Global Cyber Bi-Weekly Report by INSS December 15 2018

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

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

ISRAEL

Amnesty demands Israel revoke NSO's license after Haaretz report on firm's negotiations with Saudis

Amnesty International has asked Israel's Defense Ministry to withdraw its defense export license from the cyber firm NSO after it had been proven that NSO had developed software that had been used in "a series of egregious human right violations." The request was made two weeks ago after an investigation by Haaretz discovered that the company had offered Saudi Arabia a system for hacking cellphones. According to sources in the Defense Ministry, which keeps track of defense exports, the Defense Ministry adhered strictly to the law while granting licenses and could not discuss the existence of NSO's license for security reasons. In a statement this summer, Amnesty International revealed that one of its employees had been targeted by a hacker using NSO software. Amnesty Israel rejected the response of the Defense Ministry and said it intended to pursue legal action.

https://bit.ly/2QAs1kZ

Armed with laptops, IDF soldiers tasked with securing Israel's cyber borders

Israeli soldiers in charge of improving the Israel Defense Forces' systems so it is hacker-proof were sent to a border for an unknown period of time, armed with just their laptops, to create solid cybersecurity measures in a new system to protect the border against cybersecurity threats. "There were concerns the system wouldn't work, and indeed that was the case," said Maj. Aleph and "everyone was in high alert, but we managed to identify the problem and solve it." Maj. Aleph is a commander in the IDF's Joint Cyber Defense Division, which operates as a technological body to provide the Israeli army and its systems with cyber defense against cyberattacks. The division is the red team

of the IDF and tries to find weaknesses in the systems and networks before others can.

https://bit.ly/2BtNphv

Israeli technology effectively prevents attacks during G20

Argentina employed Israeli technology to provide security during the G20 Leaders' summit in Argentina, and it detected several unauthorized drone incidents. The participation of leaders from nineteen countries and the European Union were not affected, despite previous fears. A contract worth more than $5 million was signed by the Defense Ministry of Argentina with its Israeli counterpart to provide cyber defense and cybersecurity services for the meeting. The Israeli technology successfully blocked incoming suspicious drones flying near global leaders. The Drone Guard system bought by Argentina was designed by ELTA Systems, a subsidiary of Israel Aerospace Industries (IAI).

https://bit.ly/2QISblK

UNITED STATE

McAfee: US companies targeted by possible North Korean hackers

According to McAfee Inc., since October, a cyber espionage campaign has been conducted targeting mostly US companies in the nuclear, defense, energy, and financial industries. Although not identified, it is projected that attempts were made against eighty-seven companies. While attribution and intentions are still ambiguous, the utilized malware has been associated with code formerly used in attacks linked to the Lazarus Group, suspected to be backed by the North Korean government. According to the computer security software company's analysis on "Operation Sharpshooter," the attacks were veiled as legitimate industry recruitment initiatives. The sophisticated malware "Rising Sun" was delivered to employees using social media platforms, with Dropbox links to Microsoft Word documents, which contained the malware, and aided access to the hackers. Thus far, the degree of network exposure achieved by the hackers remains unclear.

https://bloom.bg/2GeUOXt

Equifax failed to match security to its growth, report says

The recently released House Oversight Committee report on the hack that compromised the data of 148 million people in 2017 highlights Equifax's failures to "modernize" its security technology and practices. The seventy-six day long campaign—one of today's most infamous data breaches—has been proclaimed by the commission to have been preventable. Largely due to oversight of the security issues, involving several expired security certificates that facilitated undetected theft of unencrypted sensitive credentials, the inadequate window of time applying the patch to the software availability, in combination of the company's growth campaign beginning in 2005, exasperated the system's liabilities. In a statement following the disclosed report, Equifax said it has engaged in steps towards improving digital security and agrees with most of the recommendations, although it claims that the committee failed to provide a sufficient amount of time to review the document, which contains "significant inaccuracies." Among the proposals were "additional oversight authorities and enforcement tools," legislation on data breach protocol, and incorporating transparency practices among companies on cyber risks.

https://bloom.bg/2SGjZn4

New flaw prompts Google to shut down Google+ for consumers within ninety days

Alphabet Inc.'s Google announced the closure of the social media platform earlier than planned, as a result of the discovery of a bug that was facilitated by a recent platform update, which could affect an estimated 52.5 million users. It could expose non-public profile information, including photos, name, age, gender, relationship status, email address, residence, and occupation details, to name the least. This is the second major security flaw incident for the company, after it acknowledged having uncovered a privacy breach in March, causing it to decide to expedite the shutdown of the consumer version of Google+ and its APIs (application programming interface) from August 2019 to March 2019 (Google states April 2019). The internet giant determined the malicious malware existed for six days, without any evidence of passwords, financial information, or national identification numbers breached, nor the exploitation of the compromised data. The announcement was made

a day before CEO Sundar Pichai testified before the House Judiciary Committee regarding the company's data collection practices.

https://bit.ly/2EkNuHh

EUROPE

Europe should be wary of Huawei, EU tech official says

The European Union should be worried about Huawei and other Chinese technology companies because of the risk they pose to the bloc's industry and security, the EU's technology chief said on Friday, echoing concerns raised elsewhere in the world. Huawei expressed disappointment at EU Tech Commissioner Andrus Ansip's comments, saying the European Union had never been asked to install technology that could be used for spying and never would.

https://reut.rs/2LsFOnE

German security office warned German firms about Chinese hacking

Germany's Office for Information Security (BSI) has issued warnings to several German firms named by the United States as possible victims of hacking attacks, a newspaper reported, adding that Chinese activity against German firms has increased. Cyber experts have long warned that Germany—with its high level of technology expertise—is a particularly attractive target for cyber attackers of all kinds, including state actors.

https://reut.rs/2Guj73D

EU negotiators reach agreement on cybersecurity act

Representatives from the European Commission, Council and Parliament on December 10 banded together to strengthen cybersecurity efforts, reaching agreement on the European Union's cybersecurity act. The measures approved will see more resources and greater responsibility afforded to ENISA, the European Union's cybersecurity agency, as well as establishing a certification framework that will set cybersecurity standards for products during the design and development stage. The Commission is set to draft the

scope of products that require obligatory certification, with a list to be finalized by 2023.

https://bit.ly/2L8YuJ3

Redacted documents: Cybersecurity breaches rising across UK defense sector

UK defense secrets are increasingly being exposed to hostile nation states after the number of security breaches in the defense sector rose this year. Heavily redacted records obtained by Sky News show an increase in incidents reported to the Ministry of Defence (MoD) between January and October compared to the same period in 2017. Sky News previously revealed that the MoD and its partners failed to protect military and defense data in thirty-seven incidents throughout the whole of last year, with military data being exposed to cyber risks posed by other states on dozens of occasions.

https://bit.ly/2R4AI6s

RUSSIA

US investigation of Russian cyber fraud during 2016 elections leads to Assange

The investigation of Russian cyber interference in the 2016 US elections by the Justice Department's Special Counsel Robert Mueller has links to Julian Assange, the WikiLeaks co-founder. The investigation does not exclude the possibility that the cyber-plot was a joint operation between Russian intelligence and Julian Assange. Thus, Assange, who received asylum in Russia, is to face US federal charges.

https://n.pr/2UDexDu

The CIA has no more doubts that Assange is working for Russian intelligence

Former CIA Director Mike Pompeo declared in 2017 that Julian Assange's WikiLeaks was an agent of a "hostile intelligence service," hinting at Russia. Today, however, the US intelligence community has little doubt that Assange

might actively be working for Russian intelligence, by publishing and committing cyber penetrations and hackings of various US official and non-official targets.

http://bit.ly/2rxxERT

Finland suspects Russian trace on GPS disfunctions during NATO military drills

Finland's Prime Minister Juha Sipilä admitted the possibility of "Russian interference" in the country's satellite navigation systems. According to Sipilä, in the north of Finland during NATO exercises, large-scale failures of GPS signals occurred. "It is technologically relatively easy to disrupt the radio signal, and it is quite possible that Russia is behind this," he said. According to Sipilä, Russia "has the means for this."

http://bit.ly/2SH5GP9

Russia is concerned about the future of digital economy

The development of digital economy was one of Russia's central discussion topics during the G20 summit in Argentina. Among other things, according to the Kremlin press release after the summit, Russian president Vladimir Putin presented his view and suggestions regarding the future of the digital economy.

http://bit.ly/2PyMS2t

MIDDLE EAST

Cyberattacks in the industrial sector on the rise due to Internet of Things

A new report warns that the growing number of potential cyberattacks is the result of the high penetration of Industrial Internet of Things (IIOT) technology in critical infrastructure and the manufacturing sector. Frost & Sullivan claimed that cyberattacks within the energy and utility industries alone cost an average of $13.2 million per year. More and more cybersecurity approaches have been adopted with the rise of cyberattacks, combined with evolving

compliance regulations by governments, and an increase in security awareness among mature and immature markets. These rising incidences of cyberattacks, coupled with evolving compliance regulations by governments and increased awareness among mature and less mature markets have accelerated the adoption of cybersecurity approaches. However, a high level of uncertainty still exists in addressing industrial cybersecurity, with existing cybersecurity services struggling to provide comprehensive visibility across both IT and OT networks.

https://bit.ly/2S8h1bg

Warnings as destructive "Shamoon" cyberattacks hit Middle East energy industry

A new and highly destructive malware, designed to wipe systems and render them inoperable, is being used to attack energy companies in the Middle East. The malware has been used on at least two companies operating in the region. The wiper malware known as Shamoon, targeted Italy's Saipem servers across the Middle East, Aberdeen, and Italy. Shamoon was previously used in an attack on oil giant Saudi Aramco, causing 30,000 computers to shut down and then was attributed to Iran. Until now, it remains unclear who is behind the latest attacks, according to cybersecurity experts from Symantec and Chronicle, an Alphabet-owned company. A heavy engineering company in the United Arab Emirates was hacked a day before Saipem.

https://bit.ly/2QISoFy

APAC

China's state run spy agency is suspected of a cyberattack on the US Marriott Hotel chain

US officials said that they believe that the Marriott Hotel cyberattack, discovered in late November, is part of the Chinese government's ongoing cyberattacks. The Marriott hotel revealed that the cyberattack, spanning over four years, could potentially expose the names, passport numbers, and credit cards information of roughly 500 million guests worldwide. At least three class action suits have been filed against the hotel in Canada, claiming the hotel and their companies were negligent in safeguarding personal information. Officials from the Justice department, the FBI, and Homeland Security testified

in front of the Senate Judiciary Committee, claiming that China is attempting to steal trade secrets and intellectual property from US companies, in order to damper its economy.

https://goo.gl/n61A13

https://goo.gl/Cm1SnM

Vietnam National Assembly passed cybersecurity law

The new law, which will go into effect on January 1, 2019, requires that all foreign companies store user data in Vietnam and be subjected to domestic law. The law requires all internet-related service providers to open a local representative office in exchange for a government license to operate within the country. The law was largely disputed by activists and NGOs, who claimed that it violates the freedom of expression in the country, where regulation is already heavily controlled and there has been a crackdown on activists, especially those who advance social issues and protests on Facebook, which includes 55 million users out of a 100 million population. Prominent bloggers and activists were arrested and given prison time of six to twenty years. The law uses key words as prohibited, especially ones who might be considered propaganda, or criticism against the state, as well as making it illegal to share, call, or campaign information relating to mass protests.

https://goo.gl/8McBFD

New cyber security law in Thailand raises alarm among Tech giants and civil society advocates

The new law will give the newly created National Cyber Security Committee (NCSC) the authority to raid personal or business computers, and even enter personal property without a court order. It can also summon people or business owners for interrogations and force them to hand over user information, and charge them on criminal offences if they refuse to comply. The US-ASEAN business council, composed of tech giants, such as Google, Facebook, Apple, and Amazon, sent a letter to the Thai government warning that this law would come at the cost of breaching cyber security privacy and civil liberties. This concern is shared by civil society advocates, who have seen a rise in Thailand's online censorship and fear that the NCSC would be able to override laws in associating "cyber threats" to online content, since the new

law does not categorize data, which may include online data. Since the death of the Thai king in 2016, there has been an upsurge of government removal requests to social media networks. Facebook removed 365 posts, and in 2017 handed over user data to the government for the first time. Google agreed to remove 93 percent of the government requests last year alone, rising by 57 percent since 2014.

https://goo.gl/3gCVLy