Global Cyber Bi-Weekly Report by INSS 1 September 2019

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

Contributors: Simon Tsipis, Robin Veldwijk, Donal Byrne, Lea Abramski

ISRAEL

Qihoo 360 and Israel to build cybersecurity technology innovation center

The Chinese internet security company Qihoo 360 (QIHU) announced that it would jointly establish China-Israel Network Security Technology Innovation Center, set up a 360 Israel Network Security Industry Development Fund, and build an industrial park for network security technology collaborative center. Qihoo hopes to introduce more Israeli companies to China through cooperation with Israel so that they can connect with the market and users. As China's leading internet security company, it can vouch for Israeli security peers and act as a bridge to help Israeli companies entering China for mutually-beneficial cooperation. Israel's population accounts for only 0.1 percent of the world's population, but its influence on cybersecurity accounts for 20 percent. One of the reasons is the Israeli government's decision to lower taxes and relax the regulation for innovation so that emerging industries and markets can flourish.

https://bit.ly/2NCmOGH

Israeli cybersecurity company Checkmarx wins US navy contract

Checkmarx announced that it was awarded a contract with the US Navy's Naval Information Warfare Center Pacific (NIWC PAC). The Israel-based cybersecurity company will help the navy improve its software security and accelerate the development of secure software applications. Checkmarx develops and markets cybersecurity technology that automatically scans code

to detect security breaches and has additional offices in the United States, Brazil, Singapore, Germany, the United Kingdom, Portugal, and France.
https://bit.ly/2ZtudKF

BlackBerry to close Israel development center

BlackBerry is closing down its Israel development. The Canadian company founded its development activity in Israel in 2015 on the basis of WatchDox, an Israeli cybersecurity company founded in 2008 that it acquired for $100 million. The company had 80 employees when it was acquired, but now has 40 employees, who will lose their jobs before the holidays. WatchDox was sold to BlackBerry after it lost its momentum in a mobile telephony market now dominated by Google Android and Apple. The company decided to switch focus from sales of telephones to security products and services. BlackBerry completely closed down its telephone business in 2016 and laid off 200 employees worldwide.
https://bit.ly/2MHgttH

Cybersecurity startup Axonius raises $20 million

Axonius Inc. completed a $20 million funding round. The cybersecurity startup develops a cybersecurity asset management service that integrates information from connected devices such as desktop computers, laptops, mobile devices, and IoT devices, enabling IT and security operations teams to manage and secure them at scale. Axonius Inc. is a Tel Aviv-based startup with 40 employees and has raised $37 million to date.
https://bit.ly/2KZX6Ke

UNITED STATES

Army Cyber Command is trying to become an information warfare force

At the TechNet conference in Augusta, Georgia, Commander Lt. Gen. Fogarty announced the development of a proposal to change the of the Army Cyber

Command to the "Army Information Warfare Command." The name change reflects the more accurate description of daily activities that the Army's cyber personnel engage in, namely "information warfare space." This was echoed by Gen. Funk, commander of Training and Doctrine Command, regarding the "application of information dominance," which he stated, "is underdeveloped and lack[s] coordinated direction." Fogarty described the future existence of units comprised of "information warfare practitioners" at each level in the Army, as concerning electromagnetic activities. The impetus for the emerging shift is the Russian disinformation campaign during the 2016 presidential election, as well as other factors, increasingly understood as more knowledge and awareness is gained about the environment and adversaries. The Army Cyber Command is in the progress of also relocating to Fort Gordon, Georgia where the new HQ will include an information operations center. Such efforts are juxtaposed by the results uncovered by the recent Government Accountability Office report, which conclusively illustrated the Army's flawed methodology, lack of assessment, and brisk activation of such units.
https://bit.ly/33ZldAw
https://bit.ly/2L6Yeuw

How an NSA researcher plans to allow everyone to guard against firmware attacks

The National Security Agency's Laboratory for Advanced Cybersecurity disclosed an open source project that has been in progress for seven years; the end product, SMI Transfer Monitor will be published on their platform Coreboot in the near future. The "anti-tamper technology" consists of "placing a machine's firmware in a container to isolate it from would-be attackers. A layer of protection is being added to the System Management Interrupt (SMI) handler—code that allows a machine to make adjustments on the hardware level." Resulting from the increased targeting risk of firmware, the potential success of breaching an endpoint's firmware enables the control of the entire system. The capacity to achieve such an attack is additionally desirable because malware and attacks are difficult to detect. The open source

methodology is nondiscriminatory, accessible even to Linux users; the NSA version is adept to be implemented as fit to the users.
https://bit.ly/2ZtSDDE

VMware announces plans to acquire Carbon Black for $2.1 billion

As more light focuses on endpoint security, the recent news of a substantial acquisition confirms its heightened value and the latest trend in the cybersecurity industry. The successful breach of a firmware's endpoint grants unimpeded access to the whole system, all while conducting the campaign in a care-free manner, as the malware and attack features remain highly undetectable. With the aim "to bolster its security offerings and ability to detect advance cyber threats," the software giant VMware is in the process of purchasing Carbon Black, an endpoint security company, for $26 a share at a total value of $2.1 billion. The Palo Alto based company, which services corporations and federal agencies, also announced its additional acquisition of Pivotal Software for $2.7 billion. According to Cybersecurity Ventures, the first half of 2019 resulted in a combination of mergers and acquisitions—in the cybersecurity industry—totaling more than $22 billion dollars.
https://bit.ly/2zlY90z

This security agency has a vision to handle cyberthreats

Grounded on the short comings from the 2016 presidential elections, the growing threats from nation-states (Russia, China, Iran, North Korea) and cybercriminals, the Cybersecurity and Infrastructure Security Agency (CISA) released a segment of the new "CISA Insights," also referred as "Defending Today Doctrine." The publication coincides with the cybersecurity "FISMA FY 2018 Annual Report to Congress," by the Office of Management and Budget. Among the many findings, in the 2018 fiscal year, the federal government sustained 31,000 cyber events. Chris Krebs, director of the Department of Homeland Security (DHS) agency, defines CISA's two main goals as "defend today and secure tomorrow." The agency's "holistic approach to security" will

apply in a cooperative, capacity building manner. The document provides fifteen guidance steps for ransomware attacks under the scope of "actions for today, actions to recover if impacted, and actions to secure your environment going forward" amid a significant surge across state and local institutions, as illustrated by the recent coordinated ransomware attack that struck 23 municipalities in Texas, following recent high profile attacks in New York, Maryland, and Florida, among others.

https://bit.ly/2ZwIU3u

https://tiny.cc/kxqubz

https://bit.ly/2Hra1CP

https://tiny.cc/iopubz

https://tiny.cc/0qpubz

Blockbuster indictment against 80 fraud suspects details a complex global scam operation

The Department of Justice unsealed charges, revealing—more than the usual—details of a multifaceted fraud (money, identity, internet) operation that was active between 2014 and 2018 and resulted in the theft of $60 million with attempts to steal $40 million more. The campaigns were employed by business email compromise (BEC) schemes and romance scams. The BEC schemes involved "scammers posing as a victim's boss, coworker other trusted friend or family member to ask the intended target to send money via email or wire transfer." The US Treasury Department "reported that BEC scams cost organizations an average of $301 million every month [in 2018]." Most of the 80 suspects are based in Nigeria, although fourteen were located and arrested in the United States. The indictment, filed in June, followed the arrest of "Africa's most promising entrepreneurs," Nigerian businessman Obinwanne Okeke, for the alleged employment of a BEC scheme costing a UK company $11 million dollars.

https://tiny.cc/jisubz

EUROPE

Biostar security software "leaked a million fingerprints"

According to researchers, over one million fingerprints and other sensitive data have been exposed online by a biometric security firm. Researchers working with cybersecurity firm vpnMentor say that they have accessed data from a security tool called Biostar 2. It is used by thousands of companies worldwide, including the United Kingdom's Metropolitan Police for controlling access to specific parts of secure facilities. The researchers in question claim they found fingerprint records, photographs of people, facial recognition data, names, addresses, passwords, employment history, and records of when they had accessed secure areas. Among the UK organizations directly affected by the breach was Tile Mountain, a homeware retailer. It is believed that a number of other British companies were also affected. Given that the Metropolitan Police use this tool, a spokesman said the force was now checking whether it was one of the affected organizations. Among other firms whose data was discovered were Power World Gyms, a gym franchise in India and Sri Lanka with 113,796 user records including fingerprints; Global Village, an annual festival in the United Arab Emirates with over 15,000 fingerprints; and Adecco Staffing, a Belgian human resources firm with 2,000 fingerprints. The UK Information Commissioner's Office said it was aware of reports about Biostar 2 and would launching a full investigation.

https://bbc.in/2OQJgOf

Employees connect nuclear plant to the internet so they can mine crypto currency

Authorities in Ukraine are investigating a potential security breach at the South Ukraine Nuclear Power Plant after staff members connected it to the internet so they could mine crypto currency. The Ukrainian Secret Service (SBU) are investigating the incident and are treating it as a potential breach of state security given that the classification of nuclear power plants is considered critical infrastructure within Ukraine. At present, it is unknown

whether the attackers might have used the mining rigs as a pivot point to enter the nuclear power plant's network and retrieve information from its systems, which consists of data about the plant's physical defenses and protections. It is also unknown how the scheme was discovered, but on July 10, the SBU raided the nuclear power plant and seized computers and equipment specifically built for mining crypto currency. This equipment was found in the power plant's administration offices and not on its industrial network. Officials believe the suspects attempted this breach given a recent spike in crypto currency trading prices. This incident is not the first time that state employees have abused their access to large sources of electricity or computing power to mine crypto currency. Similar incidents have also occurred in recent months in Russia, Australia, and Romania.
https://zd.net/2KW6U8e

Eurofins Scientific: Cyberattack leads to backlog of 20,000 forensic samples

The largest forensic services provider in the United Kingdom recently experienced a cyberattack resulting in the backlog of almost 20,000 samples. Eurofins Scientific was targeted by a "highly-sophisticated" ransomware virus, which has led British police to stop working with the company. The National Police Chiefs' Council (NPCC) is now clearing the backlog, which includes blood and DNA specimens. It warned of delays to police investigations and court cases, which could jeopardize the justice system. Assistant Chief Constable Paul Gibson said that, "The security and integrity of the criminal justice system is of the highest possible priority, which meant we had to take stringent steps to ensure that police data had, firstly, not been manipulated or changed and, secondly, was suitably protected for the future." Eurofins carries out DNA testing, toxicology analysis, firearms testing, and computer forensics for UK police forces. It deals with more than 70,000 criminal cases in the United Kingdom each year. The global testing firm was forced to pay a random to the attackers of the cyberattack to restore access to its computer network. The ransomware attack hit the company, which accounts for more

than half of the UK forensic science provision. Ransomware is a computer virus that prevents users from accessing their system or personal files. Messages sent by the perpetrators demand a payment in order to unlock the frozen accounts. The use of private firms and police laboratories to carry out forensic science work was stepped up after the closure of the state-owned Forensic Science Service in 2012. The National Crime Agency is still investigating the attack.

https://bbc.in/2U8q3GR

RUSSIA

NSA expects future Iranian-Russian cyber warfare collaboration

The National Security Agency (NSA) sees direct collaboration in cyber warfare between Iran and Russia against the West and the United States in particular, as both of these countries are under pressure of sanctions. The Kremlin is particularly disturbed that the United States appears ready and willing to impose its will on how the Russian internet develops, especially when it comes to issues such as freedom of speech for government opponents. Now that economic sanctions have transformed into military action—including the shoot-down of a US Navy drone—Iran is looking for ways to act behind the scenes in order to inflict damage on the United States, both in the Middle East and on US soil. Thus, the NSA anticipates high probability of future collaboration of Iran and Russia targeting Western cyber objectives.

https://bit.ly/329QVcx

Czech Republic accusing Russia of cyberattacks

The attack on the databases of the Czech Ministry of Foreign Affairs occurred in June. Reputable Czech diplomatic and defense authorities claim that Russia is involved in the attack. Czech MPs demand the convening of a parliamentary security committee in connection with the attack. Last year, the Czech Republic's Ministry of Foreign Affairs also possibly was hacked by Russia,

when attackers gained access to more than 150 mailboxes of the Foreign Ministry staff and copied emails and attachments.

https://bit.ly/2ZfJ1Bj

APAC

Chinese spies have their sights on cancer research

The cancer rate in China has surged in recent years, which has led the Chinese authorities to look for an answer to the problem. However, they appear to have found a useful tool in the country's cyber capabilities. It has come to light that over a two-year period and on multiple occasions, hackers of the Chinese government have targeted organizations involved in cancer research. In at least one case, more than one group has gone after the same organization displaying evidence of relentless pursuit of research data. In two separate cases Chinese hackers targeted the same US cancer research organization, first, with a malware-laced document referencing conferences the organization had hosted and then by spear phishing(email scam) employees of the same entity. The hunt for cancer research appears to have gone beyond US organizations. In late 2017, the attack group known as APT10, which US officials have tied to China's civilian intelligence agency, attacked health care organizations in Japan with documents related to cancer research conferences. Cancer research is but one segment of the medical sector allegedly pursued by these groups. According to the company FireEye, "Targeting medical research and data from studies may enable Chinese corporations to bring new drugs to the market faster than Western competitors." Hackers have demonstrated an interest in collecting health records in bulk in recent years. China is the most notable sponsor of health care-focused espionage but not the only one. Others have included Russia and Vietnam.

https://bit.ly/2U3itgG

Hacking group targets organizations focused on North Korea's missile program

Hackers using web infrastructure associated with a known North Korean threat group are behind a dormant phishing campaign that is targeting the foreign offices of at least three different countries, as well as a number of research organizations. These include the French Foreign Office, the Slovakian Foreign Office, Stanford University, and a UK think-tank. Each target has previously focused their work on North Korea's nuclear efforts, or on the international sanctions issued as punishment for their previous international actions. The attacks are aimed at tricking diplomats or other civilians into entering information into a malicious website. The hackers in question can then use that information to spy on the affected email inbox. It is not exactly known who is behind the operation, though it has been linked to an IP address called the Kimsuky campaign, which Palo Alto Networks and others previously have associated with North Korea. The most notable page appeared to be a Stanford University secure email service, which encouraged faculty and students to use the portal in question, to send "moderate or high risk data." Stanford also happens to be home to the Center for Security and Cooperation and the Asia Pacific Research Center, which examines North Korea-related issues. This further explains the motivations behind the attack.
https://bit.ly/2PdzF4t

YouTube disables 210 channels spreading disinformation about Hong Kong

YouTube has made a decision to disable 210 channels, which are believed to be working as part of a "coordinated" influence operation against pro-democracy protesters in Hong Kong. The Chinese government has sought to portray them as terrorists or paid demonstrators despite the peaceful nature of their protests. Facebook and Twitter therefore decided that they had would remove accounts spreading disinformation on Beijing's behalf. Chinese officials have sought to disrupt international media coverage showing that

protests in the semi-autonomous territory are mostly peaceful. Many of the protesters have called for the resignation of Hong Kong's leader, Carrie Lam, who is backed by Beijing. The specific difference between these videos, pushed by state-run media as Communist Party boosterism and coordinated disinformation, was not immediately clear. However, their lingering existence on YouTube highlights the challenge and nuance that goes into mitigating the spread of propaganda. YouTube in its statement also said many of these channel operators used virtual private networks (VPNs) to disguise their true location. In announcing its own takedown, Twitter said many of the 936 accounts it suspended also used VPNs to shield their activity on the site. Unlike Facebook and Twitter, which are censored in China, Google does have realistic business prospects in the world's most populated country.
https://bit.ly/31XC9W2

A first in cyber "capture the flag"

Students from the US Army Cyber School and the Japanese Defense Forces participated in what service leaders are describing as the first international "capture the flag" type event. The event was hosted at the Georgia Cyber Center, a state of the art facility in Augusta, which is part of the US Army. The international exercise sought to improve both organization's relationship but also aimed at sharing best practices between the key allies in areas relating to cybersecurity. Todd Boudreau, deputy commandant at the Army Cyber School, said that "as our students see students from another coalition partners, they're likely to see them one day on an operations floor. We want to start that [trust] real early so we can build those bridges right away." He went onto say that "the services share those things both within DoD [Department of Defense] and then with the other nations as well, again, it's a team sport." Army leaders hope to expand the event. Next year, Boudreau said service officials are in talks for a second game. Representatives from the German military have already expressed interest, he said.
https://bit.ly/2ZoBjVK

"China Chopper" web shell makes a comeback in Lebanon and other Asian countries

Talos, Cisco's Security and Intelligence Research Group, uncovered the return of the web shell better known as China Chopper. A web shell is a script that allows attackers to remotely access servers running web applications. The hacking tool was initially discovered nine years ago, most notably known for its near undetectable nature and its implementation by groups linked with "Chinese state-backed hacks." According to Talos, the malicious code has remained simple—singular code line—and has seemingly "proliferated [in] the number of threat actors using it... over the last two years." Talos has recognized diverse use of tools, techniques, and goals in the three most active campaigns, targeting a government organization and web-hosting provider in Asia, as well as an organization in Lebanon. In contrast to the previously publicized context of China Chopper, in which the same groups were associated to events, Talos considers the involved actors in these campaigns to be different, which has additionally been confirmed by technical forensics.
https://tiny.cc/e24ubz

MIDDLE EAST

Are you a victim of cybercrime? Do not hesitate to report to Dubai police

The Dubai police have reminded the population to report cyber-oriented crimes such as fraud, using the official platform "e-crime," a quick and easy way to report online crimes without visiting the police station. The "e-crime" website launched by the Dubai police provides a platform where Dubai residents can report cybercrimes: all they have to do is fill a form and add all the information related to the incident. The most reported cybercrimes include "cyber extortion, online hacking, internet fraud, and online identity theft." The initiative aims to simplify the reporting process, encouraging people to report cybercrimes and to deter individuals from adopting criminal

behavior. Furthermore, the platform works only for residents in the geographical scope of Dubai City.
https://bit.ly/30KMJ2k

Saudi Arabia calls for increased tech innovation to combat cyberattacks

According to information security expert Eng. Samer Omar, the increasing amount of cyberattacks has caused Saudi Arabia to institutionalize and legislate on cyber threats issues. This tech innovation should support the recently released "Vision 2030" project, including digital information, e-Government development, and protection of data and systems. As Omar states, Saudi Arabia is investing huge efforts in many fields to develop the cyber sector and encourage a considerable transformation with the involvement of universities, institutions, and companies from the private sector. In 2018, the Kingdom led the Arab countries in the number of cyberattacks against it and was 17th in the world. Saudi Arabia's flourishing economy (recently ranked among the top 20 global economies) has made it a particularly privileged target for cybercriminals. It emphasizes the importance of freshly launched institutions that work to build and develop strategies to fight cyber threats, such as the National Cyber Security Agency and the Saudi Arabia Federation for Cybersecurity, Programming, and Drones (SAFCPSD).
https://bit.ly/2LbLNha

UAE leads Arab region in e-government and mobile services maturity

According to a report published by the UN Economic and Social Commission for Western Asia, the United Arab Emirates have been ranked first among the Arab countries in the Government Electronic and Mobile Services (GEMS) Maturity Index. The indicator measures the national achievements in the digital transition, mainly the countries' capacity to provide online services to the population. The report stated that the availability of services reached 90

percent in the UAE and that 80 percent of the population has access to services. Director General of the Telecommunication Regulatory Authority (TRA) Al Mansoori explained that being ranked first in the GEMS Maturity Index was the result of governmental efforts in the digital transformation. This index monitors countries' e-transition and annually measures their maturity in the field, allowing a comparison between countries' performance. The evaluation is based on three criteria: availability and sophistication of the services, satisfaction of the population, and public scope of the services.
https://bit.ly/2Zorke0

LATIN AMERICA

Hackers take over government Twitter accounts

The Secretariat of Security and Civilian Protection (SSPC) reported that hackers targeted social media accounts belonging to Mexican government departments and officials. While taking over victims' accounts, the hackers posted messages explaining that their behavior was motivated by political reasons. For example, they published that "This account has been hacked due to the owner's corruption" on an official's Twitter account, in addition to few anti-corruption messages. So far, the attacks were performed on Twitter, but the SSPC warned that the attackers might extend their hacks on other social media. The Secretariat found out that the attacks were carried out from Spain, Guatemala, El Salvador, and Panama. Some recommendations were made by the Federal Police to prevent further attacks, such as changing passwords, installing and updating antivirus software, and being cautious before downloading any application or file coming from unknown or suspicious sources. The event comes after the SSPC suggested the launch of an awareness campaign to warn officials of cyberthreats.
https://bit.ly/30Fl7vy
https://bit.ly/2Pii5MF

Brazil Central Bank moves to follow IMF crypto classification guidelines

The Brazilian Central Bank has adopted the classification of cryptocurrencies set by the International Monetary Fund (IMF) guidelines. The Central Bank announced that it will follow the IMF line and implement the classification of cryptocurrencies as non-financial products. In other words, cryptocurrencies will be classified as goods in the balance sheet and put under valuables. According to the report issued by the Central Bank of Brazil, the cryptocurrencies are assets that "come into existence as outputs of a production process (mining, project development)." Selling and purchasing such products include foreign exchange contracts and their execution. Given that, cryptocurrencies' operations should be recorded in the country's import and export statistics. Since Brazil is a net importer of crypto assets, this adoption of the IMF classification is likely to lower the trade surplus on Brazil's balance sheet.

https://bit.ly/2ZhwGwt

https://bit.ly/2RrU1CG

Venezuelan state airline begins accepting the Petro

The Venezuelan state airline Conviasa will start to accept payment in Petro, the state's oil backed cryptocurrency. Joselit Ramirez, the Superintendent of Cryptoactives (the national entity in charge of the cryptocurrencies and related activities), announced that it will be possible to use the "Petro App" to purchase plane tickets. The Petro endured false starts on several platforms, attracting criticism within the crypto community. International sanctions have also restricted its trading since American citizens are not allowed to purchase it. However, this announcement comes after Traki Stores, one of the biggest retail store chain in Venezuela began accepting Petro. The autonomous Intellectual Property Service (SAPI) in charge of the registration of trademarks and intellectual property is also accepting the Petro. Ramirez also announced that other websites were about to accept this cryptocurrency as a form of payment.

https://bit.ly/2zrTytT