Global Cyber Bi-Weekly Report by INSS

February 01 2019

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

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

ISRAEL

Invoking Operation Entebbe, Netanyahu says Iran conducts daily cyberattacks against Israel

At the Cybertech Conference in Tel Aviv, Prime Minister Binyamin Netanyahu highlighted Israeli readiness in the face of Iranian cyberattacks. "Iran [cyber]attacks Israel on a daily basis," he addressed and "Iran threatens us in many other ways." The head of Israel's Shin Bet internal security agency is reported to have warned that Israel was bracing for a state-driven cyber invention in its April 9 general election. The Israeli prime minister also claimed that "every country needs the combination of a national cyber defense effort and a robust cybersecurity industry. And I think Israel has that and has that in ways that are in many ways unmatched." The cyber threats against Israel have led to a growing interest in high tech development, which have brought leading international companies to Israel.

https://bit.ly/2Uwh2GM

Israel, New York City, and the Netherlands forge cybersecurity partnership

Jerusalem Venture Partners (JVP), a leading Israeli investor, announced that it is partnering with the Netherlands as well as several startups to create and nurture a cybersecurity ecosystem involving Israel, the Netherlands, and JVP's new cyber investment center in New York, Hub.NYC. The cooperation is the result of an effort to meet the increasingly globalized challenges of the cybersecurity industry. "It is an honor to join JVP in creating new collaborations in cybersecurity," said Prince Constantijn, director of StartupDelta, and "our cybersecurity industry is growing fast with cutting-edge solutions and talent, and we are thrilled to continue to expand these offerings to the world."

https://bit.ly/2FL30gZ

Investment in Israeli cyber exceeds $1 billion for first time in 2018

A report by Start-Up Nation Central revealed that Israel's cybersecurity industry investments exceeded $1 billion in 2018. Only American cybersecurity companies surpass Israel's growing cyber field in terms of investment. The 450 active cybersecurity companies in Israel raised a total of $1.19 billion last year, creating a 47 percent increase since 2017. The report also shows that non-Israeli investors are more dominant on the Israeli market, participating in 65 percent of the 117 investment deals concluded in 2018. "The last few years have been very dramatic for enterprises that are collecting massive amount of data," said Nir Falevich, and "due to the GDPR regulations, what happened in the United States during the 2016 election campaign with Facebook and Cambridge Analytica, and the massive data breaches."

https://bit.ly/2sTBeX2

UNITED STATE

Apple disables group chat on FaceTime after discovery of bad bug

In November 2017, Apple discovered a bug on MacOS, which enabled users to circumvent system logins and access administrative accounts. The shortcoming led the company to promote its value of security and privacy, as seen on billboards around the Consumer Electronics Show in Las Vegas. Yet, earlier this week, another bug was discovered, which functions on any system where FaceTime was installed, causing the group chat feature on the application to be inaccessible. It also permitted users to eavesdrop through video and audio before the recipient picks up and exploits the software despite recipient actions of silencing or terminating the call.

https://bit.ly/2MJhzlK

United States announces disruption of "Joanap" botnet linked with North Korea

The Justice Department's efforts to neutralize suspected North Korean botnet referred to as "Joanap," has taken an assertive turn. For nearly a decade, the malicious software along with the Brambul worm, "a brute-force authentication malware," has targeted Microsoft Windows, compromising computers on a global scale, and affecting "the media, aerospace, financial, and critical infrastructure sectors." In part of its extensive operation, a recent court ordered search warrant authorized the "FBI to control servers that mimicked computers within the botnet," allowing the agency to garner more information, identify and notify victims, demonstrating the FBI's subsequent expanded power in cyberspace.

https://bit.ly/2GcNKJl

Intelligence chiefs single out China in threat hearing

With ambitious efforts against China over espionage and intellectual property theft allegations, the Justice Department announced a cumulative 23-count indictment against the Chinese telecommunications goliath Huawei, followed by strong discourse against the East Asian state at the Worldwide Threat Assessment, where the US intelligence community convened. The report findings valuated China as the United States' top cyber threat, not excluding Russia, North Korea, and Iran. The assessment offered insight into the growing complexity of the cyber threat, including the rise of "Chinese digital aggression," their increasing capabilities, their cost-effective use of publicly available tools, and outsourcing of hackers. The report elaborated on regional and sector specific targets, alongside adversarial efforts increasingly aided by cyber capabilities in gaining "political, economic, and military advantages over the United States and its allies and partners." Heads of the six intelligence agencies referred to the scope of cyber threats on a global level with a cautionary assertion that "the post-World War II international system is coming under increasing strain amid continuing cyber [threats]." Director of National Intelligence Daniel R. Coates stated that the US election security will remain a top priority for the intelligence community.

https://bit.ly/2G07d0s

Medigate raises $15 million in Series A funding for medical device security

The dependability and continued development of internet-connected medical devices has simultaneously increased the risk facing health care providers, facilities, and people. This vulnerability is exasperated by the limited to non-existent set of standards, or accessible security measures fitting to the unique category of medical devices and their networks. A demand and opportunity in this niche sector have seen a growing number of medically related cybersecurity startups entering the market. Medigate, a startup focusing on cybersecurity services related to the healthcare industry, raised $15 million dollars in series A funding. Medigate's platform provides particular security functions beyond the elementary gages as in IP addresses, to considering the different models and functionality of medical devices. This process includes identifying and monitoring such devices on networks for skeptical behavior.

https://bit.ly/2UyX6TJ

EUROPE

Airbus data breach affects employees in Europe

European aerospace corporation Airbus disclosed a security breach that affected its commercial aircraft manufacturing business. The company said the security breach "resulted in unauthorized access to data." According to a press release, Airbus said that "some personal data was accessed," but "mostly professional contact and IT identification details of some Airbus employees in Europe."

https://zd.net/2CSJHi0

Cumbria health trust hit by about 150 cyberattacks in five years

The NHS in Cumbria has been hit by more than 150 cyberattacks in five years, the BBC has revealed. Of these, 147 were directed at University Hospitals of Morecambe Bay NHS Trust (UHMBT), which runs hospitals in Barrow, Kendal, Morecambe, and Lancaster. The trust said it had spent £29,600 in 2017 dealing with the effects of cyberattacks. The "vast majority" were "untargeted and unsuccessful," it said.

https://bbc.in/2BhTY7h

UK Consumers not happy with PSD2 fraud rules

UK consumers could undermine attempts by EU regulators to improve fraud screening, according to a new survey by FICO. The predictive analytics firm polled 500 consumers in the United Kingdom, Germany, Spain, and Sweden to better understand their attitudes to the new PSD2 banking regulations. A key part of these rules is a new requirement on banks, card issuers, and payment service providers (PSPs) to enforce so-called strong customer authentication (SCA).

https://bit.ly/2MSkYPD

EU agency says Iran likely to step up cyber espionage

Iran is likely to expand its cyber espionage activities as its relations with Western powers worsen, the European Union digital security agency said on January 28. Iranian hackers are behind several cyberattacks and online disinformation campaigns in recent years as the country tries to strengthen its clout in the Middle East and beyond, according to a Reuters Special Report published in November.

https://reut.rs/2DF2HCd

UK intelligence agency launches new mission of training girls in cyber skills

Britain's national intelligence agency has unveiled plans to train about 600 teenage girls in cyber skills this year in a bid to get more women into the male-dominated field. The Government Communications Headquarters (GCHQ) said it would choose girls aged 12 and 13 to take part in four-day courses in coding, cryptography, logic, and protecting networks following a nationwide competition in January. A spokesman from the GCHQ unit, the National Cyber Security Center, said the aim was to encourage more young people—particularly girls—to work in cybersecurity with figures showing that only 11 percent of the global cyber workforce is female.

https://reut.rs/2Skwf05

Germany seeks to bolster cyber defenses ahead of European Parliament election

German officials are racing to bolster cybersecurity after a far-reaching data breach by a 20-year-old student laid bare the vulnerability of Europe's largest economy ahead of a critical European Parliament election in May. Officials say they are anxious to close security gaps and raise awareness ahead of the upcoming election, where voters from across the European Union will choose lawmakers for the parliament, amid concerns that foreign powers or right-wing forces could seek to manipulate the election. "We have to think about preventive measures," Interior Minister Horst Seehofer told Reuters.

https://reut.rs/2sZjaLt

RUSSIA

New revelations shows extent of Russian meddling in US elections

Oxford University's Computational Propaganda Project and network analysis firm Graphika have revealed new information about the scope of Russian cyber interference in the 2016 US elections. According to new findings, the size and scope of the Russian campaign was far more extensive and thorough than previously understood. The new report concludes that the main target of Russian interference was to make Donald Trump their preferred candidate for US president. The findings, as first reported by the Washington Post, said that Russians working for a group called the Internet Research Agency (IRA) began experimenting with social media to influence local elections in 2009 and expanded its operations to US elections in 2013 using Twitter. It gradually added other popular social media sites to its campaign, including YouTube, Facebook, and Instagram, using race and social issues such as gun rights, immigration, and police brutality to sow division and discontent.

http://bit.ly/2WvlCXx

Facebook apparently gave the Kremlin access to its users' database

Facebook apparently gave permission to the Kremlin to gain access to all its user data. According to the New York Times, under a special arrangement

with Facebook, so-called "integration partners," search engines Netflix, Spotify, Bing and the New York Times itself received some level of privileged access to users' data. Facebook defended those partnerships in a carefully worded statement. The statement names only Facebook's American partners, conspicuously omitting mention of two of the foreign companies that were also granted special access, China's Huawei and Russia's Yandex, whereas Yandex is a Russian search engine that previously handed over its user data to Russia's secret police.

http://bit.ly/2Wvw2q0

Ending 2018: Putin among most dangerous people on the internet

The "Most Dangerous People on the Internet in 2018" survey, conducted by Wired.com, puts Russia and Vladimir Putin among its "best" candidates, briefly summarizing Russia's cyber activities during the 2018, including hacking the international Olympic committee in January, due to doping ban scandal; attacking the Pyeongchang Olympic 2018 winter games; hacking the chemical lab, which investigated Skripals' poisoning; and an unprecedented cyberaggression against Ukraine, its closest neighbor.

http://bit.ly/2WxrOhU

Feasibly Muller "caught the tail" of Russian social media meddling in 2016

The US lawyer defending the indicted Russian company Concord Management and Consulting has been fighting to free evidence in its case, which the Justice Department has locked down because it is sensitive to national security. Concord Management and Consulting is accused of backing a Russian conspiracy to distribute politically charged social media posts to American voters. It is the only one among twenty-six Russians and three companies indicted by Mueller to enter a plea in US court.

https://cnn.it/2HDQpOE

MIDDLE EAST

Iran likely to step up cyber espionage

The EU digital security agency said that Iran's deteriorated relations with Western powers could lead to expanding its cyber espionage activities. In recent years, governments have dealt with a vast range of cyberattacks and online disinformation campaigns operated by Iranian hackers to strengthen the country's influence in the Middle East and beyond. In January, Iran was sanctioned by the EU because it is not obeying the 2015 nuclear deal with the world powers and had started testing ballistic missiles and plotting assassinations on European soil. The European Union Agency for Network and Information Security (ENISA) said in a report that "newly imposed sanctions on Iran are likely to push the country to intensify state-sponsored cyber threat activities in pursuit of its geopolitical and strategic objectives at a regional level."

https://bit.ly/2RR2Tad

Super cyber weapon used by UAE to spy on iPhones of foes

iPhones of activists, diplomats, and rival foreign leaders were hacked with a sophisticated spying tool called Karma, showing how potent cyberweapons are in the hands of smaller nations. According to five former operatives and program documents, a team of former US government intelligence operatives helped the United Arab Emirates to monitor hundreds of targets beginning in 2016, from the Emir of Qatar and a senior Turkish official to a Nobel Peace human-rights activist in Yemen. Lori Stroud, one of the American operatives, would use methods learned from a decade in the US intelligence community to help the UAE hack into the phones and computers of its enemies.

https://bit.ly/2UtgK3e

APAC

Japan is preparing to survey over 200 million gadgets for cybersecurity

The government-backed National Institute of Information and Communications Technology will start survey on routers, webcams, and web connected appliances, to check for vulnerabilities ahead of major events, such

as the Rugby World Cup, the Olympic Summer Games, and major conferences taking place year round. Researches will review common but unsafe IDs and passwords, such as "abcd," "1234" or "admin," to see if devices are accessible to hackers. The survey will not review smartphones but may examine café routers, which allow web free access to cell phones. The survey will notify ISPs about vulnerable users without breaking into individual gadgets to view data. Cybersecurity, especially in world sporting events, has become considerably important, as it uses new technology, from ticketing to broadcasting.

https://goo.gl/FXyirh

Singapore: A New partnership between BH Global and SASA-Software announced

BH Global, which provides comprehensive solutions in supply chain management, will team up with SASA-Software, owned by Kibbutz Sasa, Israel, which specializes in CDR technologies. Based out of Singapore, and as an extended arm of Sasa-Software (Israel), Sasa-APAC will integrate CDR technologies into the region and be in charge of appointing, training, and qualifying its regional channel partners. Athena Dynamics Pte Ltd. (ADPL), the local branch in Singapore, has worked in collaboration with SASA since 2014, successfully deploying CDR technologies and protecting private and public networks, including government agencies, financial institutions, health sector, and classified networks, such as military, water, energy, and FSI sensitive infra-structures. The growing partnership will provide a strategic platform to introduce and proliferate this technology to the entire Asia-Pacific region.

https://goo.gl/oAmVvY

India's largest bank leaked account data of millions of customers

The government-owned State Bank of India has secured an unprotected server, hosted in a regional Mumbai-based data center, which has allowed anyone to access financial information, such as bank balances and recent transactions, of millions of its customers. The bank did not protect the server with a password, allowing anyone to be able to access the information. It is not sure for how long the server was unprotected, but it was discovered by a security researcher, who then notified Tech Crunch. The bank uses a system called SBI Quick, which allows customers to text the bank, or makes a missed

call, to retrieve information back by text messages, with account balance and transactions. By using key words, the service recognizes the customer's phone and will send a text with the latest transactions, or account balance. It can also be used to block an ATM card aand make inquiries about loans. The leak revealed that the back-end text message was exposed. For reference, the bank sends out roughly three million text messages a day. The data could potentially be used to profile and target individuals with high account balances. After the magnitude of the leak was revealed by Tech Crunch, they turned to India's National Critical Information Infrastructure Protection center, and the data was secured overnight.

https://goo.gl/QJQf11