Global Cyber Bi-Weekly Report by INSS October 01 2018

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

Contributors: Simon Tsipis, Anna Danilova, David Libin, Gal Sapir, Stefan Weenk, Michal Beit Halachmi

ISRAEL

UAE used Israeli software to spy on Saudi Arabia and Qatar

A New York Times report revealed that Israeli intelligence gathering software, created by the Pegasus program of the NSO Technologies Ltd., has been used in attempts to spy on Qatar's Emir Tamim Bin Hamid Al Thani, Lebanese Prime Minister Saad Hariri, and a Saudi Prince. The malware can be used to hack smartphones by sending the target device a convincing message that contains a link. If the addressee clicks on the link, the malware is installed on the device, and data such as locations, recordings, and emails can be obtained. Lawsuits are filed against NSO by a Qatari citizen and five Mexican human rights activists and journalists, claiming the company committed illegal espionage in 2014–2016. The spyware also surfaced in Panama, as lawsuits have been filed against Panama's ex-president Ricardo Martinelli for spying illegally on around 150 individuals between 2012 and 2014, and also targeting a staff member of Amnesty International.
https://bit.ly/2Q8yAr8

Forter secures $50 million for e-commerce fraud detection technology

The Israeli-American startup company Forter, specialized in developing products to protect online retailers from fraud, has secured $50 million in financing to develop its e-commerce fraud detection technology. The company uses machine learning to create an identity database that currently covers over 180 million US consumers and 50 million consumers in 188

countries. The CEO of Forter, Michael Reitblat, said that the company is investing the financing in research and development to expand the platform and to accelerate its ambition to expand globally. The funding was led by March Capital Partners, which provided another $50 million earlier on, bringing the total funding to $100 million. The company was founded in 2013 by Michael Reitblat (CEO), Liron Damri (president), and Alon Shemesh (chief analyst) to prove that conventional tactics were inadequate for the realities of online commerce.

https://bit.ly/2OoreS7

UNITED STATES

Facebook's worst security breach hammers users' trust once again

The social media behemoth is facing another crises less than six months after the Cambridge Analytica scandal. Facebook has uncovered a security breach that exposed as many as 50 million accounts. The identity or amount of hackers connected to the attack are still unknown, including what the hackers did with the data, their motive, and target profile. The criminal or criminals exploited several software bugs to obtain login access, enabling them to act as the user on their profile or any other applications they accessed by using Facebook. Although the vulnerabilities have been resolved, many questions have gone unanswered. Chief Executive Officer Mark Zuckerberg pledged in April during the congressional hearings on the Cambridge Analytica crisis "to protect user data above all else and invest more in security," and only days before the security flaw was discovered, Zuckerberg wrote that the "company was better prepared for attacks by foreign actors." This breach has exposed the technical security problem of the widely used platform, and has significantly undermined Zuckerberg's assertions, posing a great challenge of the public's trust. Within hours of the announcement, a class-action suit was filed by users in California.

https://bloom.bg/2NN4vj6

Department of Defense releases first new cyber strategy in three years

Department of Defense's revamped documents lay out the focus of its cyber efforts, notably, on China and Russia. The unclassified summary highlights the vision of a new strategic era of "great power competition." The cyberspace strategy describes five objectives: guaranteeing the joint force ability to achieve its missions in cyberspace; strengthening the force by conducting cyberspace operations that increase military advantages; defending US critical infrastructure from malicious activity that can cause a significant cyber incident; securing DoD information and systems, including non-DoD-owned networks against malicious activity; and expanding the departments cyber cooperation by increasing interagency, industry, and international partnerships. The strategy further highlights the need to remain consistently engaged and to "defend forward" by means of acting outside the boundaries, which are in line with the new Cyber Command's leader General Paul Nakasone, who recently stated the need to "act forward" in order to better defend against adversaries. The strategy comes at a time of other changes occurring in the DoD, including the Cyber Command's elevated status to a unified combatant command, with new authorities, acquiring responsibilities, which in the past were presidential, to conduct cyber operations abroad, to fully cyber teams, and to update the DoD's cyber doctrine.
https://bit.ly/2Qkchhr

The Marines want to test all recruits for cyber skills

Starting in October, all applicants to the Marines will be given a cyber test. As part of the Marine Corps' latest cyber talent recruitment efforts, the aptitude management mechanism will assist in screening those eligible to fill roles in the new cyberspace operations occupational field. The test was designed by the Air Force and includes questions from four categories: networking and communications, computer operations, security and compliance, and software programing and web design. This direction comes at a time when the Marine Corps needs to reinforce its strength and capability as the modern battlefield

is evolving. The Marine Corps requested an increase in budget related to cyber, electronic warfare, and information operations, complementing the recently approved expansion for the Marine Corps Cyberspace Command.
https://bit.ly/2NSQeBx

EUROPE

Cyberattacks cost German industry almost $50 billion according to study

Two thirds of Germany's manufacturers have been hit by cyberattacks, costing the largest economy in Europe some 43 billion euros ($50 billion), according to a survey published by Germany's Information Technology sector association. Industry association Bitkom surveyed 503 top managers and security chiefs from across Germany's manufacturing sector and found that the small and medium-sized companies, which are the economy's backbone, are particularly vulnerable to cyberattacks.
https://reut.rs/2p4BVej

EU lawmakers push for cybersecurity, data audit of Facebook

European Union lawmakers are set this month to demand audits of Facebook by Europe's cybersecurity agency and data protection authority in the wake of the Cambridge Analytica scandal. A draft resolution submitted to the civil liberties and justice committee of the EU Parliament urged Facebook to accept "a full and independent audit of its platform investigating data protection and security of personal data." According to Claude Moraes, the chairman of the EU parliamentary committee, "Not only have Facebook's policies and actions potentially jeopardized citizens' personal data, but then they have also had an impact on electoral outcomes and on the trust citizens pose in digital solutions and platforms." The committee aims to adopt the resolution, which will almost certainly be modified, by October 10 and put it to the full assembly for endorsement in late October, well ahead of EU elections next May.

https://bit.ly/2NUoHQg

Britain to create a 2,000-strong cyber force to tackle Russian threat

Britain is significantly increasing its ability to wage war in cyberspace with the creation of a new offensive cyber force of up to 2,000 personnel, according to Sky News. The plan by the Ministry of Defence and GCHQ comes amid a growing cyber threat from Russia and following the use of cyber weapons for the first time to fight the Islamic State. The new force—expected to be announced soon—would represent a near fourfold increase in manpower focused on offensive cyber operations.

https://bit.ly/2xq6HmK

RUSSIA

NATO to combat Russian "fake news" phenomenon

NATO is to launch a new program for its military personnel, on using internet data and distinguishing propaganda content, as an effort to combat the "fake news" phenomenon, that is widely used by Russia, according to the alliances' sources. The Russia Today news agency quoted NATO sources, and stated that "NATO believes that social networks have become a platform to effectively disseminate propaganda and misinformation."

http://bit.ly/2Nahbvi

New US strategy on cybersecurity stresses Russian threat in particular

According to the assistant to John Bolton, the head of the White House National Security committee, there is a defensive and offensive aspect in the new US strategy on cybersecurity. Particular attention is being given to Russia's activity in cyberspace.

http://bit.ly/2xTY9Vt

Ukrainian military's usage of elementary passwords might have caused penetration

The Communications and Information Systems' Department of the Armed Forces of Ukraine denied the claim that elementary passwords were used for access to the servers of the troops' automated command and control system. Earlier, Ukrainian journalist Alexander Dubinsky claimed that the military personnel used passwords such as "admin" and "123456." According to Dubinsky, this "allowed the enemy, until the summer of 2018, to scan information of the Ukrainian military" and might have been used by Russia to penetrate the forces' command and control networks.
http://bit.ly/2QdTl3I

ASIA PACIFIC

Microsoft India and Data Security Council of India launch program to incorporate women into cybersecurity

The three-year program, named "CyberShikshaa," will initially train one thousand women from underprivileged areas in ten different locations. The women, all science graduates between the ages of 20–27, will be offered employment opportunities in the ever growing cybersecurity field. The four month training course will include theory, case study, and practical hands on experience.
https://goo.gl/xXoWc5

China may attempt to sabotage Taiwan's November elections

According to the Taiwanese government, China, Russia, and North Korea may test cyber hacking tools in the upcoming November local elections, intended to undermine the president, who, together with her Democratic Progressive Party, refuses to recognize Beijing's government's claim to Taiwan. The tests may involve new malware tools usually used to target government agencies. Last year, 360 successful cyberattacks targeted Taiwan's government, possibly compromising sensitive and confidential data. However, this is compared to

20–40 unsuccessful monthly attacks on various governmental and military bodies.

https://goo.gl/WkxbzB

United States, Japan, and Australia offer alternative internet cable to Papua New Guinea

The joint venture is consulting with Papua New Guinea's government, offering an alternative to the offer by Huwaei, the Chinese telecommunications company, which denies its connections to the Chinese government. Last August, the Australian government blocked Huawei 5G services, sighting security risks. The United States regards the company as a major cybersecurity threat. The US House Intelligence Committee found that Huawei was tied to the Chinese government—specifically, the Chinese army—and said that it had received internal company documents proving Huwaei's ties to an entity of an elite cyber warfare unit within China's People's Liberation Army. Australia had offered to finance an initial undersea cable to Papua New Guinea and Solomon's islands, as the latter initially signed with Huawei in 2017, but later cancelled the deal due to Australia's offer.

https://goo.gl/UqgNfu

MIDDLE EAST

Botnets remain a threat to Gulf states, although weaponized hacks have decreased

Microsoft's chief security engineer suggested that the Gulf Cooperation Councils remains a lucrative target for cyber hacks, especially those utilizing botnets. Botnets can remotely take control of a device. Riyadh itself was infected by 43.1 percent of bots in the region, followed by Dubai at 24.7 percent. David Weston, Microsoft's chief security engineer, noted that the number of attacks has decreased year by year. He also said that the price of weaponized exploit has increased, indicating that the number of people who

can orchestrate sophisticated attacks has decreased. The more common attacks are those that utilize a human operator, along with a phishing attack.
https://bit.ly/2zLHAMD

FireEye identifies Iranian group phishing for intellectual property

FireEye has identified the hacking group, APT33, as having made phishing attacks on targets in the energy sector in the states of the Gulf Cooperation Council. FireEye assumed that recent energy sanctions on Iran had resulted in APT33 to search for strategic intelligence and intellectual property in the energy sector of the GCC states. The hackers used Farsi and operated according to Iranian time. This group previously targeted aviation sector and energy sectors in Japan, South Korea, United States, and Saudi Arabia, with the goal of stealing intellectual property.
https://bit.ly/2MGzR5z

A UAE bank has started the first sound-based payment technology in the region

The technology, which was developed in collaboration with FINTECH partners, will enable money transfers and person-to-person exchange of currency. The innovative technology enables sound waves, instead of technical hardware, to access the payment. The question of how secure the systems are remains unanswered; however, being at the cutting edge of technology does not hurt and making payments based on the customer's voice is an effective way of moving away from passwords, which can be hacked.
https://bit.ly/2zL5cB9

LATIN AMERICA

A CamuBot attack has been targeting Brazilian banks, with phishing attack

A CamuBot attack, which is closely related to a phishing attack, has been recently targeting Brazilian banks. This attack is unique in that it relies upon both a person who phones the target and the phishing attack. The hacker will phone the customer and direct them to giving their credentials to a fake site, which is meant to impersonate the real bank's website. The hackers specifically target people who are involved in business and professional networks they deem profitable to hack. Banks can only protect against these attacks by using two-factor authentication, in other words, a second password.
https://bit.ly/2xRb3U5

Banks in Latin America prepare for another year of cyberattacks

Banks in Latin America are preparing for another assault of cyberattacks this coming year. According to the Organization of American States, in a report on 191 banks in Latin America, the vulnerability of banks resulting from of rapid digitization is noted. Malware was the most common attack, with 80 percent of banks reporting it. Daily malware and phishing attacks were reported at 22 to 24 percent of the banks. Almost half of the banks still have not adopted tools, such as big data, machine learning, and artificial intelligence, as their defensive measures.
https://bit.ly/2DBbMy3

AFRICA

Attempt to hack South Africa's server of the Department of Labor unsuccessful

A cyberattack on the external-facing servers of South Africa's Department of Labor was confirmed to be unsuccessful, said its Information Technology unit. The unit confirmed there was an attempted Distributed Denial of Service (DDoS) attack but reassured that the server was not compromised, following media reports over the weekend stating that the hack was successful. A DDoS

attack is when an attacker, or attackers, attempt to make it impossible for a service to be delivered. The cyberattack was "attempted through the external Domain Name Server (DNS), which is sitting at the State Information Technology Agency (SITA)," said the Acting Chief Information Officer, Xola Monakali. The department and SITA have started an investigation into the cyberattack.

https://bit.ly/2x8fpoE

Cyber crooks hijack Kenya's coveted digital revolution

Kenya's increasing position as a continental leader in digitalization of the critical infrastructure is disadvantaged due to existing gaps in current cybersecurity laws. The small and medium enterprises and the financial sectors are the most vulnerable to cyberattacks. Africa's Cyber Security report estimates the cost of cyberattacks in Kenya at $210 million. Cyberattacks are mainly focused on infiltrating bank infrastructure and payment systems using sophisticated malware. Analysts believe Kenya's thriving digitalizing economy could backfire, since businesses rely on technology and are not yet protected against aspects, such as Bring Your Own Device (BYOD) and the Internet of Things (IoT). A lack of information security experts and a lack of awareness or investment in information security make Kenya's infrastructure vulnerable against the constantly changing malicious software attacks by cybercriminals.

https://bit.ly/2zLIqJh