved listening to short audio clips from Skype conversations to grade them for quality. The contractor accessed the recordings, which were selected to help grade and improve Microsoft's services. "They just give me a login over email and I will then have access to Cortana recordings," he told the Guardian. "I could then hypothetically share this login with anyone." He said that he and other contractors were instructed to access the clips through company-issued accounts that all shared the same password. He added that employee vetting

was practically nonexistent. The contractor was able to listen to incredibly sensitive audio recording through this system. On top of the usual security risks associated with such low cybersecurity, the employee noted that his location in China made the recordings especially vulnerable. "Living in China, working in China, you're already compromised with nearly everything," he said.

http://bit.ly/30awmNe

US Army plans to expand Asian security efforts to counter China

The US Army plans to deploy two specialized task forces to the Pacific capable of conducting information, electronic, cyber, and missile operations against Beijing, according to a Pentagon official. It is envisaged that the task forces will be deployed over the next two years, US Army Secretary Ryan McCarthy said at an event in Washington. "The Army is reinvigorating our presence and disposition in the Pacific," McCarthy said, because "China will emerge as America's strategic threat." The units, called Multi-Domain Task Forces, would help neutralize some capabilities China and Russia already possess. The units would potentially be equipped with long- range precision weapons, hypersonic missiles, precision-strike missiles, electronic warfare, and cyber capabilities, McCarthy said, without citing any locations. Having "the US Army, with modernized weaponry" in the region "changes the calculus and creates dilemmas for potential adversaries," McCarthy said.

http://bit.ly/2R6O3ZR

Microsoft seizes 50 websites used by North Korean hackers to gather intelligence

Microsoft said it was issued a court order to seize 50 websites used by a hacker group with ties to North Korea, which targeted government employees, universities, human rights organizations, and nuclear proliferation groups in the United States, Japan, and South Korea. The group, known as

Thallium, uses the network of websites, domains, and connected computers to send out "spear phishing" emails. Hackers gather as much information on targets as they can to personalize messages and make them appear legitimate. When the target clicks on a link in the email, hackers are then able to "compromise their online accounts, infect their computers, compromise the security of their networks, and steal sensitive information." Microsoft showed an example of one of Thallium's spear phishing messages. It looks very much like a standard notification that comes with signing into a Microsoft account in a new location. One big difference, Microsoft says, is the group combined the letters "r" and "n" in the domain name to look like the first letter "m" in "microsoft.com." Through its Digital Crimes Unit and Threat Intelligence Center, Microsoft has positioned itself as an important line of defense against so-called "nation state" hacking organizations. Microsoft has in recent years taken on hacking groups with ties to China, Iran, and Russia.
http://bit.ly/2tRvzoc

MIDDLE EAST

Saudi cyber authority uncovers new data-wiping malware, and experts suspect Iran is behind it

Saudi authorities uncovered a new version of data-wiping malware suspected to be led by Iranian attackers. According to a technical report from Saudi Arabia's National Cybersecurity Authority (NCA), the hackers left several clues on the unnamed targeted network when they executed the virus. The report does not identify the authors but stated that the attack could be the work of state-sponsored hackers. Cybersecurity experts analyzed some of the characteristics of the attack and argued they showed similarities to previous attacks from Iran. The malware, which occurred on December 29 and was nicknamed Dustman, is believed to be a variant of a malware previously used in data-wiping attacks last year operated by APT34 and uncovered by IBM—a hacking group linked to the Iranian regime. According to Adam Meyers, the vice president of the cybersecurity company CrowdStrike, Dustman is

"consistent with Iranian capability and operations going back to 2012," referring to the attack against Aramco. The Saudi report comes after the killing of Qassem Soleimani and following numerous warnings from US officials as well as cybersecurity experts regarding potential Iranian retaliations.

https://bit.ly/369Kis8

Kuwait's state news agency says hackers breached its Twitter

The Kuwaiti news agency (KUNA) stated that its Twitter account followed by more than 34,000 users has been hacked. The agency reported on its Twitter page that a defense minister had stated that the US military was planning an "imminent withdrawal" from Kuwait. Soon after, the global news agency Reuters published an article based on the news that had been falsely reported by KUNA. According to Tareq al-Muzraem, the head of the Kuwaiti communication office, the account has been hacked and a malicious actor had posted fake news. Since then, the Kuwaiti agency has deleted the information and has published many updates on its official website. The agency has stayed silent regarding details of the attack and those responsible for the breach. Since around 13,000 American soldiers are based in Kuwait, it represents one of the main US military positions. This breach followed Iranian strikes on two bases in Iraq where American are currently stationed, in retaliation for the killing of Qassem Soleiman.

https://bit.ly/37e2IJF

LATIN AMERICA & CARIBBEAN

Minister Montalvo: "We are a reference in cybersecurity in the Caribbean and soon we will be at the regional level"

The Dominican Republic has had a cybersecurity national strategy for a year and a half, providing mechanisms to provide a "safer cyberspace." This program seeks to create secure places for consumers. According to Gustavo Montalvo, minister of the presidency, the strategy was established in 2018

with the aim to protect private, public, and academic sectors from cyberattacks, while common attacks in the country include phishing and ransomware. Through the National Cybersecurity Center and the national strategy, the Caribbean country works in four areas: institutional strengthening, critical infrastructure protection, spreading culture in cybersecurity, and establishing national and international alliances to contribute to a safer cyberspace. According to Montalvo, this strategy has been successful, and in the short time since its inception, they have been able to provide support to more than 50 government entities and respond to incidents in more than 20 state institutions. Part of the duties of this program is monitoring around 200 institutional web portals as a preemptive measure against attacks. According to the 2018 Global Cybersecurity Index, of which 175 countries participated, the Dominican Republic ranked 92, having moved up from being 125 in 2017.
https://bit.ly/2G3xEjZ

Cybersecurity in 2020: What should be known

Lumu Technologies launched its trends regarding cybersecurity for 2020. According to Ricardo Villadiego, founder and CEO of the company, companies of all sizes and budgets were vulnerable to cyberattacks in 2019, illustrating that even investing in cybersecurity does not simultaneously translate into protection. Villadiego stressed the need to improve "the implementation of efficient processes that manage to protect the assets of an organization and thus avoid compromises." As CIO Mexico news portal points out, there are around 1,200 security manufacturers of all kinds, including mobile, cloud, infrastructure, access, and identity management, which offer various solutions for the cybersecurity industry in Mexico. A common and significant problem in Mexico is ransomware; despite the recommendation to not accept or pay these threats, companies have no option if they want to retrieve access to their data. "According to the FBI's 2018 Internet Crime Report, 1,493 ransomware cases were reported in 2017, which cost each victim an average of US $ 3.6 million."

https://bit.ly/30DydKC

Why is Brazil so vulnerable to cyberattacks?

Phishing and DDoS campaigns are the most common attacks in Brazil. During 2019, the number of cyberattacks increased, particularly against government networks. 19,150 incidents were reported in 2019, a growth of 25 percent compared to 2018. The losses recorded by Brazilian companies resulting from cyberattacks was US $20 billion, affecting around 70 million people, which is a third of the national population. One of the reasons Brazil is a favorite target for cyberattacks is due to the high number of users and utilization of cloud services. Additionally, Brazilian companies do not invest in protection in terms of monitoring, identification, and prevention. Moreover, although 70 percent of Brazilians have access to internet via smartphones and computers, the lack of protection needs to be taken into account.

https://bit.ly/2G7BbgX