Global Cyber Bi-Weekly Report by INSS July 15 2018

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

Contributors: Simon Tsipis, Ido Sivan, Anna Danilova, Sneha Mukherjee, Bryan McCarthy

ISRAEL

Iranian hackers tried to impersonate Israeli cybersecurity company

ClearSky, an Israeli cybersecurity firm, reported that it, too, has joined the list of victims of Iranian hackers that have impersonated legitimate websites. Last month, the company discovered that a hacker group called "Charming Kitten," which had perpetrated previous attacks, was still operating. The group is connected to the Iranian government and is deemed an "advanced persistent threat," meaning it is comprised of sophisticated hackers. ClearSky's most entertaining discovery so far, however, relates directly to the company. As the website Bleeping Computer reported last week, the Charming Kitten group impersonated ClearSky itself by creating a website almost identical to that of the Israeli firm, with a slightly different address: the imposter site ended in ".net" rather than in ".com." ClearSky researchers found some broken links in the fake site, leading them to think it is still being developed. The obvious question is what did the Iranian hackers hope to achieve with this impersonation. The answer lies in one significant difference between the two sites: Unlike the original site, the Iranian version allows users to register. This would enable the hackers to steal information from ClearSky's customers, who would think they were merely registering to receive updates from the company.

https://bit.ly/2J9nME9

IDF cyber defenders prepare their responses to the "unknown threat"

IDF assessments place cyber warfare on par with the potential damage that conventional weapons can cause. And in some cases, cyberattacks can surpass the damage caused by known threats like missiles, and a cyber arms race is

raging between Israel and its foes, parallel to the conventional arms race that is also under way. Israel's Prime Minister Netanyahu spoke at a cyber security conference late last month in Tel Aviv about the challenges that Israel and all civilized countries face from adversaries now bent on cyberattacks. "We cannot go back to the world of levers, pulleys, and couriers. Since we are going forward, we are absolutely vulnerable," he said. "Our airlines can be brought down; our fighter planes can be brought down." Prime Minister Netanyahu said that Israel receives about 20 percent of the global investment in the cybersecurity sector and noted Israel's cyber security center in Beersheba, which combines military, business, and high-tech know-how. He added that there is "no silver bullet" against cyber threats. "This is a supreme test for our civilization. It's going to be tested not only by criminal organizations [and] by terrorists, but by other states. We have to combine forces."

https://bit.ly/2m1DVCH

United States

NATO summit boosts cybersecurity amid uncertainty

Though the recent NATO summit involving President Trump and Secretary of State Mike Pompeo was full of heated exchanges over expenditures, a few notable advancements were made with regards to cyber security and cyber warfare. NATO has agreed to establish a new cyber operations center at the NATO Joint Force Command and has agreed to integrate cybersecurity into NATO operations.

https://bit.ly/2Ngwtz4

Senators press federal election officials on state cybersecurity

US senators are concerned that many the election systems of many states are completely electronic and not able to be audited. They expressed these concerns to the head of the US Election Assistance Commission (EAC). The EAC informed the senators that each state chooses from which private company they source election equipment and that there is no legislation that election systems have to be auditable.

https://bit.ly/2Lj1h4O

United States charges twelve Russian hackers with DNC cyberattacks

US Special Counsel Robert Mueller filed charges against twelve Russian hackers responsible for the 2016 Democratic National Committee (DNC) hacks. Interestingly but not surprisingly, all twelve defendants are officers in the GRU, Russia's military intel agency. Although massive amounts of data was gleaned from the spear phishing operation and other smaller operations on US state election boards, there are not yet any allegations that it affected the outcome of the election.

https://cnet.co/2Lb2GKL

EUROPE

Cyberattacks are now a matter of when not if for UK businesses

For a growing number of UK companies, being hit by a cyber breach is not a matter of "if" but rather "when," according to a new report by the firm KPMG based on a poll of 150 UK leaders. However, when compared to the rest of the world, the United Kingdom is performing well, according to the report. 39 percent of businesses said they agreed with the inevitability of being attacked, compared to a global average of 49 percent, which KPMG says is "disheartening, but optimistic."

https://bit.ly/2tWLRZA

United Kingdom: NHS accidentally leaks data of 150,000 patients

The National Health Service (NHS) has reported that a coding error in its patient data management system has resulted in the leaking of data of 150,000 patients. According to a statement released by the Parliament, NHS Digital recently identified a supplier defect in the processing of patient objections to the sharing of their confidential health data. The data for these

patients was used in clinical audit and research aimed at driving improvements in outcomes for patients without their consent.

https://bit.ly/2NTPYyG

Data privacy laws in Europe a boon to jobseekers

The sweeping new privacy law that went into effect in the European Union in May has significantly boosted demand for data protection expertise, according to Indeed, a job posting site. A report from the popular recruitment site found that job openings for data protection officers have skyrocketed 829 percent since 2016 as organizations took steps to comply with the General Data Protection Regulation (GDPR). By some estimates, GDPR has created some 75,000 job openings globally in the cybersecurity and data protection space.

https://bit.ly/2urPNCq

RUSSIA

Eastern EU members to cyber defend themselves from their Soviet ex-patron

The head of the Lithuanian Ministry of Defense, Raymundas Caroblis, said that six EU countries intend to sign an agreement for the establishment of Rapid Reaction Forces against cyberthreats. Most of these states are the ex-Soviet republics or ex-Soviet satellites, such as Estonia, Romania, Croatia, and Lithuania. It comes shortly after the European Parliament's January announcement of its intentions to strengthen cybersecurity because of the "Russian threat."

http://bit.ly/2NMt2RN

Russian breakthrough? Russia has developed a computer based on new components

A unique optical supercomputer that has huge advantages over traditional computers was developed at Sarov's Russian Federal Nuclear Center, by the Russian Research Institute of Experimental Physics. The development is based on so-called photonic computer (FVM), in which the computational processes

are "built" on the interaction of laser radiation pulses, and not on the work of electronic components, as in conventional computers.

http://bit.ly/2L7Dodj

Russia obsessed with internet content distribution in its territory

The Russian State Duma Committee on Information Policy, Information Technologies, and Communications approved legal amendments, according to which distributing materials from foreign media outlets on the internet that are financed from abroad can also be recognized as foreign media agents. Thus, according to this law amendments, persons that distribute foreign content through internet will be considered as agents of foreign states.

http://bit.ly/2L3nWSK

ASIA PACIFIC

India and UK to cooperate on cybercrime and cybersecurity

Minister for Law and Justice and Electronics and IT Ravi Shankar Prasad visited the United Kingdom from July 6 to 10, 2018 at the invitation of the David Gauke, the UK secretary of state for justice. The minister appreciated the tremendous interest shown by UK companies in India's digital story and listed some of the key areas, such as skill enhancement, Fintech, and emerging technologies such as AI and Cyber Security as the possible areas of growth where UK IT firms could leverage the growth potential and size of India's growing digital economy—expected to reach the size of a trillion dollars in the next few years—for its own growth.

https://bit.ly/2Lq1pN3

CSOCs help fight cyberattacks as China's network security market verges on boom

To help enterprises combat the threat of cyberattacks, the France-based Thales came up with Cybersecurity Operations Centers (CSOCs), which keep a watchful eye on their internet infrastructure and internal systems around the

clock. The firm is already operating CSOCs in five countries and regions, namely Canada, France, Hong Kong, the Netherlands, and the United Kingdom. A report released by CCID Consulting in March predicted that China's network security market will reach 73.89 billion yuan ($11.07 billion) by 2020, an annual compound growth rate of 21.7 percent yearly. To further improve national cybersecurity, the Ministry of Public Security issued a draft on graded protection of cybersecurity for public comment on June 27. The regulation classified five levels of cyber protection system based on the seriousness of threats, stating that without permission or authorization, internet operators must not collect data and personal information that is irrelevant to their services.

https://bit.ly/2KZICMc

Vietnam follows China with tough new cybersecurity law

A new cybersecurity law in Vietnam may usher in an era of increased online censorship, privacy-invasive data processing methods, and deprivation of internet connections for organizations and individuals who publish "prohibited" content. Drafted by the country's Ministry of Public Security, the law was passed by the National Assembly on June 12, 2018, despite the rare public opposition expressed by some lawyers and netizens. The legislation goes into effect on January 1, 2019. The law also places significant regulatory requirements on foreign technology companies. Similar to China's Cybersecurity Law passed in 2017, Vietnam's new law requires internet companies to locally store data and establish headquarters or representative offices in Vietnam.

https://bit.ly/2z626sT

Senior defense officials meet in Singapore to discuss regional security cooperation

Senior defense officials from the Association of Southeast Asian Nations (ASEAN) countries and eight partner countries in the Asia Pacific region met in Singapore this week to discuss ideas to strengthen regional security cooperation. In particular, officials discussed stepping up counter-terrorism cooperation among ASEAN defense establishments in the areas of "resilience, response, and recovery" to deter terrorist attacks, ensure swift responses to terror threats, and enhance rehabilitation and recovery efforts for areas

affected by terrorism. The key areas of discussion were counter-terrorism, humanitarian assistance, disaster relief, maritime security, and cybersecurity.

https://bit.ly/2mlehcj

Fourth Joint Cyber Security Center opens in Perth to protect resources sector

The federal government has opened its fourth Joint Cyber Security Center (JCSC) and first in Western Australia with a focus on protecting the state's energy and resources sector. The centers are public-private cyber-threat sharing centers intended to facilitate collaboration between cybersecurity experts and the sharing of information on potential threats and security challenges. Each facility hosts cybersecurity experts in government, business, and academia to help share data and advice through an information-sharing portal. So far, centers have been opened in Sydney, Melbourne, and Brisbane, with another expected to open in Adelaide later this year. The JCSC facilities are funded as part of the government's $47 million program laid out in 2016.

https://bit.ly/2JrxQsB

Japan strengthens cybersecurity cooperation with EU ahead of Olympics

Japan and the European Union are strengthening their cooperation on cybersecurity ahead of the 2020 Tokyo Olympic and Paralympic Games, where the city is expected to face significant cyberthreats. The Tokyo Organizing Committee of the Olympic and Paralympic Games already suffered a potential hack in 2015, making its website inaccessible for over twelve hours. According to the National Institute of Information and Communications Technology, which monitors cyberattacks on Japan, the volume of data subject to cyberattacks increased from 25.6 billion packets in 2014 to 150.4 billion packets in 2017. In 2017, Japan identified thirteen sectors of critical infrastructure in the fourth edition of its cybersecurity policy and called for an all-out effort by the public and private sectors to protect them. The sectors included aviation services, government and administrative services, medical services, and credit card services.

https://bit.ly/2L2owRB

MIDDLE EAST

Gulf firms must transition beyond prevention strategies

Gulf firms are still investing in traditional prevention methods in their cybersecurity, according to the vice-president of Gulf Business Machines Hani Nofal. Nofal, also mentioned that firms trying to build large prevention systems need to remember the Titanic. According to Nofal, firms must focus on "detecting the iceberg," and having the lifeboats necessary to survive the crash. Detection, response, and prediction together will be required investment for Gulf firms that wish to utilize artificial intelligence in their cyber defense.

https://bit.ly/2mkrkuC

New Egyptian cybercrime law limits freedom of speech

Egypt in recent years has continued its prosecution of online journalist communities. The arrests of different types of people, from activists to poets, are made on the charge of spreading false news. The new Anti-Cyber and Information Technology Crimes Law makes service providers retain user information, such as tracking data, for the Egyptian state. Any website that incites against the state will be shut down according to Article Seven of the new law. Telecommunications companies must retain user data for 180 days. The law also authorizes broad surveillance powers.

https://bit.ly/2NOjiXg

LATIN AMERICA

Mexican banks put on alert for hacking

Mexican banks have been put on alert by the state of Mexico, according to an unnamed source who was not authorized to speak to the press. In May, a cyberattack siphoned three hundred million pesos, or 15.3 million US dollars, resulting in the coordination between the Mexican state and the banking system in Mexico. Bitso, a Mexican cryptocurrency trading platform was also recently hacked.

https://reut.rs/2Jc1mlZ

Brazil's senate passes data protection law

Inspired by the European Union's General Data Protection Regulation (GDPR), the Brazilian law has detailed rules on collection of data, processing, and storage of personal data. The bill establishes in law the national data protection authority, with the responsibility of regulating data protection and enforcing sanctions against the non-compliant. There must be a legal basis for collection, and biometric data has more restrictions. The data protection authority will be able to require that companies have a data protection officer and undergo a privacy assessment.

https://bit.ly/2Nb8rpo

AFRICA

African states need Computer Emergency Response Teams

Only 18 of 54 African countries have set up Computer Emergency Response Teams (CERTs), according to Mauritanian CERT National Computer Board member, Kaleem Usmani. This leaves African states in a position of vulnerability with regard to coordination. Vincent Ngundi, the head of the Kenyan CERT, said that since 90 percent of cyber infrastructure is controlled by private companies, the government should help to assist their coordination.

https://bit.ly/2NQnWny

Nigerian banks will be required to ensure their cybersecurity

Banks in Nigeria will be required to report all cyber incidents to the Nigerian central bank after it mandated banks to incorporate cyber risk management with their institution's wide risk management as well as corporate governance. Banks will be required to have a chief information security officer. Within this new framework, banks will be required to take full responsibility for cyber incidents.

https://bit.ly/2zHHJme

Kenyan cybersecurity company ventures into Mauritius

Local business consulting and IT services firm Serianu has announced plans to venture into the Mauritian market. The firm's managing director, William Makatiani, says the expansion includes setting up a cybersecurity training center in Mauritius that can train up to about 500 locals per year on cyberattack preparedness.

https://bit.ly/2umZDps

Africa's cybersecurity workforce challenge

Africa suffers from a cybersecurity skill gap. In order to better understand the skills gap, Check Point recently surveyed 450 IT professionals across the world, asking them questions about their challenges in managing their organizations' security. The results were startling. Check Point found that 77 percent of all respondents were concerned with their security teams' capabilities to deal with current and future cybersecurity challenges. Chief Information and Security Officers tend to manage around ten to fifteen completely separate solutions for their security. Given the sheer number of technologies that each professional needs to handle, it should not come as a surprise that the survey found that 64 percent of the respondents' teams expressed difficulty in managing their security workload.

https://bit.ly/2LbBdJ2